1. User Guide 14
1.1 User Guide. Introduction 16
1.2 Software Lifecycle Policy 18
1.3 Description of the Software Package 19
1.3.1 Basic principles of building a security system based on the Axxon One software package 20
1.3.2 Axxon One features: reference information 21
1.3.3 Functions of the Distributed Security System 25
1.3.4 Network Topologies of the Axxon One Software Package 26
1.3.5 Characteristics of Axxon One 27
1.3.6 Implementation requirements for the Axxon One software package . . 28
1.3.6.1 Limitations of Axxon One 29
1.3.6.2 Operating system requirements 31
1.3.6.3 Disk storage subsystem requirements 32
1.3.6.4 Hardware requirements 35
1.3.6.5 TCP/IP Network Bandwidth Requirements 36
1.3.6.6 Requirements for BIOS configuration 37
1.3.6.7 Running Axxon One VMS in Virtual Machines 38
1.3.6.8 General information about updating Windows OS 39
1.3.7 Interface of the Axxon One Software Package 40
1.3.8 Ports used by the Axxon One Software Package 41
1.3.9 Requirements for Personnel Quantity and Qualifications 42
1.4 Installing the Axxon One Software Package 43
1.4.1 Installing equipment 44
1.4.1.1 Types of Devices Used 45
1.4.1.2 Connecting IP Devices 46
1.4.1.3 Configuring IP Devices in Windows 47
1.4.1.4 Video capture cards pins 48
1.4.1.4.1 WS-216 video capture card pins 49
1.4.2 Installation the Axxon One Software Package 51
1.4.2.1 Installation 52
1.4.2.2 Repairing Installation 64
1.4.2.3 Removal 66
1.4.2.4 Silent install (Quiet Mode) 69
1.4.2.5 Updating Drivers Pack 72
1.4.2.6 Update 73
1.4.2.7 Automatic update of a remote Client 74
1.5 Licensing of the software product 75
1.5.1 Axxon One license types 76
1.5.2 Licensing methods 79
1.5.3 Product activation utility 80
1.5.4 License Activation 83
1.6 Launching and closing the Axxon One software package 84
1.6.1 Startup 85
1.6.1.1 Starting a Server 86
1.6.1.2 Starting the Axxon One Client 87
1.6.1.3 Running multiple Axxon One Clients 91
1.6.1.4 Axxon One in demo mode 92
1.6.1.5 Automatic Start of the Client 93
1.6.2 Shutdown 94

1.6.2.1 Shutting down an Axxon One Client 95
1.6.2.2 Shutting down a Server 96
1.6.3 Automatic Server restart 97
1.6.4 Switching Users Quickly 98
1.6.5 Cross-System Client 99
1.6.6 Connecting LDAP users 101
1.6.7 Connecting to Another Server Quickly 102
1.7 Configuration of Axxon One 103
1.7.1 General information on system configuration 104
1.7.1.1 System configuration: stages 105
1.7.1.2 Applying and resetting settings 106
1.7.1.3 Display of parameters in interface 107
1.7.1.4 System objects 108
1.7.1.5 Object search 109
1.7.2 Hardware configuration 111
1.7.2.1 Configuring domains 112
1.7.2.1.1 The Domain object 113
1.7.2.1.2 Operations with domains 114
1.7.2.1.3 Cases of domain configuration 118
1.7.2.2 Searching, adding, configuring and removing IP devices 120
1.7.2.2.1 Bulk creation of IP devices 126
1.7.2.3 Configuring system objects for devices 128
1.7.2.3.1 The Server Object 129
1.7.2.3.2 The Camera object 134
1.7.2.3.3 The IP Server Object 180
1.7.2.3.4 The Microphone Object 183
1.7.2.3.5 The PTZ Object 184
1.7.2.3.6 The Channel object 187
1.7.2.3.7 The Input Object 188
1.7.2.3.8 The Output Object 191
1.7.2.3.9 The Speaker object 192
1.7.2.3.10 The Embedded storage object 195
1.7.2.4 Particulars of Configuration of Devices 196
1.7.2.4.1 AGRG-IO-16/8-WD-DS Sensor-Relay cards 197
1.7.2.4.2 Axis IP Devices 202
1.7.2.4.3 CCTV Keyboards 203
1.7.2.4.4 CH VM-Desktop USB multifunction controller 212
1.7.2.4.5 Configuring Vivotek Panoramic PTZ 213
1.7.2.4.6 Video capture cards 214
1.7.2.4.7 Joysticks 217
1.7.2.4.8 Sony IP Devices 218
1.7.2.4.9 Setting up Tibbo relay/loop boards 219
1.7.2.5 Configuring Tracking objects 221
1.7.2.5.1 Configuring Tag&Track Lite 222
1.7.2.5.2 Configuring Tag & Track Pro 223
1.7.2.6 Receiving Events from External Systems 230
1.7.2.6.1 Event source object 231
1.7.2.6.2 Configuring POS devices 232
1.7.2.6.3 Receiving Axxon PSIM Events 240
1.7.2.6.4 Configuring Receiving Events from CommaxComplexServer 241

1.7.2.7 Configuring video camera groups 244
1.7.2.7.1 Creating a Group object 245
1.7.2.7.2 Adding video cameras created in the system to Group objects . 246
1.7.2.7.3 Creating a system of groups and subgroups 247
1.7.2.7.4 Managing Group and Video camera objects 248
1.7.2.8 Automatic copying of data from local Servers to a centralized Server 250
1.7.3 Configuring archives 252
1.7.3.1 General information about configuring archives 253
1.7.3.2 Creating archives 255
1.7.3.2.1 Creating a local archive 256
1.7.3.2.2 Creating a remote archive 259
1.7.3.2.3 Creating a cloud archive 263
1.7.3.2.4 General information about the Round-robin algorithm 275
1.7.3.3 Creating an archive based on existing archive volumes 276
1.7.3.4 Configuring recording to an archive 277
1.7.3.5 Setting the default archive 279
1.7.3.6 Configuring data replication 280
1.7.3.7 Configuring access restrictions to archive 281
1.7.3.8 Editing archives 282
1.7.3.9 Configuring a write limit on the archive volume 283
1.7.3.10 Protecting video footage from FIFO overwriting 284
1.7.3.10.1 Setting up a macro for automatic copying of protected records 285
1.7.3.10.2 Setting up record protection 286
1.7.3.11 Increasing capacity of an archive volume 287
1.7.3.12 Removing archive volumes 288
1.7.3.13 Removing archives 289
1.7.3.14 Information about the filled archive volume 290
1.7.3.15 Saving the archive when replacing the video signal device . . . 292
1.7.4 Configuring detection tools 293
1.7.4.1 General information about detection tools and their sub-tools . . 298
1.7.4.2 Processors used for detection tools operation 301
1.7.4.3 Hardware requirements for GPU-based video decoding 303
1.7.4.4 Installing DetectorPack add-ons 304
1.7.4.5 Configuring detection tools and their sub-tools 307
1.7.4.6 General information on metadata 312
1.7.4.7 Neural analytics 315
1.7.4.7.1 General information on neural analytics 316
1.7.4.7.2 Hardware requirements for neural analytics operation 318
1.7.4.7.3 Data collection requirements for neural network training . . 319
1.7.4.7.4 Optimizing the operation of neural analytics on GPU in Windows OS 321
1.7.4.7.5 Optimizing the operation of neural analytics on GPU in Linux OS 324
1.7.4.8 General settings of the detection tools 327
1.7.4.8.1 Selecting Nvidia GPU when configuring detection tools . . . 328
1.7.4.8.2 Configuring the minimum and maximum size of detected objects 330

1.7.4.8.3 Configuring a skip area 332
1.7.4.8.4 Configuring a detection area 333
1.7.4.8.5 Configuring perspective 334
1.7.4.8.6 Configuring the scanning mode 336
1.7.4.8.7 Displaying the number of detected objects 338
1.7.4.9 Standard detection sub-tools 340
1.7.4.9.1 General information on the standard detection sub-tools . . 341
1.7.4.9.2 Camera requirements for the standard detection sub-tools 343
1.7.4.9.3 Configuring Line Crossing 344
1.7.4.9.4 Configuring Loitering In Area 349
1.7.4.9.5 Configuring Stop In Area 352
1.7.4.9.6 Configuring Motion In Area 355
1.7.4.9.7 Configuring Entrance In Area 358
1.7.4.9.8 Configuring Exit From Area 361
1.7.4.9.9 Configuring Multiple Objects 364
1.7.4.9.10 Configuring Move From Area To Area 366
1.7.4.10 Category: Trackers 370
1.7.4.10.1 Abandoned Objects Detection VI 371
1.7.4.10.2 Abandoned Objects Detection (Street) VI 380
1.7.4.10.3 Neurotracker 389
1.7.4.10.4 Object Tracker 400
1.7.4.10.5 Object Tracker VL 411
1.7.4.10.6 Stopped object detector 432
1.7.4.10.7 Motion detection 440
1.7.4.10.8 Privacy Masking 447
1.7.4.11 Category: Face 454
1.7.4.11.1 Face Detection VL 455
1.7.4.11.2 Face Detection VA 474
1.7.4.11.3 Masks Detection 486
1.7.4.11.4 Configuring face recognition based on the created lists . . 487
1.7.4.11.5 Configuring macros when working with face lists 488
1.7.4.11.6 Configuring integration with FaceCube 495
1.7.4.11.7 Face Detection TV 496
1.7.4.12 Category: Vehicle 507
1.7.4.12.1 Configuring vehicle license plate recognition based on the created lists 508
1.7.4.12.2 License Plate Recognition BRS 515
1.7.4.12.3 License Plate Recognition IV 521
1.7.4.12.4 License Plate Recognition RR and Vehicle Recognition RR . 532
1.7.4.12.5 License plate recognition VT 566
1.7.4.12.6 Vehicle Recognition XR 596
1.7.4.13 Category: Poses 605
1.7.4.13.1 Person-Based Privacy Masking 606
1.7.4.13.2 Pose Detection 612
1.7.4.14 Category: Production Safety 638
1.7.4.14.1 Audio Analytics Detection IV 639
1.7.4.14.2 Object Presence Detection 644
1.7.4.14.3 Fire Detection 650
1.7.4.14.4 Equipment detection (PPE) 656
1.7.4.14.5 Smoke Detection 673

1.7.4.14.6 Water Level Detection 679
1.7.4.14.7 Glow detector 687
1.7.4.14.8 PPE detection VL 693
1.7.4.15 Category: Retail 714
1.7.4.15.1 Barcode Detection 715
1.7.4.15.2 Crowd Estimation VA 723
1.7.4.15.3 Neurocounter 729
1.7.4.15.4 Queue detection 739
1.7.4.15.5 Visitors Counter 746
1.7.4.16 Category: Service 756
1.7.4.16.1 Audio Loss 757
1.7.4.16.2 Noise Detection 760
1.7.4.16.3 Signal Detection 763
1.7.4.16.4 Tampering Detection 766
1.7.4.17 Scene Analytics detection tools 772
1.7.4.17.1 Functions of Scene Analytics detection tools 773
1.7.4.17.2 Video requirements for scene analytics detection tools . . . 774
1.7.4.17.3 Configuring Scene Analytics Detection Tools 780
1.7.4.18 Category: Embedded 787
1.7.4.18.1 General information about embedded detection tools . . . 788
1.7.4.18.2 AxxonSoft Tracker in Axis devices 789
1.7.4.18.3 Face Detection and Temperature Control with Mobotix M16 TR cameras 792
1.7.4.18.4 Embedded vehicle speed measurement radar 800
1.7.4.19 Configuring Inputs 804
1.7.4.20 Checking the triggering of a detection tool 805
1.7.4.21 Automatic Rules 807
1.7.5 Configuring macros 808
1.7.5.1 General information about the macros 809
1.7.5.2 Create Macros 811
1.7.5.3 Configuring start conditions for event-driven macros 814
1.7.5.3.1 Specific parameters for triggering a face recognition macro 819
1.7.5.3.2 Triggering macros by statistical data 820
1.7.5.4 Settings specific to actions 822
1.7.5.4.1 Wait for event 823
1.7.5.4.2 Wait for timeout 826
1.7.5.4.3 Wait till previous action finishes 827
1.7.5.4.4 Record to archive 830
1.7.5.4.5 Initiating an alarm in the system 833
1.7.5.4.6 Stopping alarm 834
1.7.5.4.7 Switch output 835
1.7.5.4.8 Switching to a PTZ camera preset 836
1.7.5.4.9 Arm /disarm a camera 837
1.7.5.4.10 Checking whether the camera is in armed mode 838
1.7.5.4.11 View camera 839
1.7.5.4.12 Open layout 840
1.7.5.4.13 Show map 841
1.7.5.4.14 Starting export 842
1.7.5.4.15 Start replication 844
1.7.5.4.16 Notifications 846

1.7.5.4.17 Starting an external program on Clients 858
1.7.5.4.18 Starting an external program on Servers 859
1.7.5.4.19 Start/stop slideshows of layouts 861
1.7.5.4.20 Enable/disable a component 862
1.7.5.4.21 Checking for archive video recordings 863
1.7.5.4.22 Switching to MomentQuest search results in archive 865
1.7.5.4.23 Executing a macro 866
1.7.5.4.24 Checking protected video records in the archive 867
1.7.5.4.25 Executing a web query 868
1.7.5.4.26 Text templates in macros 869
1.7.5.5 Cyclical macros 872
1.7.6 Configuring user permissions 874
1.7.6.1 Creating and configuring roles 877
1.7.6.2 Connecting to an LDAP catalog 886
1.7.6.3 Working with users 888
1.7.6.3.1 Creating local users 889
1.7.6.3.2 Locking a user account 892
1.7.6.3.3 Creating LDAP connections 893
1.7.6.3.4 Synchronize LDAP users 894
1.7.6.3.5 Deleting users 895
1.7.6.4 Configuring the user security policy 896
1.7.7 Configuring layouts 898
1.7.7.1 Creating and deleting layouts 899
1.7.7.2 Rename Layouts 901
1.7.7.3 Reorder Layouts 902
1.7.7.4 Layout copying 903
1.7.7.5 Editing layouts 904
1.7.7.5.1 Switching to layout editing mode 905
1.7.7.5.2 Selecting a layout for editing 906
1.7.7.5.3 Configuring layout cells 907
1.7.7.5.4 Configuring viewing tiles 919
1.7.7.5.5 Configuring information boards 930
1.7.7.5.6 Configuring Alarms Panel on a layout 945
1.7.7.5.7 Exiting Layout Editing mode 946
1.7.7.6 Share Layouts 947
1.7.7.7 Configuring special layouts 948
1.7.7.7.1 Creating special layouts 949
1.7.7.7.2 Configuring Alarmed cameras layout 951
1.7.7.7.3 Configuring Marked cameras layout 953
1.7.7.8 Configuring user-defined slide shows 955
1.7.7.9 Setting the default layout 956
1.7.7.10 Setting a layout ID 957
1.7.8 Configuring Video wall 958
1.7.9 Configuring the interactive map 961
1.7.9.1 Adding a new map 962
1.7.9.2 Adding system objects to the map 964
1.7.9.2.1 Adding video cameras 965
1.7.9.2.2 Adding inputs and outputs 968
1.7.9.2.3 Adding switches to another map 969
1.7.9.2.4 Adding macros 970

1.7.9.3 Configuring cameras on the map 971
1.7.9.3.1 Configuring a camera in standard map viewing mode 972
1.7.9.3.2 Configuring cameras with an embedded GPS tracker 974
1.7.9.3.3 Configuring cameras in immersion mode 975
1.7.9.4 Attaching a map to a layout 977
1.7.9.5 Configuring the floors 978
1.7.9.5.1 Creating a new floor 979
1.7.9.5.2 Configuring floor location on the map 982
1.7.9.5.3 Editing a floor 983
1.7.9.5.4 Removing a floor 984
1.7.9.6 Removing objects from the map 985
1.7.9.7 Setting keywords for geomap search 986
1.7.9.8 Changing map type and display 987
1.7.9.9 Renaming the map 988
1.7.9.10 Sorting of map lists 989
1.7.9.11 Deleting a map 990
1.7.10 System preferences 991
1.7.10.1 Server settings 992
1.7.10.1.1 Configuring Forensic Search MomentQuest in Archive . . . 993
1.7.10.1.2 Setting up privacy masking 996
1.7.10.1.3 Configuring hardware video decoding for display on the Client 1002
1.7.10.1.4 Configuring automatic response when Axxon One integrity check fails 1007
1.7.10.1.5 Configuring storage of the system log and metadata . . . 1008
1.7.10.1.6 Configuring Alarm processing 1010
1.7.10.1.7 Configuring PTZ control 1011
1.7.10.1.8 Configuring schedules 1012
1.7.10.1.9 Configuring the Server ports 1016
1.7.10.1.10 Configuring the Server logging level 1017
1.7.10.1.11 Configuring NTP synchronization 1018
1.7.10.1.12 Vector maps in Axxon One 1019
1.7.10.1.13 Connecting the Axxon One domain to AxxonNet 1025
1.7.10.2 Client settings 1027
1.7.10.2.1 Configuring the user interface 1028
1.7.10.2.2 Configuring how Axxon One starts 1050
1.7.10.2.3 Configuring export 1058
1.7.10.2.4 Configuring audio on the Client 1065
1.7.10.2.5 Configuring hot keys 1066
1.7.10.2.6 Configuring video capturing on operator monitor 1074
1.7.10.2.7 Configuring the Client logging level 1078
1.7.11 Configuring Failover VMS 1079
1.7.11.1 General information about a failover system 1080
1.7.11.2 Ports used by the failover system 1082
1.7.11.3 Supervisor Web-Interface 1083
1.7.11.4 Creating a cluster 1084
1.7.11.5 Failover Database 1088
1.7.11.6 Configure a Failover System Cluster 1089
1.7.11.6.1 Setting up basic configuration 1090
1.7.11.6.2 Setting up a configuration with the backup Server 1094

1.7.11.6.3 Creating and configuring independent nodes 1098
1.7.11.6.4 1+1 cluster configuration 1100
1.7.11.6.5 Suspending a Server within a cluster 1105
1.7.11.6.6 Disbanding a cluster 1106
1.7.11.7 Set up access to a supervisor 1107
1.7.11.8 Configuration backup and restore for failover VMS 1109
1.7.11.9 Transferring the configuration from a common security server to a failover system 1110
1.7.11.10 Monitoring the status of a cluster 1111
1.7.11.11 Connecting to a Node and Configuring of an Axxon domain . 1113
1.7.11.12 Configuring automatic connection to nodes 1114
1.7.11.13 Updating Servers within a cluster 1115
1.7.11.14 Setting network interfaces for system nodes operation 1117
1.7.11.15 Changing ports in the nodes of the failover system 1118
1.7.11.16 Connecting the Client to the Failover Server behind NAT . . . 1119
1.7.11.17 Changing logging levels for the Consul and Nomad processes in a failover system 1121
1.7.12 Self-diagnostics service 1123
1.7.12.1 General information about the self-diagnostics service 1124
1.7.12.2 Starting and stopping the self-diagnostics service 1125
1.7.12.3 Viewing metrics in the self-diagnostics service 1126
1.7.12.4 Viewing self-diagnostics metrics using third-party Grafana | Prometheus software 1130
1.8 Working with Axxon One 1132
1.8.1 Main Elements of the User Interface 1133
1.8.1.1 Surveillance window 1134
1.8.1.1.1 Color Coding of Frames 1137
1.8.1.1.2 Viewing Tile Context Menu 1138
1.8.1.1.3 Time Display 1139
1.8.1.1.4 Display of Video Statistics 1140
1.8.1.1.5 Video Surveillance Mode Selection Tabs 1141
1.8.1.1.6 Advanced Archive Navigation Panel 1142
1.8.1.2 Information boards 1144
1.8.1.3 The Archive Navigation Panel 1145
1.8.1.3.1 Show and Hide the Archive Navigation Panel 1146
1.8.1.3.2 The Structure and Function of the Archive Navigation Panel . 1147
1.8.1.3.3 Events filter 1149
1.8.1.3.4 The Timeline 1150
1.8.1.3.5 Events List 1153
1.8.1.3.6 The Playback Panel 1155
1.8.1.4 Video wall panel 1156
1.8.1.5 Monitor panel 1157
1.8.1.6 The Layouts panel 1158
1.8.1.7 Interactive Map 1159
1.8.1.8 Camera Search Panel 1160
1.8.1.9 Alert panel 1161
1.8.1.10 Objects Panel 1163
1.8.1.11 The PTZ Control Panel 1165
1.8.1.12 Story board 1167

1.8.2 Video Surveillance 1168
1.8.2.1 Video Surveillance Modes 1169
1.8.2.2 Functions Available in All Video Surveillance Modes 1170
1.8.2.2.1 Scaling the surveillance window 1171
1.8.2.2.2 Digitally Zooming Video Images 1173
1.8.2.2.3 Video image processing 1177
1.8.2.2.4 Rotate Video Image 1181
1.8.2.2.5 Tracking objects 1183
1.8.2.2.6 Operator comments 1187
1.8.2.2.7 Switching to other camera via a link in the Camera window . 1192
1.8.2.2.8 Viewing titles from POS terminals 1193
1.8.2.2.9 Partial decoding of video 1195
1.8.2.2.10 Displaying information from a detection tool (mask) . . . 1196
1.8.2.3 Real-time video surveillance 1197
1.8.2.3.1 Switching to Live Video Mode 1198
1.8.2.3.2 Video Surveillance Functions Available in Live Video Mode 1199
1.8.2.3.3 Arming and Disarming a Video Camera 1200
1.8.2.3.4 Controlling a PTZ Camera 1201
1.8.2.3.5 Functions for tracking of moving objects 1217
1.8.2.3.6 Managing Outputs 1221
1.8.2.3.7 Displaying the input status 1223
1.8.2.3.8 Selecting video stream quality in a Surveillance window (GreenStream) 1224
1.8.2.3.9 Autozoom 1226
1.8.2.3.10 Autoreplace Offline Cameras on Layouts 1228
1.8.2.3.11 Snapshot 1229
1.8.2.3.12 Viewing selected camera's detection tool triggering events 1230
1.8.2.3.13 Removing a camera from a layout 1231
1.8.2.4 Video surveillance in archive mode 1233
1.8.2.4.1 Switching to Archive Mode 1234
1.8.2.4.2 Video Surveillance Functions Available in Archive Mode . . 1236
1.8.2.4.3 Selecting an Archive 1237
1.8.2.4.4 Viewing a combined Archive 1238
1.8.2.4.5 Synchronized playback of archives 1239
1.8.2.4.6 Compressed playback of archives (TimeCompressor) 1240
1.8.2.4.7 Viewing recorded video with operator comments 1245
1.8.2.4.8 Viewing External Archives 1246
1.8.2.4.9 Delete a part of an archive 1247
1.8.2.4.10 Navigating in the Archive 1248
1.8.2.4.11 Displaying the causes of triggered Scene Analytics detection tools 1258
1.8.2.4.12 Viewing the results of a saved search query 1259
1.8.2.4.13 Manual Archive Replication 1261
1.8.2.4.14 Tag & Track Lite in Archive mode 1262
1.8.2.5 Video surveillance in alarm management mode 1263
1.8.2.5.1 Video surveillance functions available in Alarm Management mode 1264
1.8.2.5.2 Switch to Alarm Management mode 1265

1.8.2.5.3 Initiating an alarm event 1266
1.8.2.5.4 Working with an assessment of an alarm event 1269
1.8.2.5.5 Working with the Alarm Management window 1273
1.8.2.5.6 Limitations when working with alarm events in case of multi-user processing 1278
1.8.2.6 Video surveillance in archive search mode 1279
1.8.2.6.1 Switching to Archive Search mode 1280
1.8.2.6.2 Archive Search mode interface 1282
1.8.2.6.3 Video surveillance functions available in Archive Search mode . 1284
1.8.2.6.4 Search in an archive of a single video camera 1285
1.8.2.6.5 Simultaneous search in an archive of several video cameras 1343
1.8.2.7 Working with fisheye cameras 1345
1.8.2.7.1 Viewing modes for video from fisheye cameras 1346
1.8.2.7.2 Fisheye cameras on an interactive map 1351
1.8.2.8 Face recognition and search 1354
1.8.2.9 Vehicle number plate recognition and search 1357
1.8.2.10 Temperature screening 1359
1.8.3 Working with information boards 1360
1.8.3.1 Resizing information boards 1361
1.8.3.2 Hiding information boards 1362
1.8.3.3 Working with Event Boards 1363
1.8.3.3.1 Options for displaying information on Events Boards 1364
1.8.3.3.2 Switching a camera linked to an Event Board to the archives . 1366
1.8.3.4 Working with System Health Boards 1367
1.8.3.4.1 Viewing server status 1368
1.8.3.4.2 Viewing camera status 1370
1.8.3.5 Working with Statistics Boards 1372
1.8.3.6 Working with Web Boards 1374
1.8.3.7 Working with Dialog Board 1375
1.8.3.8 Working with an Alarm Board 1377
1.8.3.9 Working with Equipment Board 1379
1.8.4 Layouts management 1381
1.8.4.1 Changing cameras on a layout 1382
1.8.4.2 Selection and Slideshow of Layouts 1383
1.8.4.3 Working with Special layouts 1385
1.8.5 Monitor management 1387
1.8.5.1 Managing monitors on a local Client 1388
1.8.5.2 Managing monitors on remote Clients within the Axxon-domain 1390
1.8.6 Audio Monitoring 1391
1.8.6.1 General Information 1392
1.8.6.2 Listening on the Client to sound from a camera microphone . . 1393
1.8.6.3 Playing back sound from Client microphone on camera speakers . 1395
1.8.7 Working with the interactive map 1396
1.8.7.1 Opening and closing the map 1397
1.8.7.2 Geomap search 1398
1.8.7.3 Changing the map tilt 1400

1.8.7.4 Scaling and focusing of map 1403
1.8.7.5 Customizing an interactive map 1404
1.8.7.6 Switching between maps 1406
1.8.7.7 Immersion mode 1407
1.8.7.8 Controlling devices from the map 1409
1.8.7.9 Grouping objects on the map 1411
1.8.7.10 Displaying device status 1413
1.8.7.11 Selecting Cameras for a Temporary Layout 1415
1.8.8 Exporting frames and video recordings 1416
1.8.8.1 Frame export 1417
1.8.8.2 Exporting Video Recordings 1419
1.8.8.2.1 Standard video recordings export 1420
1.8.8.2.2 Instant video export 1423
1.8.8.2.3 Simultaneous export of videos from multiple cameras . . . 1424
1.8.8.2.4 Simultaneous export of all event videos 1426
1.8.8.3 Configuring export area and masks 1428
1.8.8.4 Viewing export progress 1430
1.8.9 Macros control 1431
1.8.10 Event control 1432
1.8.10.1 Control in Live Video mode 1433
1.8.10.2 The System Log 1434
1.8.10.2.1 Setting Event Search Filters 1435
1.8.10.2.2 Event search procedure 1436
1.8.10.2.3 Refreshing Event Search Results 1437
1.8.10.2.4 Viewing Event Search Results 1438
1.8.10.2.5 Exporting Event Search Results 1439
1.8.10.2.6 Switching to archive video of specific events 1440
1.8.11 Working with Axxon One through the Web-Client 1441
1.8.11.1 Web-Client overview 1442
1.8.11.2 Hardware and software requirements for the Web-Client operation 1443
1.8.11.3 Starting and logging in to the Web-Client 1444
1.8.11.4 Web-Client GUI 1447
1.8.11.5 Web-Client configuration 1449
1.8.11.6 Searching for video cameras in the Web-Client 1453
1.8.11.7 Working with layouts in Web-Client 1456
1.8.11.7.1 Summary of how to work with layouts in Web-Client . . . 1457
1.8.11.7.2 Selecting and searching for a layout 1458
1.8.11.7.3 Creating a new layout in the Web-Client 1459
1.8.11.7.4 Editing and deleting layouts in Web-Client 1462
1.8.11.7.5 Selecting the default layout in Web-Client 1463
1.8.11.7.6 Copying layouts in the Web-Client 1464
1.8.11.7.7 Sharing layouts in the Web-Client 1465
1.8.11.7.8 Creating a temporary layout in the Web-Client 1467
1.8.11.8 Real-time video surveillance in the Web-Client 1469
1.8.11.9 Controlling PTZ cameras through the Web-Client 1471
1.8.11.9.1 Controlling a PTZ camera through the Web-Client by using presets 1472
1.8.11.9.2 Changing the optical zoom of a PTZ camera in the Web-Client 1473

1.8.11.9.3 Changing the positioning speed of a PTZ camera in the Web-Client 1474
1.8.11.9.4 Changing the tilt of a PTZ camera in the Web-Client . . . 1475
1.8.11.10 Viewing video archives through the Web-Client 1476
1.8.11.11 Archive position selection panel for the Web-Client 1479
1.8.11.12 Archive search in the Web-Client 1481
1.8.11.12.1 Types of archive search in the Web-Client 1483
1.8.11.12.2 Building a Heat Map 1484
1.8.11.12.3 Simultaneous search in multiple camera Video Footage via the Web-Client 1486
1.8.11.12.4 Reporting the search results 1487
1.8.11.13 Viewing video camera detection tool triggerings in the Web-Client 1488
1.8.11.14 Running macros in Web-Client 1489
1.8.11.15 Viewing and processing alarms in Web-Client 1490
1.8.11.16 Listening to a camera's microphone via the Web-Client 1492
1.8.11.17 Digital video zoom in the Web-Client 1493
1.8.11.18 Export in the Web-Client 1494
1.8.11.19 Viewing Camera and Archive Statistics 1499
1.8.11.20 Working with bookmarks in the Web-Client 1500
1.8.11.21 Working with interactive map via the Web-Client 1502
1.8.11.21.1 Displaying an interactive map in the Web-Client 1503
1.8.11.21.2 Changing the display of the map on a layout via the Web-Client 1504
1.8.11.21.3 Zooming and moving the map in the Web-Client 1505
1.8.12 Working with Axxon One Through the Mobile Clients 1506
1.8.13 Changing user password 1507
1.9 Description of utilities 1508
1.9.1 Axxon One Tray Tool 1509
1.9.2 Activation utility 1510
1.9.3 Axxon Support Tool 1513
1.9.3.1 Purpose of the Support.exe Utility 1514
1.9.3.2 Launching and Closing the Utility 1515
1.9.3.3 Description of the Support.exe utility interface 1516
1.9.3.4 The Processes Service 1517
1.9.3.5 Collecting Data on the Configuration of Servers and Clients Using the Support 1519
1.9.4 Log Management Utility 1521
1.9.4.1 Starting and closing the utility 1522
1.9.4.2 Configuring the Server log storage and archiving options 1523
1.9.4.3 Configuring the logging levels 1524
1.9.4.4 Configuring the Client log storage options 1525
1.9.4.5 Configuring Client RAM usage logging 1526
1.9.5 Digital signature verification utility 1527
1.9.6 Backup and Restore Utility 1530
1.9.6.1 Purpose of BackupTool.exe 1531
1.9.6.2 Starting and quitting BackupTool.exe 1532
1.9.6.3 Roll back the local configuration to a selected restore point . . . 1535
1.9.6.4 Roll back the global configuration to a selected restore point . . 1539
1.9.6.5 Configuration backup 1540

1.9.6.6 Configuration restore 1543
1.9.6.7 Changing the Server name 1546
1.9.7 POS-terminal log collection utility 1548
1.9.8 Console utility for working with archives 1550
1.9.9 Network settings utility 1553
1.10 Appendices 1554
1.10.1 Appendix 1. Glossary 1555
1.10.2 Appendix 2. Known issues in the Axxon One Software Package . . 1558
1.10.2.1 Possible errors during installation 1559
1.10.2.2 Possible Errors During Start-Up 1562
1.10.2.3 Possible Errors During Operation 1563
1.10.3 Appendix 3. Assigning of the domain takes place when the Axxon One server is installed 1565
1.10.4 Appendix 4. Using Axxon One with antivirus software 1566
1.10.5 Appendix 5. Using CH VM-Desktop USB multifunction controllers with Axxon One 1568
1.10.6 Appendix 6. Hotkeys in Axxon One 1571
1.10.7 Appendix 7. Automated configuration backup and restore 1574
1.10.8 Appendix 8. Using Axxon One with NAT 1575
1.10.8.1 Consolidating the Servers from different networks into Axxon domain 1576
1.10.8.2 Connecting the Client to the Server behind NAT 1578
1.10.8.3 Connecting the Web and Mobile Clients to the Server behind NAT . 1580
1.10.8.4 Audio transmission from the Client's microphone behind NAT to the Server's or camera's loudspeaker 1582
1.10.9 Appendix 9. Creating system variable 1584

User Guide

Export to PDF

User Guide. Introduction

Software Lifecycle Policy

Description of the Software Package

Basic principles of building a security system based on the Axxon One software package

Axxon One features: reference information

Functions of the Distributed Security System

Network Topologies of the Axxon One Software Package

Specifications of the Axxon One Software Package

Implementation Requirements for the Axxon One Software Package

Interface of the Axxon One Software Package

Ports used by the Axxon One Software Package

Requirements for Personnel Quantity and Qualifications

Installing the Axxon One Software Package

Installing equipment

Installation the Axxon One Software Package

Licensing of the software product

Axxon One license types

Licensing methods

Product activation utility

License Activation

Launching and Closing the Axxon One Software Package

Startup

Shutdown

Automatic Server restart

Switching Users Quickly

Cross-System Client

Connecting LDAP users

Connecting to Another Server Quickly

Configuration of the Axxon One Software Package

General information on system configuration

Hardware configuration

Configuring Archives

Configuring detection tools

Configuring Macros

Configuring user permissions

Configuring Layouts

Configuring Videowall

Configuring the Interactive Map

Working with the Axxon One Software Package

Main Elements of the User Interface

Video Surveillance

Working with information boards

Layouts Management

Monitor Management

Audio Monitoring

Working with the Interactive Map

Exporting Frames and Video Recordings

Macros control

Event Control

System preferences

Configuring Failover VMS

Self-diagnostics service

Working with Axxon One Through the Web-Client

Description of utilities

Axxon One Tray Tool

Activation Utility

Axxon Support Tool

Log Management Utility

Digital signature verification utility

Backup and Restore Utility

POS-terminal log collection utility

Console utility for working with archives

Network settings utility

Appendices

Appendix 1. Glossary

Appendix 2. Known issues in the Axxon One Software Package

Appendix 3. Assigning of the domain takes place when the Axxon One server is installed

Appendix 4. Using Axxon One with antivirus software

Appendix 5. Using CH VM-Desktop USB multifunction controllers with Axxon One

Appendix 6. Hotkeys in Axxon One

Appendix 7. Automated configuration backup and restore

Appendix 8. Using Axxon One with NAT

Appendix 9. Creating system variable

User Guide. Introduction

On the page:

- General Information
- Purpose of the Document
- Purpose and functionality of Axxon One

General Information

No part of this document can be reproduced or transmitted in any form or by any means without the prior written permission of AxxonSoft.
The *Axxon One* trademark is the property of AxxonSoft. All other trademarks included in this document are the property of their respective owners.
All information contained in this document is current as of the publication date. AxxonSoft reserves the right to change or update this document without the prior notification of or to any third party.

Purpose of the Document

User guide contains the information necessary for building, implementing, and operating a security system based on *Axxon One*.
User guide contains a detailed description of the process of installing, configuring and working with *Axxon One*, using Windows users as an example. For the features of installing and configuring *Axxon One* in Linux OS, see Linux OS Administrator's Guide.
The structure of this document enables the user to get acquainted with the software package and then, depending on the user's level of training, choose sections of interest for a more detailed study. The sections in this guide, whether they are informative or serve as a reference, have their own internal structure.
Introduction and Description of the Software Package are intended to generally acquaint the user with the technical features and functionality of *Axxon One*, as well as with the key stages of building a security system based on the software package.
Recommendations to the user/administrator for installing the software and configuring hardware are presented in detail in Installing the Axxon One Software Package. Licensing of the software product contains manuals on how to register a license to use *Axxon One*.
Startup and shutdown of the software package are described in Launching and closing the Axxon One software package.
Configuration of Axxon One presents step-by-step instructions on configuring user-specific settings and activating the required functionality. This information is useful for system administrators as well as for operators with permissions to manage system settings.
Recommendations on configuring the user interface, working in various video surveillance modes, and utilizing the functional capabilities of *Axxon One* are presented in Working with Axxon One.
Description of utilities contains a description of additional software utilities employed when working with the software package.
Appendices contains a glossary of the product's basic terms and definitions. It also lists all known issues that you may encounter while using *Axxon One*.

Purpose and functionality of Axxon One

Axxon One is a video and security system management software (VMS) platform that combines neural network video analytics, forensic archive search, a user-friendly interface, and the ability to integrate with external access control, alarm and perimeter security systems.

Security systems based on *Axxon One* range from home security systems (for an apartment or a house) to professional large-scale distributed security systems for businesses of any size (car service centers, shops, factories, airports, government offices, and so on).

Video and audio surveillance of protected facilities, video analytics, and rapid response to suspicious situations without operator involvement, and storage and export of obtained data are just a few of *Axxon One*'s many functions.



We constantly expand the functionality of *Axxon One* by adding new capabilities in response to customer requests and incorporate the latest developments in AI and video analytics.

Software Lifecycle Policy

On page:

- Software Lifecycle Phases
- Software Technical Support
- Standard Period for Release of Software Updates
- Licensing Policy with Regard to Software Updates

Software Lifecycle Phases

The software source code repository is divided into 3 branches:

- **trunk** - current changes;
- **stabilization** - preparation of a new release;
- **release** - the latest official release.

During the development process, all new software features are added to the **trunk** branch.

After reaching *Feature Complete* status, all changes from the **trunk** branch are moved to the **stabilization** branch.

From that time on, only software fixes that are critical for this version are added to the **stabilization** branch. These fixes are also duplicated in the **trunk** branch.

After the version stabilization is completed, all changes are moved from the **stabilization** branch to the **release** branch, and a new development phase begins.

Software Technical Support

After purchasing a license key, the Customer can receive full technical support throughout the key's validity period or until the end of the software lifecycle if the license is unlimited in time.

Standard Period for Release of Software Updates

Release	Standard period
Major release	1 – 1.5 years
Minor release	3 – 5 months
Bug and security fixes*	3 – 5 weeks

Major and minor releases are available on the company's official website. Releases with bug and security fixes can be requested from te chnical support.

***** Software bugs can only be fixed in the latest official release.

Licensing Policy with Regard to Software Updates

- New software versions are fully compatible with the license keys of previous versions.
- After the softwarehas been updated, all the features previously specified in the license key will be available in the new version.
- New software features that are subject to licensing will not be available until the license key is updated.

Description of the Software Package

Basic principles of building a security system based on the Axxon One software package

Building a security system based on the *Axxon One* software package includes the following recommended stages:

1. Selecting a configuration for the security system (with the help of professionals)
2. Building a separate local area network with restricted access
3. Calculating the sufficient bandwidth required for each segment of the local area network
4. Selecting and configuring the software and hardware platform on which the selected security system configuration will be implemented (selecting and configuring personal computers to act as servers and clients in accordance with the requirements, as referenced in the section titled Implementation Requirements for the Axxon One Software Package, Operating system requirements)
5. Selecting and connecting reliable equipment that is optimally suited for a specific security system (with the help of professionals)
6. Training personnel to work with the *Axxon One* software package in accordance with the requirements (see the section titled Requirements for Personnel Quantity and Qualifications).

Axxon One features: reference information

On the page:

- Micromodule architecture
- Support for IP devices
- Support for analog cameras in Axxon One
- Video and Audio Detection Tools
- Video archive
- Interactive 3D Map
- User Interface
- Face Recognition
- Number Plate Recognition
- Receiving Events from External Systems

The advanced features available in *Axxon One* are continuously updated and extended.

Axxon One offers virtually unlimited opportunities for system scaling, task-based customization, and reallocation of resources (based on changes in the number or quality of video and audio monitoring tasks) at end-user sites.

Video surveillance systems based on *Axxon One* can scale infinitely: there are no restrictions on the number of video Servers, workstations or video cameras.

Support for over 10000 models of IP cameras is included, as well as remote access from mobile devices and a web interface. *Axxon One* supports touchscreens.

Micromodule architecture

The micromodule architecture of *Axxon One* video management software allows implementing different video management system functions as different operating system processes. Each function is the responsibility of a different micromodule; a dispatcher module monitors the functioning of the micromodules. If a function encounters an error and a process is quit unexpectedly, the dispatcher module automatically relaunches the corresponding micromodule. This does not affect the performance of other processes or the functioning of the VMS overall.

Support for IP devices

Drivers Pack

IP devices support in *Axxon One* is provided through the *Drivers Pack* Module specially developed by AxxonSoft and regularly updated to support new IP devices.

Drivers Pack allows adding support for new IP devices without having to wait for the release of new versions of *Axxon One* and without reinstalling the entire system.

See Documentation Drivers Pack.

Multistreaming

Many of today's IP devices can transmit two video streams with different video parameters and compressed in different codecs. *Axxon One* supports Multistreaming i.e. receiving two streams from a camera simultaneously: high-quality and low-quality, which allows taking advantage of this feature of IP equipment to optimize the CPU load on the video Server and the Client workstation.

See The Camera object.

GreenStream

The GreenStream feature saves bandwidth and Client CPU resources. It automatically chooses a video stream from a camera to the Server, and then to the Client, depending on the resolution at which the video is currently displayed on the Client.

See Selecting video stream quality in a Surveillance window (GreenStream).

Embedded video camera analytics

Axxon One supports on-board detection embedded in video cameras. This means that when on-board detection tools are triggered, *Axxon One* is notified and can use these events to drive system reactions. On-board detection does not burden the CPU of the video Server and makes use of uncompressed video (completely bypassing the compressing/decompression process), and therefore provide extra stability in difficult conditions such as poor visibility.

See General information about embedded detection tools.

Fisheye cameras and ImmerVision lenses

Support for fisheye cameras and ImmerVision lenses allows dewarping video from a fisheye camera or camera with an ImmerVision panomorphic lens to obtain several "normal" flat images with different frame aspect ratios for display on the Client screen. One of the resulting virtual cameras can be a virtual PTZ camera.

See Working with fisheye cameras.

ONVIF support

AxxonSoft is a member of ONVIF (the Open Network Video Interface Forum), which work toward the development and promotion of international standards for network security and video surveillance system interfaces. ONVIF is supported in *Drivers Pack*.

See Features of configuring and working with cameras connected via ONVIF.

RTSP support

Many IP devices support multimedia streaming via RTSP. *Axxon One* supports receiving such streams without requiring integration of the relevant camera via Drivers Pack.

See Configuring connection of single-channel devices.

Support for analog cameras in Axxon One

Alongside IP devices, *Axxon One* allows you to use analog cameras in your video surveillance system. Analog cameras are more affordable and are well-suited for many installations without high video resolution requirements. In addition, *Axxon One* allows creating hybrid systems that combine both analog and IP cameras.

Video and Audio Detection Tools

Axxon One video management software incorporates a powerful system for analysis of video images. It includes the following video detection tools:

1. Tampering detection.
2. Motion detection.
3. Neurotracker.
4. Object tracker.
5. Pose detection.
6. Equipment detection (PPE).
7. Person-based privacy masking.
8. Fire Detection.
9. Smoke Detection.
10. Water Level Detection.
11. Neurocounter.
12. Queue detection.
13. Visitors counter.

In addition to the video detection tools, *Axxon One* has three audio detectors:

1. Noise Detection.
2. Audio Loss detection.
3. Signal Detection.

Macros can be set to automatically run when a detection tool is triggered (on a per-detector basis). Multiple detection tools can be combined into complex conditional rules.

See Configuring detection tools.

Video archive

For storing archive in *Axxon One*, you can use both local and network file storage with the SolidStore system, or object storage.

SolidStore

SolidStore is a file new system for reliable video storage developed by AxxonSoft especially for storing video archives. By optimizing the reading/writing process we managed to achieve three important advantages:

- Enable high read/write speeds, approaching the physical access speed limit of the hard disk.
- Increase the service life of the hard disk.
- Solve the problem of data fragmentation.

Cloud archive

Cloud archive is an object file system for storing video archive in cloud storage (for example, Amazon S3, Microsoft Azure). Using a cloud archive allows you to reduce the price of data storage and set up flexible integration with AxxonSoft VSaaS. According to Amazon, the reliability of using an object archive is up to 99.999999999%.

See Configuring archives.

TimeCompressor

Time Compressor allows the user to set a time range for video footage and get a short video clip of all moving objects in the scene. Objects and events captured at different times are displayed simultaneously in a condensed motion events summary. Time Compressor is especially convenient for viewing large archives that feature a relatively small number of active objects.

See Compressed playback of archives (TimeCompressor).

Forensic Search in Archive

The *Axxon One* video management software (VMS) utilizes VMDA—a database developed by AxxonSoft for indexing and storing descriptions of observed scenes. Along with video recording, this database allows archiving characteristics of all moving objects in the scene, and then uses these characteristics to perform quick searches of the video recordings (MomentQuest technology).

See Forensic Search for Fragments (MomentQuest).

Interactive 3D Map

Interactive 3D Map superimposes camera locations on a site map and displays camera views in the same window. Cameras in the current layout are color-coded by current status. Operators can instantly pinpoint where a selected camera is located on the map and identify the corresponding location of interest.

Immersion Mode

When enabled, this mode overlays a translucent video image on the map; fixed objects in the frame (furniture, doors, etc.) are combined with their depictions on the map. This allows easily seeing where a person or car is located and where it is going.

OpenStreetMap

OpenStreetMap support is available in *Axxon One*. The site map is downloaded from the Internet and the user selects the necessary area and scale. Additional map data is downloaded in real time, if needed, when zooming in/out or scrolling.

> **Note**
>
> To work with OpenStreetMap maps in *Axxon One*, you need to purchase an OpenStreetMap license.

Virtual PTZ cameras on the map

The Virtual PTZ Camera function becomes available when the map contains at least one fisheye camera. This function allows viewing video from a fisheye camera directly on the map. Click anywhere in the fisheye video shown in a layout cell to dewarp the source video, with digital zoom and click-to-focus.

See Working with the interactive map.

User Interface

Editable camera layouts

Axxon One allows you to create custom camera layouts. Layouts can be configured in any way the user wants and the aspect ratios of Surveillance windows can be fine-tuned. Editable layouts efficiently fit different cameras with different aspect ratios on the same screen, as well as support display of dewarped fisheye camera footage.

See Configuring layouts.

Autozoom

Autozoom helps to monitor moving objects by automatically adjusting the level of digital zoom. Autozoom shows close-in video for parts of the frame that contain a moving object or objects and follows them as they move, just as a movie camera does when taking a close-up shot.

See Autozoom.

Face Recognition

Axxon One includes an algorithm for recognizing human faces in a video frame and subsequent search for them in a video archive of several cameras. You can search by an uploaded photo or by an image of a person's face selected in a video archive frame. The system will return the video fragments from the archive where the searched person is present as search results.

See Face search.

Number Plate Recognition

Axxon One also includes an algorithm for recognizing vehicle number plates. The recognized number plates are saved to a database and matched with a video archive of several cameras. If a number plate contains similar characters, the system generates several hypotheses during the recognition. This increases the probability of a successful search for a particular number in a generated database.

See Search by LPs.

Receiving Events from External Systems

Axxon One includes a new feature set that is capable of receiving events from various external devices and systems—POS terminals, access control units, external software, etc.

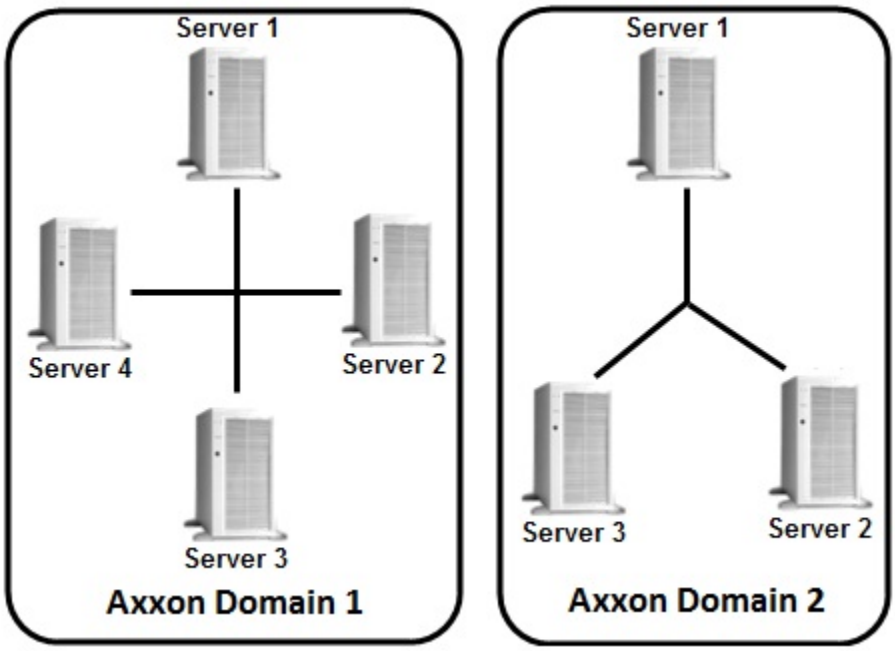
See Receiving Events from External Systems.

Functions of the Distributed Security System

You can create a distributed system within an Axxon Domain on *Axxon One*.

Axxon Domain – a selected group of computers on which the server configuration of the *Axxon One* software package is installed. Linking the servers in a group makes it possible to set up interaction between them, thus organizing a distributed system.

Servers are interoperable only if they belong to the same Axxon domain. At the same time, each Server of the domain operates independently and has its own DB.



A distributed security system based on the *Axxon One* software package offers the user the following functional capabilities:

1. Viewing and manual processing of video and audio data from several servers on one client;
2. Controlling video cameras connected to various servers from one client;
3. Configuring all servers of the distributed system on one client;
4. Execution of automatic responses when detection tools are triggered (audio notification, triggering of relays, e-mail notification, etc.) within the distributed system.

Note

If a Server is not accessible by NetBiosName or some TCP and UDP ports are closed, it is possible to build a distributed security system on a virtual private network (VPN). For example, with the help of OpenVPN. Detailed information on OpenVPN and examples of virtual private network configuration are given in the official documentation.

Suppose, the Server relies on a defined port range (see Installation), and you want to set up a surveillance system based on several networks. You do not have to use VPN in that case. Use port forwarding instead.

Axxon Domain configuration is described in detail in the section titled Configuring domains.

Network Topologies of the Axxon One Software Package

Axxon One supports both decentralized and star network topologies.

The decentralized architecture better suits smaller systems.

The star architecture is more practical for creating large centrally monitored distributed systems where no local monitoring is required on remote sites.

Attention!

If your system is based on star topology, please take into account the following:

1. In a failover (see General information about a failover system) and non-failover systems, the Client must have access to all Servers (located centrally).
2. In a failover system, all Manager Servers must have access to each other (located centrally).

Characteristics of Axxon One

Security systems based on *Axxon One* have the following primary characteristics.

Characteristics	Value
Number of Servers in the distributed system	Unlimited
Number of Clients that support simultaneous connection to the Server	Unlimited
Number of Servers that simultaneously transmit video to a Client	Unlimited
Number of video capture channels for "live video" processing on one Server	Unlimited
Number of detection tools per camera	Unlimited
Number of simultaneously processed signals coming from microphones	Unlimited
Number of audio output channels (to speakers, headphones, and so on)	Depends on the sound card used for audio playback
Number of PTZ devices used	Unlimited
Number of event sources (POS devices)	Unlimited
Number of user roles and users	Unlimited
Number of objects simultaneously tracked by the Object tracker	Up to 25
Number of license plate recognition channels	Determined by the license, number is unlimited
Number of face recognition channels	Determined by the license, number is unlimited
Number of connected mobile Clients or Web-Clients	Unlimited
Number of videowalls	Unlimited
Number of maps	Unlimited
Support for analog cameras	Yes (via video capture cards)
Support for IP devices	IP cameras and IP video servers. This list is continuously expanding: support for new hardware is added via updates to *Axxon Driver Pack*
CPU support	64-bit (x64)
Number of archives in the system	Unlimited
Maximum archive size	Unlimited
Video compression algorithms	MJPEG, MPEG-2, MPEG-4, MxPEG, H.264, H.264+, H.265, H.265+
Audio compression algorithms	PCM, ADPCM, g711, g726, aac, mp2
Available video image resolutions	Resolutions supported by video cameras
Support for embedded camera analytics	Yes
Support for touchscreens	Yes

Implementation requirements for the Axxon One software package

Limitations of Axxon One

> **Attention!**
>
> It is not recommended to delete or modify any *Axxon One* files without prior consulting with AxxonSoft technical specialists.

When working with *Axxon One*, keep in mind the limitations that the developer has imposed on the system in order to ensure its operability.

No.	Limitation
1	To work with *Axxon One,* the following requirements for OpenGL must be met: 1. Version 2.0 and higher. 2. The following extensions must be available: **ARB_vertex_program**, **GL_EXT_blend_func_separate**, **GL_ARB_frame buffer_object**. Extensions availability can be checked with the *OpenGL Extension Viewer* program (download). This program also contains a large database of OpenGL support in video cards of various vendors
2	*Axxon One* Client cannot be started if the scale of all items on the screen (DPI) is over 100%. If the screen resolution is set lower than 1280*960 pixels, the correct operation of *Axxon One* isn't guaranteed
3	The Server and the Client must be of the same version. If not, the correct operation of *Axxon One* isn't guaranteed
4	For the correct operation of *Axxon One*, the OS must use the UTF-8 locale
5	Downgrade to a previous version of *Axxon One* is not allowed
6	In one LAN, two Servers with the same name are not allowed, even if they belong to different Axxon-domains. If the name of the Client computer and the name of the Server computer in the LAN are the same, the correct operation of *Axxon One* isn't guaranteed
7	Maximum video frame rate in the Client is 50 FPS. When *Axxon One* is running in the safe mode, the frame rate decreases
8	To install *Axxon One*, you must log in to Windows as an administrator
9	For the correct installation of *Axxon One*, there must be no spaces at the beginning of the name of the folder which contains the installer
10	For the correct and full-feature operation of *Axxon One*, the system must not limit network activity between all Servers and Clients. If during *Axxon One* installation, certain ports were specified, the access to these ports via the TCP and UDP protocols must be enabled. Otherwise, access to all ports must be allowed in the system. For the Client to operate correctly, disable unnecessary network interfaces on the Server. If you want the Server to work with only one network interface, set its gateway and mask in the network settings utility (see Network settings utility)
11	To ensure proper functioning of *Axxon One*, it is imperative to employ distinct IP addresses for all network interfaces on the Server. Or utilize the interface mask to specify a designated set of addresses where the Server will operate (see Network settings utility). Failure to maintain unique IP addresses among the Servers may result in complications pertaining to intercommunication among the Servers themselves, as well as between the Client and the Server
12	Time must be synchronized among all computers in the system (configured by the user)
13	If you have edge storage enabled in the system, synchronization between the Server and the IP device is necessary (see The Embedded storage object). Lack of synchronization may lead to bad DB entries of events detected on the device
14	Before installing *Axxon One*, make sure the video card drivers on the computer are fully up to date

15	NetBIOS name of a computer must meet the following requirements: • contains only Latin characters, digits, and a "-" character; • does not exceed 15 characters
16	The face detection tool requires a CPU supporting SSE4.2, FMA3 or AVX2.0 instruction sets
17	The Client cannot be started on a remote desktop through the standard *Remote Desktop Connection* Windows utility
18	If a computer is connected to an Active Directory domain, one of the following conditions must be met to enable disk access: 1. Disk Access Control Lists must contain only local or built-in groups and users. 2. Create an **AxxonFileBrowser** user in the domain and add it to the **Users** group (see Installation). This behavior is typical only of the file systems that have access permissions (for example, NTFS)
19	Hibernation mode and sleep mode are not supported. Before you switch the computer to these modes, stop the Server (see Shutting down a Server)

Operating system requirements

On the page:

- Windows OS
- Windows Server OS
- Linux OS

Attention!

- For *Axxon One* to work corectly, the operating system needs to be up to date—the latest updates must be downloaded and installed.
- Only 64-bit versions of operating system are supported.

Windows OS

- **Windows 11** [4]: Home, Pro, Education, Pro Education, Pro for Workstations, Enterprise;
- **Windows 10**: Pro, Enterprise, Education, Home Edition;
- **Windows 10 IoT** [3]: Enterprise, Enterprise LTSB 2016, Enterprise LTSC 2019.

Windows Server OS

- **Windows Server 2022** [4]: Standard, Essentials, Datacenter, Azure Datacenter;
- **Windows Server 2019** [4]: Essentials [2], Standard, Datacenter;
- **Windows Server IoT 2019** [4];
- **Windows Server 2016** [1, 4]: Essentials [2], Standard, Datacenter.

Linux OS

- **Debian**: 12, 11, 10, 9 [5];
- **Ubuntu**: 22, 20, 19, 18.

Linux OS Administrator's Guide

Limitations of Axxon One in Linux OS

Attention!

[1]—neural analytics is not applicable (see Hardware requirements for neural analytics operation).

[2]—there are restrictions, posed by OS edition (2 physical processors)—see http://www.microsoft.com.

[3]—Core edition is not supported.

[4]—Full Installation type is supported. Server Core Installation type is not supported (see Possible Errors During Operation).

[5]—the basic Face detection cannot work (see Configuring Face detection).

Disk storage subsystem requirements

On the page:

- General requirements
- Storage requirements
  - Minimum requirements
  - Size of the archive
  - System log database
  - Metadata database
  - The system logs
  - Self-diagnostics service

General requirements

For *Axxon One* VMS operation, the disk subsystem should match the following requirements:

1. The number of input/output operations (IOPS) of the device should not be less than the IOPS of *Axxon One* VMS.
   Axxon One records the archive in blocks of 4 MB every 10 seconds. However, if the block is not filled in 10 seconds, a smaller fragment of the block will be recorded, which will be added to later.
   Archive playback is also performed in blocks (except when reindexing, see Console utility for working with archives).

   Below you can see how you can estimate the IOPS for *Axxon One* VMS.

	If the average bitrate per camera is less than ~3.6 Mbps	**If the average bitrate per camera exceeds ~3.6 Mbps**
IOPS during archive recording Archive recording includes both data input (recording) and output (reading) operations	IOPS (recording) = 0.29 * N IOPS (reading) = 0.035 * M	IOPS (recording) = 0.065 * M IOPS (reading) = 0.035 * M
IOPS during archive playback Archive playback includes only output (reading) operations	IOPS (reading) = 0.035 * R * S	
IOPS during simultaneous recording and playback	IOPS (recording) = 0.29 * N IOPS (reading) = 0.035 * M + 0.035 * R * S	IOPS (recording) = 0.065 * M IOPS (reading) = 0.035 * M + 0.035 * R * S

where

- N is the number of cameras being recorded;
- M is the cumulative bitrate of all cameras being recorded, in Mbps;
- R is the cumulative bitrate of all cameras being played back from the archive at normal speed (1x), in Mbps;
- S is the playback speed.

2. If you use RAID storage, specify the write-back policy for recording to cash memory.

Storage requirements

The disk subsystem capacity of *Axxon One* Server should be estimated taking into account the resolution, the compression algorithm, the frame rate of the recorded video signal, the number of video cameras from which the recording to disk(s) takes place and other recording parameters. In addition, the size of the system log and metadata databases should be considered.

Minimum requirements

You need at least 10 GB of free disk space on Windows OS and 5 GB on Linux OS to install the *Axxon One* VMS package in the **Server and Client** configuration.

See the storage calculations below, taking into account the size of the archive, the size of the database and the size of the archive of the system logs.

Size of the archive

The capacity of the disk subsystem can be calculated by the formula:

Capacity of disk subsystem (MB) = Time of storing archive (days) * Cameras number * Rate of recording (FPS) * 3.51 * Time of guaranteed recording from a camera (h/day) * Average frame size (KB),

where

Time of storing archive is the required time for storing an archive from one camera, days;

Cameras number is the number of cameras from which recording to the archive takes place;

Rate of recording is the frame rate of recording to the archive, frames per second;

3.51 = (60 sec in min * 60 min in hour) / (1024 KB in MB) is the factor used for KB/s in MB/h conversion;

Time of guaranteed recording from a camera is the number of hours of guaranteed recording from one camera per day;

Average frame size is the average size of the camera frame in KB.

Note

Average frame size of 640x480 resolution is:

Video codec	Average frame size
H.264	from 8 KB to 17 KB
MPEG4	from 8 KB to 35 KB
MJPEG	from 23 KB to 60 KB

Average frame size may vary over a wide range depending on the vendor, the model and the settings of the camera and video image complexity.

Note

To calculate the frame size you can use the ratio, that when increasing the vertical or horizontal resolution two times, the average frame size will be increased four times (this rule is a relative and can be applied only to some camera models).

Examples of calculating the capacity of the disk subsystem (without the capacity of the system log and metadata databases) are presented below.

Recording parameters	Calculating results
4 cameras with 25 FPS and 640x480 resolution, guaranteed recording of 24 hours per day during one week	H.264: from 500 GB to 1 TB MPEG4: from 500 GB to 2 TB MJPEG: from 1.3 TB to 3.5 TB
16 cameras with 12 FPS and 640x480 resolution, guaranteed recording of 12 hours per day during one week	H.264: from 500 GB to 1 TB MPEG4: from 500 GB to 2 TB MJPEG: from 1.3 TB to 3.5 TB
4 cameras with 25 FPS and 1280x960 resolution, guaranteed recording of 24 hours per day during one week	H.264: from 2 TB to 4 TB MPEG4: from 2 TB to 8 TB MJPEG: from 5.3 TB to 14 TB

System log database

The capacity of the system log database should be taken into account when the capacity of the disk subsystem is calculated. The estimated capacity of the system log database is calculated by the formulas:

Capacity of system log database (low detection tools activity) = D * T * (0.04 GB / day);

Capacity of system log database (average detection tools activity) = D * T * (0.12 GB / day);

Capacity of system log database (high detection tools activity) = D * T * (0.48 GB / day);

where

D is the total number of detection tools created in the system,

T is the estimated duration of system log storage, days.

Metadata database

The following formulas can be used to determine the required disk size for the metadata database:

Size of metadata database = N * T * (0.5 GB / day) – sufficient disk size;

Size of metadata database = N * T * (1 GB / day) – sufficient disk size plus reserve space;

Size of metadata database = N * T * (5 GB / day) – sufficient disk size plus a large reserve,

where

N is the number of detection tools in the system actively recording metadata. One video camera can have several detection tools with metadata (see General information on metadata),

T is the period of time (number of days) that metadata will be stored. By default, T = 30 days.

If you have less than 15 GB of free disk space, the metadata database is overwritten - the new data is written over the oldest data.

The system logs

When calculating the disk subsystem capacity, it is necessary to include at least 1 GB for the system logs archive.

Self-diagnostics service

When calculating disk subsystem capacity, note that self-diagnostics service may generate up to 100 MB of data per day.

The depth of the service internal database is limited to 7 days and 512 MB.

Hardware requirements

Axxon One is designed for use on computers.

You can determine the required hardware configuration (RAM, CPU, and hard disk) using the AxxonSoft Platform Calculator. See the documentation for the calculator here.

Disk storage subsystem requirements

TCP/IP Network Bandwidth Requirements

Hardware requirements for GPU-based video decoding

Hardware requirements for neural analytics operation

Hardware requirements for the Face Detection TV and its sub-tools

Hardware requirements for the Face Detection VA and its sub-tools

Hardware requirements for the Face Detection VL and its sub-tools

Hardware requirements for License Plate Recognition IV

Hardware requirements for License Plate Recognition RR and Vehicle Recognition RR

Hardware requirements for License Plate Recognition VT

Attention!

If *Axxon One* is installed on a computer with two processors, we recommend disabling Hyper-threading.

Minimum RAM requirements

At least 8 GB of RAM is recommended. For a specific calculation, use the platform calculator. If you increase RAM speed by using the memory at a higher frequency or using the memory in dual-channel (or more) mode, it will reduce CPU usage and boost the performance of *Axxon One*.

Minimum and recommended requirements for graphics cards

Minimum and recommended requirements for graphics cards are given below.

Recommended requirements	Discrete NVIDIA GPU: GeForce 1030 1GB or higher. Integrated GPU: Intel UHD Graphics 630 or higher
Minimum requirements	Discrete NVIDIA GPU: GeForce 7300LE / GeForce 200 or higher (512MB) Discrete AMD GPU: Radeon HD 5000, Radeon HD 6000 or higher. Integrated GPU: Intel HD Graphics 530. OpenGL version 2.0 or higher. Availability of the **ARB_vertex_program**, **GL_EXT_blend_func_separate**, **GL_ARB_framebuffer_object** extensions for OpenGL You can check the availability of extensions using the OpenGL Extension Viewer program (download).

We recommend using the latest drivers for both integrated and discrete graphics cards.

Attention!

If several graphics cards are installed in the system, select the graphics card that meets the minimum requirements as the main graphics card in the OS settings.

TCP/IP Network Bandwidth Requirements

Network bandwidth is a limiting factor in distributed system performance. The bulk of the information streamed over the network is video data. For example, the data flow (video stream) from remote cameras, such as used to monitor ATMs, is sent via communication channels.

> ⚠ **Attention!**
>
> The minimum bit rate through the communication channel (network bandwidth consumption / goodput) for the Axxon One VMS, should be at least **2 Mbit/s**.

To determine the required TCP/IP network bandwidth for video transmission from IP devices and some video capture cards, we recommend you to use Axxon Platform Calculator (check the **Total bitrate from ip devices (Mbit/s)** parameter).

Requirements for BIOS configuration

For the performance of *Axxon One*, especially for video decoding, the frequency of the processor is important. The higher the frequency, the higher the performance of *Axxon One* on a given platform.

On modern computers, the energy saving mode is activated in BIOS by default. Using this mode on multiprocessor systems leads to a partial load of CPU cores and reduces the performance of the I/O subsystem.

For better performance of *Axxon One*, you must configure the computer BIOS as follows:

> ⚠ **Attention!**
>
> Different manufacturers of motherboards call these technologies differently. So, for each specific motherboard model, you must always check the documentation for that model to find out the name of the technology.

Action	Technology	Reason
Enable	E-Cores	To get the calculation results with the actual load
Disable	Turbo Boost	The clock rate and displayed CPU load can vary from server to server depending on the cooling system
	Hyper-Treading	Uneven load of processor cores
	Intel Speed Shift	To keep the processor clock from dropping below the base clock
	Enhanced Intel SpeedStep (EIST)	Reduces the operating clock of the CPU
	Energy saving	To keep the processor clock from dropping below the base clock
	Smart throttling	Abrupt reset of processor clock

Running Axxon One VMS in Virtual Machines

The *Axxon One* VMS can be run in the following virtual machines:

- VirtualBox (all versions);
- VMware (all versions);
- Hyper-V (all versions).

Attention!

To run the Client, 3D acceleration must be enabled.

Note

The operating system in a virtual machine must meet the general requirements.

If you use VirtualBox on Windows 7 SP1 and in Hyper-V, you won't be able to access a Guardant USB key from the guest system.

In Hyper-V, you can use third-party utilities (for example, USB Network Gate) instead.

General information about updating Windows OS

It is necessary to update Windows OS and its components to ensure the correct operation of *Axxon One*. Otherwise, unexpected errors and system malfunctions may occur.

You can update Windows OS automatically (see the official Microsoft documentation).

For Servers, it is necessary to define a maintenance period during which the downloaded updates can be installed manually after *Axxon One* is safely shut down.

If automatic update is not configured, you should check for updates at least once a week. Typically, important updates are released monthly. You can check the updates using the Windows Update service (see Get the latest Windows update).

Regardless of the options you choose, some updates are not installed automatically. These include optional updates and updates that require you to accept new terms of use. When these updates become available, the Windows Update service will notify you that they are ready to be installed.

In some cases, it may be necessary to install specific Windows OS updates to ensure the *Axxon One* operation (see Installation, Error when installing Drivers Pack).

Interface of the Axxon One Software Package

Axxon One Client has 2 basic interfaces: Layouts and Settings .

To switch the two, click the tabs at the top of the screen.

Note

If there are no cameras in VMS, the tab is not available.

Attention!

You can configure access to any given tab and buttons in the top panel individually for each user role (see Configuring user permissions).

When you are configuring VMS, the top panel shows tabs with different groups of settings, the button for switching to the system log, current user name and the **Exit** button.



When you select **Server** or any child object in the **Hardware**, **Archive** or **Detection Tools** tabs, the upper panel shows the current CPU and network load for the selected Server (or the Server to which the object selected on the specified tabs belongs).



In the Layouts interface in the upper pane, you see the following elements:

1. Camera search panel.
2. System time.
3. Context menu.
4. Video surveillance mode selection tabs.
5. Video wall management panel.
6. Monitor management panel.
7. Layouts panel.
8. Macro menu.
9. Layout scaling buttons.



In the Layouts and Search interface, you can hide the top panel. To do this, click the button in the top right corner. To show the top panel, hover over it with the pointer.

Note

To pin the top panel, click the button.

In Full Screen (see Configuring the Client screen mode (full screen or window)), to collapse the client window, click the button.

Ports used by the Axxon One Software Package

Appendix 8. Using Axxon One with NAT

Ports	Changeable	Installation type	Process	Open the port*
20040 (Windows, Linux) 20041 (Windows, Linux) 20042 (Linux) 20108 (Windows, Linux)	No	Server and Client	Self-diagnostics service	Not required
20109	Yes	Server and Client Client	gRPC API (see Configuring the Server ports) Client to Server connection	Required
20110	Yes	Server and Client	PostgreSQL database (see Configuring the Server ports)	Required
20111–20210	Yes	Server and Client	Server (see Installation, Network settings utility) Communication between Servers within the same Axxon-domain	Required
80 (Windows) 8000 (Linux)	Yes	Server and Client	Web server (see Configuring the Web-Server)	If necessary + HTTPS port 443
554 (Windows) 20554 (Linux)	Yes	Server and Client	RTSP server (see Configuring an RTSP Server)	Not required
8080	Yes	Server and Client	Virtual input (see Configure virtual inputs)	Required
8888	No	Server and Client Client	Client HTTP API (see Client HTTP API)	Not required
4000 4646–4648 8300–8302 8500 8600	No	Failover Server and Client	Failover (see Ports used by the failover system)	Required

* In a configuration including several Servers in firewalled LANs, or port forwarding on the router under NAT environment.

Requirements for Personnel Quantity and Qualifications

The following roles have been defined for operating the *Axxon One* software package:

1. Security system administrator.
2. Security system operator.

In special cases, one person can perform the functions of both the administrator and the operator.

The main duties of the administrator are to:

1. Update, configure, and monitor the operability of the security system's hardware.
2. Install, update, configure, and monitor the operability of basic and system software.
3. Install, configure, and monitor software applications.
4. Manage user accounts (this duty can be carried out by a user entrusted with system administrator permissions).

The administrator must have the skills necessary for network configuration, including routing and firewall, as well as NetBIOS, DNS, and NTP network services.

Besides, the administrator must have high qualifications and practical experience installing, configuring, and administering the software and hardware employed in the software package.

The software package is structured so that all accessible functionality can be managed by one administrator or administration responsibilities can be divided among several users.

The main duties of an operator are to:

1. Work with the software's GUI (graphical user interface).
2. Optimize the performance of the personal computer to carry out tasks using the functionality provided in the software package.
3. Create roles and users in the system (if the user has been granted the appropriate permissions).

The system operator must have experience with, and be a qualified user of, PCs running Microsoft Windows and must be able to easily perform basic operations.

Installing the Axxon One Software Package

Installing equipment

Types of Devices Used

An IP device is the source of the video signal (video data) for the *Axxon One* software.

> **Note**
>
> You can connect analog video cameras to *Axxon One* via video capture cards, which the software defines as IP devices.

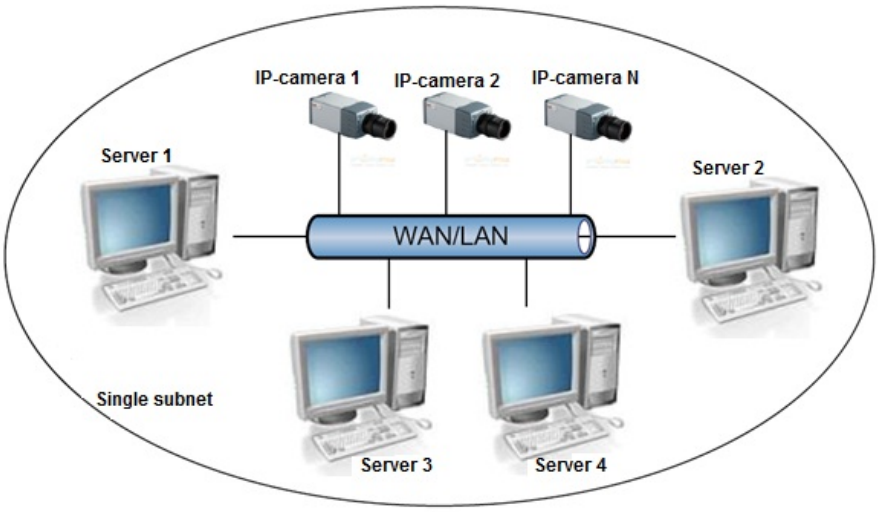
The following types of equipment are IP video and audio surveillance devices:

1. IP video cameras.
2. Various types of IP video servers.

IP video servers which use analog video cameras directly connected to them, digitize the analog video signal, and transmit it to users via TCP/IP. When working with analog video cameras connected to IP video servers, users can utilize the same video image viewing and transmission functions as with IP video cameras.

Connecting IP Devices

To work with IP devices, you need to connect the *Axxon One* server to the local network where the required IP devices are enabled.



To ensure support for IP devices on an external network:

- The IP devices must have an external static IP address.
- The necessary ports on the network equipment must be opened.

> **Attention!**
>
> If these requirements are met, IP devices should be properly handled. However, correct functioning is not guaranteed.

Based on the video signal coming in from the IP device, an assessment is made of the guarded location and the system responds to events registered for that location. The content and quality of the obtained video information depends on how the IP device is installed and configured. There are a number of rules that must be followed to obtain a high-quality video signal. In particular, high-quality peripheral equipment (hubs/routers) must be used; we advise against use of Home and Office-class devices, which are not intended for use in such security systems.

> **Note**
>
> IP devices connected to such equipment will transmit a video stream with an unacceptably long delay (from 1.5 to 3 seconds per frame)

Detailed information about creating a local network and connecting IP equipment to it is presented in the corresponding reference documents.

Configuring IP Devices in Windows

IP devices can be configured in Windows by using the following software:

1. Software included with the IP device. This software is used to accomplish the following tasks:
    a. Searching for network devices connected to the local network.
    b. Preliminary IP address assignment (without account of routing).

    > ⚠ **Attention!**
    >
    > Without assigning preliminary IP addresses to the devices, it is not possible to access their Web interface.

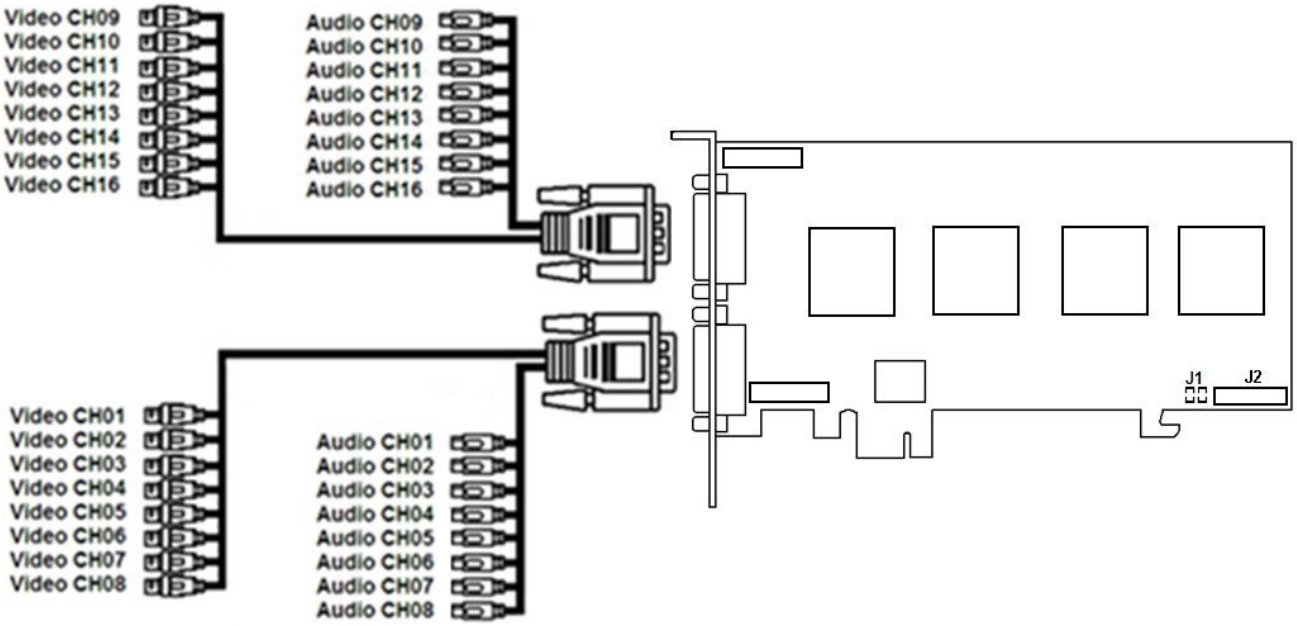
2. Web interface of the IP device. This interface is used to accomplish the following tasks:
    a. Configuring the IP devices with consideration for routing.
    b. Configuring modes for the IP devices to work with video and audio signals.
    c. Viewing video images coming in from IP devices in standard Web browser mode.

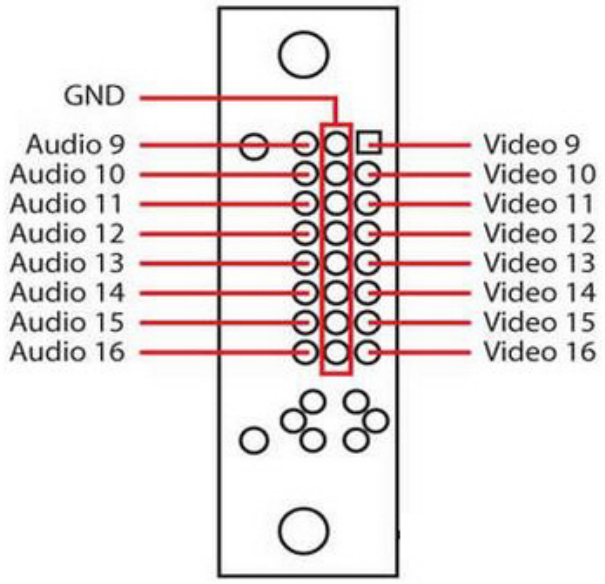
Configuration of IP devices in Windows is described in detail in the official reference documentation for the respective devices.

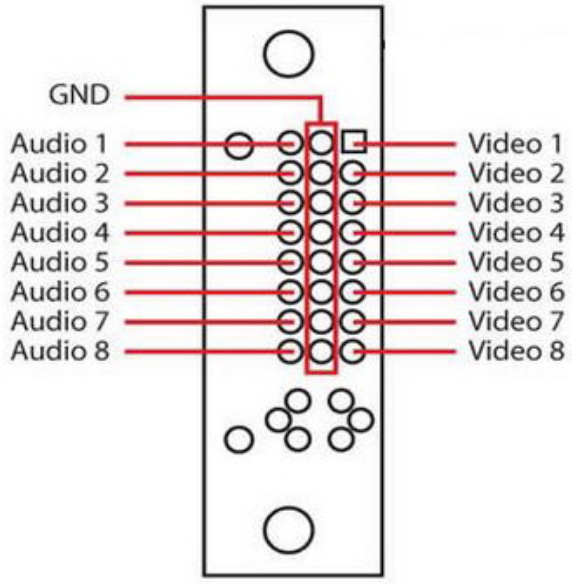
Video capture cards pins

WS-216 video capture card pins

WS-216 video capture card has two external DVI-I pins. Video and audio connection is performed with the help of DVI-I/BNC and DVI-I /RCA stubs correspondingly. Simultaneous connection of up to 8 cameras and up to 8 sound sources to one external pin of WS-216 video capture card is possible. The Watchdog cable is connected to the J1 pin. DI/DO card is connected to the J2 pin.




GND
Audio 9
Audio 10
Audio 11
Audio 12
Audio 13
Audio 14
Audio 15
Audio 16
Video 9
Video 10
Video 11
Video 12
Video 13
Video 14
Video 15
Video 16

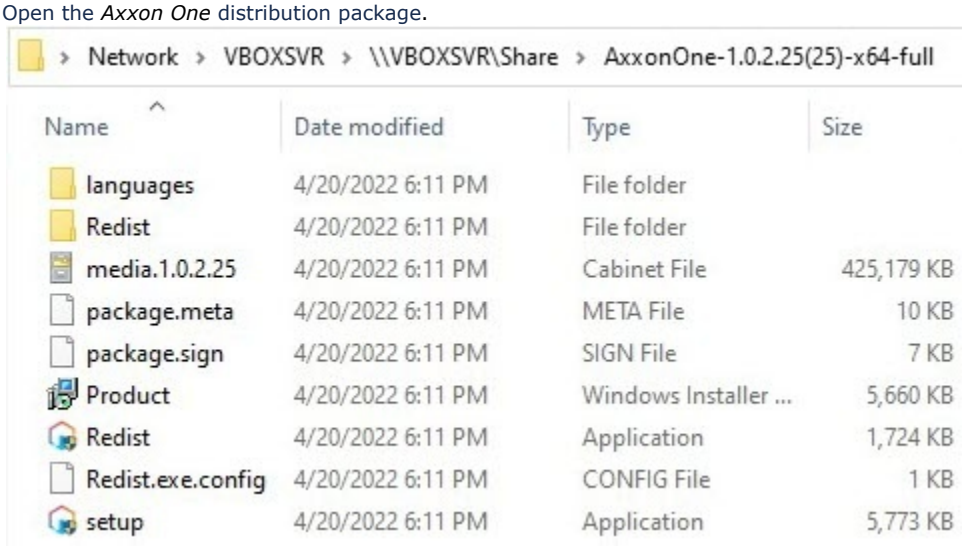

GND
Audio 1
Audio 2
Audio 3
Audio 4
Audio 5
Audio 6
Audio 7
Audio 8
Video 1
Video 2
Video 3
Video 4
Video 5
Video 6
Video 7
Video 8

Installation the Axxon One Software Package

Installation

To install *Axxon One* with any type of installation, do the following:

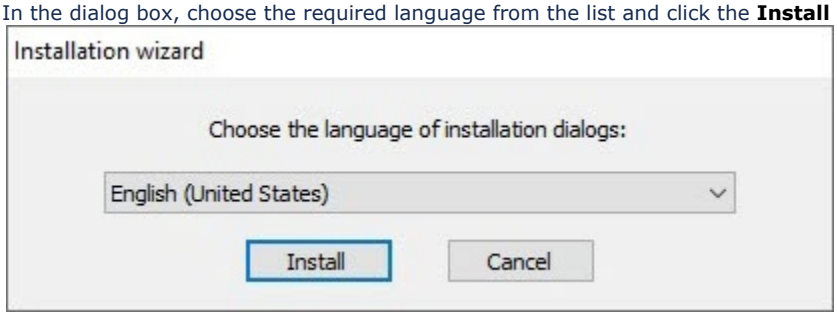
1. Open the *Axxon One* distribution package.



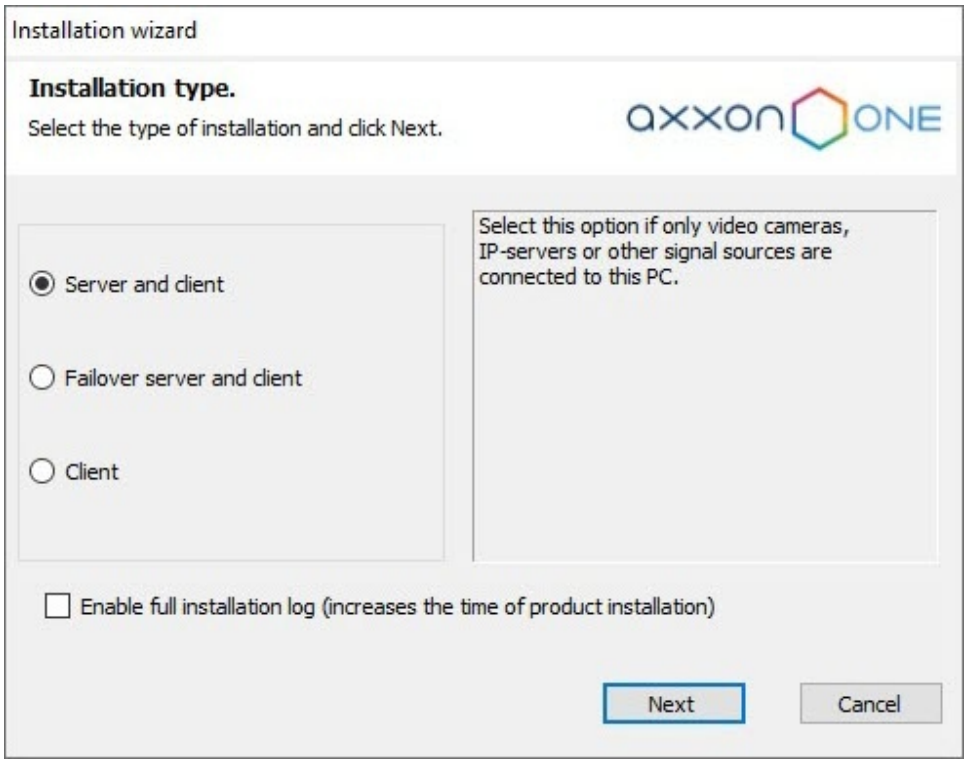
2. Run the **setup.exe** executable file file.

> **Note**
>
> If you cannot run the installation files downloaded from the internet, allow running programs and unsafe files in Windows OS.

3. In the dialog box, choose the required language from the list and click the **Install** button.



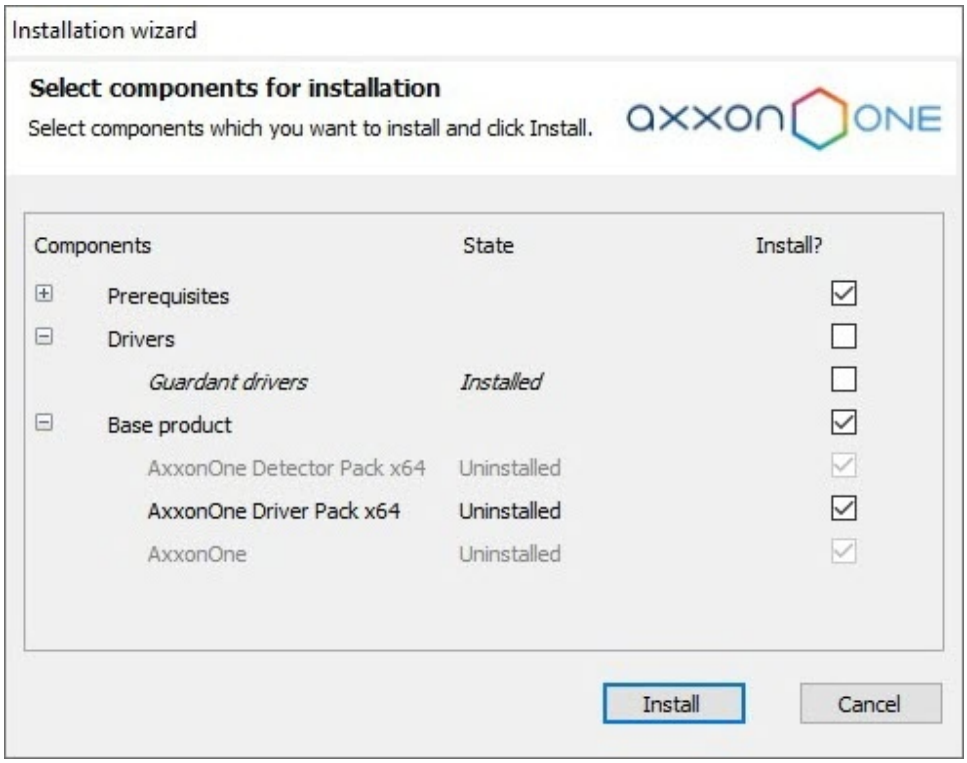
4. Select the *Axxon One* installation type in the dialog box by clicking the appropriate option button:
   a. **Server and client**—installs client and Server services. We recommend selecting this type of installation if you use no more than five Servers in one place that must work within the same domain. *Axxon One* Server:
      i. Interacts with devices (cameras, microphones, inputs, outputs, and so on) that constitute a security system.
      ii. Stores archived data on its own disk space and interacts with archives located in network storage.
      iii. Stores databases of events and databases of object motion metadata.
      iv. Analyzes the incoming video using detection tools.
      v. Keeps configurations of the security system, user settings, custom layouts, macros, and so on.
   b. **Failover server and client**—installs client and Server services enhanced with the FailOver capability. In emergency (power outage, network problems), the FailOver technology restores the Server configuration on another Server (see Configuring FailOver VMS). We recommend selecting this type of installation if you use from 5 to 30 (minimum 3) Servers in one place that must work within the same domain.
   c. **Client**—installs only the client application that allows the user to connect to any Server and perform administration /management/monitoring operations with the protected facility based on the permissions granted by the administrator.



Note

- We offer a separate installation package containing only the *Axxon One* Client. To obtain it, contact our technical support. You can download additional packages from the official website. This installation package is intended only for Client updates. You cannot install it on a computer where *Axxon One* was not previously installed.
- If you use more that 30 Servers in one place or if they are located in different places, and you need to have a single user management on all Servers, you must consult an AxxonSoft manager or technical support service.

5. To record all installation-related events to a log file, select the **Enable full installation log (increases the time of product installation)** checkbox.
6. Click the **Next** button.
   A dialog box with a selection of components for installation opens.



Note

To view the list of components that will be installed, click ⊞.

Attention!

- On Windows 11 OS and Windows Server 2019 OS, errors can occur in the Server operation when Guardant drivers are installed. We don't recommend installing Guardant drivers. Installation of Guardant drivers is disabled by default.
- For the correct installation of Guardant drivers, you must disable the check of the drivers digital signature in the operating system and disable Secure Boot in BIOS.

7. Select checkboxes next to the components that you want to install. We recommend installing all components.

Note

By default, the *Axxon One* distribution package includes only the basic *DetectorPack.* For the information on installing *DetectorPack* add-ons, see Installing DetectorPack add-ons.

8. Click the **Install** button. All selected components will be installed. The installation process can take considerable time. After that, the preparation process for the *Axxon One* installer will be initiated.



Attention!

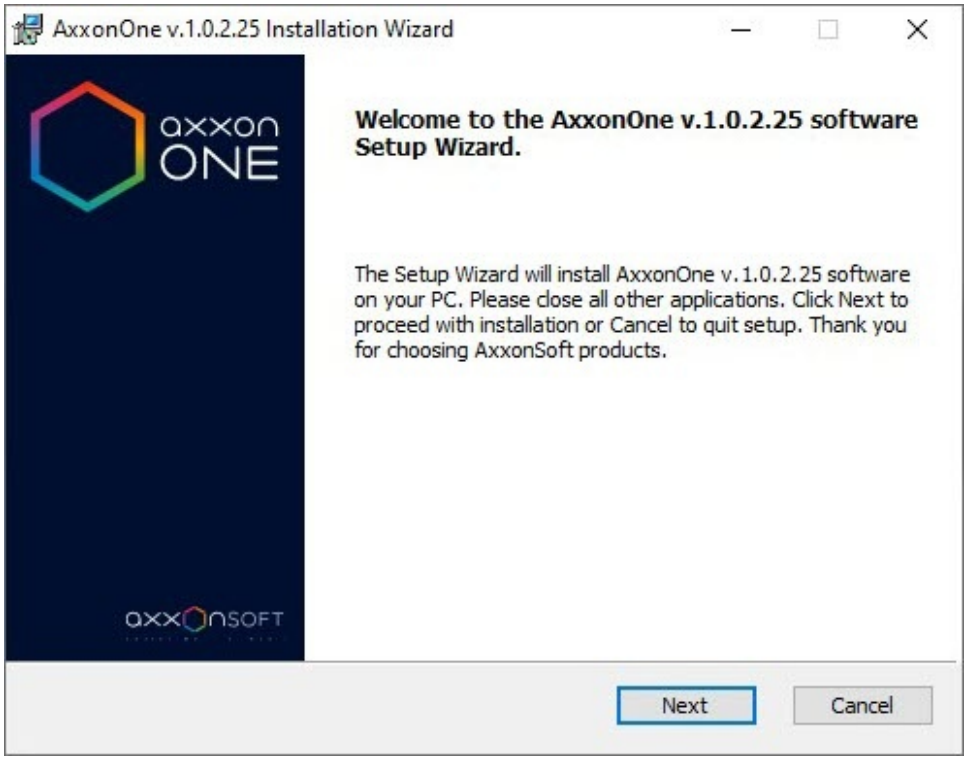
Starting with *Axxon Driver Pack* 3.51, this driver package requires the Windows update KB2999226 to be installed. If this update isn't installed in the system, you will see a warning. To continue installation, download the update from the Microsoft official website. When installing the update, consider the bitness of your system.

Note

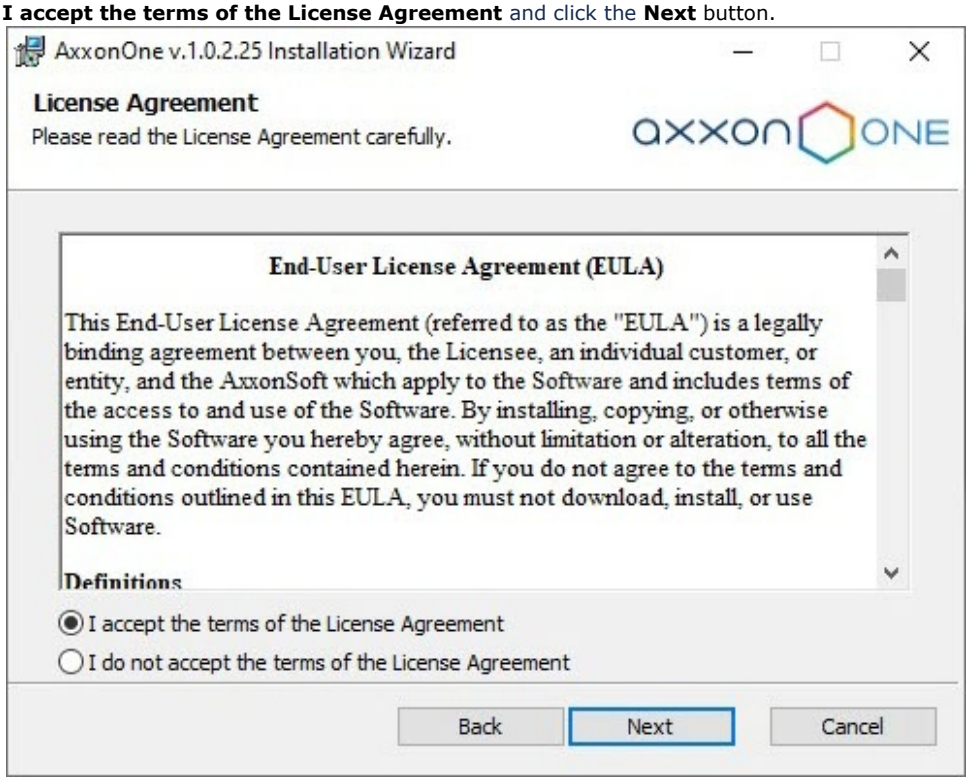
The following software is installed among the prerequisites:

a. PostgreSQL 10.8.0 Server database. If an older version of PostgreSQL is installed, it is updated to version 10.8.0. A new log database is automatically created (name: ngp, user name: ngp, password: ngp). By default, PostgreSQL is installed on the system disk. You can change the path using the command line options of the installation file (see Silent install (Quiet Mode)).
b. *NET Framework 2.0*, *.NET Framework 3.5 SP1* and *.NET Framework 4.0.*
c. Acrobat Reader that is necessary for exporting in PDF format and printing freeze frames (see Frame export).

9. Click the **Next** button on the welcome screen of Installation Wizard.



10. To proceed with installation, carefully read and accept the terms of the license agreement by selecting the radio button next to **I accept the terms of the License Agreement** and click the **Next** button.



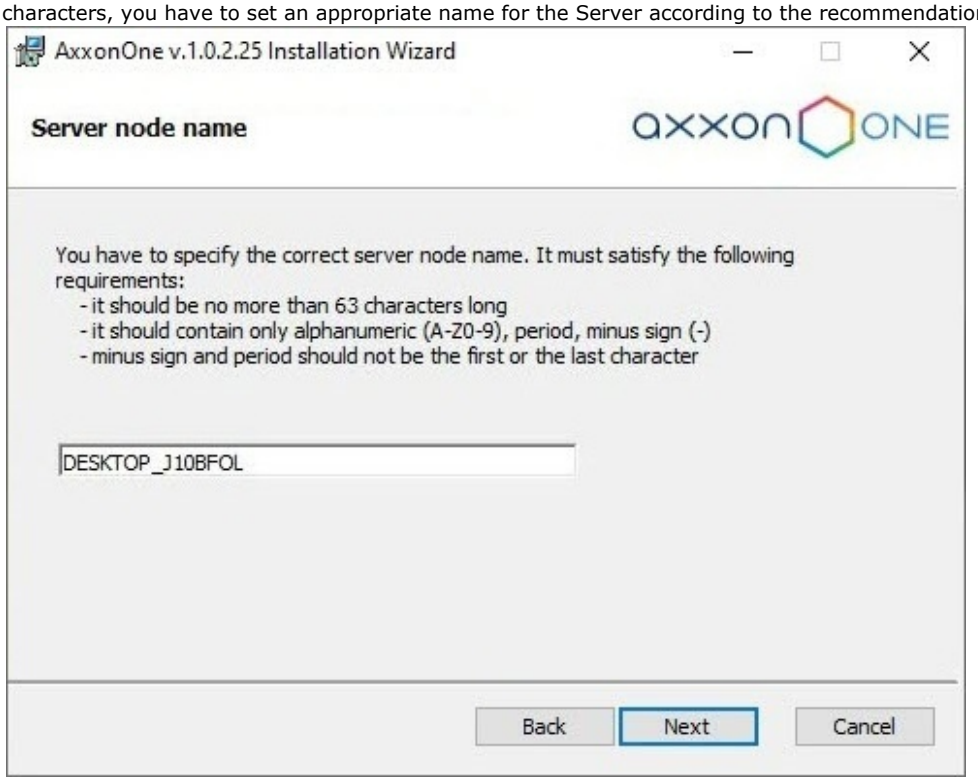
11. Select the folder for storing the log database and the metadata database used in *Axxon One*.

Attention!

- You can specify the path to the folder for storing the database only once during the installation process. If necessary, you can change it, but you will need to reinstall *Axxon One* (without losing the configuration and video archive).
- The path to the folder for storing the log database and the metadata database must contain only Latin letters and numbers.
- By default, the log database and the metadata database will be located in the X:\AxxonOneData\ folder (in the Data and vmda_db subfolders, respectively), where X is the drive letter with the largest amount of free memory. In future, the metadata database can be placed in the network storage (see Configuring storage of the system log and metadata).
- To reduce the load on the system disk, we recommend storing the log database and the metadata database on a separate physical disk. To calculate the required amount of disk space for the log database, the metadata database and *Axxon One*, you can refer to Disk storage subsystem requirements.

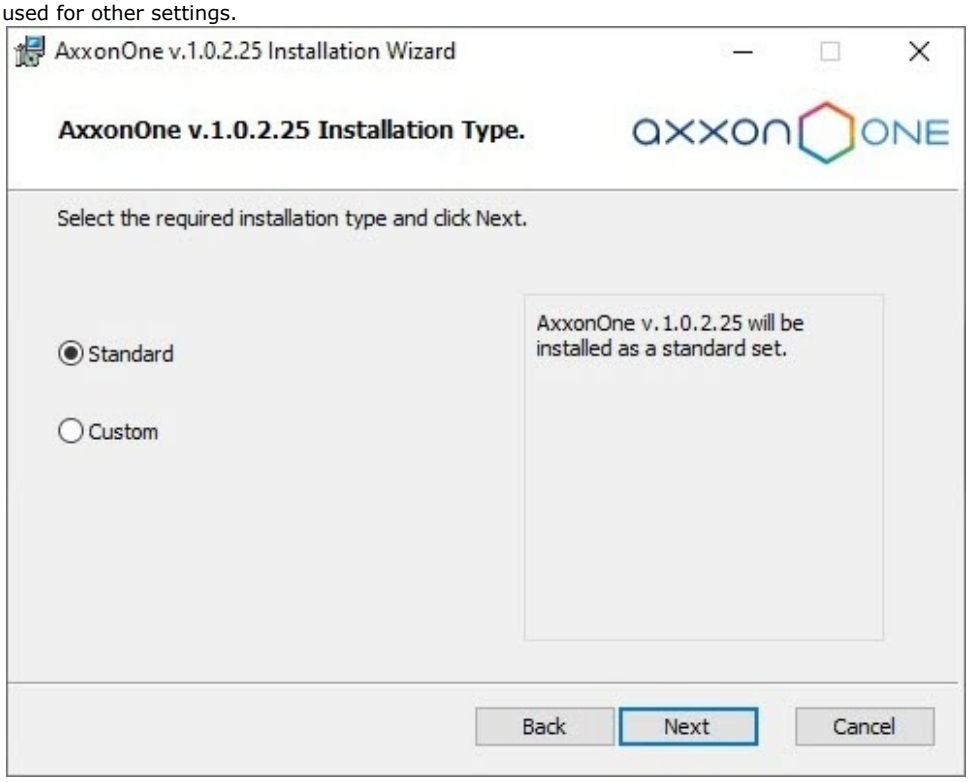


12. By default, shortcuts are added to both quick launch bar and desktop. Clear the corresponding checkboxes if it's not required.
13. By default, upon connecting to the Server, the Client can be automatically updated (see Automatic update of a remote Client). If it's not required, clear the **Create an archive for automatic update** checkbox. In this case, you can save *Axxon One* install ation time, but the Clients will not be automatically updated upon their connection to the Server.
14. Click the **Next** button.
15. By default, the *Axxon One* Server name is identical to the computer name. If the computer name contains forbidden characters, you have to set an appropriate name for the Server according to the recommendations, and click the **Next** button.



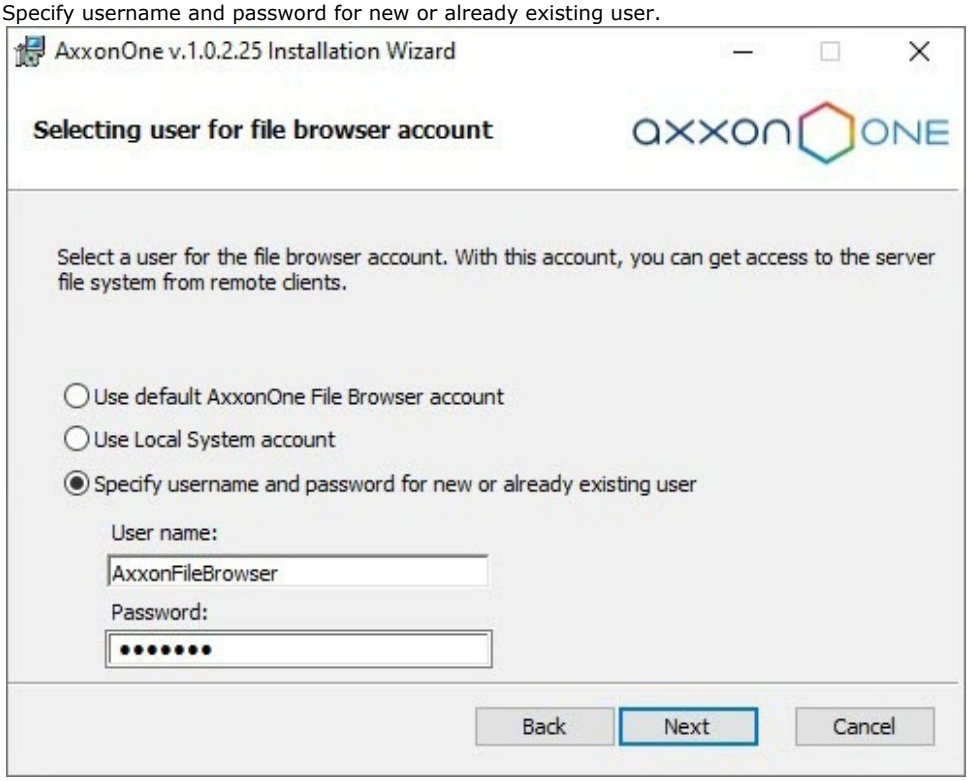
16. In the window that opens, select an installation method and click the **Next** button.
If the **Custom** installation method is selected, you can perform advanced configuration of the installation of *Axxon One*.

If the **Standard** installation method is selected, you are prompted to select an Axxon-domain (Step 25). Default values will be used for other settings.



17. Select a user account in the file browser:

    a. Use default AxxonOne File Browser account.
    b. Use Local System account.
    c. Specify username and password for new or already existing user.

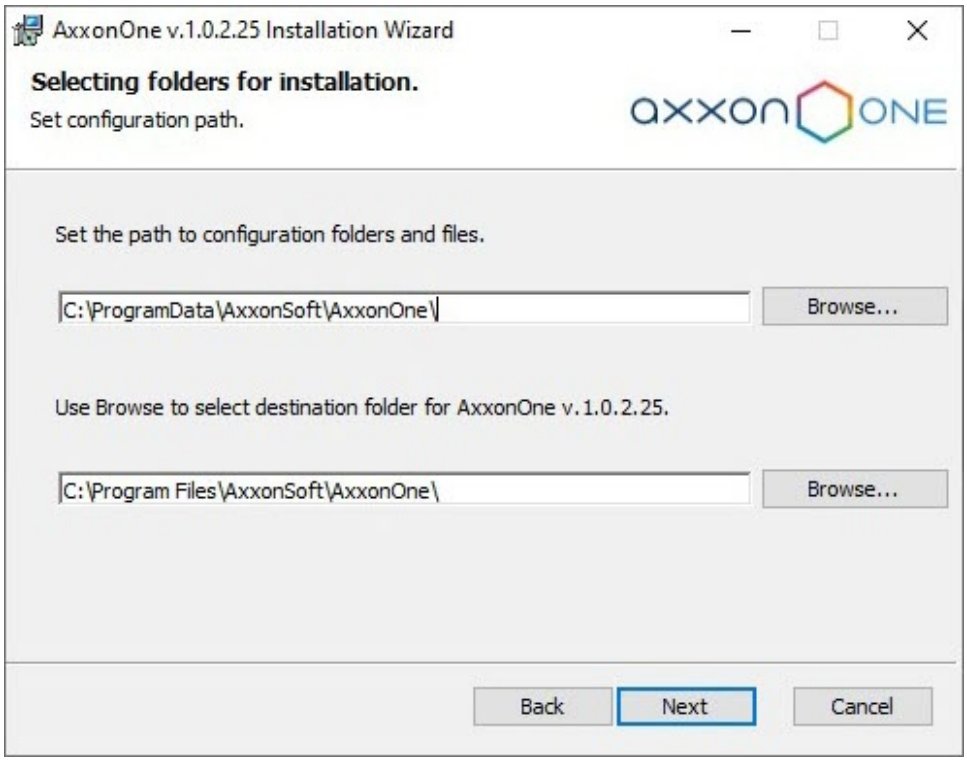


Attention!

- The file browser helps to navigate through the Server's file system (such as when choosing disks for archive volumes). The user account for the Windows file browser will be created with administrator privileges.

- After installation of *Axxon One*, make sure that a file browser account has been created in Windows and belongs to the Administrators group.

18. Specify the path to *Axxon One* folders and configuration files. By default, the files and folders of the configuration are stored in the C:\ProgramData\AxxonSoft\AxxonOne\ folder.

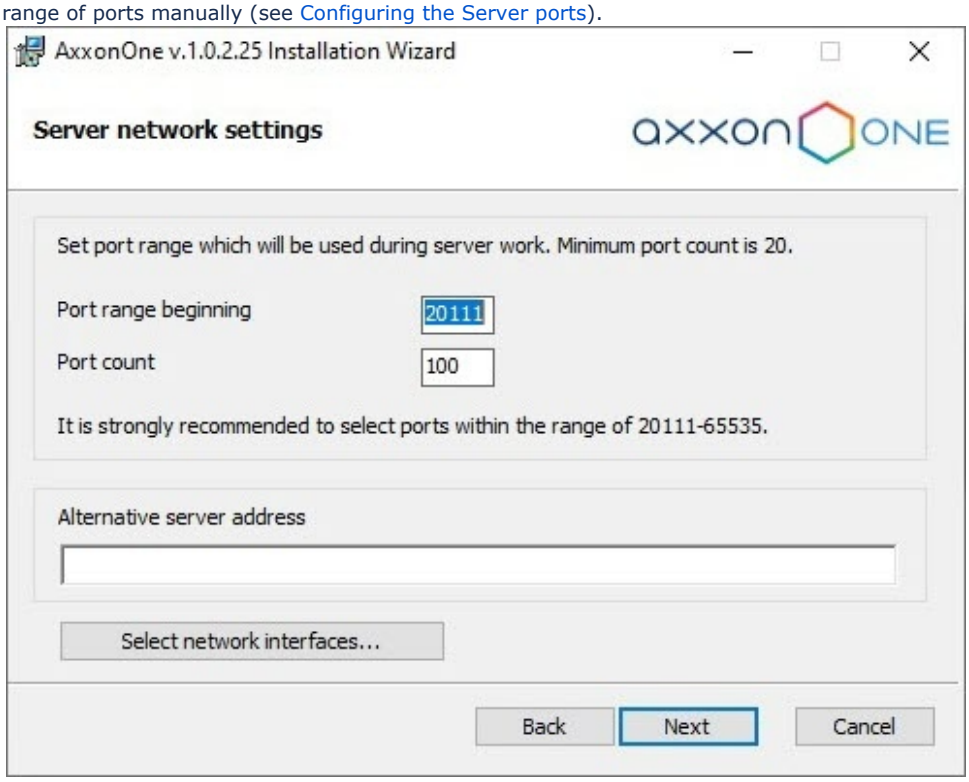


Attention!

The specified paths must contain only Latin characters and numbers.

19. Specify the path to the folder for installing *Axxon One*. By default, *Axxon One* will be located in the C:\Program Files\AxxonSoft\AxxonOne\ folder.
20. Click the **Next** button.
21. Specify the range of ports to be used for the Server. To do so, specify the lower end of the range, as well as the number of ports. This range can be used by the local network administrator to forward the port manually in cases where it is necessary to give the Client access to the Server from another network. The minimum possible number of ports is 20.

For a full list of ports, see Ports used by the Axxon One Software Package. After you install *Axxon One*, you can change the range of ports manually (see Configuring the Server ports).



Note

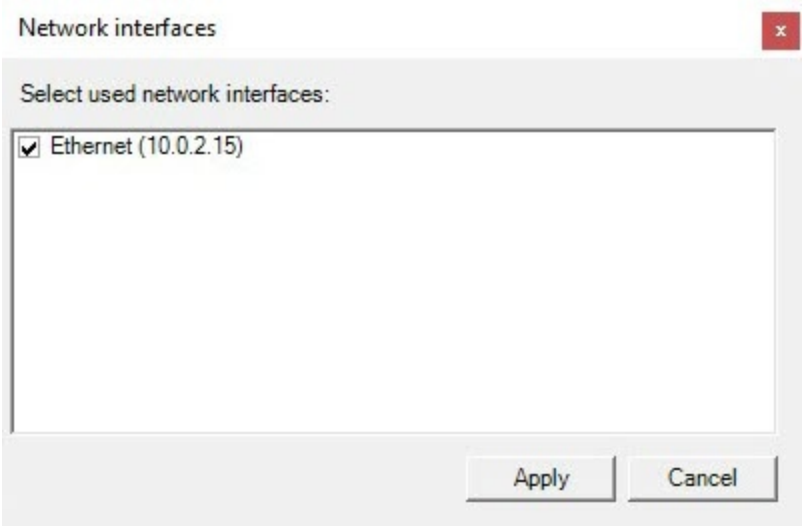
Connected devices will only work on ports from the specified range. If not enough ports are allocated, then some of the devices may not work or can be unstable.

The number of ports that you select affects the scalability of the system. Keep the following in mind when specifying the number of ports:

- After the Server is installed, it occupies **10 ports**, including one for sending emails (via the SMTP service, see The Email notifier object).
  Attention! The **Failover server and client** installation type (see Configuring Failover VMS) uses 9 base ports and preset port ranges for each node (see Ports used by the FailOver system);
- In a 64-bit configuration, **4 ports** are required for any number of IP devices. In a 32-bit configuration, **4 ports** are required for each **32 cameras**;
- Each archive requires **1 port**;
- **1 port** is required for viewing archive in the Web-Client;
- **2 ports** are required for each decoded video stream on the currently opened layout in the Web-Client;
- **2 ports** are required for mobile Client;
- **2 ports** are required for any number of speakers in the system (see The Speaker object);
- **1 port** is required for recording metadata into the database;
- **2 ports** are required for operation of service detection tools;
- **2 ports** are required for operation of scene analytics detection tools;
- **2 ports** are required for operation of scene analytics detection tools based on neurotracker;
- **2 ports** are required for operation of neurocounter.

22. If necessary, specify an alternative Server address—the external address of the switch if the Server is behind the NAT. Interface specification format: "IP address1 or DNS name1, IP address2 or DNS name2".
23. To restrict visibility of the Servers on particular networks in the list of Servers during *Axxon One* configuration, do the following:

    a. Click the **Select network interfaces** button. The **Network interfaces** window opens.



b. By default, use of all available network interfaces on the Server is allowed, meaning that Servers on the relevant networks are visible in the list. If you don't want for the Servers on the networks of certain network interfaces to be visible in the list, clear the relevant checkboxes.

> **Note**
>
> Depending on the network topology, it will still be possible be reach the Servers manually (if broadcasting is allowed between the network segments).

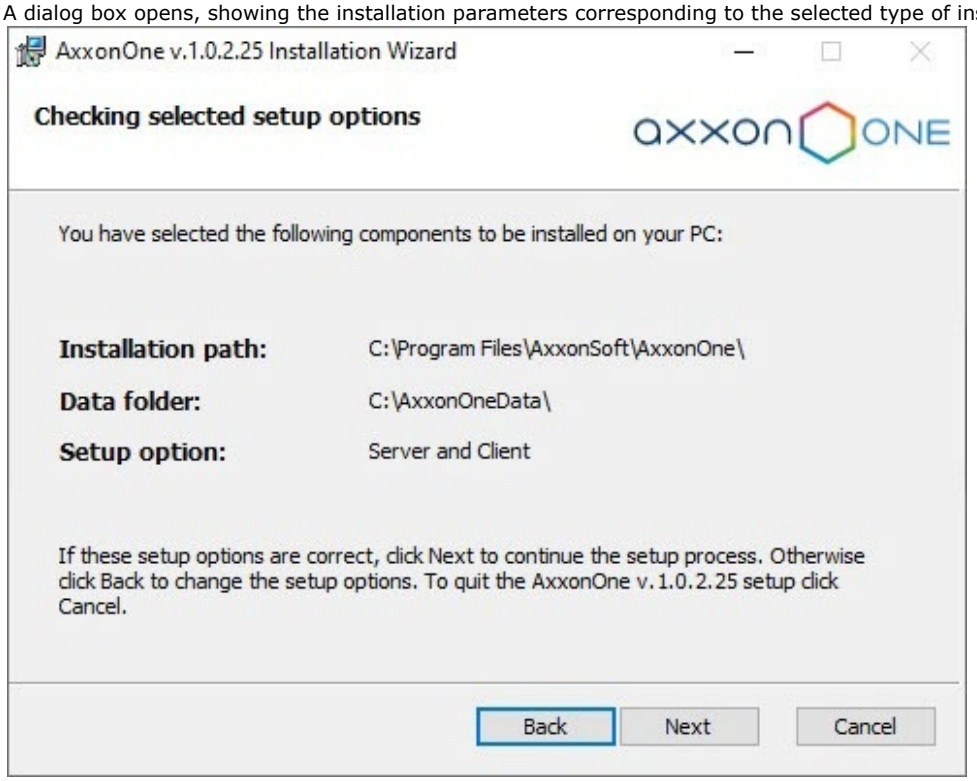
c. Click the **Apply** button.

24. Click the **Next** button.
25. Create a new Axxon-domain with the name **Default** (for the definition of an Axxon-domain see Appendix 1. Glossary). If you want to add the computer to an Axxon-domain at a later time, select **Server will be manually added to already existing domain later**. Click the **Next** button.

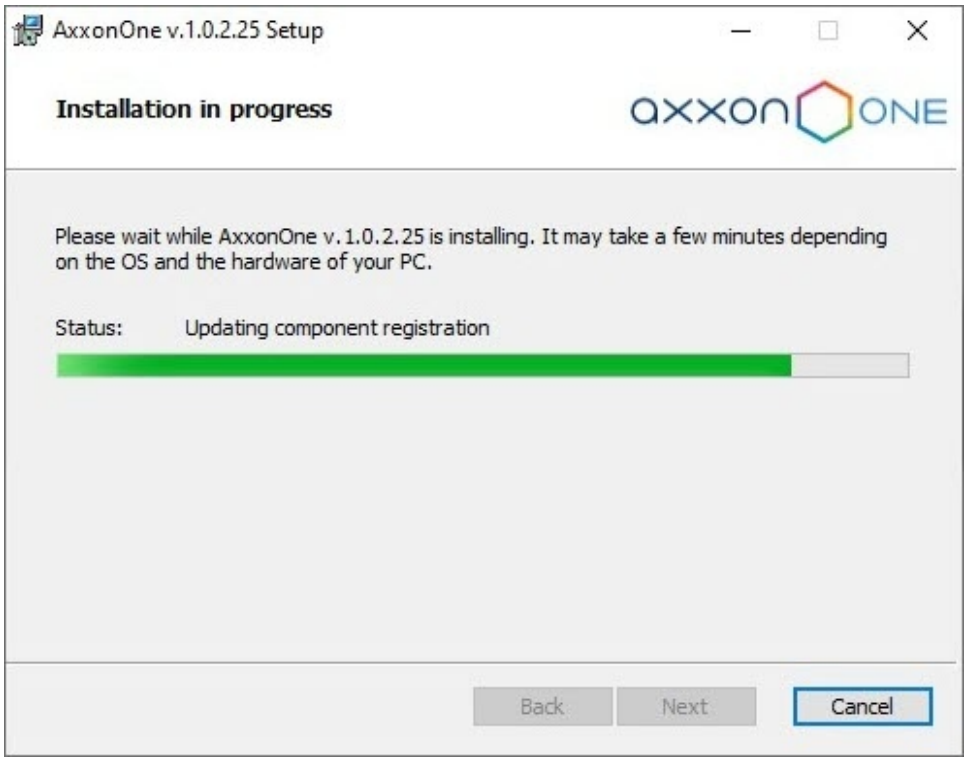
> **Note**
>
> - When reinstalling *Axxon One*, you have the option of using the previous domain (select **Use existing configuration**).
> - Using the same Axxon-domain name doesn't guarantee that the Servers will be in the same Axxon-domain. To place all Servers into one Axxon-domain, you must use *Axxon One* interface to add each Server to the necessary Axxon-domain. Axxon-domain configuration is described in detail in Configuring Axxon-domains.



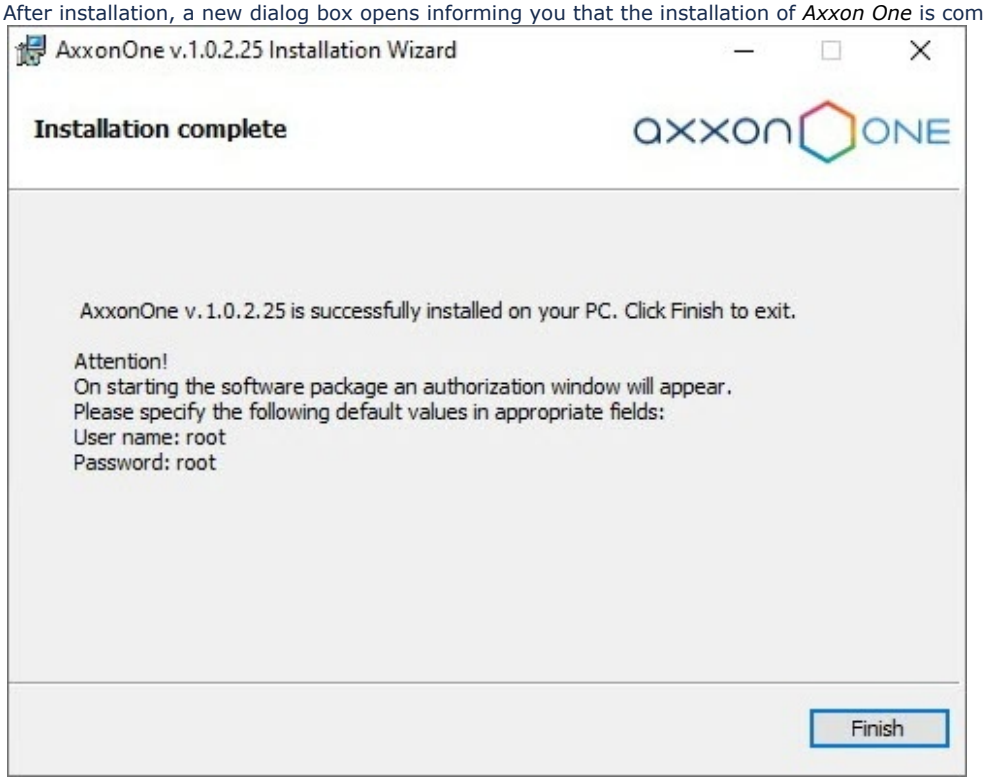
A dialog box opens, showing the installation parameters corresponding to the selected type of installation.



26. Verify your installation settings and click the **Next** button to begin installation of *Axxon One*. Installation of *Axxon One* is then performed.



After installation, a new dialog box opens informing you that the installation of *Axxon One* is completed.



27. Click the **Finish** button to confirm completion of the installation.

Installation of *Axxon One* is now complete.

Installing Axxon One in Linux OS

Transferring the Axxon One configuration from Windows OS to Linux OS

Repairing Installation

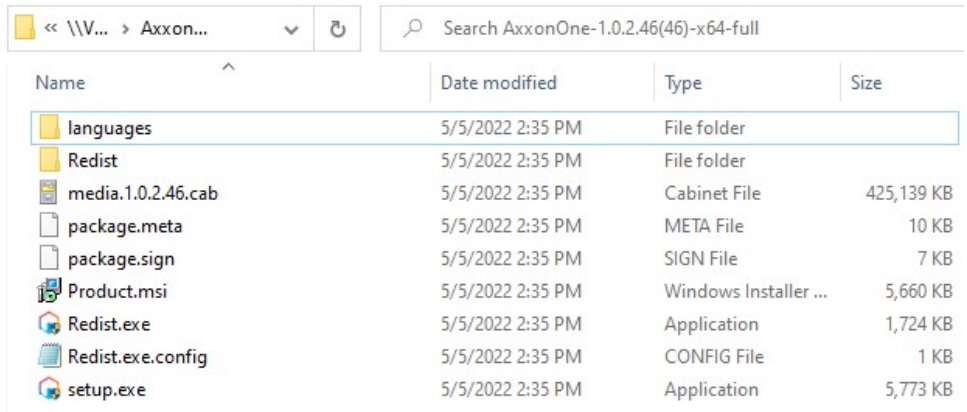
A repair installation is used to re-install all components of the *Axxon One* software package.

To start a repair installation, launch the *Axxon One* software without removing the current installed version of the program.

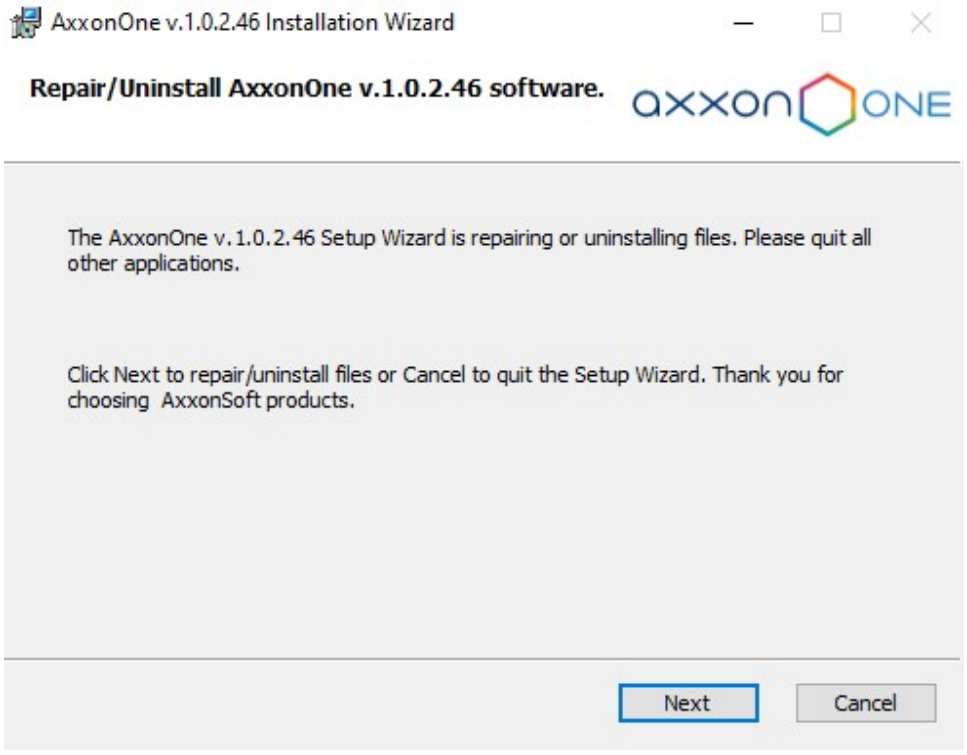
> **Note**
>
> To ensure that *Axxon One* is re-installed correctly, all related applications should be closed before starting the repair installation.

To run a repair installation of the *Axxon One* software, you must perform the following steps:

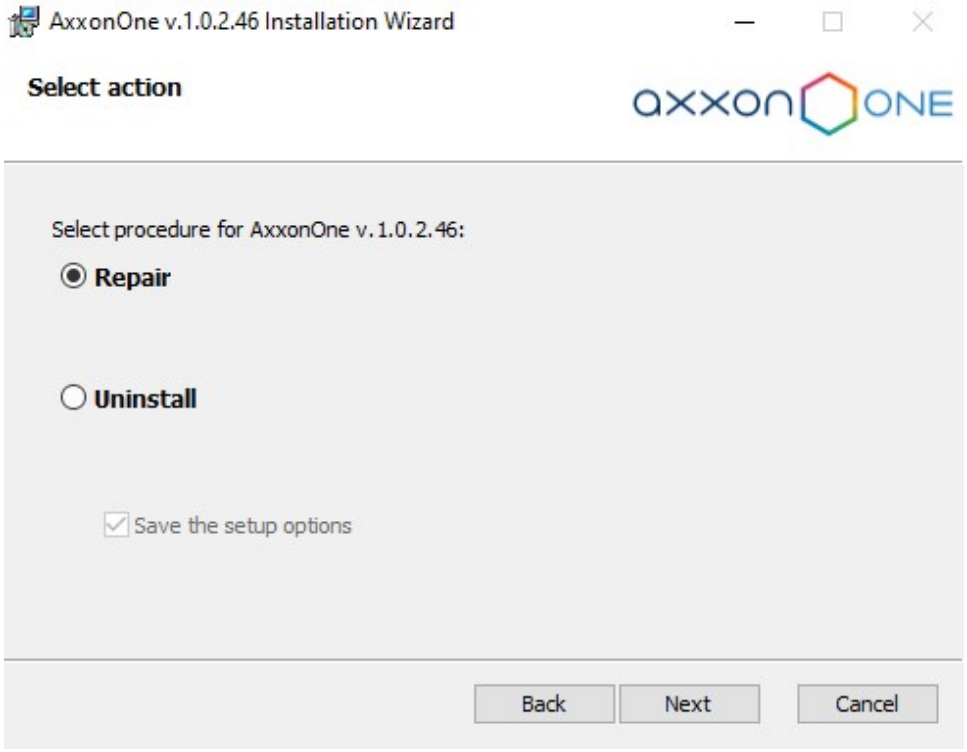
1. Open the *Axxon One* distribution package.



2. Run the setup file.
3. Click **Next** on the setup wizard's welcome screen.

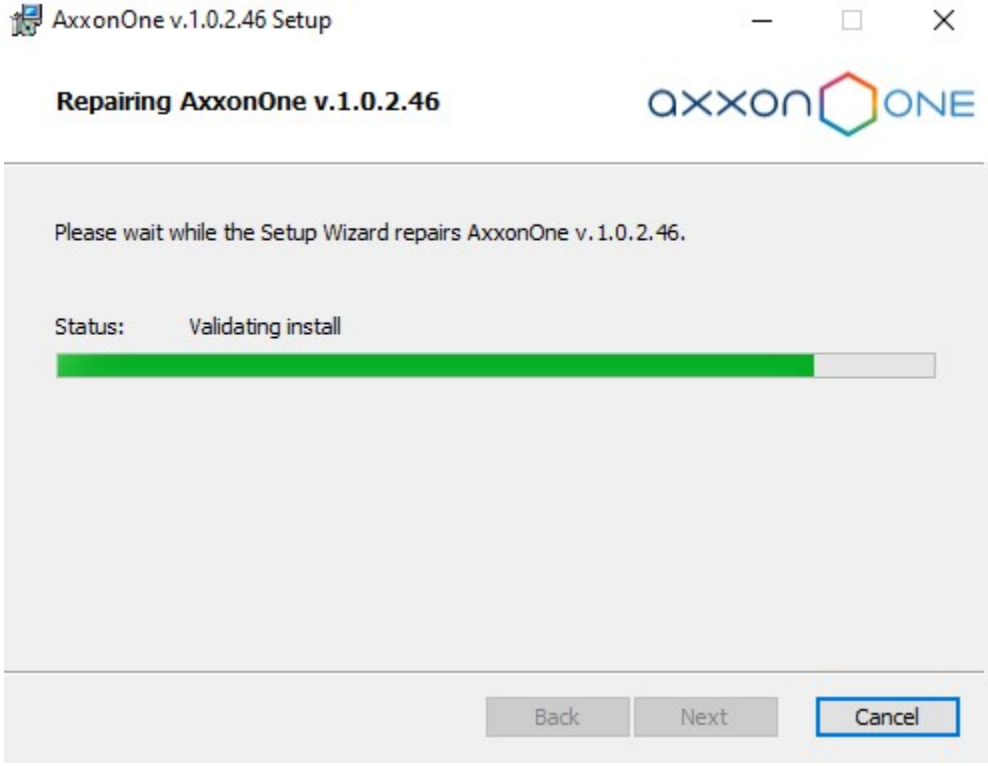


4. A dialog box will appear, allowing you to choose an operation.



5. Select the **Repair** option and click **Next**.

A dialog box will appear, showing the *Axxon One* repair process.



A dialog box will appear, indicating the completion of the repair process. Click **Finish**. Repair of *Axxon One* is now complete.

Removal

The *Axxon One* installation program can also remove the software. Use this option when you need to remove all components of *Axxon One* from your computer.

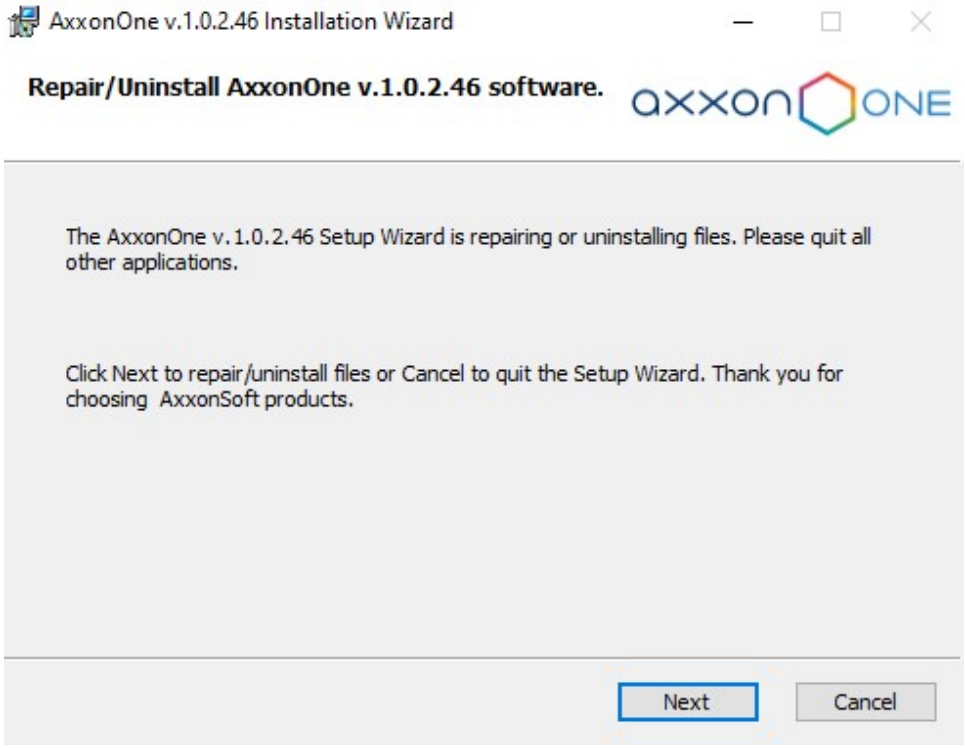
> **Note**
>
> All related applications should be closed before beginning removal of the *Axxon One* software.

You can run the *Axxon One* uninstaller via one of the following methods:

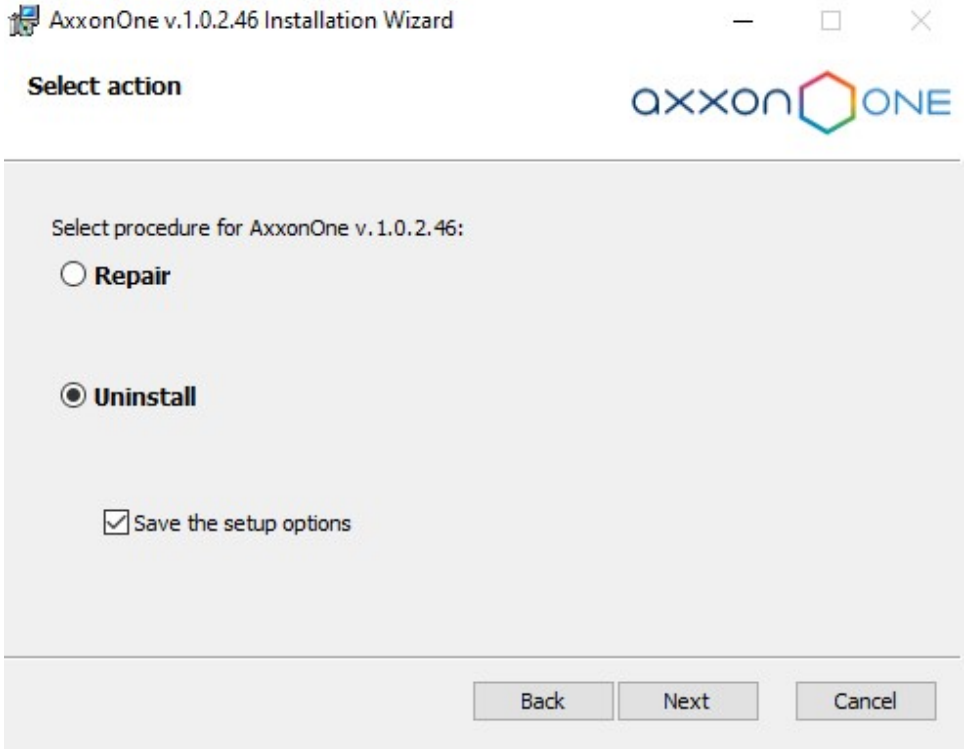
1. From the **Start** menu.
2. Using **Add or Remove Programs** in the Windows control panel.
3. By starting the executable file named setup.exe, which is included with the installed version of the product.

When you do this, the setup wizard's welcome screen appears. To remove *Axxon One*, you must observe the following procedure:

1. Click **Next** on the setup wizard's welcome screen.

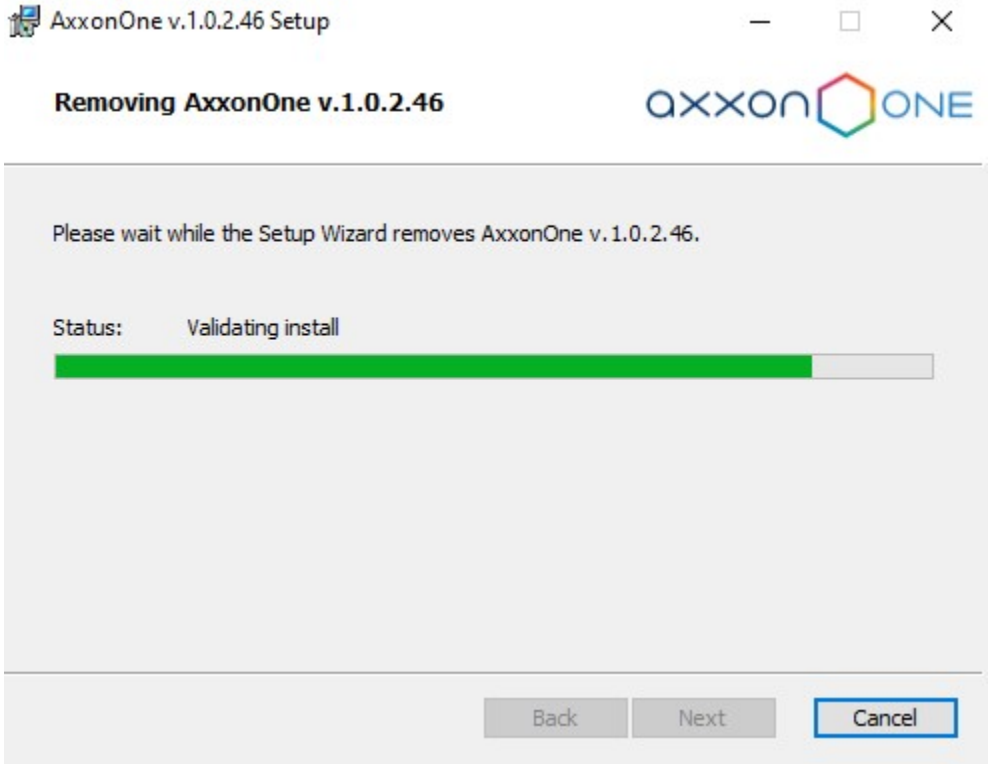


A dialog box will appear, allowing you to choose an operation.



2. Select **Uninstall**.
3. To save your *Axxon One* settings in a database, select the **Save the setup options** check box. This option may be useful when updating the product.
4. Click **Next**.

A dialog box will appear showing the *Axxon One* removal process.



A dialog box will appear, indicating the completion of the removal process. Click **Finish**. Removal of *Axxon One* is now complete.

Note

To completely remove *Axxon One*, use the Windows Control Panel to remove the following software:

1. Postgres NGP.
2. DetectorPack.
3. Axxon Drivers Pack.
4. Guardant Drivers.

Silent install (Quiet Mode)

You can run *Axxon One* installation in quiet mode (unattended setup with no user intervention).

> **Note**
>
> During installation you may have to reboot the system. After rebooting the installation will continue automatically.

When Redist.exe process ends and not listed in Windows Task Manager, the installation is complete.

This mode of installation can be configured by adding command-line options to setup.exe. See the command-line options in the table.

Command-line option	Description
/? or /help	Open the Help window
/x or /uninstall	Remove *Axxon One* and save the configuration
/x/removeall	Remove *Axxon One* and delete the configuration
/r or /repair	Repair *Axxon One*
/qn or /quiet	Silent install
/norestart	Disable automatic reboot of the system during installation
/debug	Log installation
/noOSCheck	Skip OS compatibility check
/postgresinstalldir="D:\Postgres"	PostgreSQL installation folder
/LANG=”en”	Select installation language: For example, en — English
/INSTALLTYPE="ServerClient"	Installation options: • ServerClient — **Server and Client** (default), • raftServer — **Failover Server and Client**, • **Client**.
/ADD="[]"	Hers is the list of components to install or remove (if you remove/uninstall software). See the possible values in the table below.
/REMOVE="[]"	Hers is the list of components NOT to install or remove (if you remove/uninstall software). See the possible values in the table below.
/dpcmd=" INSTALL_BOSCH_VIDEOSDK=\"no\""	**Bosch VideoSDK** driver Installation (see notes). • no — do not install, • yes — install.
/CMD="[commands]"	Basic installation options and values. Commands are [option] = \ "[value] \" or [option] = [value]" . See available installation options in the table below.

> **Attention!**
>
> Occasionally, when installing the **Bosch VideoSDK** driver, the CLI window opens. To continue with installation, close this window.

/ADD and /REMOVE values:

x64
Acrobat

BaseProduct
IPDriverPack_x86
Guardant_amd64
Postgres
dotnetfx35_x86
Redist2005_x86
Redist2010_x86
DetectorPack

Installation options:

Installation options	Description
QUICKLAUNCH_SHORTCUT='1'	Create shortcut: • 1 — Yes (default), • 0 — No.
DESKTOP_SHORTCUT='1'	Copy shortcut to desktop: • 1 — Yes (default), • 0 — No.
INSTALLDIR='[%ProgramFiles%\AxxonSoft\AxxonOne]'	*Axxon One* installation folder
NGP_IFACE_WHITELIST="0.0.0.0/0"	Network interfaces The default value is "0.0.0.0/0" (all available network interfaces) Format of network interfaces: "IP-address1 / number of unit bits in the mask, IP-address2 /number of unit bits in the mask"
NGP_ALT_ADDR="0.0.0.0"	Setting the outside local address for a Server behind the NAT). Format of network interfaces: "IP Address1 or DNS-name1, IP address2 or DNS Name2"
PORT_RANGE_START="20111"	The initial value of the port range for Server. 20111 — default.
PORT_RANGE_COUNT="100"	Number of ports in use. The minimum number is 20. 100 — default.
Options for **Server and Client** installation	
PATH_TO_DATA = 'X:\AxxonOneData', where X is the letter of the disk with the most free memory	Directory for storing the log database and metadata database. Default is X:\AxxonOneData. The PATH_TO_DATA parameter should be after the INSTALLDIR parameter.
FBUSER_TYPE='DEFAULT'	User account for file explorer: • DEFAULT — create a new account; the default name selected will be AxxonFileBrowser, • SYSTEM — select an account from the Local System, • SPECIFY — create a new account; choose the user name and password.
FBUSER_NAME='[AxxonFileBrowser]'	Setting a user name and password for an account in file explorer. When you choose SPECIFY of the FBUSER_TYPE parameter
FBUSER_PSW='[Axxon2.0.0]'	
CONFIG_PATH='[CommonAppDataDirectory]'	Path to configurations files and folders

DOMAIN_NAME_TYPE = '[NewDomain]'	Select Axxon-domain: • NewDomain — create new Axxon-domain (default), • WithoutDomain — do NOT add Server to Axxon-domain, • TheSameDomain — use existing Axxon-domain.
WHATDBUSE = '[EXIST]'	• EXIST — use existing log DB (default) • NEWDB — create new DB
WHATVMDADBUSE = '[EXIST]'	• EXIST — use existing object tracking DB (default) • NEWDB — create new DB

The command for silent installation of *Axxon One* may look like:

setup.exe /quiet /norestart /debug /INSTALLTYPE="ServerClient" /REMOVE="Guardant_amd64" /CMD="
CREATE_QUICKLAUNCH_SHORTCUT=\"0\" PORT_RANGE_COUNT=\"50\" DOMAIN_NAME_TYPE=\"WithoutDomain\""

This will launch installation with the following options:

1. Quiet mode (/quiet);
2. no reboot (/norestart);
3. log installation to file (/ debug);
4. **Server and Client** (/ INSTALLTYPE = "ServerClient");
5. No *Guardant* drivers (/ REMOVE = "Guardant_amd64");
6. And with the following properties (/ CMD =):
    a. no shortcut (="CREATE_QUICKLAUNCH_SHORTCUT=\"0\");
    b. 50 ports for Server (PORT_RANGE_COUNT="50");
    c. Server NOT added to Axxon-domain (DOMAIN_NAME_TYPE = '[WithoutDomain]').

Updating Drivers Pack

To install the latest version of Drivers Pack, do as follows:

1. Run the IPDriverPack.msi file.
2. After the installation is complete, restart the Server (see Shutting down a Server, Starting a Server).

Update

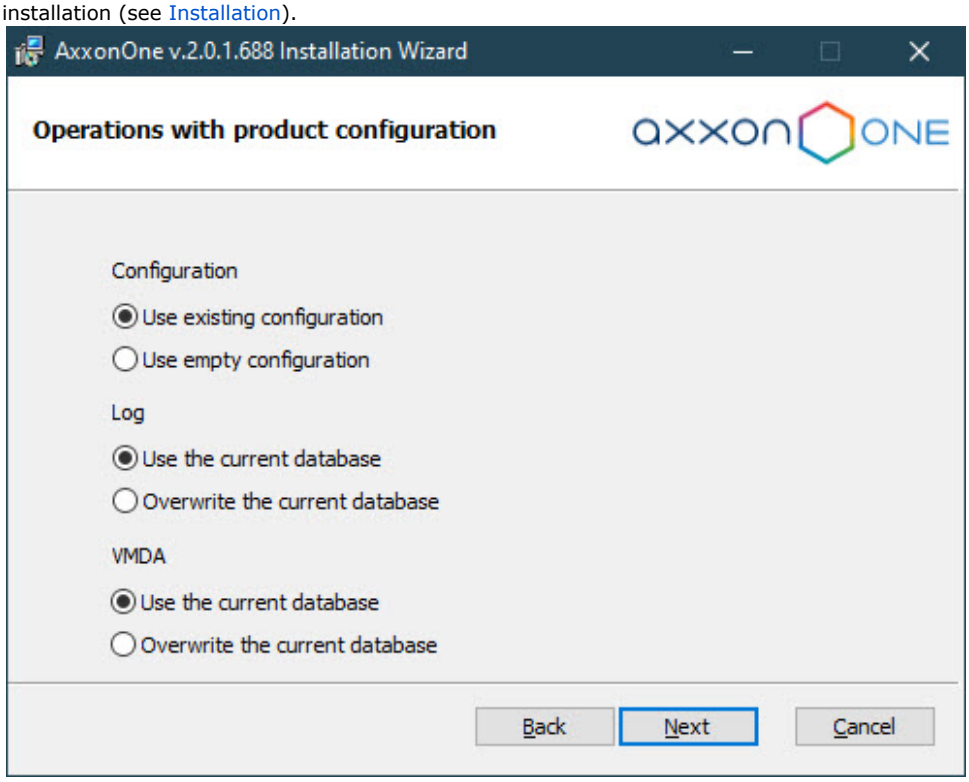
Before you start updating, do the following:

- back up your configuration (see Backup and Restore Utility);
- stop the Server (see Shutting down a Server). If you run multiple Servers in the Axxon-domain, make sure to stop them all.

> **Note**
>
> When you work with the Failover system, we recommend updating the Servers through a supervisor interface (see Updating Servers within a cluster).

To update, do the following:

1. Run the new build installer. You do not need to remove the previous build.
2. Install the build using the previous settings, existing configuration and database. The procedure is the same as for a new installation (see Installation).



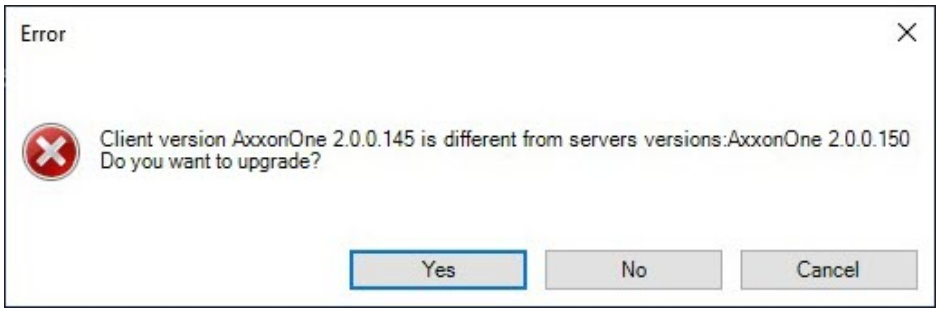
> **Attention!**
>
> - In *Axxon One 2.0* and newer, there are no restrictions on database location. To reduce the load on the system disk, we recommend storing the metadata database and the log database on a separate hard disk.
> - When you update *Axxon One,* only the basic *DetectorPack* is updated. If you installed the *DetectorPack* add-ons, you must update them to the version of the basic *DetectorPack* (see Installing DetectorPack add-ons).

Automatic update of a remote Client

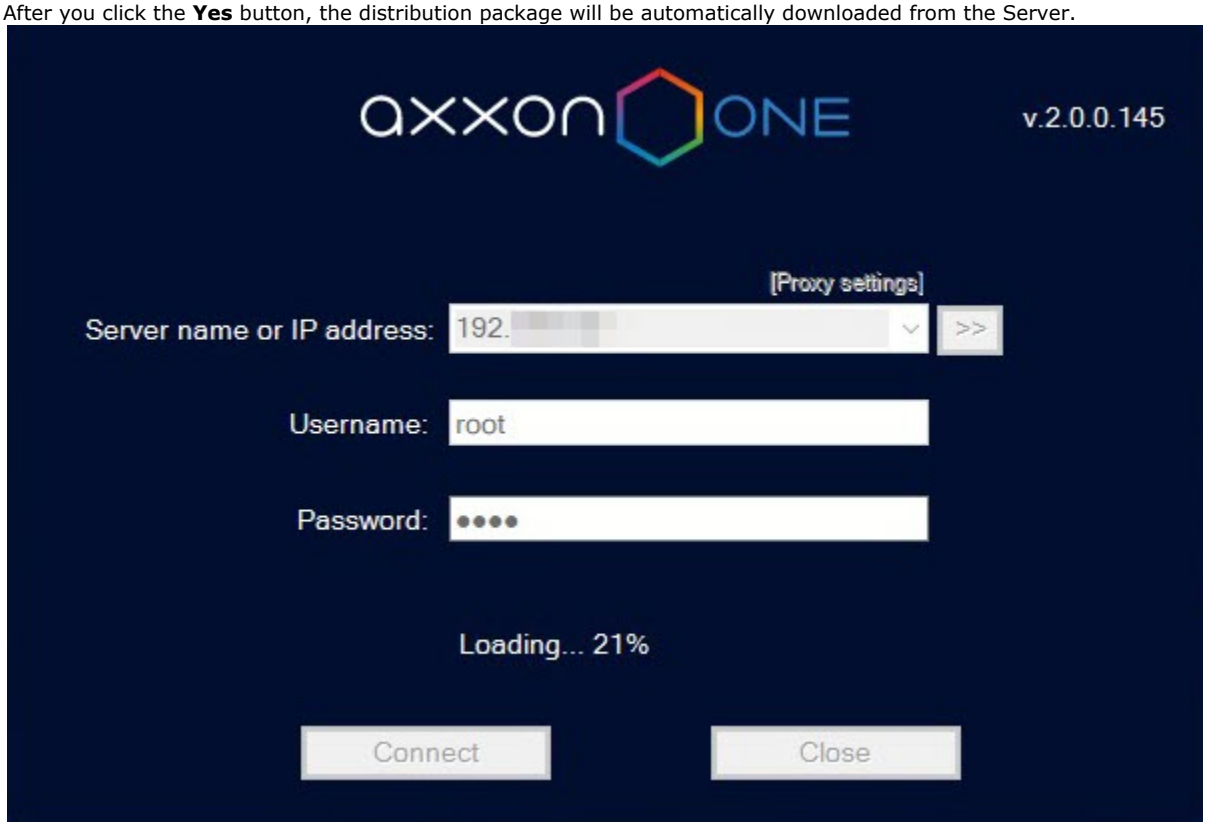
If a Server software version is higher than the Client version, you will be prompted to update your Client software automatically.

Attention!

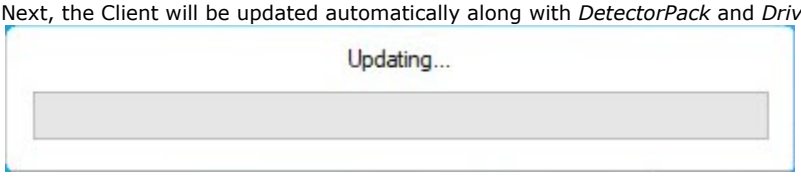
- You must launch the Client as administrator to update it automatically.
- If the Client computer has a Server installed, no update will be possible.



After you click the **Yes** button, the distribution package will be automatically downloaded from the Server.



Next, the Client will be updated automatically along with *DetectorPack* and *DriverPack* driver modules (if required).



Note

You may need to restart your computer during updating.

When the update is complete, the Client will start automatically.

Licensing of the software product

Axxon One license types

Creating an activation request

Activating the Axxon One Free license

There are 6 types of *Axxon One* license: **Axxon One Demo**, **Axxon One Free**, **Axxon One Start, Axxon One Professional**, **Axxon One Enterprise** and **Axxon One Unified**. Upon installation, the software will be launched in *Axxon One* Demo mode. You should activate *Axxon One* VMS to utilize the full feature set of the security software package. You can activate the software by distributing an activation key on the system. Data on all the types of *Axxon One* licenses is presented in the table below.

Functionality	Type of license	Axxon One Demo (8:00-18:00)[1]	Axxon One Free	Axxon One Start[8]	Axxon One Professional	Axxon One Enterprise	Axxon One Unified
Maximum number of Servers in a distributed system		Unlimited	1	1	30	30	Unlimited
Maximum number of cameras in a distributed system		Unlimited	4	64	Unlimited	Unlimited	Unlimited
Free Software Updates		No	No	Yes	Yes	Yes	Yes
Support for SD cards (edge storage, playback only)		Yes	No	Yes	Yes	Yes	Yes
Macros (event response wizard)		Yes	No	Yes	Yes	Yes	Yes
AxxonData Reports		Yes	No	Yes	Yes	Yes	Yes
Scene analytics detection tools		Yes	No[2]	No[2]	Yes	Yes	Yes
Line crossing		No	No	No	Yes	Yes	Yes
Abandoned objects		No	No	No	Yes	Yes	Yes
Time Compressor		No	No	No	Yes[8]	Yes[8]	Yes[8]
Cross-System Client		No	No	No	Yes	Yes	Yes
Advanced archive search: • MomentQuest smart forensic search • Face search[6] • Search by LPs		Yes	No[3]	No[3]	Optional	Yes	Yes
Tag&Track multicamera object tracking		Yes	No	No	Optional	Yes	Yes
Retail Analytics: • Visitors Counter • Queue detection • Heat map • Barcode Detection		Yes	No	No	Optional	Yes	Yes
Face Mask Detection		No	No	No	Optional	Yes	Yes
Neurotracker		Yes	No	No	Optional	Yes	Yes
Stopped object detector		Yes	Optional	Optional	Optional	Optional	Optional
Fire Detection		Yes	No	No	Optional	Yes	Yes
Smoke Detection		Yes	No	No	Optional	Yes	Yes
QR/Barcode reader		Yes	No	No	Optional	Yes	Yes
Neurocounter		Yes	No	No	Optional	Optional	Optional
Abandoned Objects Detection VI		No	No	No	Optional	Optional	Optional
Abandoned Objects Detection (Street) VI		No	No	No	Optional	Optional	Optional

Pose detection[6] includes: • Man down • Raised arms • Crouched man • Social distancing	Yes	No	No	Optional	Optional	Optional
Equipment detection (PPE) and PPE detection VL include: • Helmets • Hi-viz vests • Protective Clothing	Yes	No	No	Optional	Optional	Optional
Integration With Access Control System	Yes	No	No	Up to 50 readers	Up to 100 readers	Optional
Integration With Fire and Security Alarms System	Yes	No	No	Optional	Optional	Optional
Integration Perimeter Intrusion Detection System	Yes	No	No	Optional	Optional	Optional
Events from external systems (POS terminals, ACFA)	Yes	No	Optional	Optional	Optional	Optional
Custom AI Analytics	No	No	No	Optional	Optional	Optional
Water Level Detection	Yes	No	No	Optional	Optional	Optional
Multicamera Tracking. Tracking follows objects across multiple camera FOVs based on appearance similarity[7]	Yes	No	No	Optional	Optional	Yes
Similarity Search[7]	Yes	No	No	No	Optional	Yes[8]
AxxonNet cloud service	Yes	No	Yes	Yes	Yes	Yes
Datacenter Domain Unification/Private Cloud	Yes	No	No	No	No	Yes
Face recognition based on the created lists	No	No	No	Optional	Optional	Optional
FaceCube external face recognition module	No	No	No	Optional	Optional	Optional
Vehicle license plate recognition based on the created lists[4]	No	No	No	Optional	Optional	Optional
Vehicle Recognition[4]	No	No	Yes	Yes	Yes	Yes
Person-Based Privacy Masking	Yes	Yes	Yes	Yes	Yes	Yes
Privacy masking	Yes	Yes	Yes	Yes	Yes	Yes
Crowd Estimation VA	No	No	No	Optional	Optional	Optional
Searching for LPR/ANPR numbers and faces on video from multiple cameras	Yes	No	No	Optional	Yes	Yes
Data replication	No	No	No	No	Yes	Yes
FailOver	No	No	No	No	Yes	Yes
Video walls management	Yes	No	No	No	Yes	Yes
LDAP authentication supported	Yes	No	No	No	Yes	Yes
Hardware Control panels Security keyboards Joysticks I/O modules	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Server ONVIF Profiles G, S, T H.265 support Edge analytics (metadata from IP devices) Configuration backup and restore Mass configuration of cameras Multicasting Hotkeys	Yes	Yes	Yes	Yes	Yes	Yes

Recorded Video / Investigation Local and network archives Events search Time slice search (search by time intervals) Simultaneous search in an archive of several video cameras Video bookmarking (searchable text comments)	Yes	Yes	Yes	Yes	Yes	Yes
Live Monitoring Service audio and video analytics Embedded detection tools (except for Axis on-board tracker[5]) Interactive 3D map GreenStream adaptive bandwidth management Tag& Track Lite OnScreen PTZ mode Support for fisheye cameras and ImmerVision lenses Export of frames and video recordings to multiple formats Information boards	Yes	Yes	Yes	Yes	Yes	Yes
Remote clients Web-Client interface iOS app (including Apple TV) Android app	Yes	Yes	Yes	Yes	Yes	Yes

Note

Information about the type of license you are using is displayed in the Server properties in the **Product type** field.

Users in the **admin** role get an informational message to renew the license 30 days or less before it expires.

[1]—the system will operate in demo mode from 8:00 AM to 6:00 PM within 30 days after installation of *Axxon One*.

[2]—all VMD-based Scene analytics detection tools are available in *Axxon One Free* and *Axxon One Start* licenses, except for the Abandoned object detection (see Setting up VMD-based Scene Analytics detection tools).

[3]—MomentQuest with metadata search from the base VMD is available in *Axxon One Start* and *Axxon One Free* licenses. It is not possible to determine the object type and color based on metadata from VMD.

[4]—it is necessary to activate the license for the following detection tools:

- Vehicle Recognition (IV);
- License plate recognition (VT) (see Licensing of the software module for License plate recognition (VT));
- License plate recognition (IV) (see Configuring License Plate Recognition IV).

[5]—the module has to be purchased separately.

[6]—with the license, you can use privacy masks based on data from the corresponding detection tools.

[7]—to be released in the next version.

[8]—country restriction. Please contact an AxxonSoft manager to find out if this functionality is supported in your country.

Disclaimer

AxxonSoft reserves the right to make changes to the specification and cost of software licenses without notice and without any obligation to make the same changes to the licenses already sold. Orders are processed in accordance with the price list valid at the time of placing the order. If a placed order contains incorrect prices or license specifications, regardless of the cause of such errors. AxxonSoft reserves the right to reject or cancel the order, even if it has already been processed.

Licensing methods

There are two licensing methods for *Axxon One*:

1. **License file only.**

   The license file contains the data on basic hardware configuration (motherboard, CPU, hard disk, video adapter, RAM, and network card) of all Servers. If you change any two basic hardware components, your license will be invalid. For example, this is the case when you change both CPU and motherboard. However, changing a graphics card or upgrading RAM will not affect the license.

   This is why, when working with *Axxon One,* consider the following:

   a. The activation request should be sent from the computer that will host the *Axxon One* Server.
   b. You can upgrade your license only if you saved the initial basic hardware configuration of all Servers.
   c. It is not possible to transfer a license from one computer to another.

2. **License file and Guardant dongle.**

   This method allows replacing the Server hardware and transferring the license to another computer. To activate *Axxon One* via this method, contact AxxonSoft to receive a license file and Guardant dongle.
   If you already have a Guardant dongle, you can perform activation yourself. To do this, connect the Guardant dongle to the computer that you wish to activate and perform the standard activation steps.

   Attention!

   You can use a Guardant Sign dongle only on Linux OS.

Note

If you install virtualization products such as VirtualBox, VmWare etc., you may lose the license. If you encounter this problem, it is recommended to remove all virtualization products from the computer hardware tree or get a new license file.

Product activation utility

License activation for the *Axxon One* software package is carried out through the product activation utility.

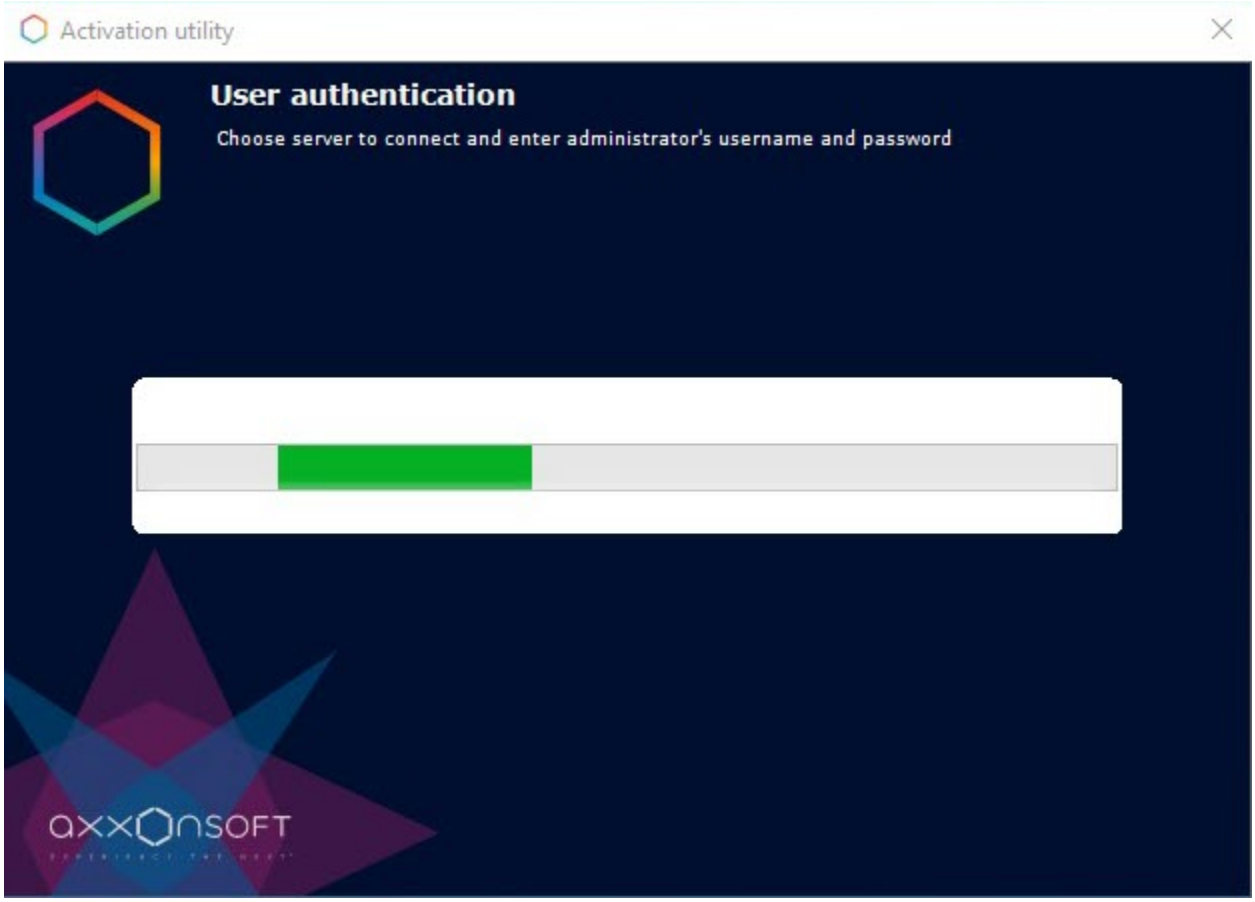
You can launch the product activation utility from the Windows **Start** menu: **Start** -> **All Programs** -> **Axxon One** -> **Utilities** -> **Program Activation**.

> **Note**
>
> The product activation utility program file LicenseTool.exe is located in the folder <Directory where *Axxon One* is installed>\AxxonSoft\Axxon Smart\bin\

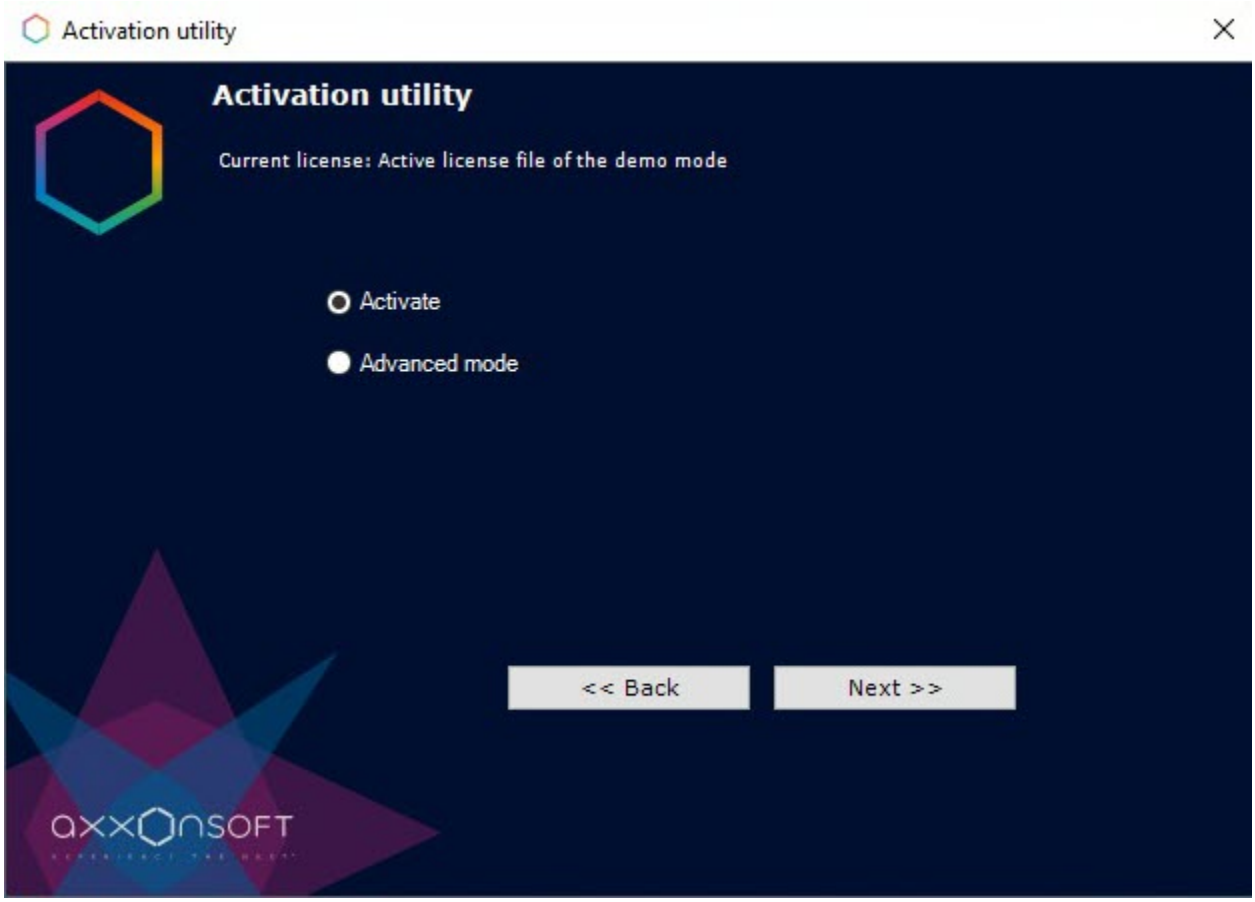
Then you must select the name of one of the Axxon Domain servers to which the license file will be applied (the file is applied to all Axxon Domain servers launched at the moment of activation) and connect to the system, under an administrator's user name and password, to continue the activation process.



The activation window will be displayed.



After the download is complete the main window of license utility will be displayed.



Note

To activate *Axxon One*, connect to a Server in the Axxon domain. Otherwise, an error message appears.

License Activation

To activate *Axxon One*, please refer to the document titled Activation Guide*,* which presents step-by-step instructions on activating, updating and upgrading *Axxon One*.

It is also recommended that you use the prompts displayed in the product activation utility's dialog boxes.

Launching and closing the Axxon One software package

Startup

Starting a Server

The *Axxon One* Server is started automatically when the operating system starts.

If the Server operation was stopped, perform one of the following actions to restart the Server:

1. Restart the system.
2. Select **Start server** from the **Start All Programs Axxon One** menu or in the *Axxon One Tray Tool* utility (see Axxon One Tray Tool).

   > **Note**
   >
   > Run the command with the administrator permissions.

3. Start the NGP Host Service.

By default, the *Axxon One* Server start time is set to 120,000 ms. If the Server does not start within the set time, the second forced attempt will be made to start the Server.

You can use the NGP_SERVICE_START_TIMEOUT_MS system variable (see Appendix 9. Creating system variable) to increase the Server start time. The value of the variable should be specified in milliseconds.

Starting the Axxon One Client

The *Axxon One* Client can be started manually using the **Start** menu, used for launching user programs in Windows.

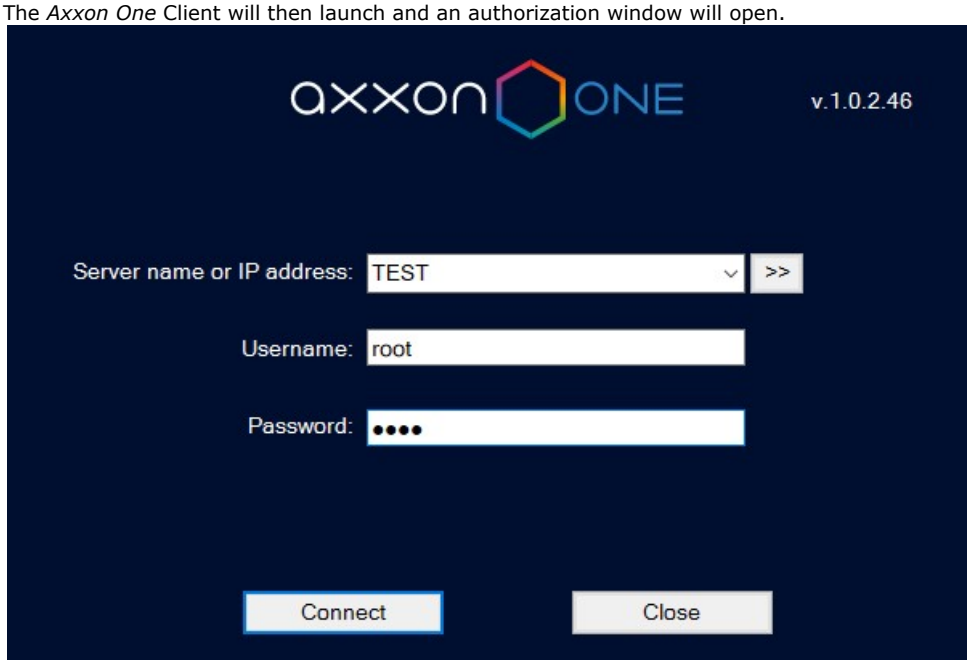
> **Note**
>
> To launch the Client from the command line, you must specify the login, password, and server parameters. All parameters are optional.
>
> For example: C:\Program Files\AxxonSoft\Axxon One\bin>Axxon One.exe --login=root --password=root --server=127.0.0.1
>
> To connect to multiple Servers (see Cross-System Client), specify their addresses separated by commas.
>
> For example: C:\Program Files\AxxonSoft\Axxon One\bin>Axxon One.exe --login=root --password=root --server=10.0.11.30, 10.0.11.34

To start working with the software, do the following:

1. Select **Start** ▸ **All Programs** ▸ **Axxon One** ▸ **Axxon One**.

   > **Note**
   >
   > - You can also start the *Axxon One* Client from the *Axxon One Tray Tool* utility (see Axxon One Tray Tool).
   > - *Axxon One* executable file Axxon One.exe is located in the <*Axxon One* installation directory>\Axxon One\bin\ folder.
   > - To start the Client in the safe mode with OpenGL software emulation, select: **Start** ▸ **Programs** ▸ **Axxon One** ▸ **Axxon One (safe mode)**.
   > - When the Client is running in the safe mode, the frame rate decreases.

   The *Axxon One* Client will then launch and an authorization window will open.

   > **Note**
   >
   > Starting the Client when the system is working in the failover mode is described in Connecting to a Node and Configuring of an Axxon domain.

2. Select a Server to connect to, and specify a port number.

   > **Connecting the Client to the Server behind NAT**

Attention!

The Client version and the Server version, to which you connect, must match. The *DriversPack* version must be the same as well. If the Server version is older than the Client version, you will be prompted to update the Client automatically (see Automatic update of a remote Client). We strongly recommended to avoid any connections if the product versions don't match.

Note

If a remote user connects to the Server, the name or the IP address of the computer with which the connection is established must be entered in the **Server name or IP address** field.

The order of the Servers in the list is the following:

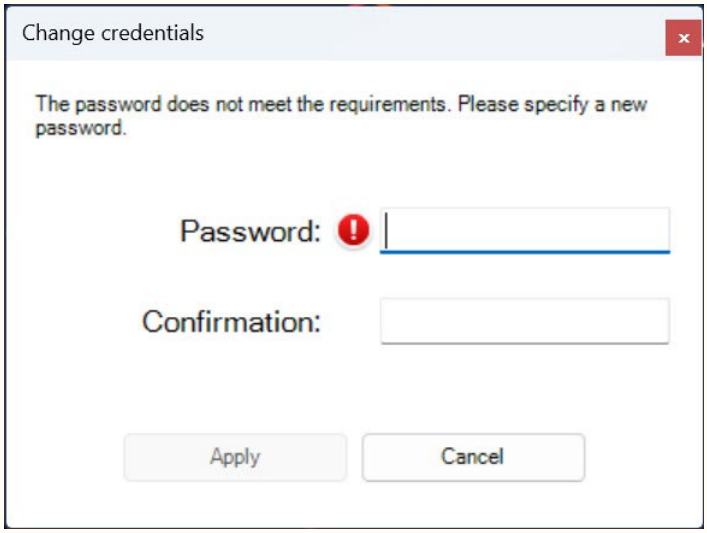
a. Preferred Servers (see Selecting Preferred Servers).
b. The last Server that was connected to.
c. Other Servers in alphabetical order.

3. Enter the username and password and click the **Connect** button.

Attention!

When you log into the system for the first time, use the username **root**, which has administrator permissions. Enter **root** into the **Username** and **Password** fields.

A window will open in which you must enter a new password.



When you hover the cursor over the icon, a tooltip will appear in which you can see the requirements for the new password (see Configuring the user security policy). Click the **Apply** button to save the new password.

You must securely save the new password (see How to recover the password of the root user (superuser)?).

The administrator then needs to configure the system for multi-user access (for details, see Configuring user permissions).

Connecting LDAP users

4. If the system administrator must confirm the user access (see Creating and configuring roles), enter the corresponding username and password and click the **Connect** button.

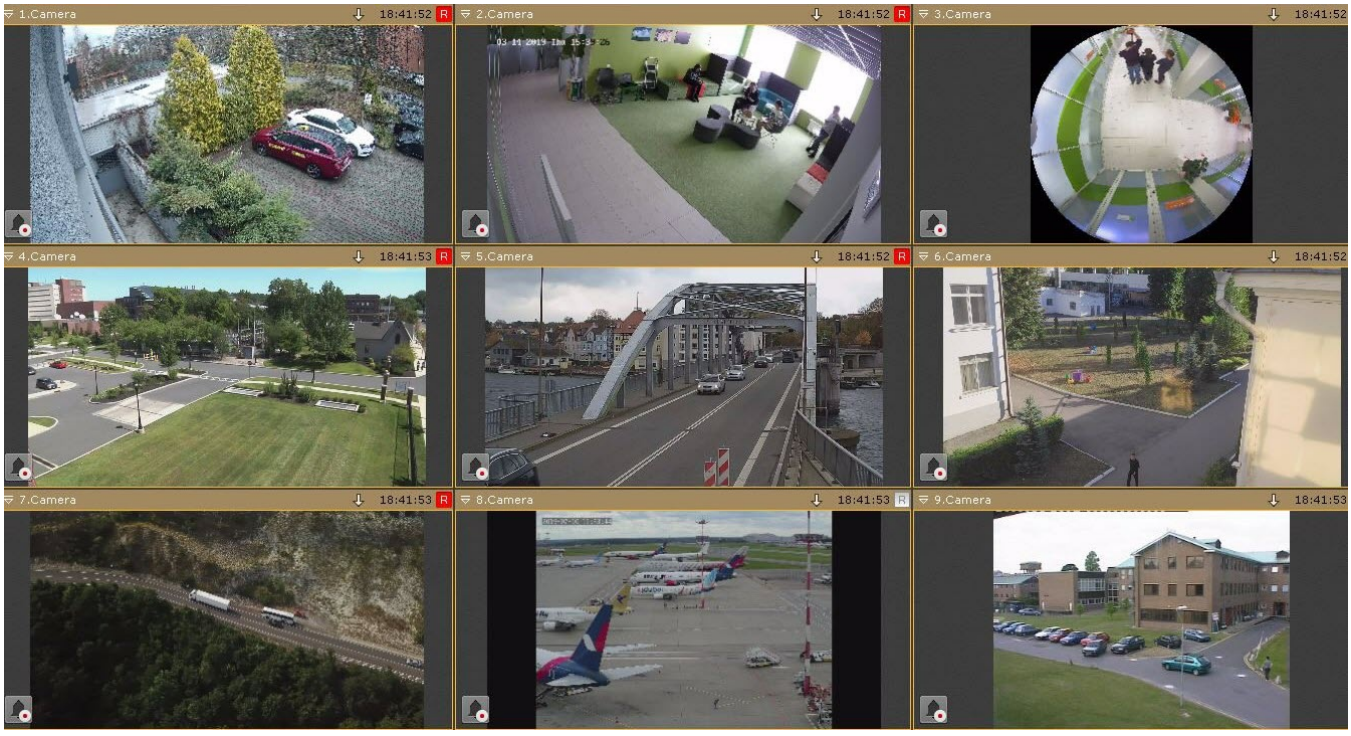


If authorization is successful, a video surveillance monitor will be displayed on the screen.

Attention!

When you first start the Client, the archive settings tab opens (see Configuring archives).

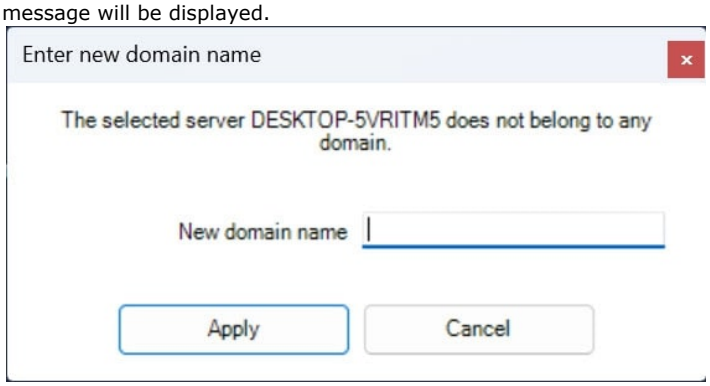
After you create the archive, you will be automatically switched to creating IP devices (see Searching, adding, configuring and removing IP devices). IP Device Discovery Wizard will launch automatically.



Note

If *Axxon One* is running in the *Axxon One* Demo mode, then after you enter the authorization parameters, a corresponding message will be displayed (see Axxon One in Demo mode).

If the Server to which you connect doesn't belong to any domain, after you click the **Connect** button in the authorization window, a message will be displayed.



To connect to the Server, you must either create a new domain based on the Server or add the Server to an existing domain.
If you choose the first option, click **Apply** in the message and follow the instructions given in Creating a new domain. For the second option, click the button and follow the instructions given in Adding a Server to an existing domain.

Running multiple Axxon One Clients

You can run multiple *Axxon One* Clients simultaneously on a single computer in order to connect to different Servers.

In this case, you must start Clients with the additional parameter --**monitor=N**, where N is the number of the monitor on which the Client is to be started.

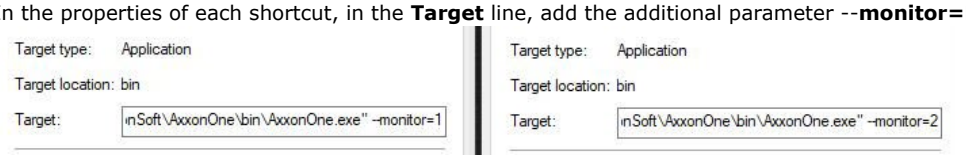
Attention!

The maximum number of running Clients is limited to the number of connected monitors that support the minimum required resolution (see Limitations of Axxon One).

You can run only one Client on a single monitor.

To run multiple Clients:

1. On your desktop, create a number of Client shortcuts equal to the number of connected monitors.
2. In the properties of each shortcut, in the **Target** line, add the additional parameter --**monitor=N**.



3. Start the Clients by using the shortcuts.

Note

If a Client is started in window mode (see Configuring the Client screen mode (full screen or window)) and moved to another monitor, the situation changes: Clients will be started on the specified monitors even if a Client is already running on one or more of them.

Axxon One in demo mode

If activation has not been completed, *Axxon One* works in demo mode.

The system will operate in demo mode from 8:00 AM to 6:00 PM. There are limitations to functionality (see Axxon One license types).

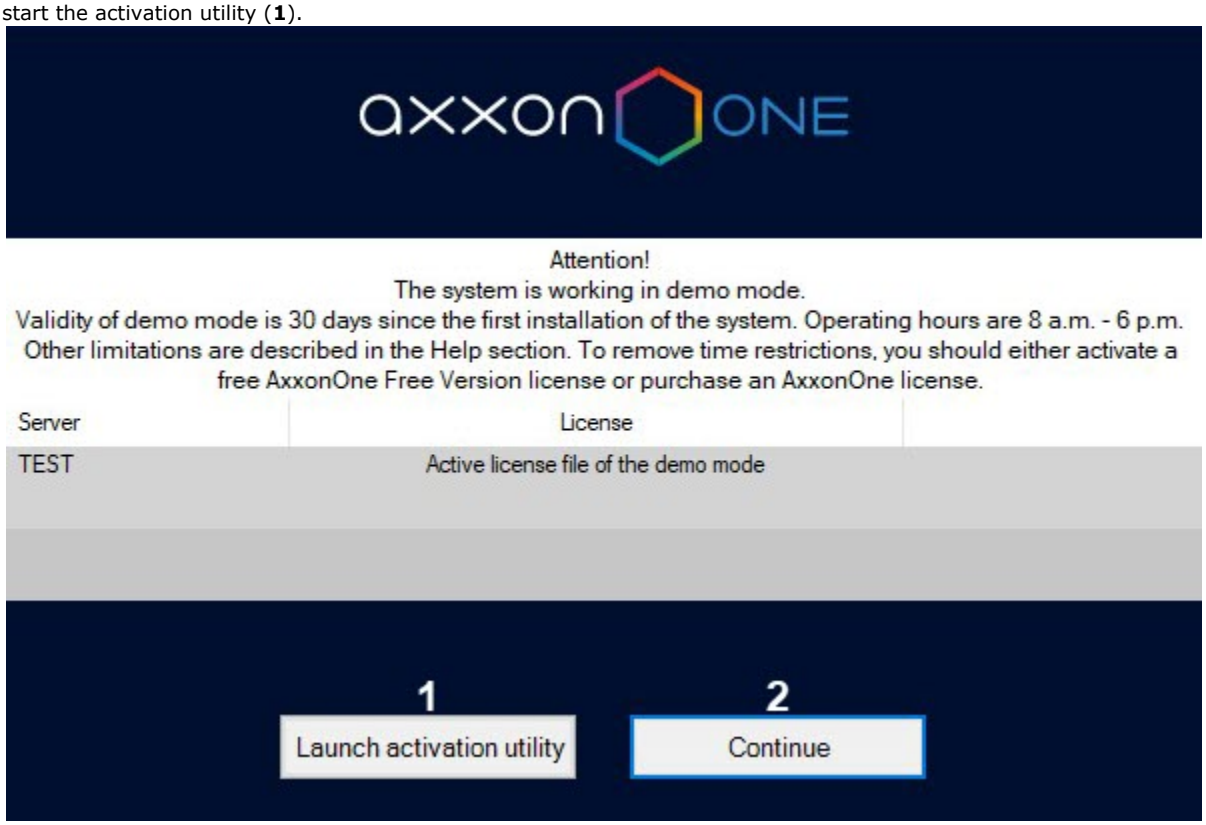
The different types of demo modes are presented in table.

Type of demo mode	Conditions	Axxon One operation
Active	*Axxon One* can be started between the hours of 8:00 AM and 6:00 PM	Using *Axxon One* in demo mode
Inactive	*Axxon One* started outside the hours of 8:00 AM and 6:00 PM	The *Axxon One* server is not available, only the system configuration can be viewed

If a Client is connected to an Axxon Domain in which there is at least one Server running in demo mode, an appropriate message is displayed, along with a list of Servers in the Axxon Domain and their types of licenses.

> **Note**
>
> The notification is displayed after successful authorization.

If an Axxon Domain includes at least one Server running in active demo mode, you will be given the option to continue working (**2**) or start the activation utility (**1**).



Automatic Start of the Client

You can use Windows Task Scheduler to configure the *Axxon One* client to start automatically at the system start-up.

It is recommended that you specify a Server start-up delay.

> **Note**
>
> You can also configure automatic authorization for the Client upon start-up (see Automatic connection).

Shutdown

Shutting down an Axxon One Client

Before closing *Axxon One*, you need to exit the user interfaces. To do this, perform one of the following:

1. Click the  button located in the top-right corner of the *Axxon One* dialog box.

   > **Note**
   >
   > If the client is opened in full-screen mode (enabled by default), the  is not displayed. In this case you can exit the user interfaces using actions 2 and 3.

2. In the **Settings** tab, click the  button.
3. In the Windows taskbar notification area, in the context menu of the *Axxon One* icon, select **Close window**.

When you perform one of these actions, the authorization window will appear. To close *Axxon One* (completely exit the client), click the **Close** button.



Shutting down a Server

To shut down the *Axxon One* Server, perform one of the following actions:

1. Select **Stop server** from the **Start All Programs Axxon One** menu or in the *Axxon One Tray Tool* utility (see Axxon One Tray Tool).

   > **Note**
   >
   > Run the command with the administrator permissions.

2. Stop the NGP Host Service.

By default, the *Axxon One* Server shutdown time is set to 60,000 ms. If the Server does not shut down within the set time, the second forced attempt will be made to shut down the Server.

You can use the NGP_SERVICE_STOP_TIMEOUT_MS system variable (see Appendix 9. Creating system variable) to increase the Server shutdown time. The value of the variable should be specified in milliseconds.

Automatic Server restart

If you change the following network settings in the operating system, the *Axxon One* Server is automatically rebooted:

- IP address;
- creating a new network connection.

> ⚠ **Attention!**
>
> While the Server restarts, the connection to cameras is temporarily lost and recording stops.

Switching Users Quickly

You can switch *Axxon One* users quickly without fully exiting the client.

To do this, follow the steps below:

1. Exit the *Axxon One* user interface (see the section Shutdown).
2. When the authorization window appears, enter the user name under which you need to log in and the corresponding password and click **Connect**.



Switching users is now complete.

Cross-System Client

Axxon One allows an operator or administrator of a security complex to connect from one Client workstation simultaneously to several Servers located in different domains and not united in a single system. Cameras connected to Servers of different domains, as well as the settings of these Servers are conveniently displayed in a single user interface. As a result, an operator can work with several independent video surveillance systems at once that aren't united into a single distributed complex.

This situation can happen when protected facilities are located at a great distance from each other, as well as if there are many objects that you want to configure together, but they must operate separately, and so on. An example of using this function is the ability of the police to connect to the security systems of stores belonging to different retail chains.

The Client connects to different domains automatically when you start it (see Automatic connection). First, it connects to the main domain. The Client connects to other domains in the background after you start it.

Note

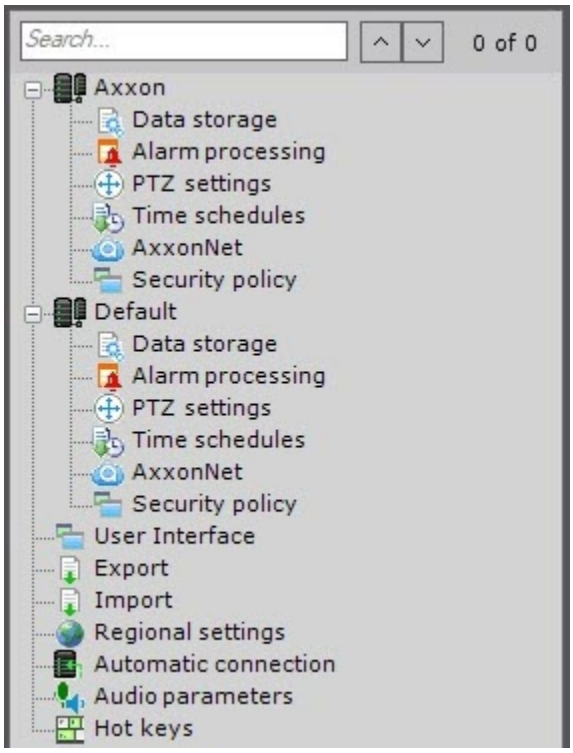
You can also connect to multiple domains manually in the Client authorization window. To do this, specify several Servers separated by commas in the format: <Server1 name or IP address>:<Connection port>, <Server2 name or IP address>:<Connection port>, and so on. The Server listed first will be the main Server (see Automatic connection).



To connect the Client to multiple domains, the following conditions must be met:

- each Server to which the Client connects has the Enterprise or Unified license activated (see Axxon One license types). For example, some Servers can have the Enterprise license activated, while others can have the Unified license activated;
- connection to all Servers is made using a single username-password pair that must be created in each domain;
- Server names must not be the same;
- IP addresses of Servers must not be the same.

When the Client connects simultaneously to several Servers from different domains, the system settings section is duplicated for each domain (see Server settings).


Search...
0 of 0
Axxon
Data storage
Alarm processing
PTZ settings
Time schedules
AxxonNet
Security policy
Default
Data storage
Alarm processing
PTZ settings
Time schedules
AxxonNet
Security policy
User Interface
Export
Import
Regional settings
Automatic connection
Audio parameters
Hot keys

Connecting LDAP users

LDAP users are connected to the system in two steps:

1. The user logs in on the LDAP server.
2. The user then authenticates on the *Axxon One* server.

Attention!

Each Client to which LDAP users are connecting must have access to the LDAP catalog.

Note

When an LDAP user connects, the user's login and password in the LDAP as configured in the Server settings are used (see Cr eating LDAP connections). The login and password in the LDAP directory are not used when connecting to the Server.

Connecting to Another Server Quickly

You can connect to another Server without fully exiting the Client.

To do this, follow the steps below:

1. Exit the *Axxon One* user interface (see the section Shutdown).
2. When the authorization window appears, select the Server to which you need to connect the Client from the **Computer** list.
3. Enter the user name under which you need to log in and the corresponding password and click **Connect**.

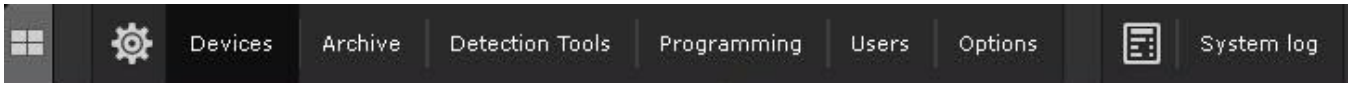
Connection to another Server is now complete.

Configuration of Axxon One

General information on system configuration

System configuration: stages

Most system configuration is performed via the **Settings** expanding menu, which contains six tabs for configuring certain parts of the system.



The main stages of system configuration are:

1. Configuring an Axxon domain.
2. Connecting and configuring hardware.
3. Configuring archives.
4. Configuring layouts and the interactive map.
5. Configuring users and roles.

Attention!

Please avoid changing system settings from different Clients simultaneously. When you change settings from Clients logged in under the same user (see Working with users), all changes are automatically synchronized. For example, if Client 1 and Client 2 are logged in as the same root user, and the layout settings are changed on one of the Clients, then the second Client will automatically switch to this layout.

Applying and resetting settings

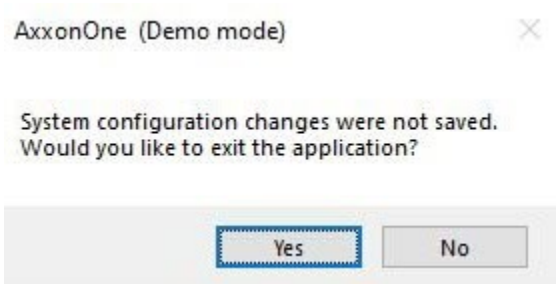
For a change in the system settings to take effect, you must click the **Apply** button.

After you click the button, a progress bar indicates that the settings are being applied. You can resume working with the system after the process completes.



If you want to discard changes and have not clicked the **Apply** button, click **Cancel**.

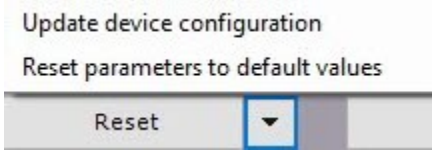
If an attempt is made to close the Client but not all changes have been saved yet, a dialog box asks whether to confirm closing or to cancel closing and save changes.



When setting up hardware, you can reset parameters to default values, or read configuration from the device at any time.

To reset parameters to default values, do the following:

1. Select the required device in the objects tree.
2. Click , then **Reset parameters to default values**.



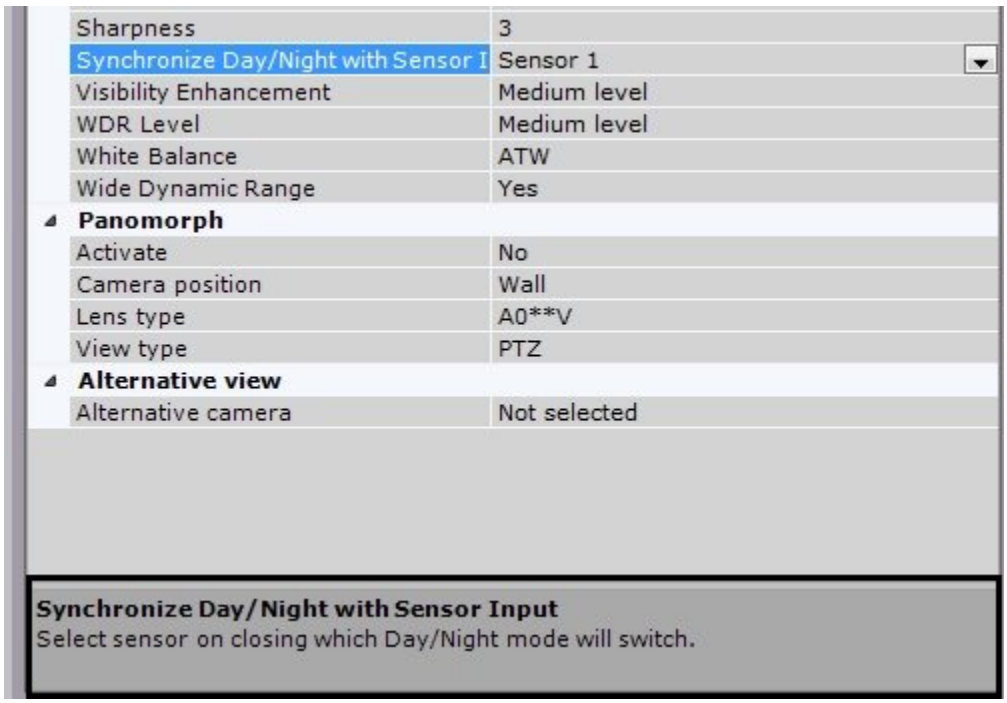
If a device's configuration differs from settings specified within the system, you can download the configuration from the device. To do it, follow the steps below:

1. Select the required device in the objects tree.
2. Click , then **Update device configuration**.

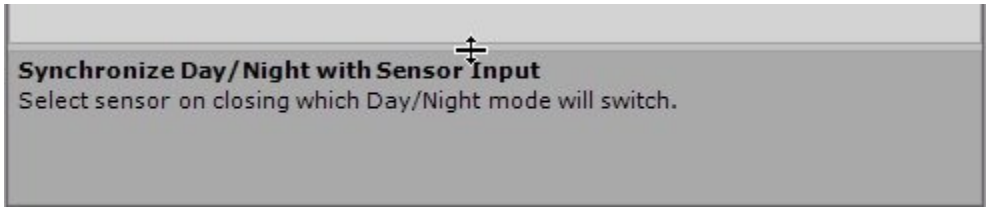
Display of parameters in interface

Most system parameters and hardware parameters are displayed in the *Axxon One* interface.

The description of a parameter is usually displayed in a special area when the relevant parameter is selected.



If the description of a parameter is truncated, you can stretch this area above the upper border.



System objects

Axxon One VMS has the following types of system objects:

1. Axxon domain objects (see Configuring Axxon-domains).
2. Hardware objects: Server, IP Server, Camera, Microphone, PTZ, Input, Output, Embedded Storage (see Configuring system objects for devices).
3. **Event Source** objects are used to integrate *Axxon One* with external systems (see Receiving Events from External Systems).
4. **E-mail** objects used in macros and automatic rules for e-mail notifications (see The Email notifier object).
5. **Export Agent** objects used in macros and automatic rules for exporting video recordings and snapshots (see Configuring export).
6. Archive objects (see Configuring archives).
7. Detection tool objects (see Configuring detection tools).
8. Role and user objects (see Configuring user permissions).
9. Macro objects (see Configuring macros).

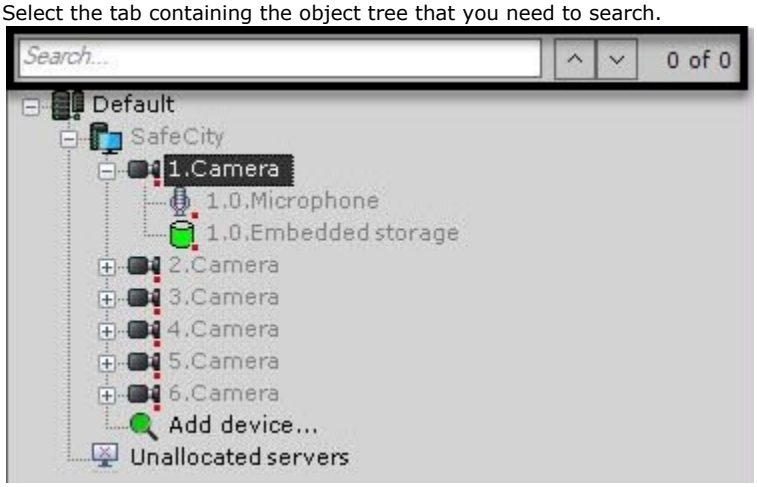
Some objects are created automatically, while others are created manually or are pre-created in the system.

Object search

Axxon One allows you to search for objects in the objects tree using only part of their name or the IP address. An object search can be performed on all tabs under **Devices**.

To search for objects, complete the following steps:

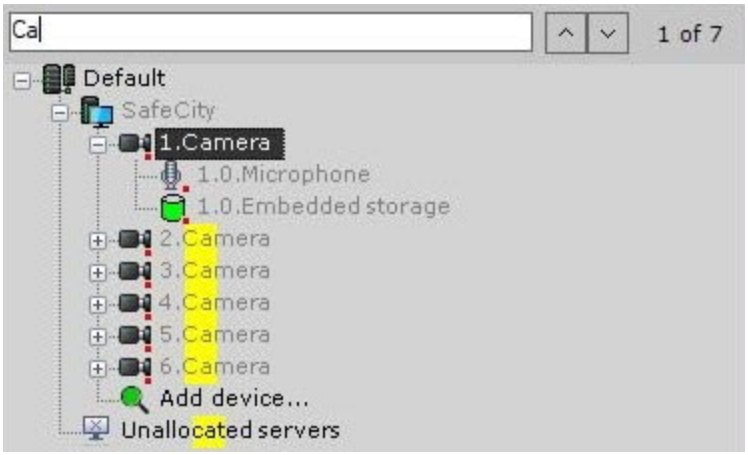
1. Select the tab containing the object tree that you need to search.



2. Enter the IP address, the full or partial name of the object in the **Search** field.

> **Note**
>
> - Search is not case-sensitive.
> - Search can also be run based on object short name.

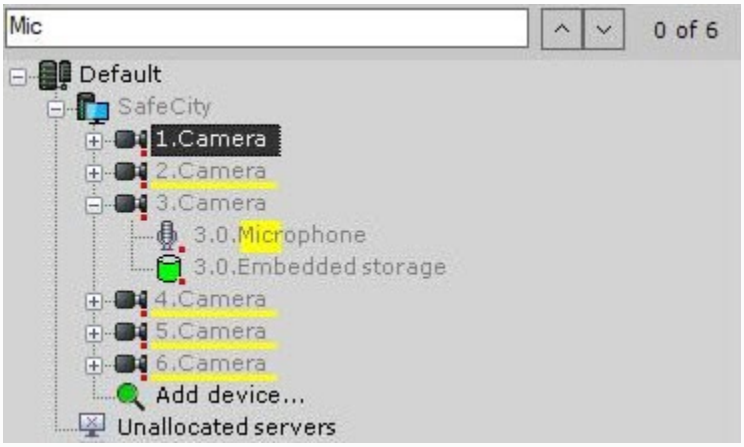
The search starts automatically once you enter something in the box. When the search is complete, you will see the number of objects found in the tree.



The parts of names corresponding to the characters you entered will be highlighted in yellow on the found objects.

Note

- If you search by an IP address, the found object will be fully highlighted.
- If a found object is located in a collapsed branch of objects, the branch will be highlighted with a yellow line.



You can use the  buttons or press **ENTER** to navigate through the search results.

The search results rotate in a loop; moving from the last object takes you back to the first object.

Note

If you move to an object located in a collapsed branch, the branch will automatically expand.

Hardware configuration

Configuring domains

A distributed system based on *Axxon One* is created within a domain, it means, a selected group of *Axxon One* Servers.

When configuring a domain, the following operations are used in the necessary combinations:

1. Creating a new domain.
2. Adding a Server to an existing domain.
3. Excluding a Server from the current domain.

> **Attention!**
>
> You cannot combine regular and Failover Servers within the same domain (see Configuring Failover VMS).

To configure a domain, you must have the appropriate permissions (see Configuring user permissions).

This section gives step-by-step instructions for each operation used in configuring a domain, and then describes typical instances of their use.

The Domain object

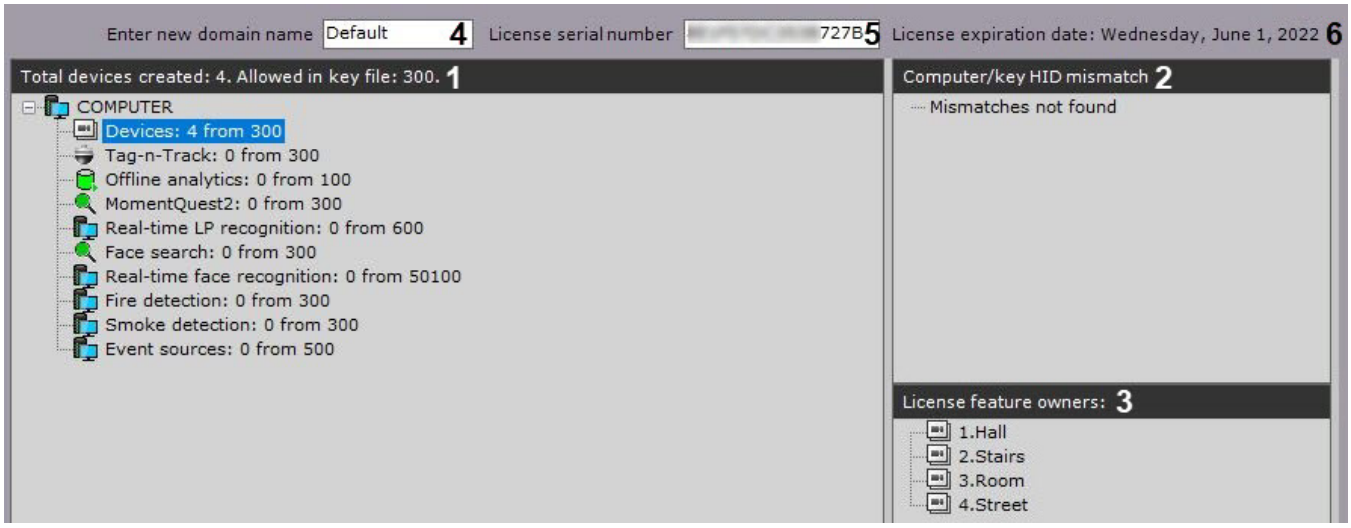
The **Domain** system object is the basic object in the system.

The **Domain** object is the parent of the **Server** objects, which correspond to the servers that are in a domain.

When you select the **Domain** object in the **Total devices created** group (**1**), the software displays information about the domain and the current license: Servers and their number, IP devices and various used functions.

Also displayed are license serial number (**5**) and license expiration date (**6**).

> **Note**
>
> The number of created devices means the total number of enabled IP video channels.



In the **Computer/key HID mismatch** (**2**) group, the license information/error is displayed.

If you select a licensing option in the relevant group (**1**), the **License feature owners** (**3**) group will include the objects currently using this license.

You can also rename the domain. To do so, enter the new name in the corresponding field (**4**) and click the **Apply** button.

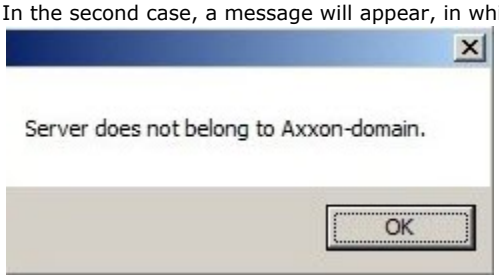
Operations with domains

Creating a new domain

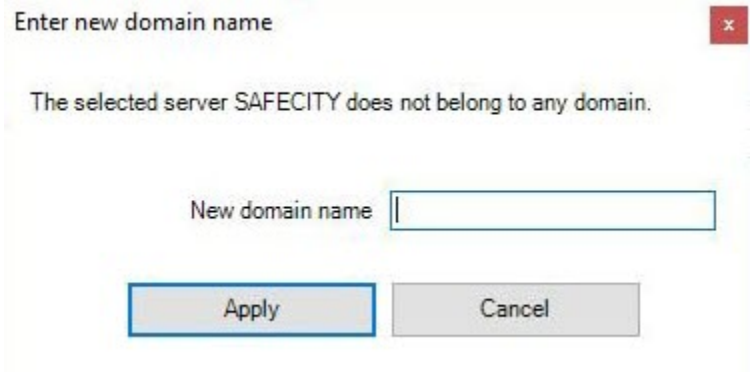
A new domain can be created in one of two ways:

1. During installation of *Axxon One* with the **Server and Client** configuration type (see Installation).
2. When attempting to connect to a Server which does not belong to a domain.

In the second case, a message will appear, in which you must click **OK** (see Startup).



The **Enter new domain name** window will appear. In the **New domain name** field, enter the domain name to create a new group of computers based on the Server and click **Apply**.



Attention!

- It is not possible to use the above steps to add a Server to an existing domain.
- Assigning the same domain name to several Servers does not guarantee that those Servers will be in the same domain.
- Different domains can have identical names.

This will create a new domain based on the Server. *Axxon One* will then be launched with the entered authorization parameters (see Startup).

Adding a Server to an existing domain

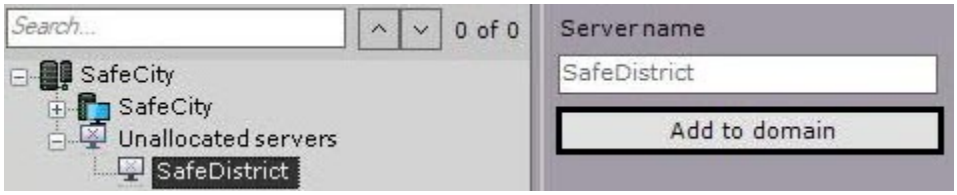
A Server can be added to an existing domain from any Server within that domain.

Attention!

- To add a Server to a domain, it is necessary to first add the new Server to the license (see Upgrading Axxon One). This does not apply to cloud licenses.
- Before configuring a distributed system, be sure to consolidate your Servers into domain.
- When consolidating the Servers into domain, each Server must have a unique IP address.
- Only unallocated Servers can be added to domain. Unallocated Servers are the Servers that don't belong to any domain.

There are two ways to add a Server to a domain, depending on whether or not it is present in the search results (in the **Unallocated servers** group).

If a Server is present in the search results, select it and click the **Add to domain** button.



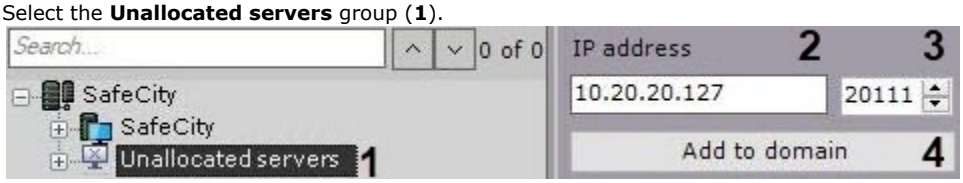
The Server will then be added to a domain from the **Unallocated servers** group.
Since the search for the unallocated Servers is conducted using the broadcast packets, the results may not include Servers located in a different subnetwork (for example, beyond a router that blocks broadcast packets).
In this case, you can add a Server to a domain manually. This option can be used with all unallocated Servers, including those present in the **Unallocated servers** group.

Consolidating the Servers from different networks into Axxon domain

Network settings utility

To add a Server to a domain manually, do the following:

1. Select the **Unallocated servers** group (**1**).



2. Enter the Server IP address (**2**).
3. Enter the Server port (**3**).
4. Click the **Add to domain** button (**4**).

The Server will then be manually added to a domain.
After a Server is added to a domain using any of the methods described, it will be displayed in the objects tree.



If a Server is not available when it is added to a domain, it will be displayed in the objects tree with the icon.

The Server will be added to a domain when it becomes available. To undo adding a Server to a domain, select the Server and click the Exclude from domain button.

Removing a Server from a domain

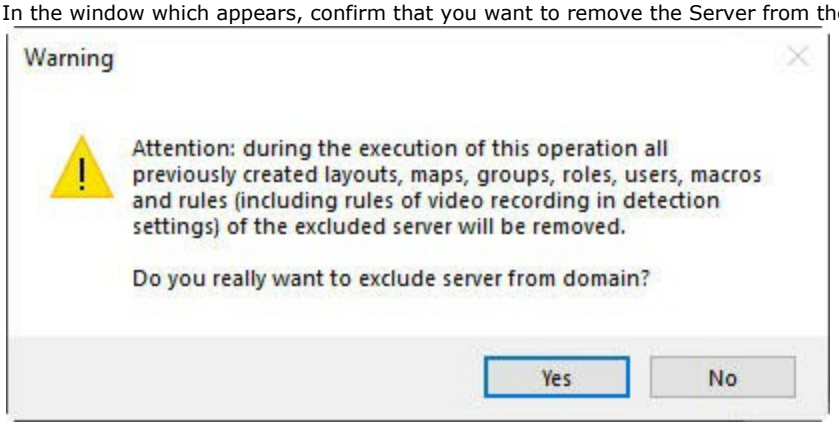
Any Server on a domain can be used to remove a Server from a domain.

Attention!

By excluding a Server, you also delete the macros, layouts, maps, object groups, roles, and users that have been created on the Server.

To remove a Server from a domain, you must perform the following steps:

1. Select the Server in the list and click the Exclude from domain button.
2. In the window which appears, confirm that you want to remove the Server from the domain by clicking the **Yes** button.



The Server will then be removed from the domain. If the current Client was connected to the excluded Server, the user interfaces will be unloaded and the user will be prompted to repeat the authorization procedure for *Axxon One* (see Startup).

Note

You can also exclude a Server from a domain using the activation utility (see Excluding the Current Server from an domain).

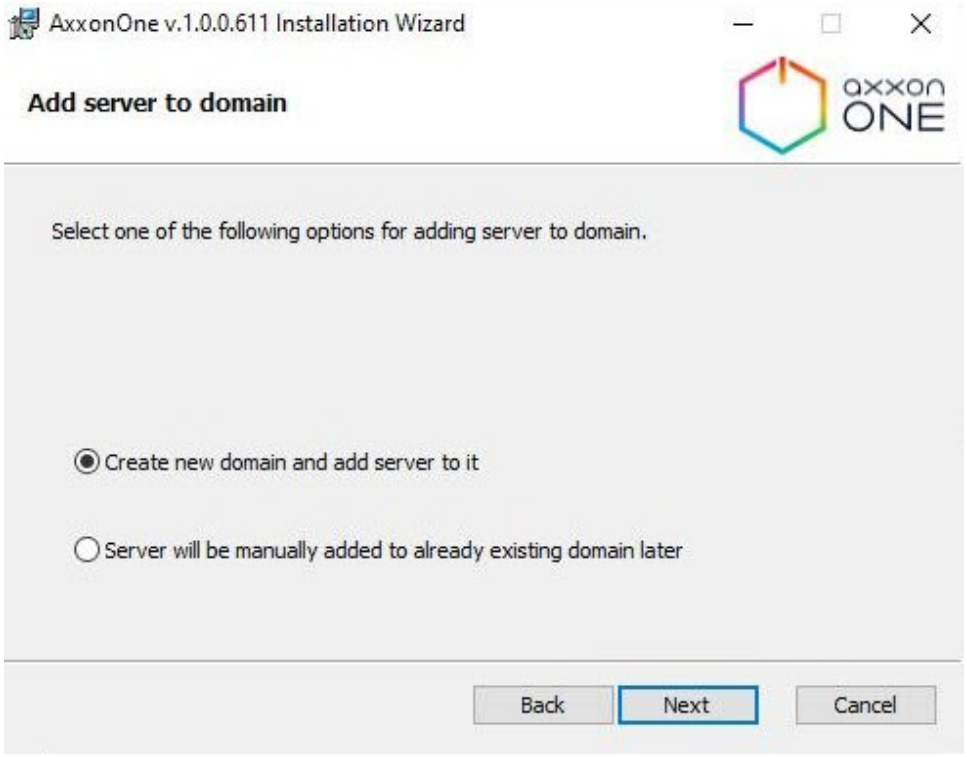
Cases of domain configuration

All possible cases of domain configuration are, to some degree, a combination of two typical cases.

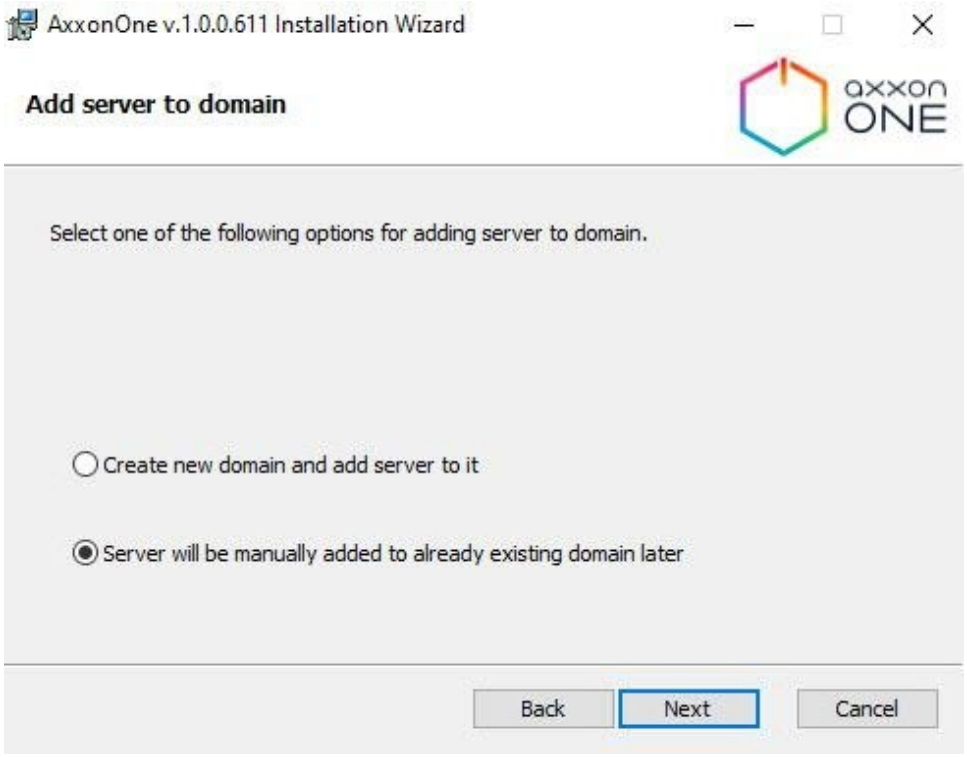
In the first typical case, the Servers for the future domain are selected before *Axxon One* installation. This case involves the following steps:

1. Selecting a Server on the basis of which a new domain will be created. Installing *Axxon One* with the **Server and Client** configuration type, indicating the name of a new domain (see Installation).

   > **Note**
   >
   > Any Server in the future domain can be selected as the primary Server.



2. Installing *Axxon One* with the **Server and Client** configuration type on the other servers of the future domain, without adding them to a domain (see Installation).



3. Connecting to the primary server.
4. Adding the remaining Servers to a domain from the primary Server according to the instructions in Adding a Server to an existing domain.

In the second typical case it is necessary to add servers which are part of another domain to a new domain. This case involves the following steps:

1. Excluding all the Servers which are to be added to a new domain from their current domains, according to the instructions in Removing a Server from a domain.
2. Naming a new domain according to the instructions in Creating a new domain, when attempting to connect to one of the Servers excluded in step 1.
3. Adding the remaining Servers to a domain from the primary Server according to the instructions in Adding a Server to an existing domain.

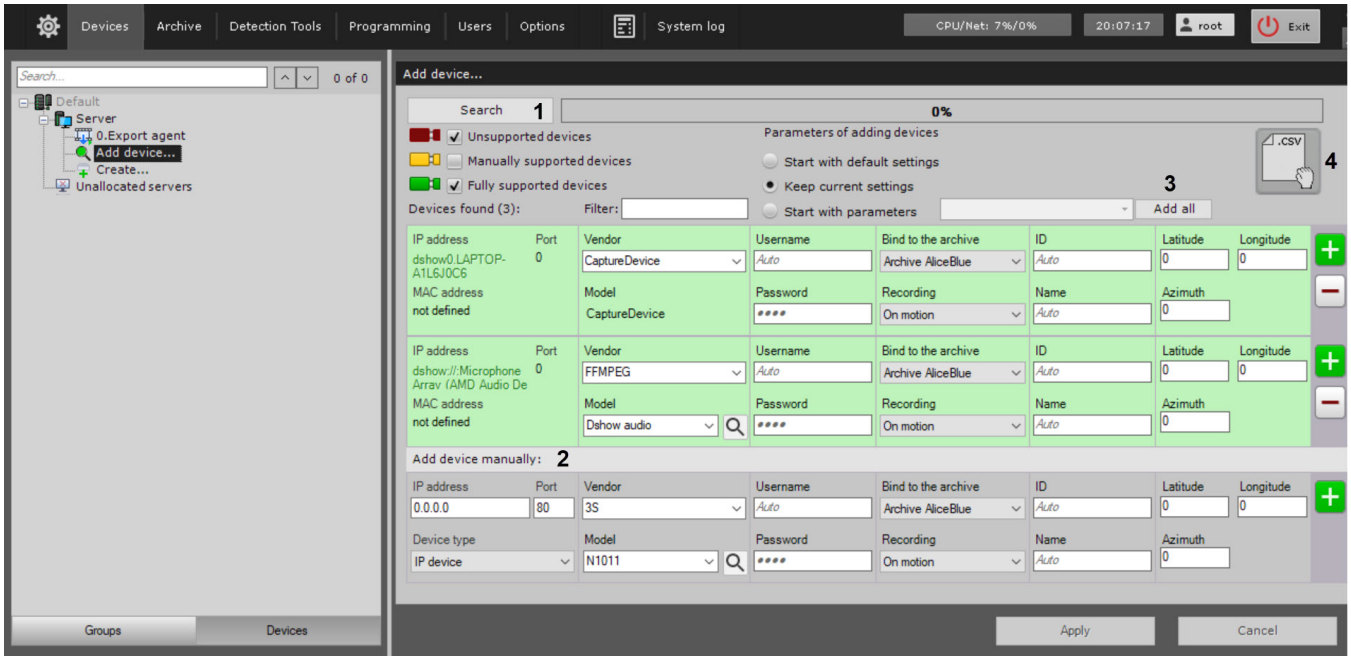
Searching, adding, configuring and removing IP devices

On this page:

- General information
- Automatic search for IP devices
  - IP devices search
  - Filtering IP device search results
- Manual input of device data
- Adding devices to the configuration
  - Modes for adding devices to the configuration
  - Configuring IP device settings
  - Adding devices
- Removing IP devices

General information

You can add IP devices to the system using the IP Device Discovery Wizard. To open the IP Device Discovery Wizard, click on the **Add device** link at the end of the Server device list.



The IP Device Discovery Wizard interface includes:

- Automatic device search.
- Manual entry of device data.
- Adding devices to the configuration.
- Bulk adding devices using .CSV files (see Bulk creation of IP devices).

Automatic search for IP devices

IP devices search

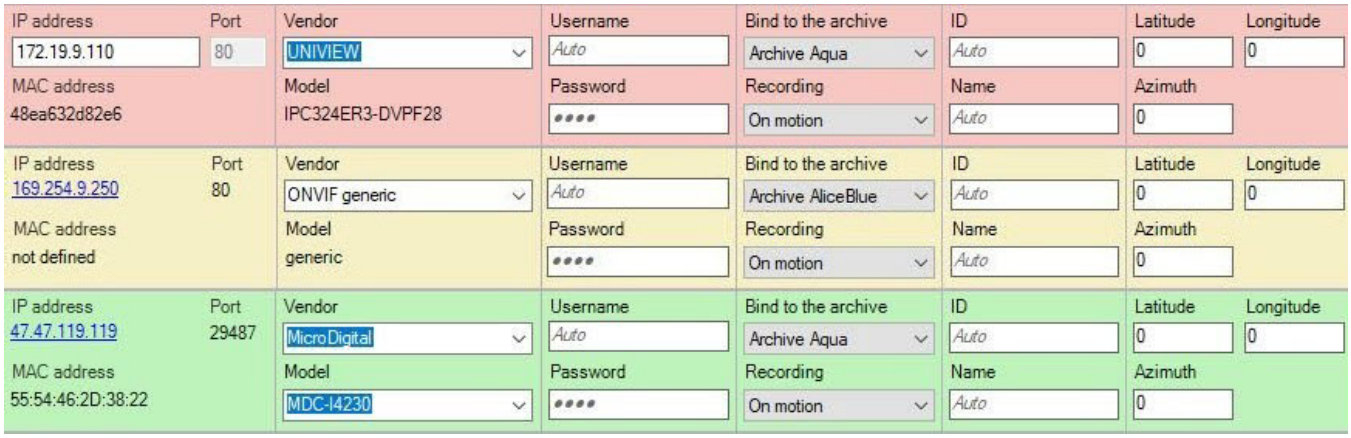
To start searching for devices, click the **Search** button. While searching, a progress bar will be displayed.



To stop devices search at any time, click the **Stop** button.

The search results are color-coded based on the status of the device.

Color of video camera icon	Description
	Fully supported device
	Manual configuration required
	*Axxon One* compatibility not guaranteed



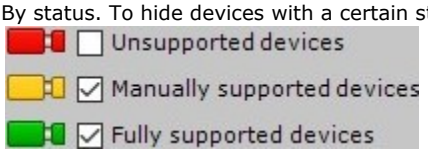
Note

- Since multicast packets are used for device search, the search results may not contain the Servers and devices from other subnets.
- If you click the IP address, you will jump to the device web interface.

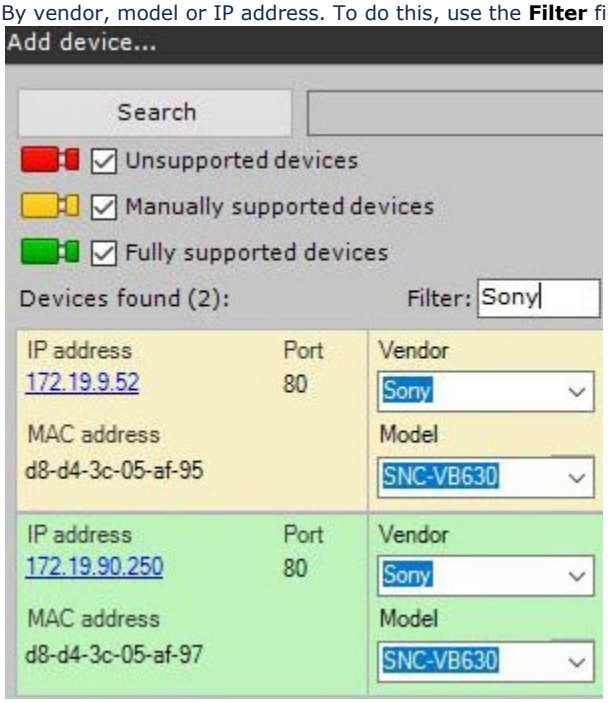
Filtering IP device search results

Search results can be filtered in two ways:

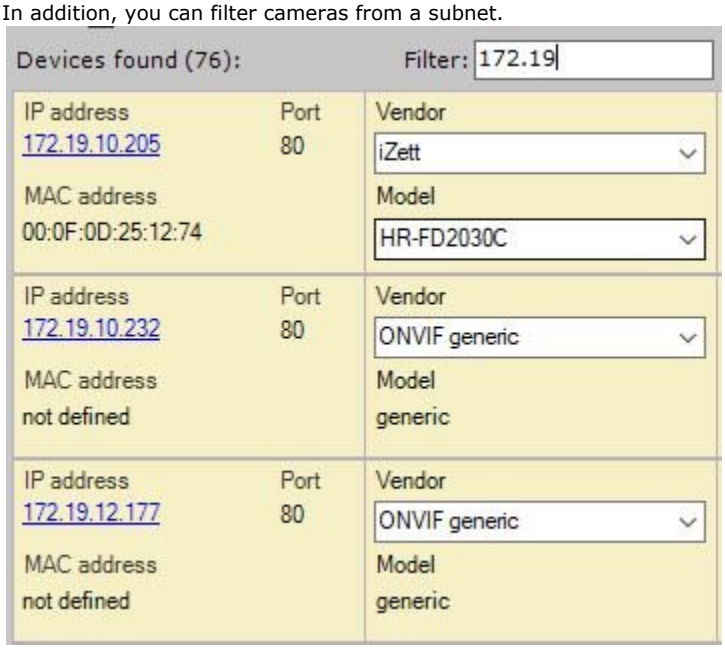
1. By status. To hide devices with a certain status, deselect the relevant checkbox.



2. By vendor, model or IP address. To do this, use the **Filter** field. For example, this filters the **Sony** devices.

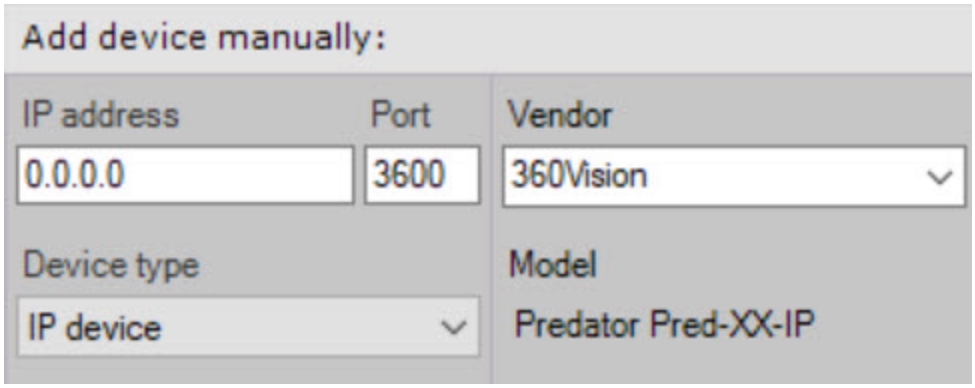


In addition, you can filter cameras from a subnet.

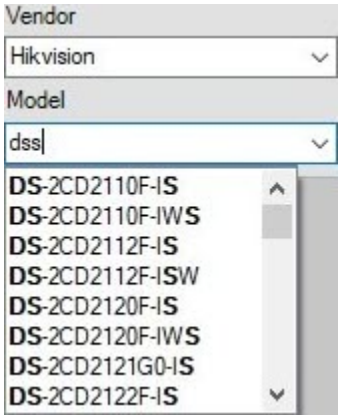


Manual input of device data

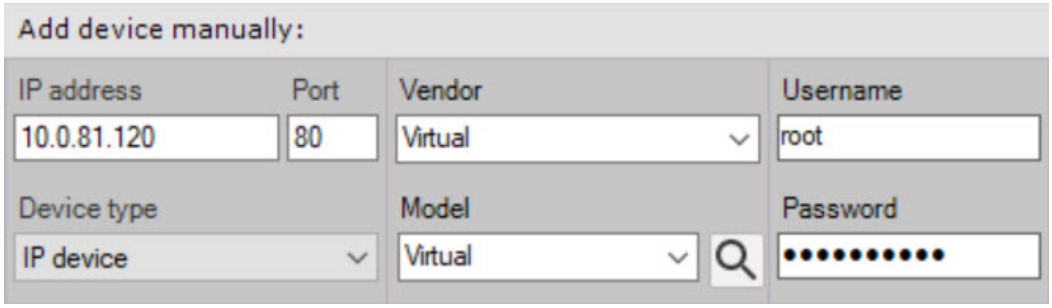
If an IP device is not shown in the search results (because it is located on a different subnet or the connection with it is temporarily lost), you can add it manually. To do this, you need to select the type of IP device to be added, specify the IP address and connection port of the device, and select the vendor and model in the area with a neutral background located under the list with automatic search results.



You can also specify the vendor and model of the device using the search in the input field.



If the device's IP address, Port, Vendor, Username and Password are set, the device Model can be automatically detected by clicking the  button.



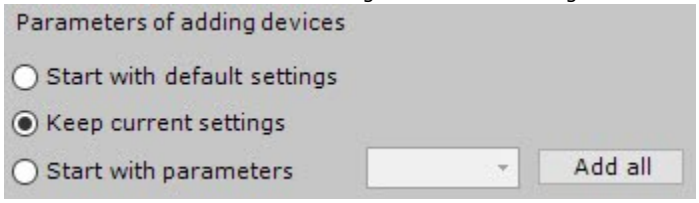
Adding devices to the configuration

To add an IP device to a configuration:

- select a mode for adding the device to the configuration;
- set the device settings, if necessary;
- the device is added to the configuration.

Modes for adding devices to the configuration

Three modes are available for adding a device to a configuration. These are described in the following table.



	Device addition mode	Description
1	Keep current settings	The IP device is added to the configuration with the current settings, as specified in the web interface
2	Start with default settings	The IP device is added to the configuration with the default settings (the default settings are determined by *Axxon One* itself). Adding a device in this mode will change the current settings of the device specified in the web interface
3	Start with parameters	The IP device is added to the configuration with the settings that have been previously specified for a device of the same model in the configuration. Select a device of the same model (the "template device") in the list. Only devices of the same model are shown in the list of search results for choosing the template device. Parameters that will be set according to the template device: firmware, video stream settings, buffering settings, **Other** settings (see The Camera object), and **Other** settings for **Microphone** and **Speaker** objects, if these are configured for the template device. This mode is best when multiple cameras of the same model are in use at a site. If this is the case, we advise to: • Add and configure one device. • Add the remaining devices, copying settings from the "template device" as described previously

Configuring IP device settings

When adding a device, you can immediately set several configuration options, such as:

- vendor and model.
- login and password.
- ID and object name.

> **Note**
>
> The object ID can contain numbers, Latin letters and the "_" sign. Once the device is created, its short name will match the specified ID (see The Camera object). In this case:
>
> - The camera ID cannot be changed, since it is used to maintain the connection with the archive when replacing the camera (see Saving the archive when replacing the video signal device).
> - The short name can be changed, and the added devices will be sorted in the object tree in ascending order of this field (see The Camera object).

- archive selection and the recording parameters (see Configuring recording to an archive):
  1. **No**—camera is linked to the archive, no recording.
  2. **Always**—continuous recording.
  3. **On motion** (default)—for the camera you are adding, either an embedded motion detection will be automatically created (see General information about embedded detection tools), or a VMD tool (see Configuring the Motion detection). An automatic rule will also be created for recording to the specified archive (see Automatic Rules). By default, recording stops when an event detection is finished.

  > **Note**
  >
  > - When creating a new device, the pre-alarm time interval for video footage recording is automatically set to 3 seconds (see Configuring recording to an archive).
  > - The embedded motion detection will be created automatically only for certain video camera models. For information about support for embedded motion detection, see the list of supported devices, the **Analytics** column. The embedded motion detection is configured through the web interface of a specific video camera. In other cases, a VMD tool will be created.

- device location coordinates in the format 53.212558; 50.204991 (coordinates are used when adding a video camera to the map, see Adding video cameras and changing size of their icons on the map).

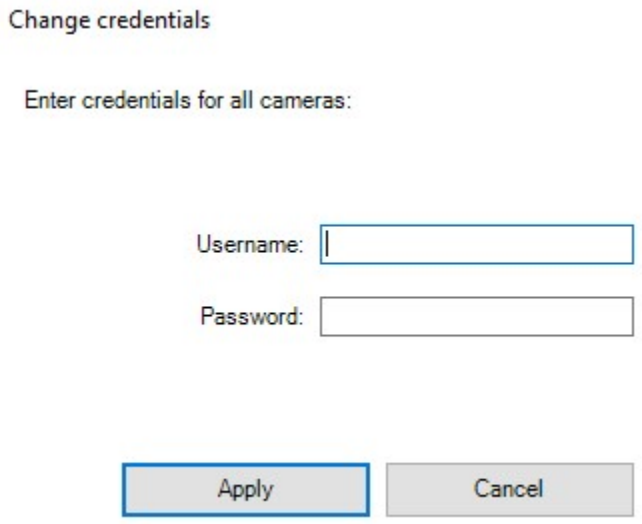
Adding devices

During a single configuration change, you can add a single device or all devices listed in the search results (other than devices for which compatibility is not guaranteed). To add one device, click the  button. To add all devices, click the **Add all** button.

> **Note**
>
> Note that if you add all IP devices at the same time, the same mode and settings will be applied to all of them.

To remove a device from the search results, click the button.

If you set no individual access parameters while adding hardware, a dialog window appears for setting unified access parameters.



Next, the device is added to the configuration.

When you add a device to the system, the **Default** permissions will be applied, which are configured for each role (see Configuring user permissions).

Removing IP devices

To remove IP devices, select one or more objects in the hardware tree by left-clicking (while holding down the Ctrl key) and click the **D elete** button.

Bulk creation of IP devices

You can create IP devices in bulk by importing their parameters from a CSV file.

> **Attention!**
>
> You have to disable the UAC first.

Do the following:

1. Create a CSV file with devices listed as follows:

```
IP address, Port, Vendor, Model, Login, Password, Identifier, Object name, Latitude, Longitude, Azimuth,
Archive name, Recording mode
```

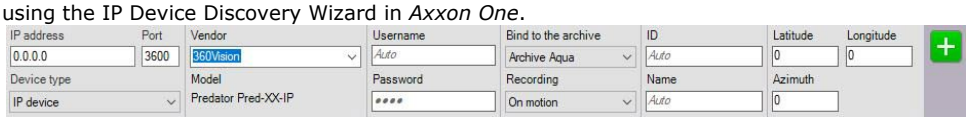
> **Attention!**
>
> - For each added camera, three parameters are required: IP address, Vendor and Model. The parameters that aren't specified will be automatically set to their default values.
>   Even if no additional parameters are set, you should still include commas.
> - All parameters are case-sensitive.
> - To separate the integer and fractional parts in coordinates, use a point.
> - If there is a comma in the device model name, in order not to violate the logic of the CSV file, it is necessary to add the \ character before the comma in the model name.
>   Example: the device model name is CO-i20DY2(2,7-9) (CO-YUC-HM96-279). In the CSV file, it is necessary to specify the model name as CO-i20DY2(2\,7-9) (CO-YUC-HM96-279).

For example:

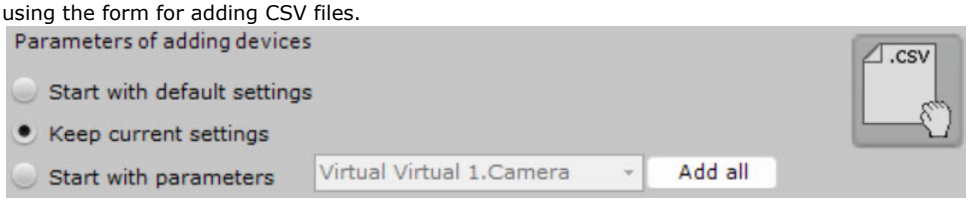
```
10.0.12.245, 80, Bosch, Dinion IP starlight 8000 MP, service, Admin12345!, 1441, Camera 1, 0, 0, 0,
Archive AliceBlue, Always
10.0.12.246,, Bosch, Dinion IP starlight 8000 MP,,,,,,,,
10.0.12.247, 80, Bosch, Dinion IP starlight 8000 MP,,,, Camera 3,,, Archive AliceBlue, On motion
```

> **Attention!**
>
> The vendor and model of the device must be specified exactly as in the list of supported devices.
>
> For correct display of the object name in *Axxon One*, the CSV file must be UTF-8 BOM or UTF-32 BOM encoded.

2. Upload the created file using the Drag&Drop method in one of the following ways:
   - using the IP Device Discovery Wizard in *Axxon One*.



   - using the form for adding CSV files.



Note

- If *Axxon One* is running in the safe mode, the CSV file must be dragged&dropped to the IP Device Discovery Wizard from the application window, which is running with the administrator rights.
- If you add a CSV file with incorrectly specified camera models or parameters, pop-up windows with warnings or error messages will be displayed. If the file is successfully uploaded, a pop-up window with success message will be displayed.

The specified devices will be added to the configuration.

Configuring system objects for devices

The Server Object

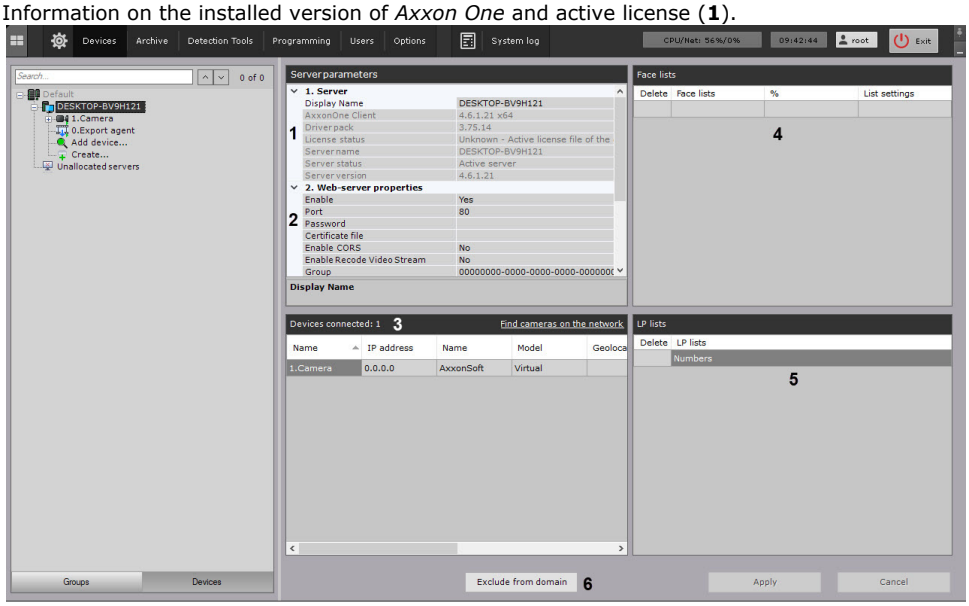
The **Server** object corresponds to a computer:

- on which *Axxon One* is installed in the **Server and Client** configuration;
- is on the Axxon-domain.

The name of the **Server** object is the same as the computer's network name by default. To change it, enter the new name in the corresponding **Display Name** field **1** and click the **Apply** button.

Click the **Server** object to view the following information:

1. Information on the installed version of *Axxon One* and active license (**1**).



2. Web-Server configuration options (**2**, see Configuring the Web-Server).
3. A list of video cameras connected to the Server, with the main parameters (**3**). Cameras are listed in a table with the following columns: **Name**, **IP address**, **Name**, **Model**, **Geolocation**, **Azimuth**, **Video Stream, Frame Rate** and **Resolution**. You can sort the table by columns.

> **Note**
>
> If no cameras have been created on a Server, you are prompted to search for IP devices on the network (the IP Device Discovery Wizard is launched, see Searching, adding, configuring and removing IP devices).

> **Note**
>
> The number of connected devices means the total number of available IP video channels, including disabled.

4. Created lists of facial templates (**4**, see Configuring face recognition based on the created lists).
5. Created ANPR lists (**5**, see Configuring vehicle license plate recognition based on the created lists)
6. The button to remove Server from an Axxon-domain (**6**, see Removing a Server from an Axxon-domain).

Configuring the Web-Server

The Web-Server allows accessing *Axxon One* remotely over the Internet (see Working with Axxon One through the Web-Client).

Attention

- On the local computer with the Web-Server running, ports from the range [9001; 9001 + number of logical cores of the processor] must be open.
- Except for H.264 format, the Web-Server transcodes the incoming video image using the MJPEG compression algorithm, which can result in high levels of incoming traffic.

To configure the Web-Server in *Axxon One,* do the following:

1. Select a **Server** object.

Server parameters		
	2. Web-server properties	
1	Enable	Yes
2	Port	80
3	Certificate file	
4	Enable CORS	No
5	Enable Recode Video Stream	No
6	Private key file	
	RTSP port	554
	RTSP/HTTP port	8554
7	SSL port	443
8	URL path	/

2. By default, the Web-Server starts automatically together with the Server. If you want to disable the Web-Server, set the value of the **Enable** parameter to **No** (**1**).
3. In the **Port** field, enter the port number on which the Web-Server will be located (**2**).
4. To connect to the Web-Server via the SSL port only, do the following:
   a. Enter the SSL port number to connect to the Web-Server (**7**).
   b. Specify a path to the private key file (**6**).
   c. Specify a path to the certificate file (**3**).

   Attention!

   - *Axxon One* supports SSL certificates in PEM format with TLS encryption v 1.2 and 1.3 and AES GCM, AES CCM and AES CBC algorithms.
     The public key must be in CRT format, the private key must be in KEY format.
   - If the private key file and certificate file are not specified in the Web-Server settings, the connection to the Web-Server will be made via **HTTP Port** only.

5. If the Web-Server should use the CORS mechanism, enable the corresponding parameter (**4**).
   Axxon One supports the following:
   a. CORS HTTP-headers for GET and POST requests.
   b. Preflight requests.
6. If the Web-Server must transcode the stream, enable the corresponding parameter (**5**). By default, the Web-Server doesn't transcode the stream, which helps to avoid unpredictable CPU load on the Server. For example, if the browser cannot playback a video in H.265 format, you must switch to a browser-supported video codec (see Real-time video surveillance in the Web-Client) or change the video codec of the camera to the video codec supported by the browser (see The Camera object).
7. In the **URL path** field, enter the prefix that is added to the Server address (**8**).
8. Click the **Apply** button to apply the configured parameters and restart the Web-Server.

The Web-Server is now configured and available over the Internet at the following address: http://<IP address of *Axxon One* Server>:<Port>/<Prefix>. For example, if the Servers IP address is **10.0.11.1**, the port is **8000**, and the prefix is **/asip-api**, then the Web-Server can be accessed at the following address: http://10.0.11.1:8000/asip-api.

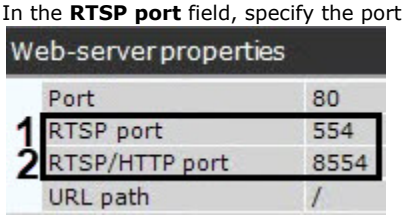
Working with Axxon One through the Web-Client

Configuring an RTSP Server

Axxon One supports RTSP streaming from cameras (see Get camera live stream and Get archive stream).

To configure an RTSP-Server:

1. Select a **Server** object.
2. In the **RTSP port** field, specify the port number that will be used for RTSP data transfer (**1**).



3. In the **RTSP/HTTP port** field, specify the port number for transfer of RTSP data via HTTP tunnel (**2**).
4. Click the **Apply** button.

Configuration of the RTSP Server is now complete.

To receive videos from an RTSP Server, use the following link format:

- **Live**: rtsp://login:password@IP-Address:554/hosts/HOSTNAME/DeviceIpint.N/SourceEndpoint.video:0:0 – high quality stream;
  rtsp://login:password@IP-Address:554/hosts/HOSTNAME/DeviceIpint.N/SourceEndpoint.video:0:1 – low quality stream.
- **Archive** rtsp://login:password@IP-Address:554/archive/hosts/HOSTNAME/DeviceIpint.N/SourceEndpoint.video:0:0 /20160907T050548.723000?speed=1.

where:

- **login:password** – user login and password in the *Axxon One* VMS.

  > **Attention!**
  >
  > For correct operation of the RTSP Server, a user name has to match the following rules:
  >
  > - start with a letter;
  > - contain only Latin, numerical and following extra characters: "/", "-", "_", ".", ":", "+".

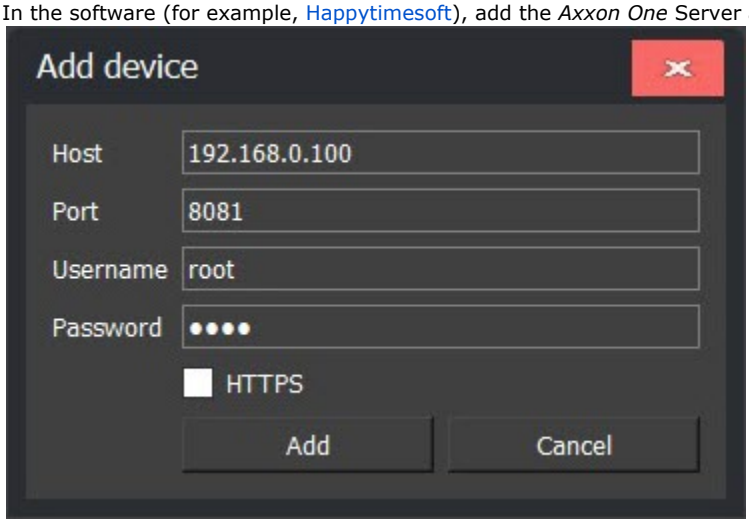
- **hosts** – permanent section of a link.
- **HOSTNAME** – Server name (should be written only in uppercase letters).
- **N** – camera ID in the *Axxon One* VMS.
- **SourceEndpoint.video:0**:0 – permanent section of a link.
- **speed** – a parameter required for receiving video streams from an Archive.

Configuring the ONVIF Server

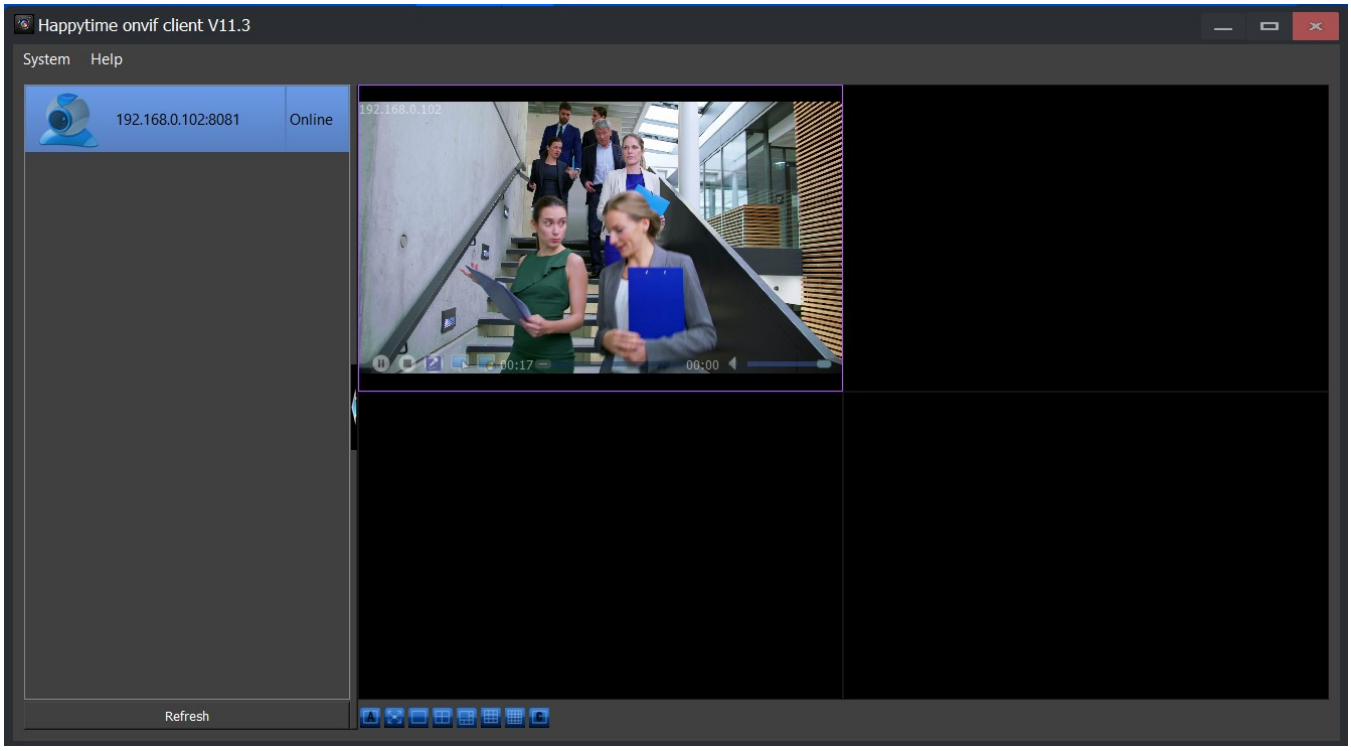
Axxon One has a built-in ONVIF Server using which *Axxon One* can be added as a video recorder to other software (for example, Onvif Device Manager (ODM) or Happytimesoft).

To configure the ONVIF Server, do the following:

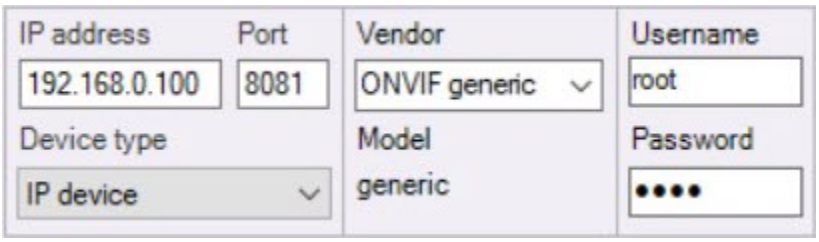
1. Install *Axxon One* 2.0 together with *DriverPack* 3.73.79 and later.
2. Shut down the Server (see Shutting down a Server).
3. Create the NGP_ONVIFSERVER_ENDPOINT system variable (see Appendix 9. Creating system variable). In the **Variable value** field,field, specify the IP address of the local *Axxon One* Server.
4. Start the Server (see Starting a Server).
5. In the software (for example, Happytimesoft), add the *Axxon One* Server as a device using the 8081 port.



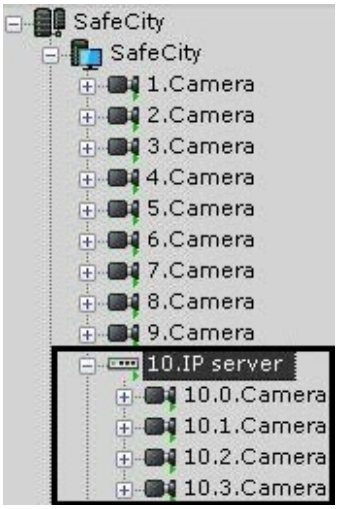
The ONVIF Server configuration is complete. The software will broadcast the video image from *Axxon One* in real time.



You can also add the ONVIF Server to another *Axxon One* Server as an ONVIF generic IP device (see Searching, adding, configuring and removing IP devices).



The ONVIF Server will be added to the configuration as an **IP server** (see The IP Server Object) with corresponding video cameras.



The Camera object

On this page:

- General information
- Configuring the camera parameters
  - Object identification parameters
  - Object features parameters
  - Authentication parameters
  - Video buffering parameters
  - Video stream parameters
  - Panomorph view parameters
  - Other parameters
  - Alternative view parameters
  - Geolocation parameters
- Camera preview window

General information

You can create and configure the **Camera** object on the **Hardware** tab. The objects tree of a camera is generated automatically according to its functions that are integrated into *Axxon One* (the presence of alarm inputs, relay outputs, PTZ device, and so on).

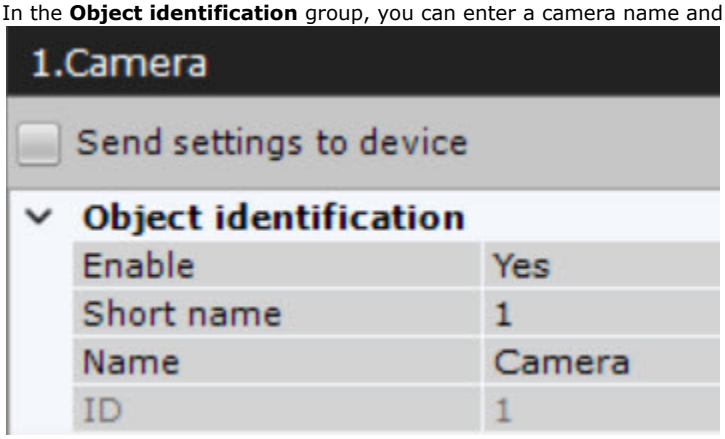
You can configure the camera recording to the archive on the **Archive** tab (see Configuring archives).

Configuring the camera parameters

When you have added a camera via the IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices), you can edit the camera's parameters. The camera parameters are grouped as follows.

Object identification parameters

In the **Object identification** group, you can enter a camera name and a short name.



By default, short name is a camera's ID. The camera ID cannot be changed, since it is used to maintain the connection with the archive when replacing the camera (see Saving the archive when replacing the video signal device). You can change short name, and the added devices will be sorted in the objects tree in ascending order of this field.

The full name of the camera in the objects tree is displayed in the <Short name>.<Name> format. You can use camera's short name in hotkeys (see Notes regarding hot key actions).

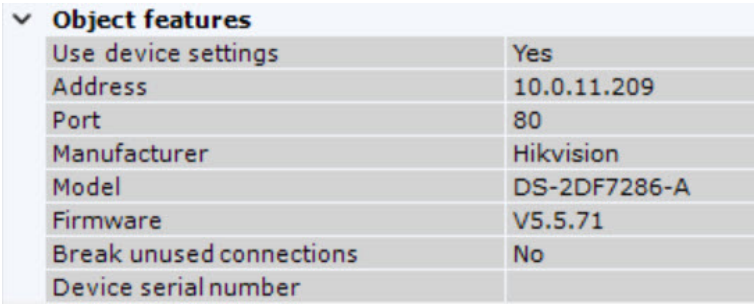
You can also disable a camera by selecting **No** in the **Enable** field.

> **Attention!**
>
> Every camera enabled in the system (including analog cameras, see The IP Server Object) is a video channel in terms of licensing (see Axxon One licensing). Disabled cameras are not subject to licensing. If you run out of camera licenses, disable offline/unused cameras.

Object features parameters

In the **Object features** group, you can see the following camera properties:

1. The IP address (assigned automatically and can be changed if necessary).
2. The port used to transmit data between a camera and *Axxon One* (this value is set to **80** by default, but can be changed if necessary). Initially, the port number is set via the camera's Web interface.
3. The MAC address.
4. Manufacturer, model, driver version, and current firmware.
5. The number of the video channel (for an IP Server).
6. Device serial number (for Axis devices only, see Axis IP Devices).



You can also configure a number of parameters shared by all cameras in this group:

1. If you want to use camera settings without overwriting them with the default settings specified in *Axxon One*, select **Yes** in the **Use device settings** field. This parameters is a reverse parameter of the **Send settings to device** checkbox, that is, when you enable one option, the other is automatically disabled, and vice versa.
2. If you want to interrupt video streaming from the camera to the Server whenever it is not needed, select **Yes** in the **Break unused connections** field.
   The following conditions must be met for the video stream transmission to be interrupted:
   a. the video stream is not displayed on either Client or Web-Client layout;
   b. the stream is currently not being recorded into archive;
   c. the stream is currently not being processed by any detection tool.

Authentication parameters

In the **Authentication** group, you can set the username and password to connect to the camera.

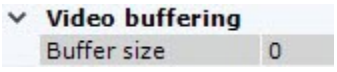


If the username and/or password for connecting to the camera are different from the factory settings, select **No** in the **Default** field and enter the current credentials.

> **Attention!**
>
> If the camera supports the Digest HTTP authorization, add the " **:** " character to the last character of the password.

Video buffering parameters

If you want to accumulate the data received from a camera to the buffer on the Clients and transfer them for processing from the buffer, set the buffer length in milliseconds in the **Video buffering** group. This value must be between 50 and 1000 milliseconds. If the **0** value is selected, video buffering is disabled.



Video stream parameters

In the **Video stream settings** group, you can see video image parameters (contrast, brightness, color saturation, and so on). When configuring these, you can look up their descriptions in *Axxon One* interface. For more detailed information, refer to the camera manual.

Video stream settings	
Brightness	50
Color Saturation	50
Contrast	50
Day/Night Autoswitch Time	50
Exposure Mode	Auto
Flicker-free	50
Image Flip	None
IR Cut Filter Sensitivity	Medium level
IR Cut Filter	Auto
Sharpness	50
Shutter Speed	1/50
WDR Level	0
White Balance	AWB1
Wide Dynamic Range	None

Note

You cannot edit these parameters if you added the camera in the **Keep current settings** mode (that is, with the parameters that were set in the web interface, see Searching, adding, configuring and removing IP devices). To be able to configure these parameters, you need to set the **Send settings to device** checkbox.

Once you set a checkbox for a camera, the checkbox is also set on all its channels and child objects.

Panomorph view parameters

In the **Panomorph** group, you can configure fisheye cameras (see Configuring fisheye cameras).

Panomorph	
Activate	No
Camera position	Wall
Lens type	Common fisheye-lens
View type	PTZ
Fit to frame	No

Other parameters

In the **Other** group, you can configure the parameters for the devices connected via the RTSP protocol (see Configuring connection of devices via RTSP).

Other	
Enable	Yes
ID	0
Name	Camera
Comment	
Default archive	hosts/
Profile	High profile
Reconnection timeout	10
RTP packet reordering	Yes
Timeout	10
Video channel No.	0

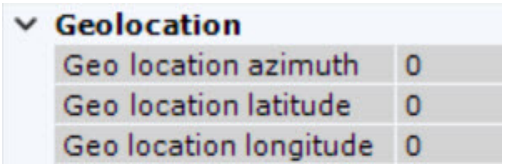
Alternative view parameters

In the **Alternative camera 1** field, you can specify any camera in the current domain that can replace this camera on the layout when it isn't connected.

Alternative view	
Alternative camera 1	**1.Camera**
Alternative camera 2	**3.Camera**

Geolocation parameters

In the **Geolocation** group, you can specify the coordinates (latitude, longitude, azimuth) of the camera location (the coordinates are used when adding the camera to the geomap, see Adding video cameras).

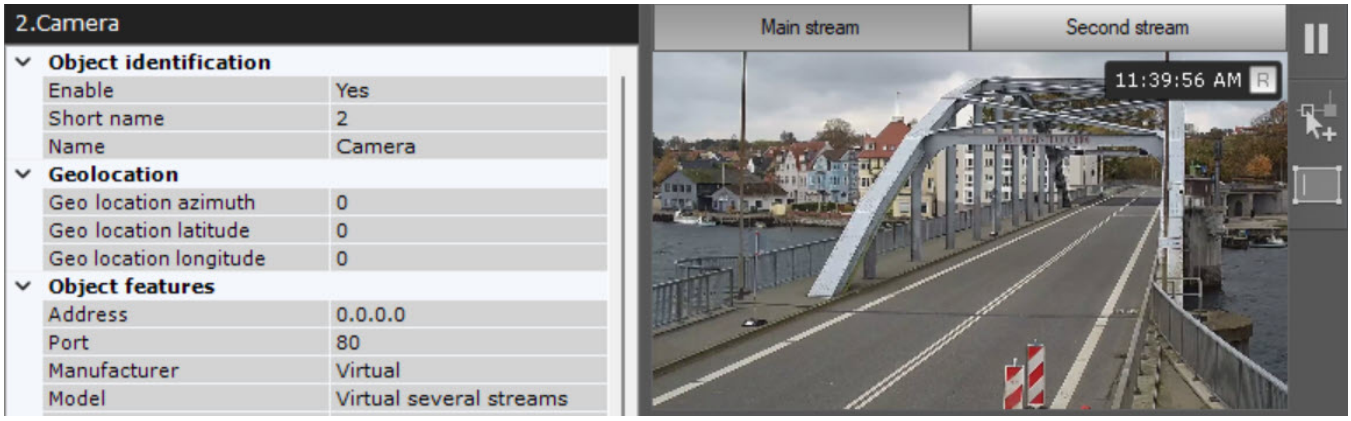


> **Note**
>
> When you specify the coordinates, only 6 decimal points are taken into account.

In a special case, when configuring an alarm layout (see Configuring Alarmed cameras layout), in these fields, you can specify the closest cameras to this one for simultaneous display.

Camera preview window

The preview window displays the video image from this camera.



If the camera supports multistreaming, then the **Main stream**, **Second stream** and other tabs are available in the window, depending on the number of added video streams (see Configuring video stream settings).

> **Note**
>
> - The indicator in the upper right corner displays the current time and recording status (see Time Display).
> - When a stream is selected in the preview window, the settings for the relevant stream are displayed. The settings for the other stream are hidden.

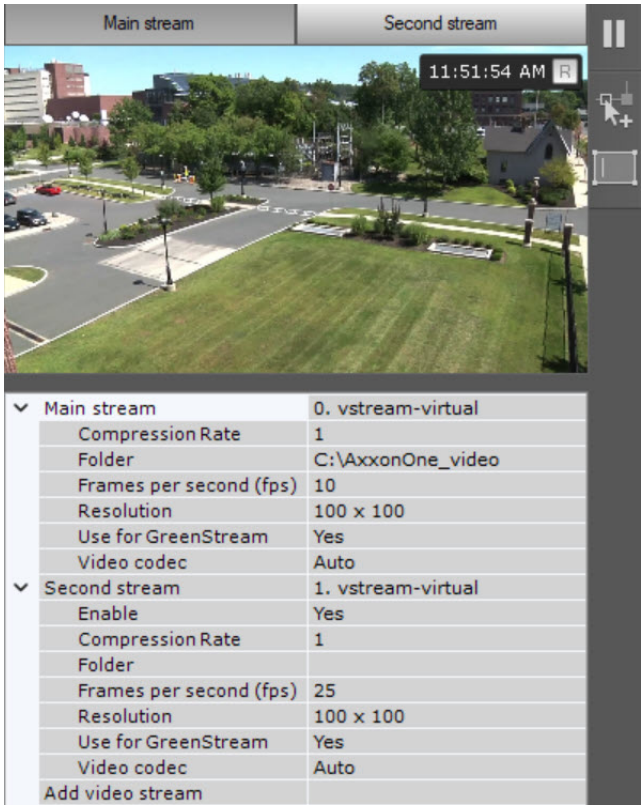
Configuring video stream settings

On this page:

- Video stream settings
- Changing the camera video streams

Video stream settings

You can configure video streams below the Surveillance window.



If the camera supports multistreaming, then when creating a camera, the stream with a higher resolution is selected as the main stream.

It is also possible to separately configure video streams: the **Main stream** and the **Second stream**. If necessary, you can configure additional video streams (third, fourth, etc.) using the **Add video stream** field.

In most cases, the following parameters are set for each stream:

- bitrate,
- compression rate,
- frame rate,
- resolution.

Detailed information on configurable parameters can be found in the official reference documentation for the camera.

Note

You cannot edit stream parameters if the camera was added in the **Keep current settings** mode (i.e. with the parameters that were set in the web interface, see Adding and removing IP devices). To be able to configure these parameters, you need to set the **Send settings to device** checkbox (see The Camera object).

By default, all added camera video streams are enabled. If necessary, you can disable the second, third and other additional video streams by selecting **No** in the **Enable** field. The main video stream of the camera is activated by default and cannot be disabled.

The **Use for GreenStream** parameter is designed to display video streams in Auto (GreenStream)/High quality/Low quality modes (se e Selecting video stream quality in a Surveillance window (GreenStream)).

Set one of the following values:

- **Yes**, to display the video stream in these modes.
- **No**, to exclude the stream from display in these modes.

If you configure video streams in the camera web interface, it is necessary to set the real value of the expected frame rate in the corresponding field to correctly display the video stream status on the Health Board (see Viewing camera status).

Attention!

- You can select any video stream for recording into archive and displaying in the Surveillance window (see Selecting video stream quality in a Surveillance window (GreenStream), Configuring recording to an archive).
- For some detection tools, you can select any video stream on which you want to perform detection (see Configuring detection tools).

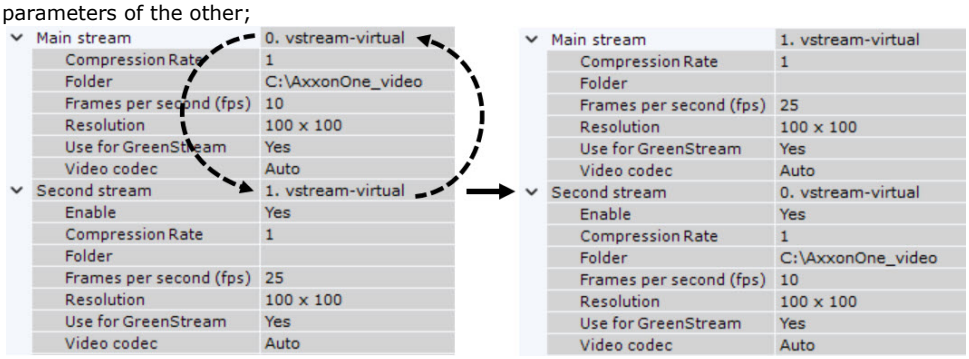
Changing the camera video streams

In *Axxon One*, each stream is assigned a corresponding video camera stream profile, for example:

Stream indication in *Axxon One*	Camera stream profile (profile name is determined by the driver)
Main	0. video_streaming_h264_QSXGA
Second	1. video_streaming_h264_VGA
Third	2. video_streaming_mjpeg

If necessary, you can change the profile for the stream, in this case:

- if a profile has already been added as a main or additional stream, the parameters of one stream are replaced with the parameters of the other;



- if a profile has not yet been added as a main or additional stream, the parameters of this video stream are changed to the default parameters.

Note

When some video stream parameters are changed, the camera may automatically restart, in which case it will become unavailable for some time (depending on the camera).

You can also change the video stream settings by sending an HTTP request to the device (see the manufacturer's official documentation) using macros (see Executing a web query, Starting an external program on Servers, Starting an external program on Clients).

Privacy mask settings

It is possible to apply a privacy mask to the video image to hide certain parts of the frame:

- when viewing live videos;
- when viewing the archive;
- on exported videos and still frames.

The detection tools that support privacy mask:

- Configuring the Face Detection TV;
- Configuring the Face Detection VL;
- Configuring Face Detection and Temperature Control;
- Masks Detection (detection of a medical or similar mask on the face);
- Configuring the Person-Based Privacy Masking;
- Configuring the People masking (based on data from pose detection tools).

Privacy mask will apply to all users who have the **View masked video** parameter set to **No** in the role configuration (see Creating and configuring roles).

Attention!

The mask will be displayed in the Client only. In the Web-Client and the Mobile Client, there will be no mask on the video image.

To configure privacy mask, do the following:

1. Select the **Video Camera** object and click the  button.

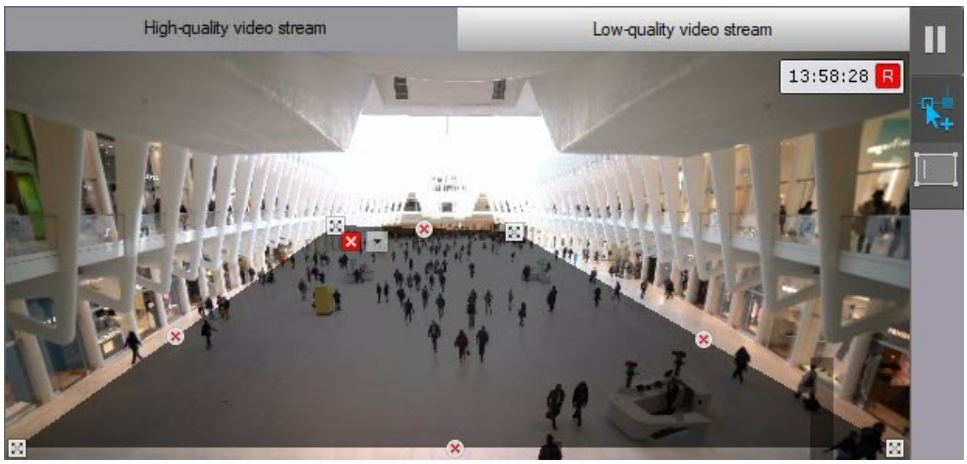
   Note

   The button is inactive, if the text overlay button is active  (see Putting a text over the camera window).

   Note

   For your convenience, you can click the  button and configure the mask on a still frame. To undo, click this button again.

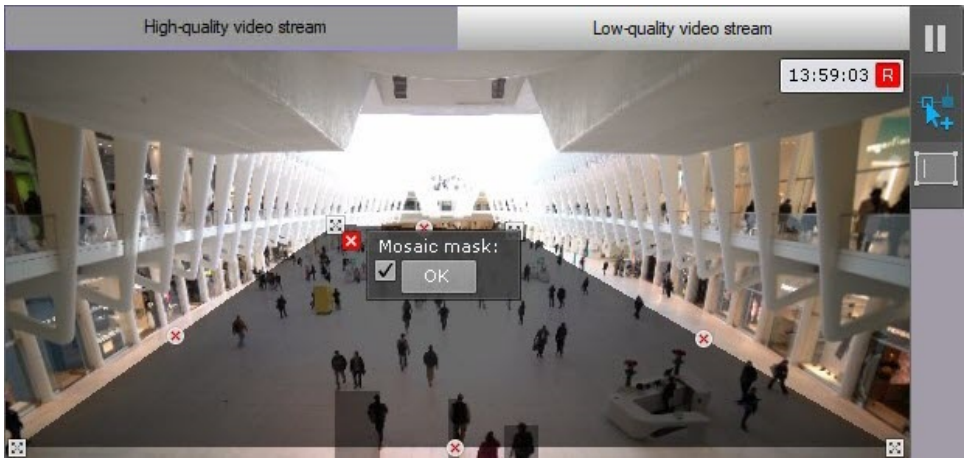
2. In the preview window, sequentially set the anchor points of the closed area that you want to hide when viewing the live video image.



> **Note**
>
> When the area is being constructed, the anchor points are connected by a two-color dotted line which outlines the area's borders.

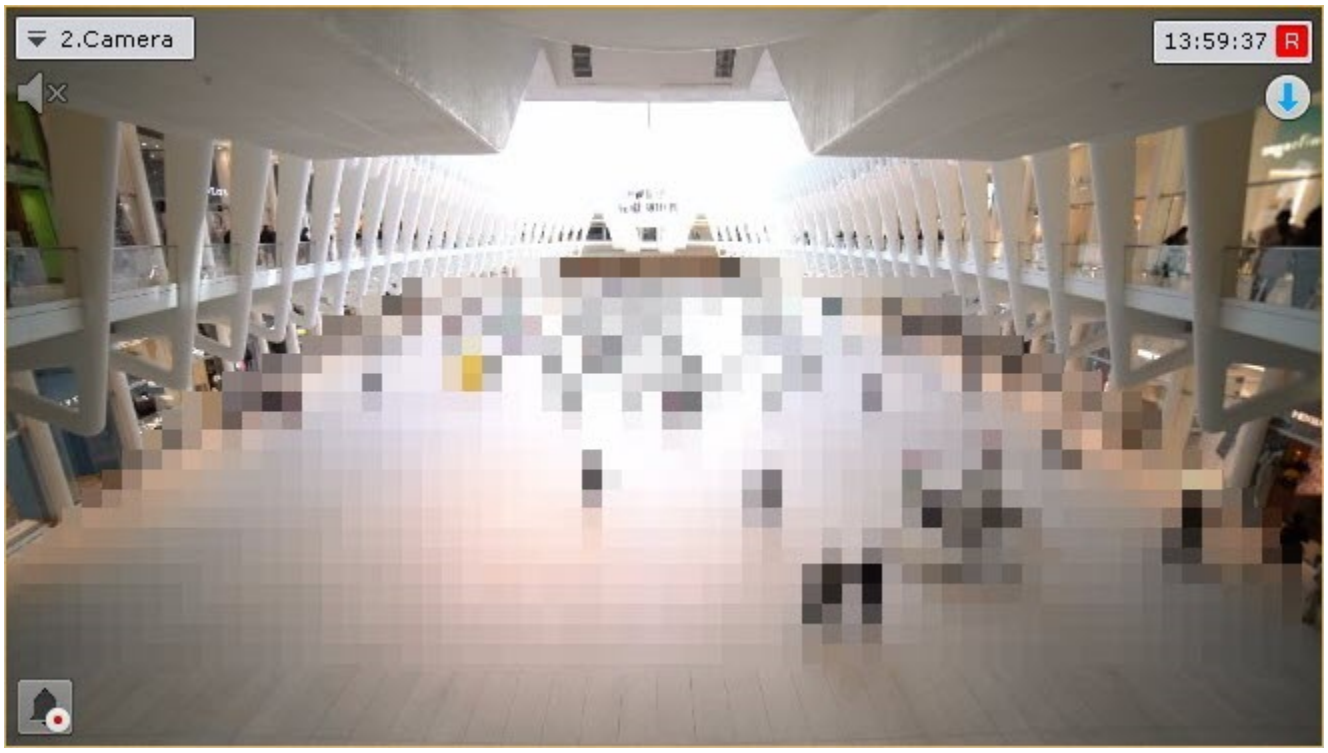
Action	Result
Left or right click in the video surveillance window	Create a new anchor point in the area
Right click on a created anchor point	Delete the area anchor point
Point the cursor to an anchor point and holding the left mouse button, move the mouse	Move the area anchor point
Click the button	Delete the area

3. You can mask the selected area with black color (by default), or with a mosaic mask. To apply the mosaic mask, do the following:
   a. Click the button.
   b. Set the checkbox.



   c. Click the **OK** button.
4. You can specify several areas.
5. Click the **Apply** button.

Privacy mask configuration is complete. When you view a video image from this camera, the selected area will be hidden.


2.Camera
13:59:37
R

Putting a text over the camera window

You can superimpose a text over video in the camera window. This text will be visible to all users in all monitoring modes but will not be present on exported frames and videos.

To put a text over the camera window, do the following:

1. Select a **Camera** object and click  .

   Note

   You cannot do it if the  button is depressed (see Privacy mask settings).

   Note

   For your convenience, you can click the  button and configure the mask on a still frame/snapshot. To undo, click this button again.

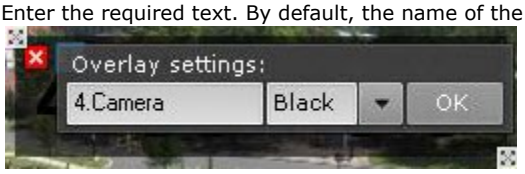
2. Click any mouse button anywhere in FoV to set two anchor points  of the rectangular area where the text will be displayed. The higher the area, the more the font size.



   Note

   To remove the area, click the  button.

3. Click  .
4. Enter the required text. By default, the name of the video camera is displayed.



   Attention!

   The text string has to fit the width of the area. If not, you cannot apply settings. For a longer text, make the area wider.

5. Select a font color from the dropdown list.
6. Click the **OK** button.
7. If required, you can set multiple text areas in different parts of FoV.

8. Click **Apply**.

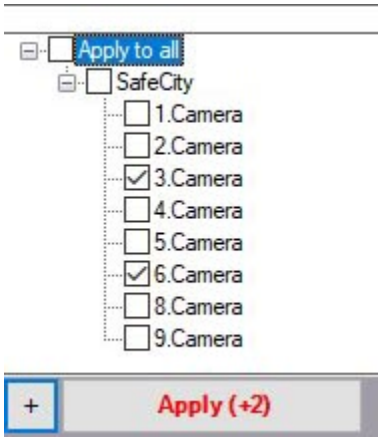
Now, the text is superimposed over the video image.



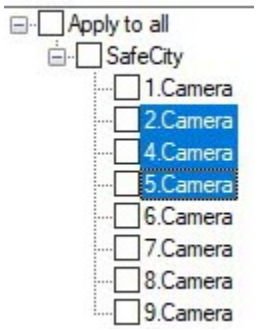
Mass configuration

You may bulk configure cameras of the same model and firmware. Do the following:

1. Configure any camera.
2. Click the + button and select cameras the same settings should be applied to.



A list of cameras of the same model and firmware opens. To quickly select multiple cameras, hold down the Shift key, select the first and last cameras the settings should be applied to. Selecting any camera from highlighted ones will result in selecting them all.



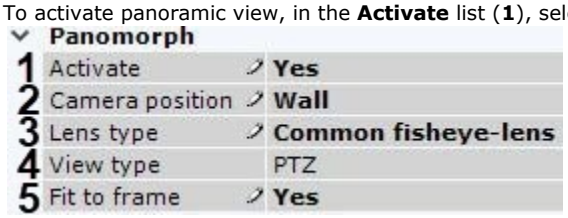
3. Click the **Apply** button.

> **Note**
>
> The number in brackets refers to the number of configured cameras.

Configuring fisheye cameras

If you are using a fisheye camera or video camera with a panomorph lens, configure the following settings of the **Video camera** object, in the **Panomorph** settings group:

1. To activate panoramic view, in the **Activate** list (**1**), select **Yes**.



2. In the **Camera position** list (**2**), select the mount of the video camera.

> **Attention!**
>
> Some system features and functions depend on the chosen position of the video camera: digital zoom, display of video in the surveillance sector on the map, and immersive mode.

3. If it is a fisheye camera, select the **Common fisheye-lens** lens type (**3**). If it is a video camera with a panomorph lens, select the corresponding type. When using wide angle dual lens XingYun devices, select the **Double sphere fisheye-lens** type.

> **Note**
>
> The types of device lenses certified by ImmerVision are listed in the document. You cannot select ImmerVision lenses in Linux.

4. If it is a video camera with an Immervision lens, select the appropriate display mode (**4**): 360° panorama with virtual PTZ (**PTZ**) or 180° panorama (**Perimeter**).
5. A typical fisheye lens with standard settings produces a skewed image in the upper part of the screen. If this is the case, enable the **Fit to frame** option (**5**)**.**

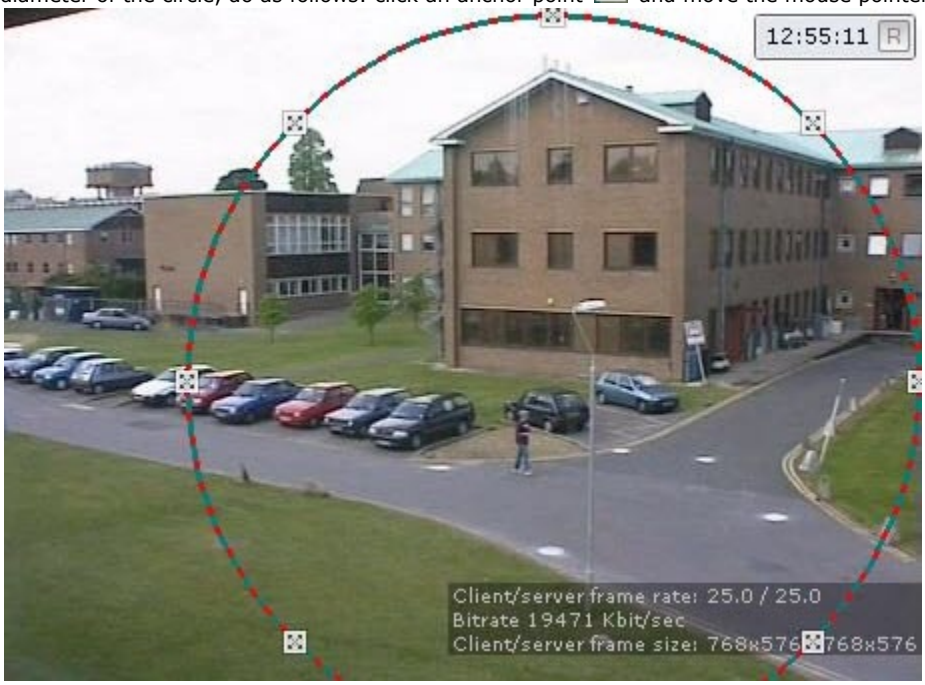
> **Attention!**
>
> If you have multiple streams from a camera, you need to calibrate each stream. To do this, before applying the settings, switch to the required stream tab in the Surveillance window (see The Camera object).

> **Attention!**
>
> Video is calibrated every time you change any parameters in the **Panomorph** group.

Manual calibration is also available. To do this:

a. Disable **Fit to frame**, select **No** in the **Enable** list and click the **Apply** button.
b. Select **Yes** in the **Enable** list.

c. Configure the video area (circle). Left-click any point inside the circle and move the mouse pointer. To change the diameter of the circle, do as follows: click an anchor point and move the mouse pointer.



d. Click the **Apply** button.

After applying the settings, the area outside the circle will be cut.

Configuration of the fisheye camera is complete.

Connecting and configuring cameras over standard protocols

Features of configuring and working with cameras connected via ONVIF

On page:

- Connection through ONVIF Generic driver
- Resolution
- IP devices on other subnets (behind a NAT)
- IP devices which partially support the ONVIF protocol

By default, all ONVIF devices in the system are added as multistreaming (the **ONVIF 2.0** driver, see Searching, adding, configuring and removing IP devices).

If the camera does not support multistreaming, then the video stream of lower quality will be disabled.

Note

In some cases (for example, if you do not have video from a camera), you may need to synchronize the time between the server and the camera when you connect them via ONVIF.

Attention!

If you connect cameras via ONVIF, auto focus (AF) and auto aperture are not available.

Connection through ONVIF Generic driver

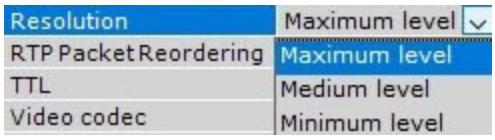
With the ONVIF Generic driver, you have the following options:

1. **Currently offline cameras can transfer their settings when they get back online.**
   To make it happen, follow the steps below:
   a. Add a camera via the ONVIF Generic driver (see Generic Drivers (General device, generic)).
   b. When the device comes online, reset its parameters (see Applying and resetting settings).
   c. Load the configuration from the device (see Applying and resetting settings).
2. **You can select another camera in object settings while keeping all layouts, macros and archive storage parameters.**
   To make it happen, follow the steps below:
   a. Add a camera via the ONVIF Generic driver (see Generic Drivers (General device, generic)).
   b. Set archive storage parameters and create macros.
   c. In **Camera** object settings, specify a new IP address and user credentials (see The Camera object).
   d. Reset device settings (see Applying and resetting settings).
   e. Load the configuration from the device (see Applying and resetting settings).

This operation will result in swapping cameras without the need to create a new object and remove the old one.

Resolution

Axxon One offers three resolutions for video from cameras connected via ONVIF: maximum, medium, and minimum.



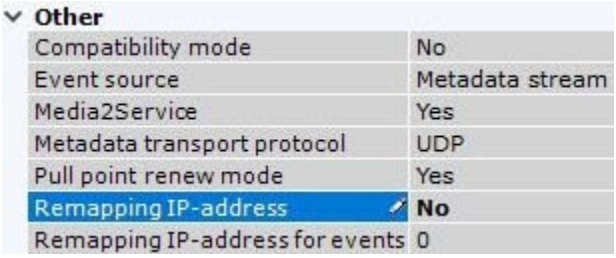
A description of the resolution levels is given in the table.

Camera type / Resolution	Maximum	Medium	Minimum
Non-megapixel	Maximum camera resolution	Average camera resolution	Minimum camera resolution
Megapixel	Maximum camera resolution	Camera resolution closest to 1024x768	Camera resolution closest to 640x480

IP devices on other subnets (behind a NAT)

By default, NAT-friendly mode is enabled for cameras connected via the ONVIF driver.

To disable NAT-friendly mode, in the settings of a camera, select the **No** value for **Remapping IP-address**.



IP devices which partially support the ONVIF protocol

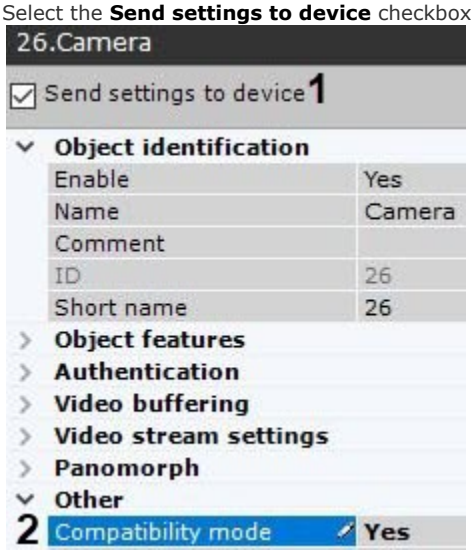
To connect IP devices which only partially support ONVIF functions to the *Axxon One* software package, you must use an ONVIF driver with compatibility mode enabled.

> **Note**
>
> Such video cameras include Hikvision models and early versions of firmware from Sony, Samsung, and others.

Compatibility mode makes it possible to receive a video image from video cameras; however, some capabilities of the *Axxon One* software package will be unavailable. Enabling compatibility mode is recommended if the connection settings are correct, but there is no video image.

To enable it you need:

1. Select the **Send settings to device** checkbox (**1**).



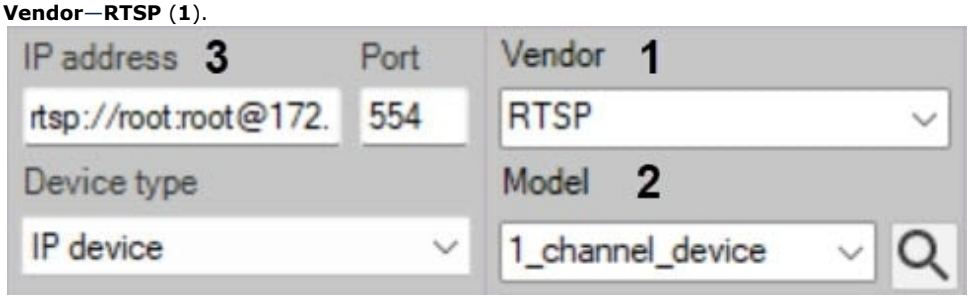
2. Select **Yes** for **Compatibility mode** (**2**).

Configuring connection of devices via RTSP

Configuring connection of single-channel devices

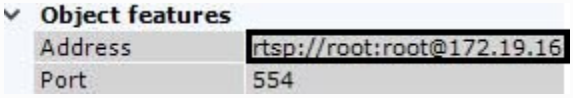
To connect a camera via the RTSP protocol using the IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices), add a camera with the following parameters:

1. **Vendor**—**RTSP** (**1**).



2. **Model**—**1_channel_device** (**2**).
3. IP address—the address of RTSP transmission (**3**). In general, the address has the following format: **rtsp://<IP address of RTSP server>:<Port of RTSP server>/<Path>**. The RTSP protocol camera connection supports up to three video streams. To connect multiple streams, enter the transmission addresses separated by a semicolon: **rtsp://<IP address of RTSP server1>:<Port of RTSP server1>/<Path>**; **rtsp://<IP address of RTSP server2>:<Port of RTSP server2>/<Path>** ; **rtsp://<IP address of RTSP server3>:<Port of RTSP server3>/<Path>**.

> **Attention!**
>
> Generally, the RTSP Server parameters (port and path) are set via the web interface of the camera. To do so, refer to the reference documentation for a particular camera.
>
> If the username or password in a URL contain invalid characters, such as "@", you have to escape these characters with special characters via the ASCII codes (in hexadecimal form). The "@" character is escaped as %40. For example, when connecting a device via RTSP, the link may look like this "rtsp://admin:New%40edge@192.168.0.75:554/RVi/1/1".

> **Note**
>
> In some cases, the address format may be different. For example, a username and password may be added to the address to connect to the camera if authentication is required.
>
> 
>
>
> It is recommended that you refer to the reference documentation for a particular camera.
>
> Even if the password field is empty, the address string must include a colon (:).
>
> A correct address may look like this: rtsp://user:@10.10.27.50:10017/...
>
> An example of an incorrect address: rtsp://user@10.10.27.50:10017/...

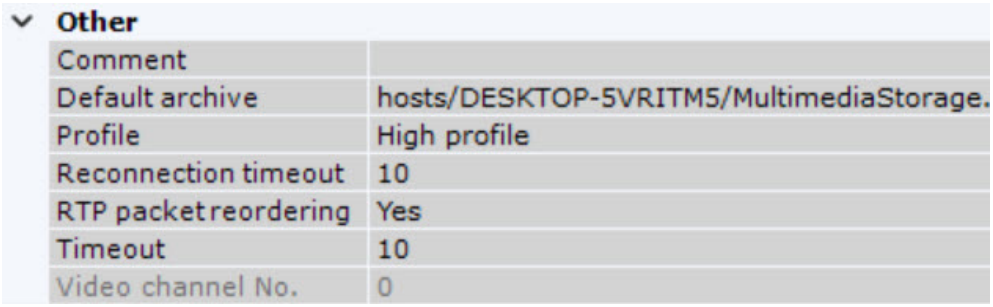
The **Camera** object will be created. If the address of the RTSP transmission is correctly specified, the preview window will display the image from this camera.

> **Note**
>
> **Port**, **Login** and **Password** can not be edited. These settings are specified in the transmission address.

If video is unavailable, refer the APP_HOST.lpint log file located in the <*Axxon One* installation folder>\Axxon One\Logs folder.

> **Attention!**
>
> If the APP_HOST.lpint log file is empty, in the log management utility, check the logging level of the *Axxon One* Server (see Configuring the logging levels). The recommended logging level is **Debug**.

To set the time in seconds after which a message about the loss of connection with the camera will be displayed, specify the value in the **Timeout** field in the camera settings.

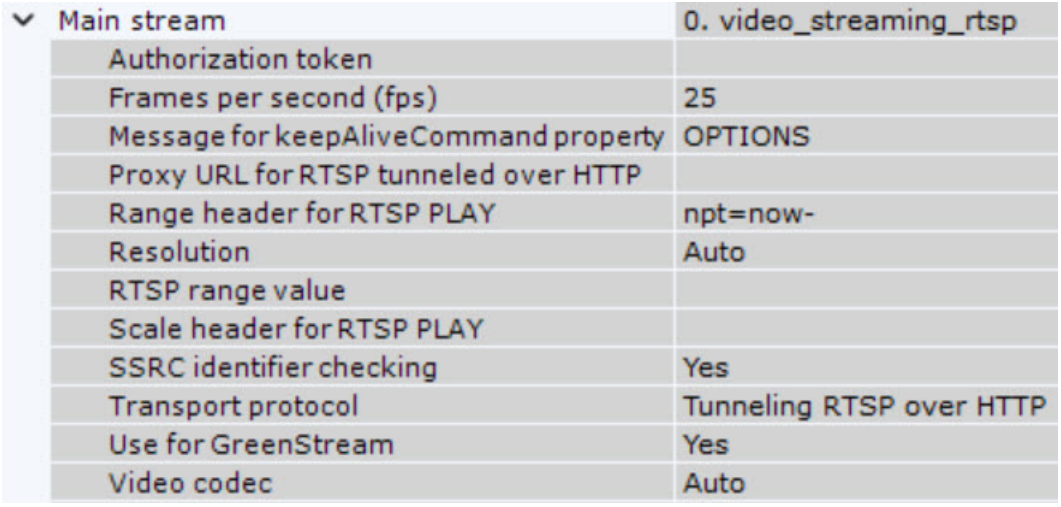


If you want to set the time in seconds after which the reconnection to the device will take place, specify the value in the **Reconnection timeout** field.

In the **Profile** field, you can select the level of the H.264/AVC video codec profile:

- **Basic profile** provides a more effective usage of resources and a low bitrate video transmission, but may have limited resolution and number of frames per second.
- **High profile** provides a higher video quality, higher bitrate, higher resolution and more frames per second. High profile is used to transmit high definition video and video at the speed of 60 frames per second.

To receive the RTSP stream via HTTPS, select the **Tunneling RTSP over HTTP** value for the **Transport protocol** parameter.



In some cases, packets may be lost or delayed due to poor connection. This may cause some packets to arrive later than the next packets in the transmission order. To change the packet arrival order, set the **Yes** value in the **RTP packet reordering** field.

Attention!

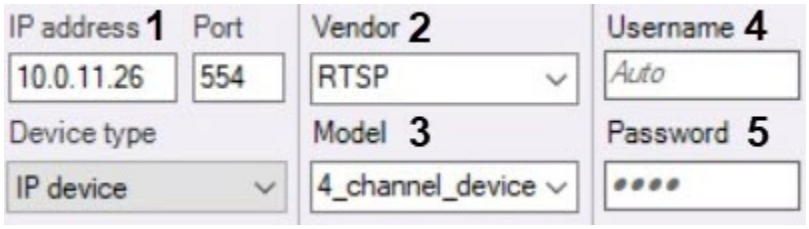
- To get good video stream from some cameras, set the **No** value for the **SSRC identifier checking** parameter in the video stream settings.
- Sometimes the camera's live stream frame rate may be displayed incorrectly. To display the frame rate more accurately, in the **Buffer size** parameter, specify a value in milliseconds. The value should be in the range from 50 to 1000 milliseconds, and should be selected empirically.

Configuring connection of multi-channel devices

To connect multi-channel devices (e.g. DVRs) over RTSP, do as follows:

1. Go to IP Device Discovery Wizard and open the manual addition field (see Searching, adding, configuring and removing IP devices).
2. In **IP address**, enter the device address (**1**).

> **Attention!**
>
> Following the IP address, add the";" symbol. Otherwise some channels may fail.

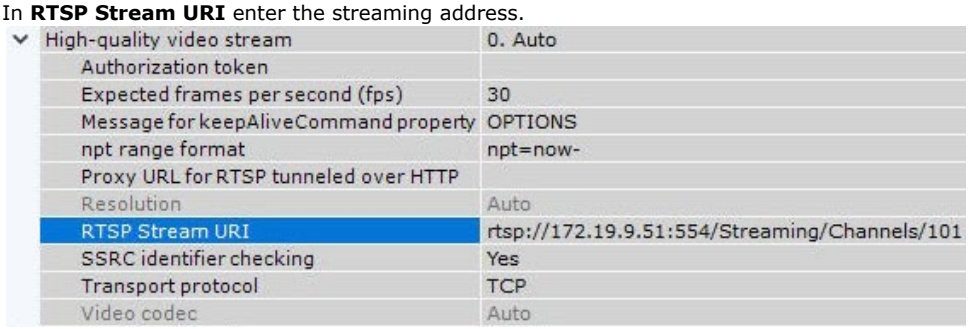


3. Select **RTSP** in the **Vendor** field (**2**).
4. In **Model**, select the model name, that shows the corresponding number of device channels (**3**). For example, for a four-channel device, select **4_channel_device**.
5. Enter the username (**4**) and password (**5**).
6. Click  .

A parent IP server object will be created hosting a number of video cameras objects equal to the number of channels on the device.

To configure channels, do as follows:

1. Select a child **Camera** object.
2. In **RTSP Stream URI** enter the streaming address.



3. Repeat the steps for all channels.

Generic Drivers (General device, generic)

General Device is a generic driver that supports nearly all devices from a particular camera vendor.

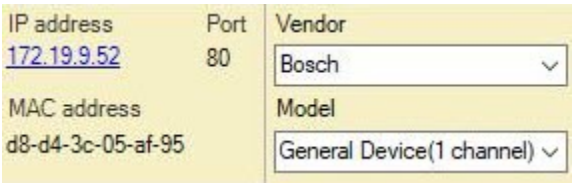
There are 2 types of generic drivers:

1. **General device**. Most configuration of General Device-connected cameras is performed via the web interface of the device. A detailed list of supported features is given on the Documentation Drivers Pack page.
2. **generic**. When connected via a generic driver, the configuration of the device is read and transferred to *Axxon One*. After that, you can configure the device from within *Axxon One*.

Connection via generic drivers is available for the following devices:

	Axis	Bosch	Panasonic	Samsung	Sony	ONVIF
General Device	+	+	+	+	+	
generic	+	+	-	-	-	+

Devices connected via General Device drivers are findable via the IP device discovery wizard. The method for adding them to the system is the same as for ordinary devices (see Searching, adding, configuring and removing IP devices).



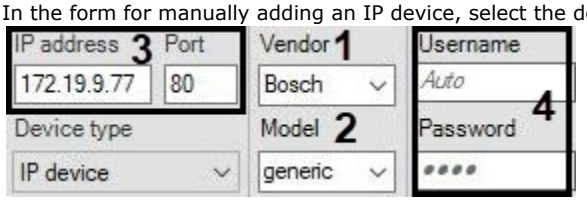
Note

Axis devices are affected by a special restriction: if the user name and password for device access do not equal the default values, the number of channels for the device is not discoverable. Therefore, all non-integrated devices whose user name and password for device access do not equal the default values will be shown in search results as 1-channel General Devices.

You should always select a generic driver manually.

If a IP device is not displayed in search results, you can add it manually:

1. In the form for manually adding an IP device, select the device manufacturer from the list (**1**).



2. In the **Model** field, select **General Device** or **generic** (**2**). For Axis and Bosch General devices, select the number of channels on the device.
3. Enter the IP address and port for the device connection (**3**).
4. Enter the user name and password for connecting to the device (**4**).
5. Click the  button.

Addition of the device is now complete.

Attention!

If a device, connected via a generic driver, is temporarily not available or it has incorrect connection settings, then it is not added to the configuration.

Connecting cameras via the GB/T28181 protocol

On the page:

- General information on GB/T28181 standard and supported functions
- Configuring an IP-device to operate via GB/T28181 standard
- Configuring IP-device connection via GB/T28181

General information on GB/T28181 standard and supported functions

Axxon One supports connecting devices via the Chinese standard GB/T28181. This standard is based on SIP over UDP (and over TCP since GB/T28181-2016). The GB/T28181 uses the following protocols over SIP:

- SDP (Session Description Protocol);
- MANSCDP (Monitoring and Alarming Network System Control Description Protocol);
- MANSRTSP (Monitoring and Alarming Network System Real Time Streaming Protocol).

This allows receiving the status of sensors, events from detectors, PTZ and relays control, access the built-in archive of the IP device (make sure to set the correct device time zone in the *Axxon One*), etc. within the SIP session. Single-channel and multi-channel devices in single-stream mode and working with the UDP and TCP transport protocols is also supported.

At the same level of the OSI model, the RTP/RTCP protocol also works in parallel with the SIP protocol, which makes it possible to use the following functions:

- video transmission (including archival) in H264, H265, or MJPEG format;
- audio transmission in G.711a, G.711u, or G.726 format in PS (Program Stream) only. Archive audio is not supported.

For the most up-to-date information on this standard and the features supported in *Axxon One*, see the Documentation Drivers Pack.

Configuring an IP-device to operate via GB/T28181 standard

Configuration of IP devices connected via GB/T28181 is performed through the web interface of the devices. Settings are not sent from *Axxon One* to the device.

Before connecting a camera via this protocol to *Axxon One*, perform the following steps to configure SIP on the device:

1. Set the Server IP to equal the Server's IP address.
2. Set the Server port (5060 by default).
3. Set the Device ID. The ID should be set on all cameras connected via the GB/T28181 protocol and must be unique. The format of the connection code (device ID and server ID) is a 20-digit number:
    a. the first 10 digits specify the address (according to the GB/T-2260-2007 standard);
    b. the next 10 digits indicate device information.
    If the IP device is located behind NAT, then forward and explicitly specify the external address of the Server, the port /port range for receiving video, and the SIP port of *Axxon One* Server. Example: 34020000001110000001/50557-51557@10.3.3.11/85.172.174.36
4. For the device to perform autodiscovery of the Server more quickly, reduce the default value of RefreshRegTime. The name of this setting may vary on some cameras.

Note.

For telemetry to work correctly, set RefreshRegTime to more than 600.

Examples of IP device settings for connection via GB/T28181 standard

Configuring IP-device connection via GB/T28181

Important!

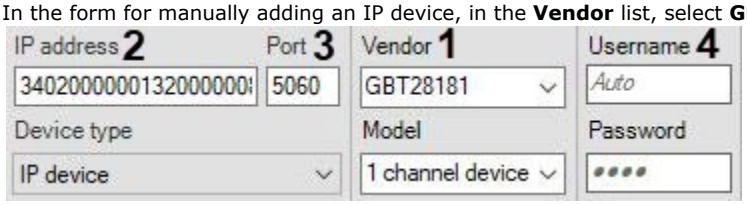
No more than one SIP server can be used for IP devices connection via the GB/T28181 protocol. This means that several **Video Capture Device** objects with **GBT28181** type can be created in the *Axxon One* hardware tree, however, the part of the address after @ must match for all of them. The server ID, local address, external address, and port must be the same for all devices. If at least one parameter is different (for example, the local IP address is not set for some device when it is set for other devices), then such a device will not start.

Note.

Axxon One does not support auto-discovery of devices connected via GB/T28181 and these devices are not added using the Camera discovery tool.

After configuring the device as described earlier, add it to *Axxon One* as follows:

1. Run the IP discovery wizard (see Searching, adding, configuring and removing IP devices).
2. In the form for manually adding an IP device, in the **Vendor** list, select **GBT28181** (**1**).



3. In the **IP address** field specify the value of Device ID parameter set during IP device configuration (**2**). The following additional parameters can be specified optionally as follows:
[gbt://]deviceID[/videoPort]@serverID[-serverLocalIP[/serverExternalIP]]
OR
[gbt://]deviceID[/videoPortFirst-videoPortLast]@serverID[-serverLocalIP[/serverExternalIP]]
where:

   - deviceID is the Device ID parameter;
   - serverID is the identifier of the *Axxon One* Server generated according to the same rules as the IP device ID (see above);
   - videoPort is the port for receiving video;
   - videoPortFirst – videoPortLast is range of ports for receiving video;
   - serverLocalIP is the local IP address of the *Axxon One* Server, which sets the network interface on which the Server should be available;
   - serverExternalIP is the global IP address of the *Axxon One* Server; this parameter is in use when the *Axxon One* Server is behind the gateway. In this case, this IP address is specified as the SIP Server IP address in the IP device settings.

   Examples.

   ```
   34020000001320000008@34020000002000000001

   34020000001320000008@34020000002000000001-10.0.40.246/113.125.160.58
   34020000001320000008@34020000002000000001-10.0.40.246
   34020000001320000008@34020000002000000001-/113.125.160.58
   34020000001320000008/50200@34020000002000000001
   34020000001320000008/50200-50210@34020000002000000001-10.0.40.246
   ```

4. In the **Port** field, enter the local port number that the *Axxon One* Server shall listen for receiving messages from the IP device (3). Usually this is the default SIP port: 5060.

   Note.

   The IP device SIP port is detected automatically.

5. The **Username** and the **Password** fields are not used (**4**).
6. Click the  button.

Connection of the camera via GB/T28181 is now complete.

Examples of IP device settings for connection via GB/T28181 standard

On the page:

- Jovision
- Bosch
- Huawei
- Hikvision
  - GB/T28181-2011
  - GB/T28181-2016
- Dahua

Examples of IP device settings and connection settings in *Axxon One* for GB/T28181 standard are given below.

Note

The protocol is usually supported by cameras for China market not having any English interface. This is why some of the screenshots below are given in Chinese.

Jovision

Configure a Jovision camera for operation via GB/T28181 standard as follows:

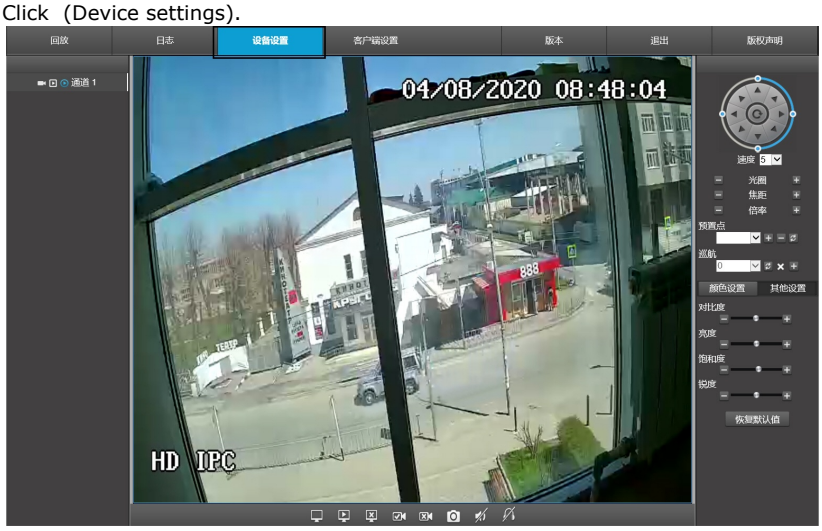
1. Perform the following settings of the IP-device:
   a. Go to the IP device web interface.
   b. Enter your login and password.



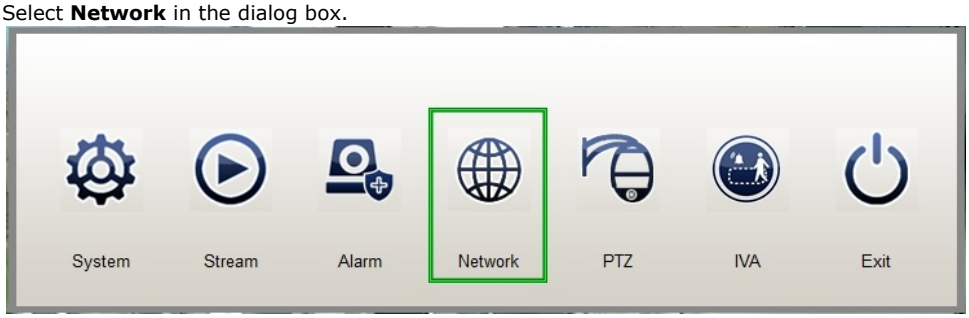
   c. Click (Confirm) in the dialog box opened.



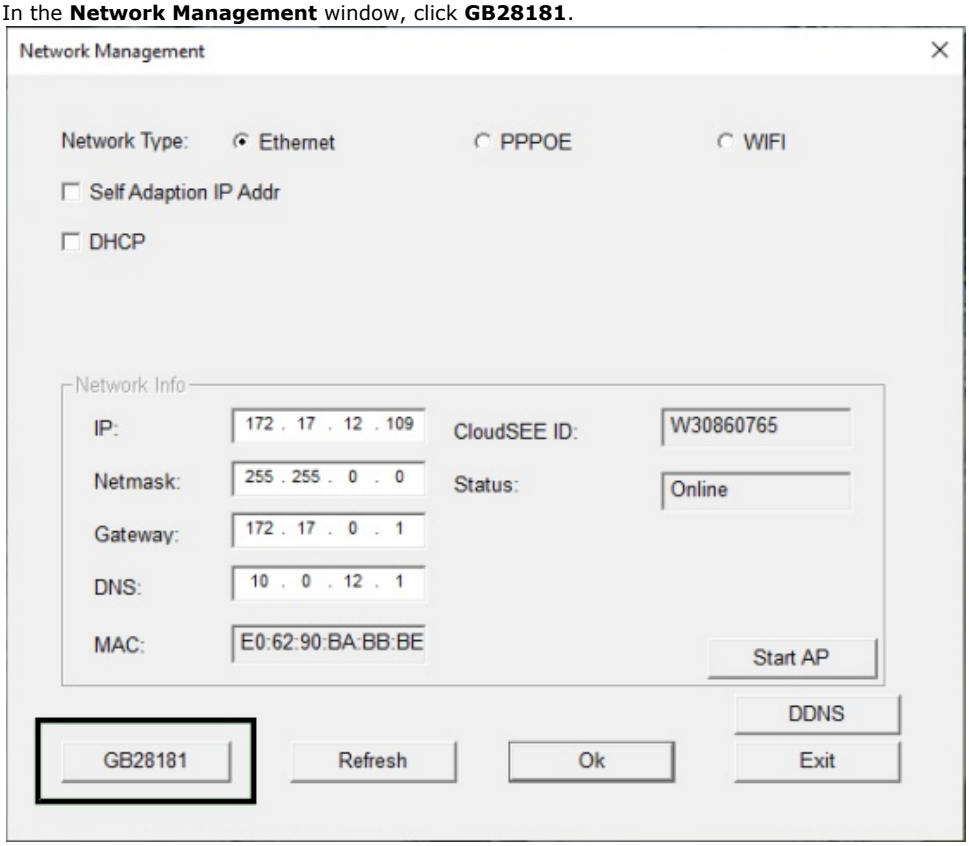
d. Click (Device settings).



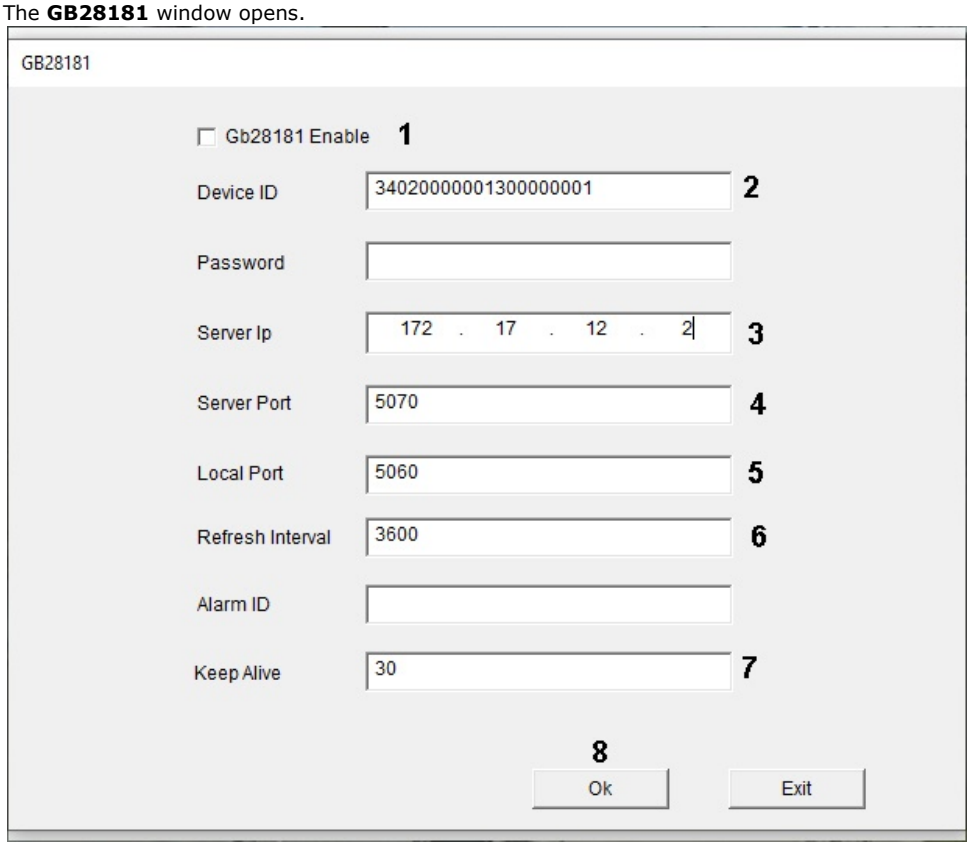
e. Select **Network** in the dialog box.



f. In the **Network Management** window, click **GB28181**.



g. The **GB28181** window opens.



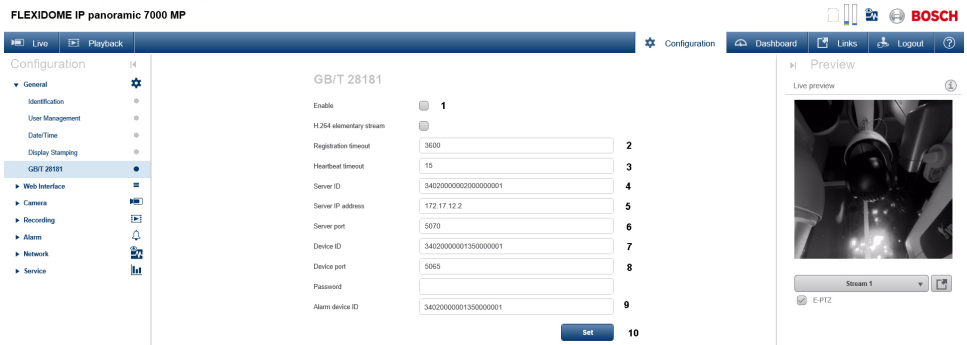
h. Set the **Gb28181 Enable** checkbox checked (**1**).
i. In the **Device ID** field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol (**2**). Example on the picture shows Device ID 34020000001300000001.
j. In the **Server Ip** field, enter the *Axxon One* server IP-address (**3**). The example shows IP 179.17.12.2
k. In the **Server Port** field, enter *Axxon One* server port number assigned for receiving messages from the IP device (**4**) The example shows port 5070.
l. In the **Local Port** field, enter the IP device SIP port number (**5**).
m. In the **Refresh Interval** field, enter the devise discovery period in seconds (**6**). The value shall not be less than 600.
n. In the **Keep Alive** field, enter the period in seconds for sending messages confirming the device activity (**7**).
o. Click the **Ok** button (**8**).

2. In *Axxon One*:
   a. Example value for the **IP address** field: 34020000001300000001@34020000001300000002-10.0.40.246/179.17.12.2 The Server ID 34020000001300000002 is not set on the Jovision device, so any Server ID can be chosen as per the conditions set in Connecting cameras via the GB/T28181 protocol.
   b. Set **Port** to 5070.

Bosch

Configure a Bosch camera for operation via GB/T28181 standard as follows:

1. Perform the following settings of the IP-device:
   a. Go to the IP device web interface.
   b. Go to **Configuration – General – GB/T 28181**.



c. Set the **Enable** checkbox checked (**1**).

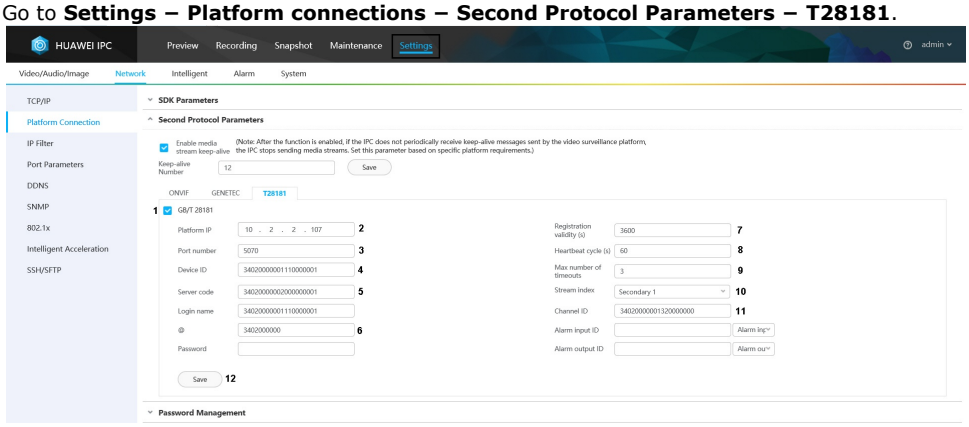
d. In the **Registration timeout** field, enter the devise discovery period in seconds (**2**). The value shall not be less than 600.
e. In the **Heartbeat timeout** field, enter the period in seconds for sending messages confirming the device activity (**3**).
f. In the **Server ID** field, enter the *Axxon One* server identification number (**4**). The example shows 34020000002000000001.
g. In the **Server IP address** field, enter the *Axxon One* server IP-address (**5**). The example shows 172.17.12.2
h. In the **Server port** field, enter *Axxon One* server port number assigned for receiving messages from the IP device (**6**). The example shows port 5070.
i. In the **Device ID** field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol (**7**). Example on the picture shows Device ID 34020000001350000001.
j. In the **Device port** field, enter the IP device SIP port number (**8**).
k. In the **Alarm device ID** field, enter the channel identification number (**9**). The same value as **Device ID** may be used.
l. Click the **Set** button (**10**).

2. In *Axxon One*:
a. Example value for the **IP address** field: 34020000001350000001@34020000002000000001-10.0.40.246/172.17.12.2
b. Set **Port** to 5070.

Huawei

Configure a Huawei camera for operation via GB/T28181 standard as follows:

1. Perform the following settings of the IP-device:
a. Go to the IP device web interface.
b. Go to **Settings – Platform connections – Second Protocol Parameters – T28181**.



c. Set the **GB/T 28181** checkbox checked (**1**).
d. In the **Platform IP** field, enter the *Axxon One* server IP-address (**2**). The example shows 10.2.2.107.
e. In the **Port number** field, enter *Axxon One* server port number assigned for receiving messages from the IP device (**3**). The example shows port 5070.
f. In the **Device ID** field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol (**4**). Example on the picture shows Device ID 34020000001110000001.
g. In the **Server code** field, enter the *Axxon One* server identification number (**5**). The example shows Server ID 34020000002000000001.
h. In the **@** field, enter the first 10 digits of the address according to GB/T-2260-2007 (**6**).
i. In the **Registration validity (s)** field, enter the device discovery period in seconds (**7**). The value shall not be less than 600.
j. In the **Heartbeat cycle (s)** field, enter the period in seconds for sending messages confirming the device activity (**8**).
k. In the **Max number of timeouts** field, enter the maximum number of Heartbeat message omissions after which the device connection is considered lost (**9**).
l. Select the video stream from the **Stream index** drop-down list (**10**).
m. In the **Channel ID** field, enter the channel identification number in the same format as Device ID and Server ID (**11**).
n. Click the **Save** button (**12**).

2. In *Axxon One*:
a. Example value for the **IP address** field: 34020000001110000001@34020000002000000001-10.2.2.107
b. Set **Port** to 5070.

Hikvision

The Hikvision cameras may support several GB/T28181 standard versions: GB/T28181-2011 and/or GB/ T28181-2016. Examples of configuration for these versions are given below.

Setup video streams as follows before you configure the GB/T28181 standard on the IP device:

1. Go to **- - -** (Settings **–** Video and Audio **–** Video).
2. Configure the main stream:

a. From the (Stream type) drop-down list, select **()** (Main stream) (**1**).

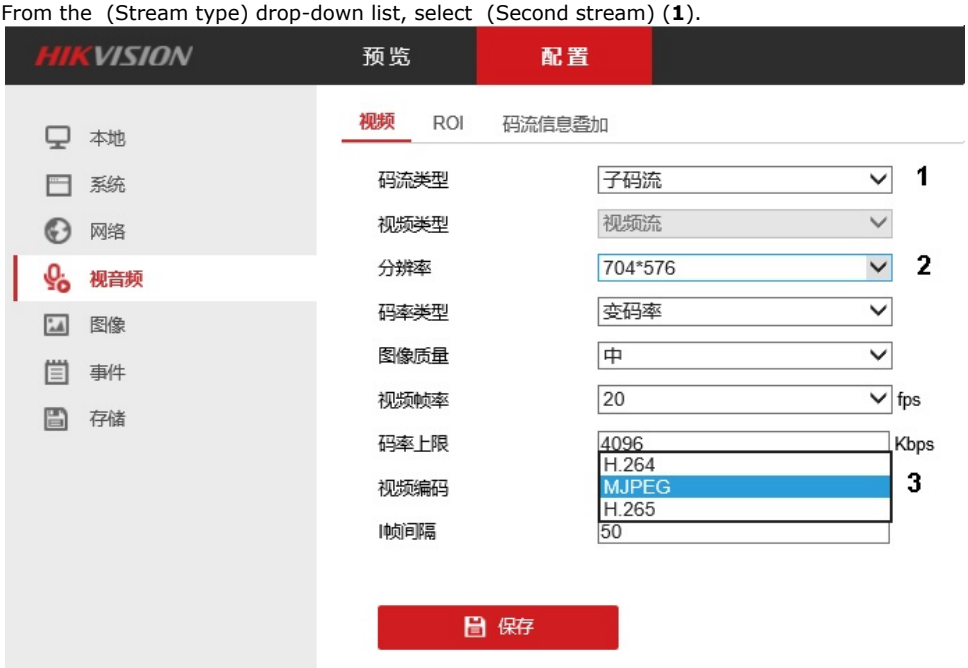


b. From the (Resolution) drop-own list, select the main stream resolution (**2**).

c. From the (Codec) drop-own list, select the main stream codec (**3**).

3. Configure the second stream:

a. From the (Stream type) drop-down list, select (Second stream) (**1**).



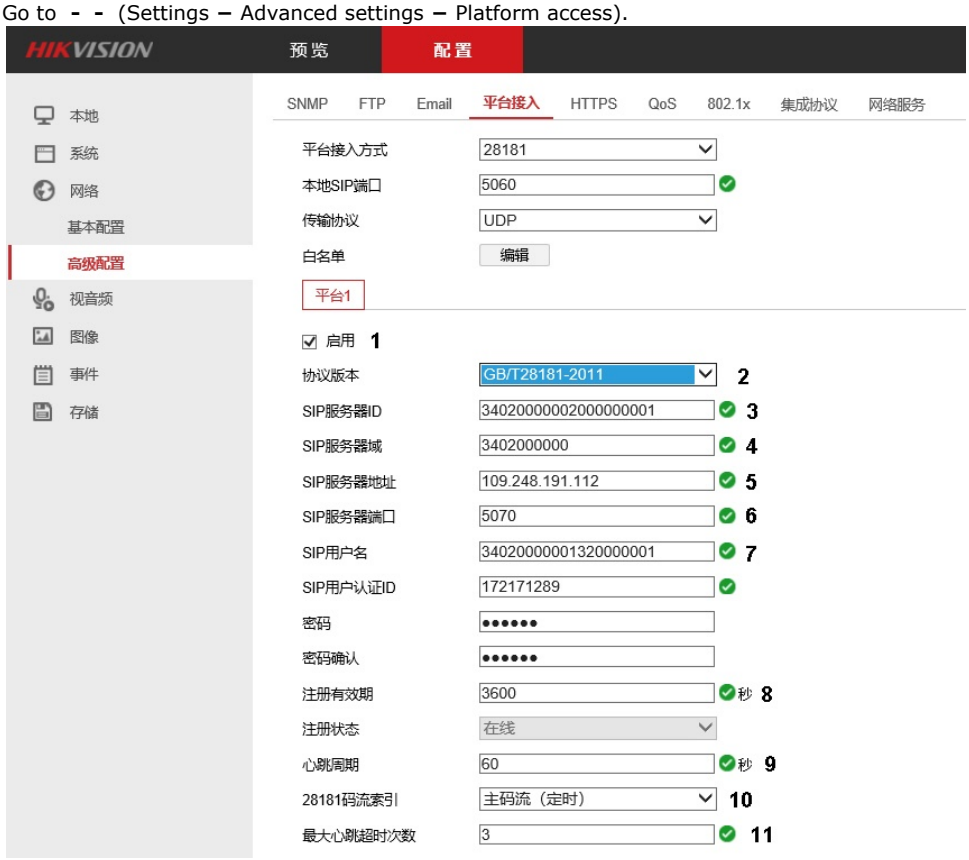
b. From the (Resolution) drop-down list, select the second stream resolution (**2**).

c. From the (Codec) drop-down list, select the second stream codec (**3**).

4. Click (Save).

GB/T28181-2011

1. Go to - - (Settings — Advanced settings — Platform access).



2. Set the (Enable) checkbox (**1**).
3. From the (Protocol version) drop-down list, select **GB/T28181-2011** (**2**).
4. In the **SIPID** (SIP Server ID) field, enter the *Axxon One* Server ID (**3**). The example shows Server ID 34020000002000000001.
5. In the **SIP** (SIP Server domain) field, enter first 10 digits of the address according to GB/T-2260-2007 (**4**).
6. In the **SIP** (SIP Server address) field, enter the *Axxon One* server IP-address (**5**). The example shows IP 109.248.191.112.
7. In the **SIP** (SIP Server Port) field, enter the *Axxon One* server port number assigned for receiving messages from the IP device (**6**). The example shows port 5070.
8. In the **SIP** (SIP user name) field, enter the device identification number as described in Connecting cameras via the GB /T28181 protocol (**7**). Example on the picture shows Device ID 34020000001320000001.
9. In the (Registration period) field, enter the devise discovery period in seconds (**8**). The value shall not be less than 600.
10. In the (Heartbeat period) field, enter the period in seconds for sending messages confirming the device activity (**9**).
11. From the **28181** (Video stream) drop-down list, select one of the streams configured earlier (**()** for Main stream or for Second stream) (**10**).
12. In the (number of timeouts for Heartbeat messages) field, enter the maximum number of Heartbeat message omissions after which the device connection is considered lost (**11**).
13. Go to the **ID** (Video channel ID) tab at the bottom of the setings page (**1**).



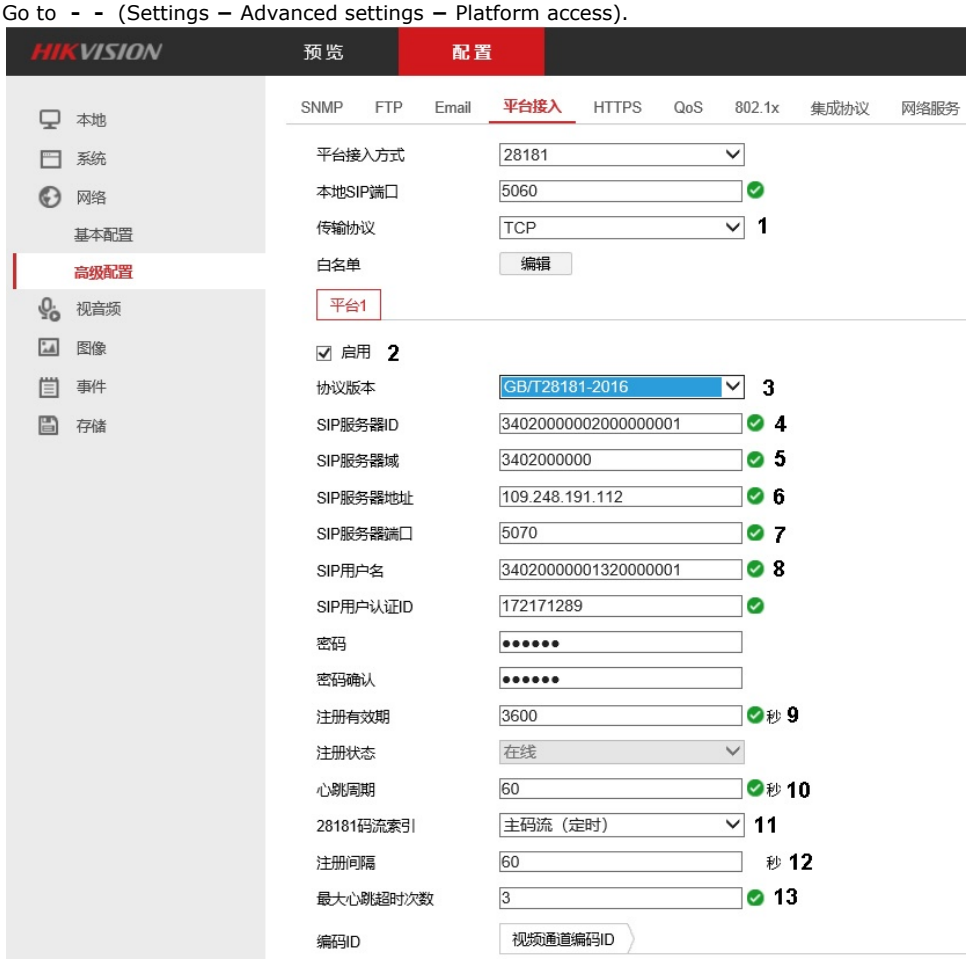
14. Enter the identifiers of all channels of the IP device in the same format as the device identifiers (**2**). The example shows ID 34020000001320000002.
15. Click the (Save) button (**3**).

In *Axxon One*:

1. Example value for the **IP address** field: 34020000001320000001@34020000002000000001-109.248.191.112
2. Set **Port** to 5070.

GB/T28181-2016

1. Go to - - (Settings – Advanced settings – Platform access).



2. From the (Transport protocol) drop-down list, select the transport level protocol to be in use: UDP or TCP (**1**).
3. Set the (Enable) checkbox (**2**).
4. From the (Protocol version) drop-down list, select **GB/T28181-2016** (**3**).
5. In the **SIPID** (SIP Server ID) field, enter the *Axxon One* Server ID (**4**). The example shows Server ID 34020000002000000001.
6. In the **SIP** (SIP Server domain) field, enter first 10 digits of the address according to GB/T-2260-2007 (**5**).
7. In the **SIP** (SIP Server address) field, enter the *Axxon One* server IP-address (**6**). The example shows IP 109.248.191.112.
8. In the **SIP** (SIP Server Port) field, enter the *Axxon One* server port number assigned for receiving messages from the IP device (**7**). The example shows port 5070.
9. In the **SIP** (SIP user name) field, enter the device identification number as described in Connecting cameras via the GB /T28181 protocol (**8**). Example on the picture shows Device ID 34020000001320000001.
10. In the (Registration period) field, enter the devise discovery period in seconds (**9**). The value shall not be less than 600.
11. In the (Heartbeat period) field, enter the period in seconds for sending messages confirming the device activity (**10**).
12. From the **28181** (Video stream) drop-down list, select one of the streams configured earlier (**()** for Main stream or for Second stream) (**11**).
13. In the (Registration interval) field, enter the device discovery interval in seconds (**12**).
14. In the (number of timeouts for Heartbeat messages) field, enter the maximum number of Heartbeat message omissions after which the device connection is considered lost (**13**).
15. Go to the **ID** (Video channel ID) tab at the bottom of the setings page (**1**).



16. Enter the identifiers of all channels of the IP device in the same format as the device identifiers (**2**). The example shows ID 34020000001320000002.
17. Click the (Save) button (**3**).

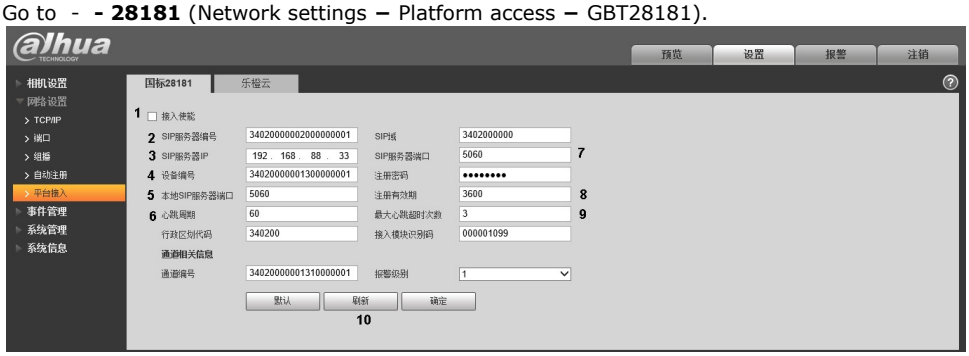
In *Axxon One*:

1. Example value for the **IP address** field: 34020000001320000001@34020000002000000001-109.248.191.112
2. Set **Port** to 5070.

Dahua

Configure a Dahua camera for operation via GB/T28181 standard as follows:

1. Perform the following settings of the IP-device:
    a. Go to the IP device web interface.
    b. Go to - **- 28181** (Network settings – Platform access – GBT28181).



    c. Set the (Enable connection) checkbox (**1**).
    d. In the **SIP** (SIP server number) enter the *Axxon One* Server ID (**2**). The example shows Server ID 34020000002000000001.
    e. In the **SIPIP** (SIP server IP address) enter the *Axxon One* server IP address (**3**). The example shows IP 192.168.88.33
    f. In the (Device number) field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol (**4**). Example on the picture shows Device ID 34020000001300000001.
    g. In the **SIP** (Local SIP port) field, enter the IP device SIP port number (**5**).
    h. In the (Heartbeat period) field, enter the period in seconds for sending messages confirming the device activity (**6**).
    i. In the **SIP** (SIP server port) field, enter the *Axxon One* server port assigned for receiving messages from the IP device (**7**). The example shows port 5060.
    j. In the (Registration period) field, enter the devise discovery period in seconds (**8**). The value shall not be less than 600.
    k. In the (number of timeouts for Heartbeat messages) field, enter the maximum number of Heartbeat message omissions after which the device connection is considered lost (**9**).
    l. Click (Update).
2. In *Axxon One*:
    a. Example value for the **IP address** field: 34020000001300000001@34020000002000000001-192.168.88.33
    b. Set **Port** to 5060.

Connecting and setting up devices with FFmpeg driver

FFmpeg generic driver is applied to receive video and audio data:

1. over RTSP and RTMP protocols (**1 channel device** model),
2. from connected USB devices (**Dshow device (USB camera)** model),
3. from the Server monitor screen (**Desktop capturer** model),
4. from the application window on the Server (**Window capturer** model, without audio).

> ⚠ **Attention!**
>
> If it is necessary to use the RTSP and RTMP protocols to broadcast video via the FFmpeg driver, then they must be pre-configured using external programs. In this case, *Axxon One* acts as a client that receives video from a third-party RTSP or RTMP server.

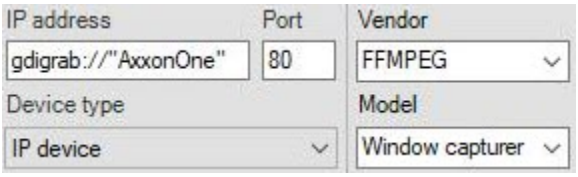
Receiving video from the application window on the Server with the FFmpeg driver

To receive video from the application window on the Server, add an object with the following address format:

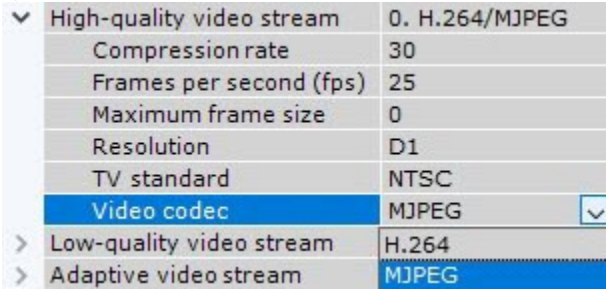
```
gdigrab://"Window title"
```

where "Window title" is the application window header.

> **Attention!**
>
> The address may contain only Latin characters. If the app window header contains some other characters, use any 3rd party utility to change them.

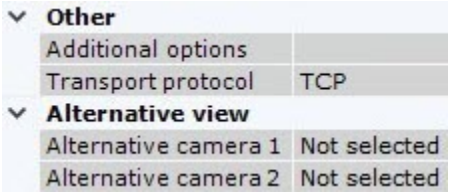


By default, videos are transmitted in MJPEG format. YUV422, H.264 and MPEG4 formats are also available.



> **Note**
>
> The YUV422 requires more network bandwidth. Take this into account when you select a format.

You can set a parameter string in the **Additional options** field.



Supported parameters	Description
-draw_mouse <int>	Mouse cursor presence. Available range: 0 to 1, default value: 1.
-show_region <int>	Capture area indication. Available range: 0 to 1, default value: 1.
-framerate <video_rate>	FPS value.
-video_size <image_size>	Video image size.
-offset_x <int>	Capture area X offset. Default value is 0.
-offset_y <int>	Capture area Y offset. Default value is 0.

An example parameter string:

```
-draw_mouse 1 -show_region 1 -framerate 25 -video_size 640x480 -offset_x 10 -offset_y 10
```

Receiving video from the remote Client screen and audio via FFmpeg driver

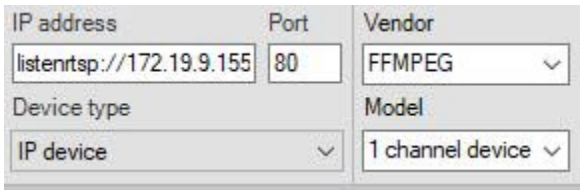
Your Server can receive video along with system audio and microphone audio from remote Client screens via the FFmpeg driver using the RTSP translation. To do it, do the following:

1. On the Server:
   a. Open the port for receiving data from the remote Client.

> **Note**
>
> The open port mustn't be occupied. You can use the following command to check if the port is available:
>
> ```
> netstat -ano | findstr :<Port>
> ```
>
> It is recommended to set ports higher than 10000.

   b. Add a **1 channel device** and specify its address in the **IP address** field in the following format.

```
listenrtsp://<Server IP address>:<Port>
```



> **Note**
>
> The RTSP link is specified optionally.
>
> ```
> listenrtsp://<Server IP address>:<Port>/<RTSP link>
> ```
>
> For example:
>
> ```
> listenrtsp://127.0.0.1:1554/live1.sdp
> ```
>
> where
> 127.0.0.1—IP address of the Server;
> 1554—RTSP port, which mustn't be occupied. To check if the port is available, you can use the command from step 1a;
> live1.sdp—RTSP link.

2. On the remote Client:
   a. Download the package of open source FFmpeg libraries from the official website.
   b. Open the command prompt, and go to the folder containing the ffmpeg.exe file.
   c. Run the following command:

```
ffmpeg.exe -f gdigrab -video_size 640x480 -i desktop -c:v <Codec> -f rtsp -muxdelay 0.1
"listenrtsp://<Server IP address>:<Port>/<RTSP link>"
```

where
– the **Codec** parameter may accept the mpeg2video, mpeg4, h264 or hevc value;
– the **video_size 640x480** and **-muxdelay 0.1** parameters may be omitted or altered.
If necessary, you can specify additional parameters in this command.

Supported parameters	Description

-draw_mouse <int>	Mouse cursor presence. Available range: 0 to 1, default value is 1
-show_region <int>	Capture area indication. Available range: 0 to 1, default value is1
-framerate <video_rate>	FPS value (number of frames)
-video_size <image_size>	Video image size (pixels)
-muxdelay <int>	Maximum demultiplexer-decoding delay (seconds)
-offset_x <int>	Capture area X offset (pixels). Default value is 0
-offset_y <int>	Capture area Y offset (pixels). Default value is 0

After the command execution, remote Client's screen is shared on your display.

Note

- The axes of the capture area are offset from the upper left corner of the main monitor.
- If the additional monitor is located to the left of the main monitor, a negative value of **offset_x** must be used to move the capture area to the additional monitor.
- If the additional monitor is located above the main monitor, a negative value of **offset_y** must be used to move the capture area to the additional monitor.

Examples of commands to share the screen of the remote Client

On the remote Client, you can run the commands to share the screen.

- If there are multiple screens on the remote Client, in order to share them all, you must run the command:

```
ffmpeg.exe -f gdigrab -i desktop -c:v <Codec> -f rtsp -muxdelay 0.1 "listenrtsp://<Server IP address>:
<Port>/<RTSP link>"
```

where
the **-video_size** parameter is missing, thus the entire video space is used.

- If there are several screens on the remote Client, they can be shared separately.

For example, to share only the first screen, you can run the command:

```
ffmpeg.exe -f gdigrab -offset_x 0 -offset_y 0 -video_size 1920x1080 -i desktop -c:v <Codec> -f rtsp -
muxdelay 0.1 "listenrtsp://<Server IP address>:<Port>/<RTSP link>"
```

Additionally, you can specify the **-pix_fmt** parameter to select the color scheme, since some video codecs may not work correctly:

```
-pix_fmt yuv420p
```

To share only the second screen, you can run the command:

```
ffmpeg.exe -f gdigrab -offset_x 1920 -offset_y 0 -video_size 1920x1080 -i desktop -c:v <Codec> -f rtsp -
muxdelay 0.1 "listenrtsp://<Server IP address>:<Port>/<RTSP link>"
```

where
the **-offset_x 1920** parameter offsets the X axis to the right by 1920 pixels, thus skipping the first screen and using the second screen.
If you want to share the third screen of the remote Client, the value of the **-offset_x** parameter is **-offset_x 3840**, i.e. the X axis is offset to the right by 3840 pixels, thus skipping the first and second screens and using the third screen.

> **Note**
>
> The value of the **-offset_x** parameter depends on the screen resolution. If the screen resolutions are different, the resolution of the individual screen must be taken into account to share it.

- It is possible to combine sharing from several specified screens.

  For example, you can run the command to share the first and second screen:

  ```
  ffmpeg.exe -f gdigrab -offset_x 0 -offset_y 0 -video_size 3840x1080 -i desktop -c:v <Codec> -f rtsp -
  muxdelay 0.1 "listenrtsp://<Server IP address>:<Port>/<RTSP link>"
  ```

  where
  the value of the **-video_size 3840x1080** parameter is the sum of the widths of the first and second screens.
  To share the second and third screens, you can run the command:

  ```
  ffmpeg.exe -f gdigrab -offset_x 1920 -offset_y 0 -video_size 3840x1080 -i desktop -c:v <Codec> -f rtsp -
  muxdelay 0.1 "listenrtsp://<Server IP address>:<Port>/<RTSP link>"
  ```

  where
  the **-offset_x 1920** parameter offsets the X axis by the width of the first screen;|
  the value of the **-video_size 3840x1080** parameter is the sum of the widths of the second and third screens.

- When using three or more screens on the remote Client, you can decode NVIDIA format into FFmpeg.
  To do this, run the following command:

  ```
  ffmpeg.exe -f gdigrab -i desktop -c:v <Codec> -f rtsp -muxdelay 0.1 "listenrtsp://<Server IP address>:
  <Port>/<RTSP link>"
  ```

  where
  the **Codec** parameter can accept the h264_nvenc (H264), hevc_nvenc (H265) values.

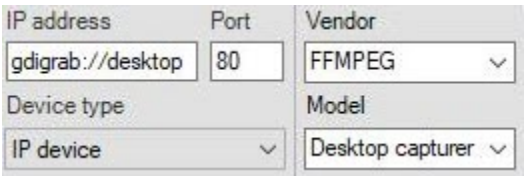
  > **Note**
  >
  > For Intel graphics cards, you must use the h264_qsv and hevc_qsv codecs, and for AMD cards—h264_amf and hevc_amf.

  The maximum screen resolution that NVENC h.264 can work with is 4096x4096 pixels. The maximum screen resolution that NVENC h.265 can work with is 8192x8192 pixels. For example, when using NVENC h.264, three screens with a resolution of 1920x1080 pixels won’t work.

Receiving video from the Server monitor with the FFmpeg driver

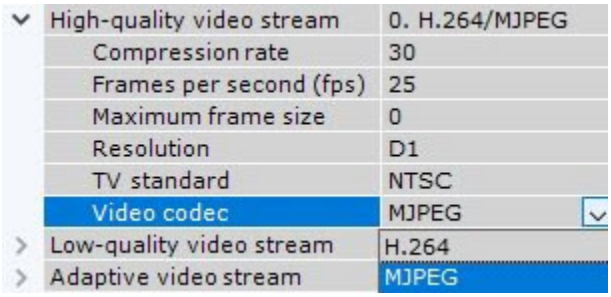
To receive video from the Server monitor screen, add an object with the following address format:

```
gdigrab://desktop
```



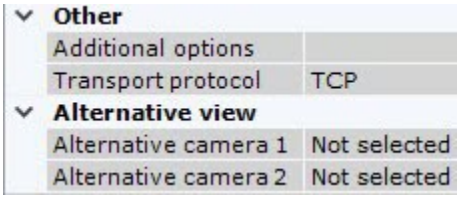
> **Note**
>
> To receive video from remote Clients, you have to use RTSP transmission (see Receiving video from the remote Client screen and audio via FFmpeg driver), or install Axxon One's Server services on your Client (see Installation).

By default, videos are transmitted from all Server monitors in MJPEG format. YUV422 and H.264 format is also available.



> **Note**
>
> The YUV422 requires more network bandwidth. Take this into account when you select a format.

You can set a parameter string in the **Additional Options** field.



Supported parameters	Description
-draw_mouse <int>	Mouse cursor presence. Available range: 0 to 1, default value: 1.
-show_region <int>	Capture area indication. Available range: 0 to 1, default value: 1.
-framerate <video_rate>	FPS value.
-video_size <image_size>	Video image size.
-offset_x <int>	Capture area X offset. Default value is 0.
-offset_y <int>	Capture area Y offset. Default value is 0.

An example parameter string:

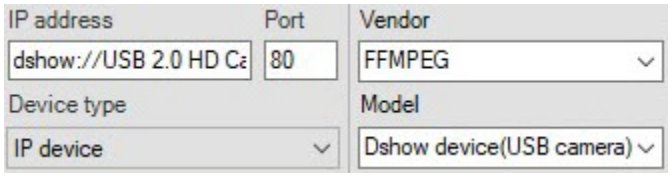
```
-draw_mouse 1 -show_region 1 -framerate 25 -video_size 640x480 -offset_x 10 -offset_y 10
```

Receiving audio and video from connected USB devices

If a device is added automatically (see Searching, adding, configuring and removing IP devices), separate objects are created for video and audio streams.

If you need to create a single object, add the device manually using the following address format:

```
dshow(<index>):///(<video_device_name>)(:<audio_device_name>)
```



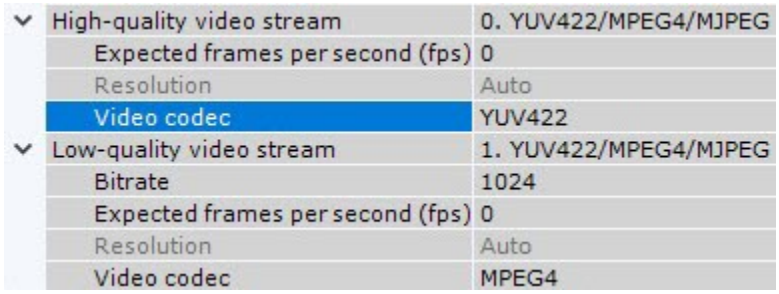
If no index is specified in the address, the value is **0**. Use a non-**zero** index if you use multiple devices with the same name.

For example:

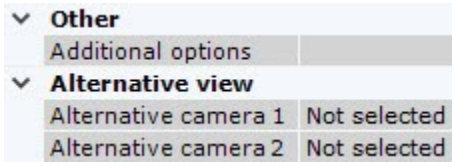
```
dshow://USB 2.0 HD Camera
dshow1://USB 2.0 HD Camera
```

> **Note**
>
> If a video or audio device is not present, it may be not specified in the address.

After you added the device, you have to set up its streams. For archive recording and transferring videos over the network, MJPEG codec is recommended; for detection purposes, use YUV422.



If required, you can set a parameter string for FFmpeg app in the **Additional options** field.



For example: receive video from a USB camera in YUV420P format, 1280x960 resolution.

```
-pixel_format yuv420p -video_size 1280x960
```

Parameters and their values differ by format and particular device. To list possible parameter values, run the following command from the Windows command line:

```
ffmpeg -list_options true -f dshow -i video="<device name>"
```

Receiving video and audio with FFmpeg driver over RTSP and RTMP protocols

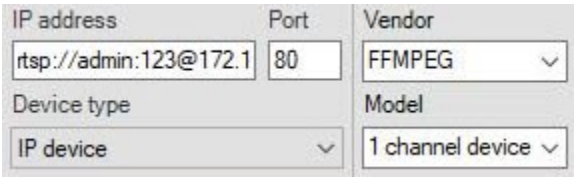
Attention!

FFmpeg currently has the following limitations:

- only one stream is supported;
- video codecs are limited to H.264/H.265, audio to AAC.

To add a device, use the following address format:

```
protocol://[login:password@]IP-address[:port][/path]
```



Note

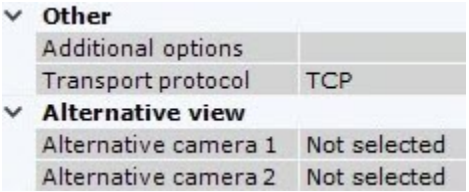
You can set login and password either in the address bar or in corresponding fields when adding the device.

If authentication parameters are specified both ways, the address bar has the priority.

Attention!

If you use the address bar method, you must specify the port number. If no port number is specified, default ports are used (554 for RTSP, 1935 for RTMP).

After you add a device, you can set a parameter string for FFmpeg app in the **Additional Options** field. Parameters and their values differ by format, particular device and protocol used.



Note

See the full list of parameters for RTSP protocol on the page.

Configuring connection of video cameras with dynamic IP addresses

Axxon One needs a permanent hostname, such as provided by DynDNS or similar dynamic DNS services to work with IP cameras that use DHCP.

Use your permanent DynDNS hostname to access an IP camera with a dynamic IP address.

Configuring virtual video cameras

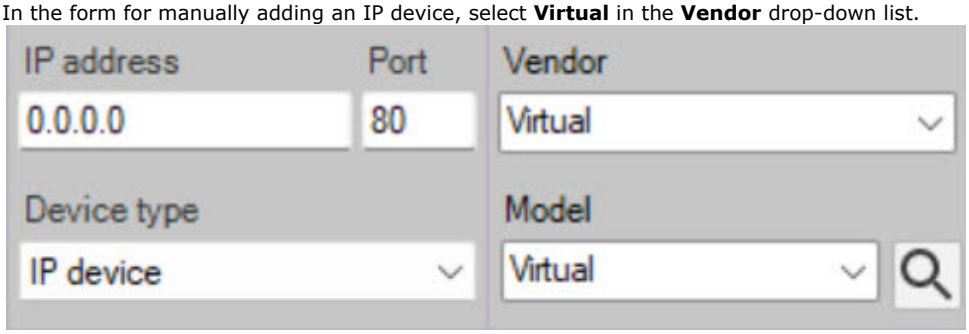
The *Axxon One* software package enables you to work with virtual video cameras.

This requires running *Axxon One* in test mode and consists of imitating a stream of video data by playing an available video clip (recording). You can play video recordings using video compression algorithms supported by *Axxon One* (see Characteristics of Axxon One).

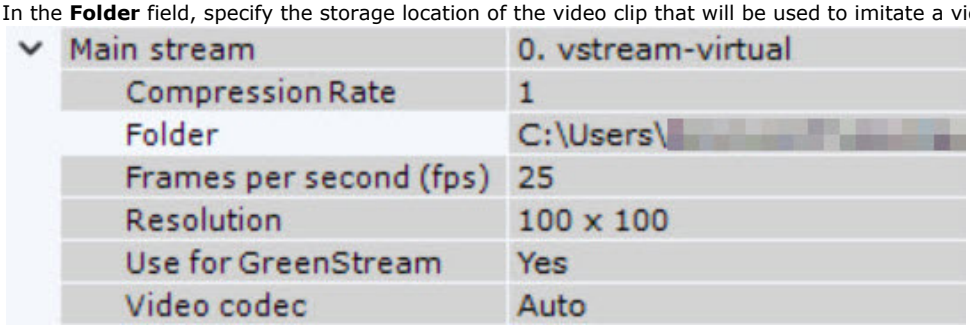
> **Note**
>
> Do not use video with B-frames.

To create and configure a virtual video camera, complete the following steps:

1. Run IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the form for manually adding an IP device, select **Virtual** in the **Vendor** drop-down list.

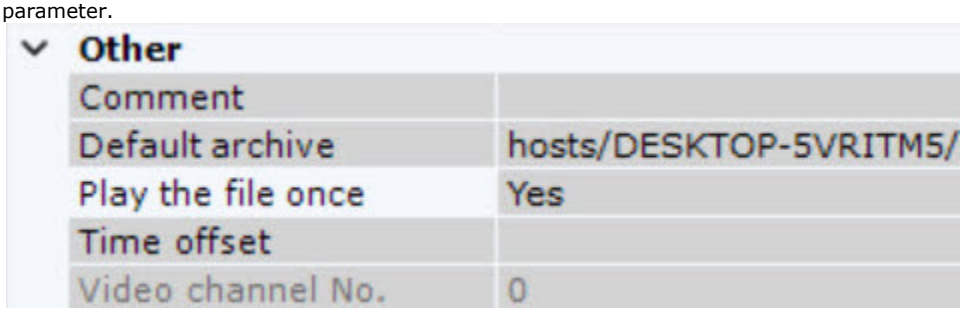


3. Select **Virtual** from the **Model** list to emulate a single-stream video camera. Select **Virtual several streams** to emulate a video camera supporting multiple streams.
4. Click the  button.
5. In the **Folder** field, specify the storage location of the video clip that will be used to imitate a video signal.



> **Note**
>
> - The name of the video file and its file path must consist only of Latin characters.
> - Scanning for files in a specified directory is limited to one minute.

6. By default, a video will be played back endlessly. To switch to one-shot playback, set **Yes** for the **Play the file once** parameter.



7. Click the **Apply** button.

Restoring default camera settings

You can restore the default *Axxon One* settings for a camera.

Current camera settings will be discarded and replaced with the defaults.

To restore default camera settings, select a camera in the device list. Click the **Reset** button and then the **Apply** button.



The IP Server Object

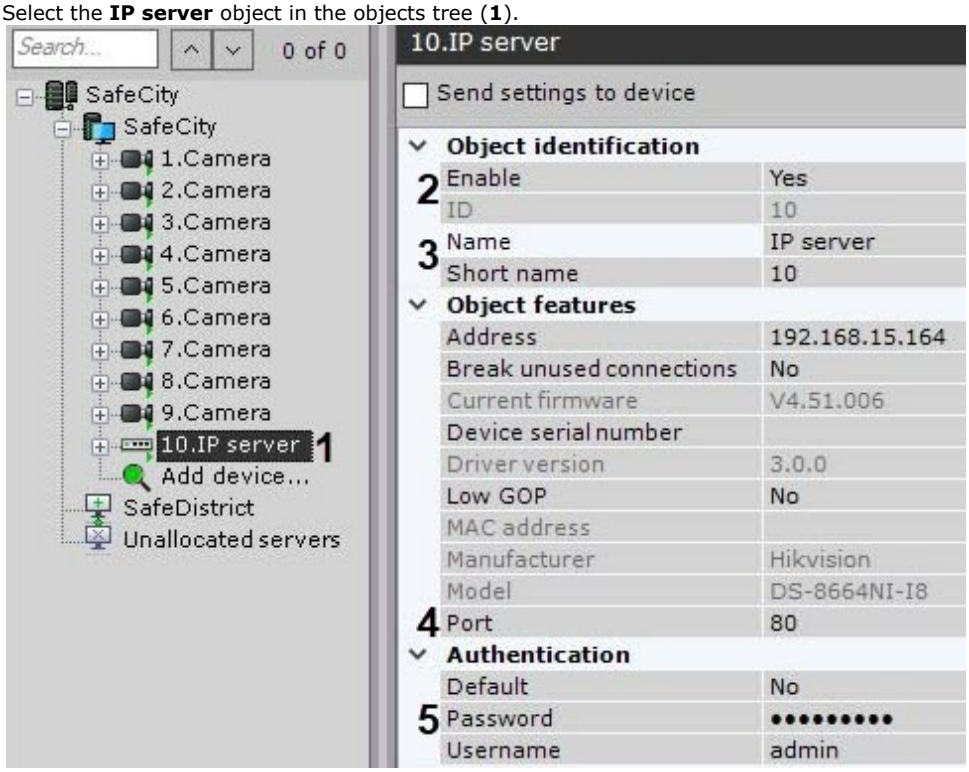
In *Axxon One*, an **IP Server** object relates to:

- video capture card;
- video server:
- control panel;
- DVR;
- input/output module.

If you configure a video capture card, video server or DVR, each video camera channel corresponds to a **Camera** object under the **IP Server** parent object.

To configure the IP server parent object, perform the following:

1. Select the **IP server** object in the objects tree (**1**).



2. Select **Yes** from the list in the **Enable** field to enable the object (**2**).
3. Enter the name of the IP server in the **Name** field (**3**).
4. Specify the number of the network port (**4**). The default value is **80**.

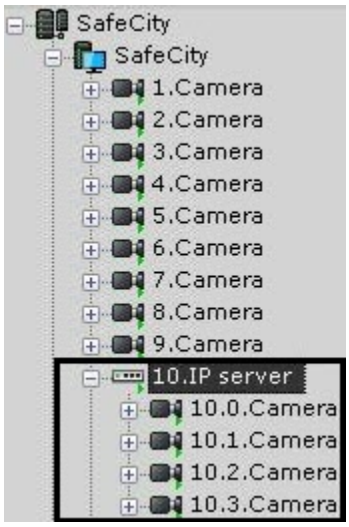
> **Note**
>
> The port number is initially set through the IP server's Web interface.

5. Set the authentication mode (**5**).

> **Note**
>
> The login and password for connecting to the IP server are set through its Web interface.

6. Click the **Apply** button.

The IP server and its video cameras will then be enabled, and the icon indicators for the IP server and video cameras in the objects tree will turn green.



Configuration of IP server channels must be performed separately for each channel (with the help of child objects of **Camera**).

Note

- Some parameters of the **Camera** child objects cannot be changed if the IP server was added in the **Keep current settings** mode (i.e. with the parameters that were set in the web interface, see Searching, adding, configuring and removing IP devices). To be able to configure these parameters, you need to set the **Send settings to device** checkbox.
- The **Send settings to device** checkbox can only be set for the IP Server parent object. Once you set a checkbox for an IP Server, the checkbox is also set on all its channels and child objects.

By default, you cannot delete child **Camera** objects from the IP server. To enable this feature, do as follows:

1. Quit Client.
2. Start a text editor and open the Axxon One.exe.config configuration file located in: <*Axxon One* installation folder Axxon One>\bin.
3. Find the line <add key="AllowIpServerChannelRemove" value="false" /> and change **false** to **true**.
4. Save the changes to the file.

You can now delete **Camera** objects from the IP server.

Attention!

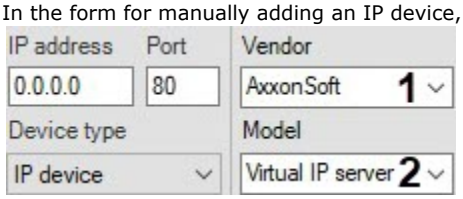
You cannot restore a deleted object. You will need to create the IP server again.

Configuring Virtual IP Servers

Axxon One supports working with a virtual IP server.

To create and configure a virtual IP server, perform the following steps:

1. Run IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the form for manually adding an IP device, select **AxxonSoft** in the **Vendor** drop-down list (**1**).



3. Select **Virtual** from the models list to emulate a single-stream video camera. Select **Virtual several streams** to emulate a video camera supporting multiple streams (**2**).
4. Click the  button.

An **IP server** object will be added. It will be used for creating 4 virtual video cameras; location of a video file to be used for signal emulation needs to be specified for each camera (see Configuring virtual video cameras).

The Microphone Object

If a microphone is part of an IP Server, then you must specify the video camera to which it will be linked in the settings of the given microphone. When you do this, the **Microphone** object will become a child of the specified **Camera** object.

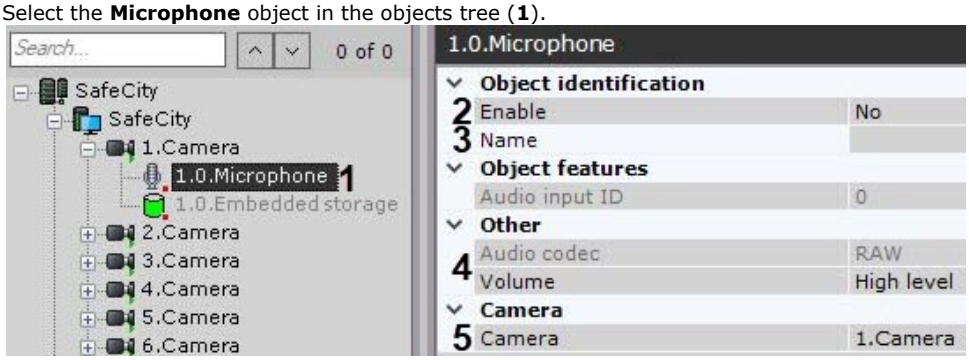
> **Atteintion**
>
> When a microphone is reassigned from one camera to another, all previously recorded audio is also transferred; when recorded video on the new camera is played, the transferred audio is played back.

> **Note**
>
> This setting is used during synchronized video and audio monitoring of a situation as well as during synchronized video and video recording to the archive (see the section Audio Monitoring).

In all other cases the **Microphone** object will automatically be displayed in the objects tree as a child of the video camera itself.

To configure the **Microphone** object, perform the following:

1. Select the **Microphone** object in the objects tree (**1**).



2. Enable the microphone by selecting **Yes** in the **Enable** field (**2**).
3. Enter the name of the microphone in the **Name** field (**3**).
4. Configure additional microphone parameters (audio codec, bit rate, etc.) in the **Other** group (**4**) using their descriptions in the interface of the *Axxon One* software package or, for more detail, in the official reference documentation of the parent video camera.
5. Choose a video camera to associate this microphone with (**5**). As a result of this operation, the selected camera will become a parent object for the microphone.
6. Click the **Apply** button.

The microphone will then be switched to its assigned work mode.

To check the microphone, do as follows:

1. In the upper-left corner of the preview window, click  .
2. Say something into your microphone.



3. If the microphone is configured correctly, you will hear audio from the Server's speakers. Pump it up if needed with the volume control.

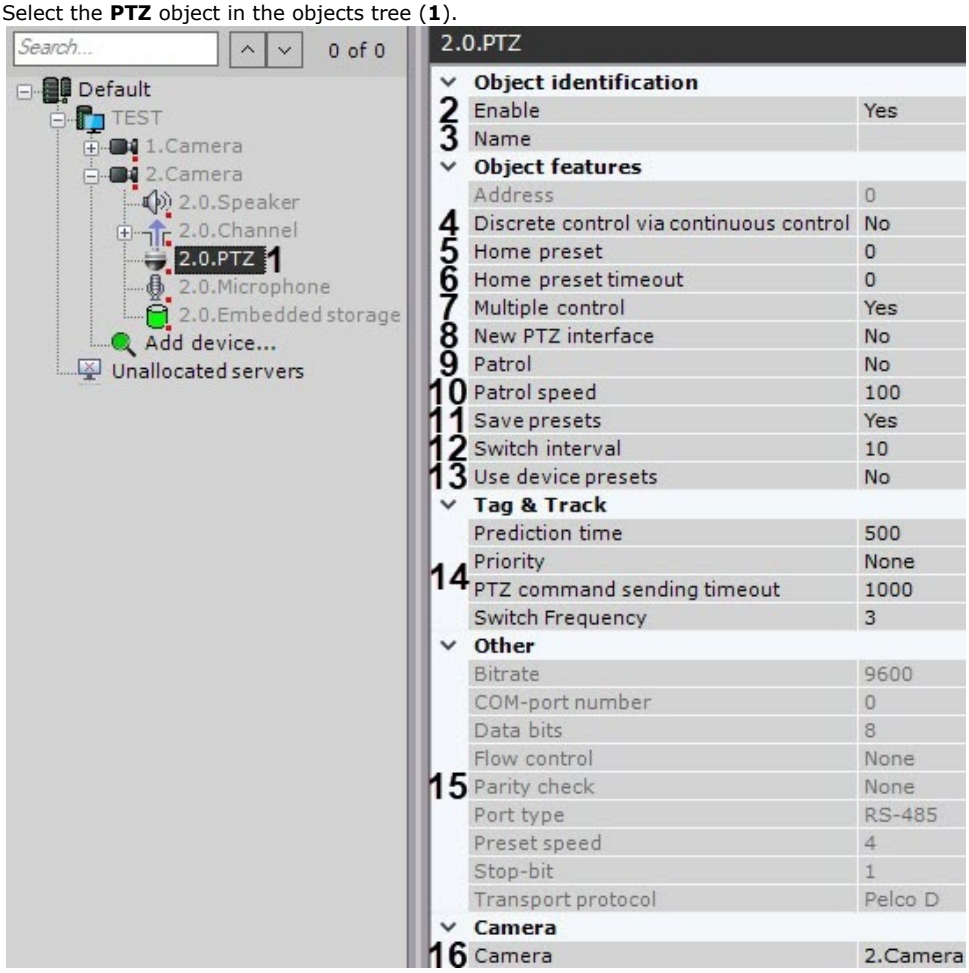
Checking microphone operation is now complete.

The PTZ Object

The **PTZ** object is displayed in the objects tree as the child object to the camera, if it is the PTZ camera.

To configure the PTZ device of the camera, do the following:

1. Select the **PTZ** object in the objects tree (**1**).



2. Enable the PTZ device by selecting **Yes** in the **Enable** field (**2**).
3. Enter the name of the PTZ device (**3**).
4. If you need to use the step buttons to control the PTZ camera even if the camera does not support this mode, select **Yes** for the **Discrete control via continuous control** parameter (**4**, see Control using step buttons and virtual joystick). In this case, the discrete PTZ control will be emulated via the continuous control commands.
5. Select the **Home preset** by specifying the required identifier (**5**). The home preset will return automatically after the time period specified in the **Home preset timeout** field (**6**).

> **Attention!**
>
> If the **Home preset timeout** value is greater than the **Operator idle time** value (see Configuring PTZ control), the **Operator idle time** value will be used.

6. To simultaneously control the PTZ camera by multiple users with the same priority, select **Yes** in the **Multiple control** list (**7**). Otherwise, only one user at a time will have a control (see Controlling a PTZ Camera).
7. To use the existing presets on the device in *Axxon One*, set **Yes** for the **New PTZ interface** parameter (**8**). The presets created on the device will automatically appear in the PTZ control panel.

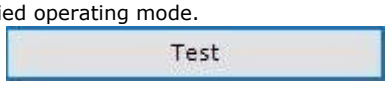
> **Attention!**
>
> If the use of the existing presets is disabled, they can be lost if the following conditions are met:
>
> 1. The recording of the presets to the device is enabled in *Axxon One* (see step 9).
>
> 2. The preset with the same ID is created in *Axxon One* (see Creating and editing presets).

8. Configure patrol:
    a. Select the default patrol mode: **Yes**—on, **No**—off (**9**). If patrolling is enabled by default, it can be stopped in PTZ control panel (see Patrolling). After you finish the PTZ control session, patrolling will resume automatically.
    b. Set the time interval in seconds at which the PTZ device will switch between the presets in the patrol mode (**12**).
    c. Set the transition speed from one preset to another in conditional units from 0 to 100 (**10**).
9. By default, the presets are recorded in the IP device. If you want to store the presets on the Server only, select **No** for the **Save presets** parameter (**11**).

> **Note**
>
> This parameter is available only for the devices that support Absolute Positioning.

10. To create the presets with the same ID in *Axxon One* (see Creating and editing presets), set **Yes** for the **Use device presets** parameter (**13**).
11. If necessary, configure the Tag & Track function (**14**, see Configuring Tag&Track Pro).
12. Depending on the camera, you may find other parameters in the **Other** group (**15**). To configure them, refer to their description in the interface or in the official documentation.
13. If necessary, select the camera to which this PTZ device should be assigned to (**16**). As a results, the object will become the child object to the selected camera.
14. Click the **Apply** button.

As a result, the PTZ device will switch to the specified operating mode.

To check the operation of the PTZ device, click the 

button. If the PTZ device is configured correctly, it will turn one step and return to its original position.

Controlling a PTZ Camera

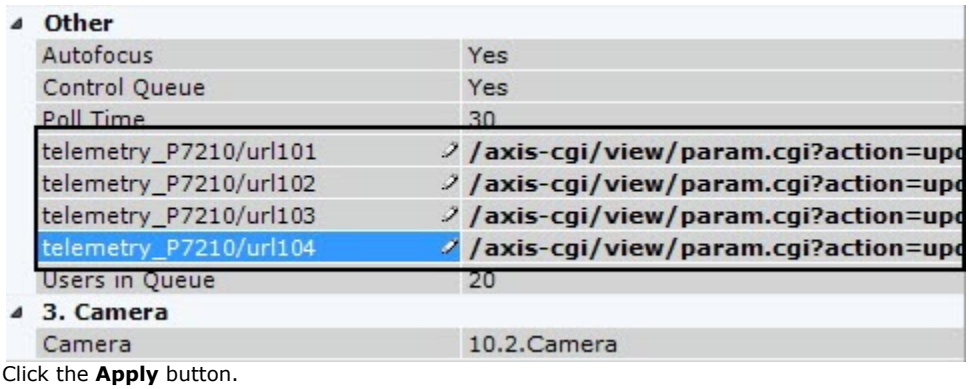
Configure HTTP-CGI commands to control Wash&Wiper

With *Axxon One*, you can control the Wash&Wiper feature in some Axis IP devices (M7016, P7216, Q7404, Q7436) using HTTP-CGI commands.

To set HTTP-CGI commands, do as follows:

1. Create presets for the camera, numbered as follows: 101, 102, 103 and 104 (see The Presets List).
2. Go to the **PTZ** object and specify commands in the appropriate fields.

   > **Note**
   >
   > The corresponding **Camera** object should have the **Send settings to device** option enabled (see The Camera object).

3. Click the **Apply** button.

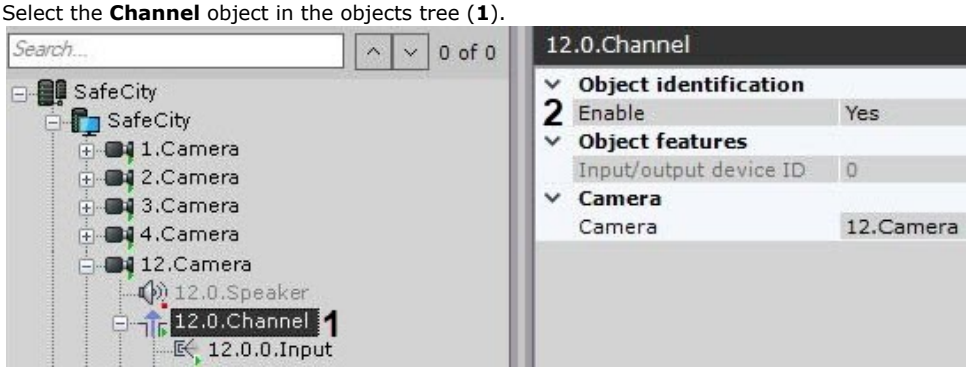
When the camera goes to the presets 101-104, this triggers a pre-configured command.

The Channel object

For I/O modules or video surveillance control panels (see CCTV Keyboards), the **Channel** object is displayed as a child object of an IP Server in the object tree (see The IP Server Object).

To configure the **Channel** object, do as follows:

1. Select the **Channel** object in the objects tree (**1**).



2. Enable the object (**2**).

> **Note**
>
> When a channel object is enabled/disabled, all **Input** and **Output** child objects are automatically enabled/disabled.

3. Click **Apply**.

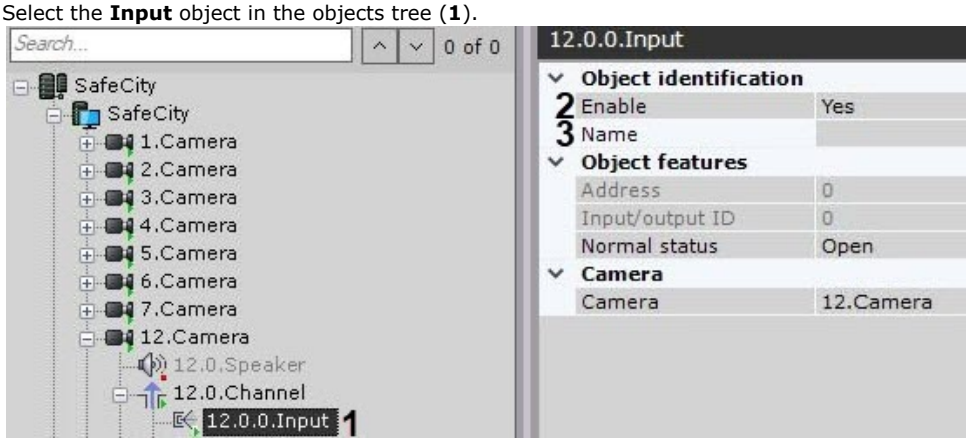
The Input Object

If a camera has a built-in or pluggable digital input, the **Input** object is displayed as a child object of the **Camera** in the object tree. The total number of **Input** objects for a camera corresponds to its number of pluggable digital inputs.

If a device is defined as an IP Server, Input will be displayed as a child of a **Channel** object in the object tree (see The Channel object).

To configure a **Input** object, perform the following:

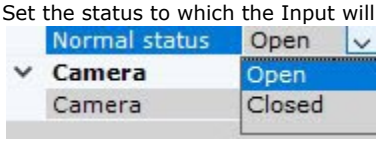
1. Select the **Input** object in the objects tree (**1**).



2. Enable the device (**2**).

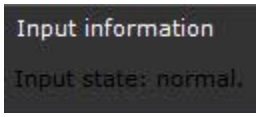
> **Note**
>
> If a input is a child of a **Channel** object, then:
>
> **a.** Turning on a input automatically enables its parent **Channel** object.
> **b.** Turning off all **Input** and **Output** child objects automatically disables their parent **Channel** object.

3. Enter the name of the Input (**3**).
4. Set the status to which the Input will be set when no alarm is present.

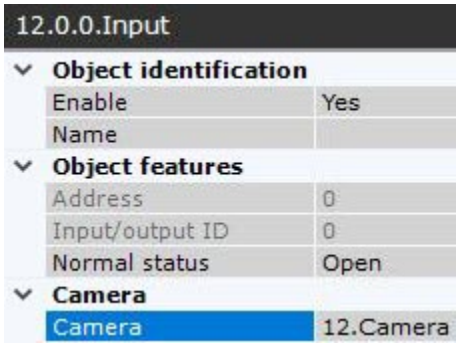


5. Click the **Apply** button.

The Input will then be switched to its assigned work mode.
The current status of the Input is displayed in the **Input information** group.



If a Input is part of an IP server, the Input settings allow choosing the video camera of the IP server it will be matched to. When you do this, the **Input** object will appear as the child object of the specified camera in the object tree.



Configure virtual inputs

Switch between virtual IP-device states (HttpListener).

The *Axxon One* software package enables you to work with virtual inputs. This involves triggering a virtual input and producing a virtual input event/alarm in the VMS. When triggered, the virtual input status switches – **Closed/Open.**

Creating and configuring virtual inputs

To create and configure a virtual input, complete the following steps:

1. Run IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the form for manually adding an IP device, select **HttpListener** in the **Vendor** drop-down list (**1**).

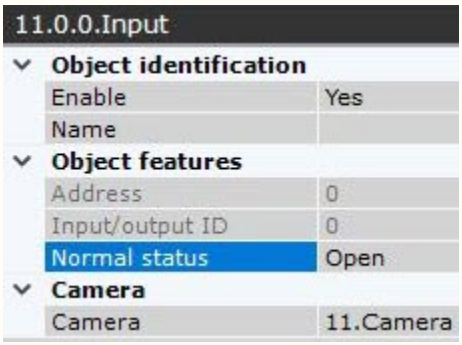


3. In the **Port** field, specify the port number that will be used Input status queries (**2**).
4. Click the  button.

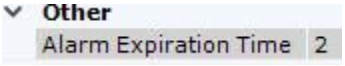
The **IP Server** object is automatically created to host 4 virtual inputs.

Attention!

For a virtual Input to work correctly, please do as follows: use the **Open** circuit.



You can configure virtual inputs in the same way as real ones. Also you can specify the time-out when virtual inputs reset their status in the **Alarm Expiration Time** field of the **IP Server** object. It ranges from 0 to 100.

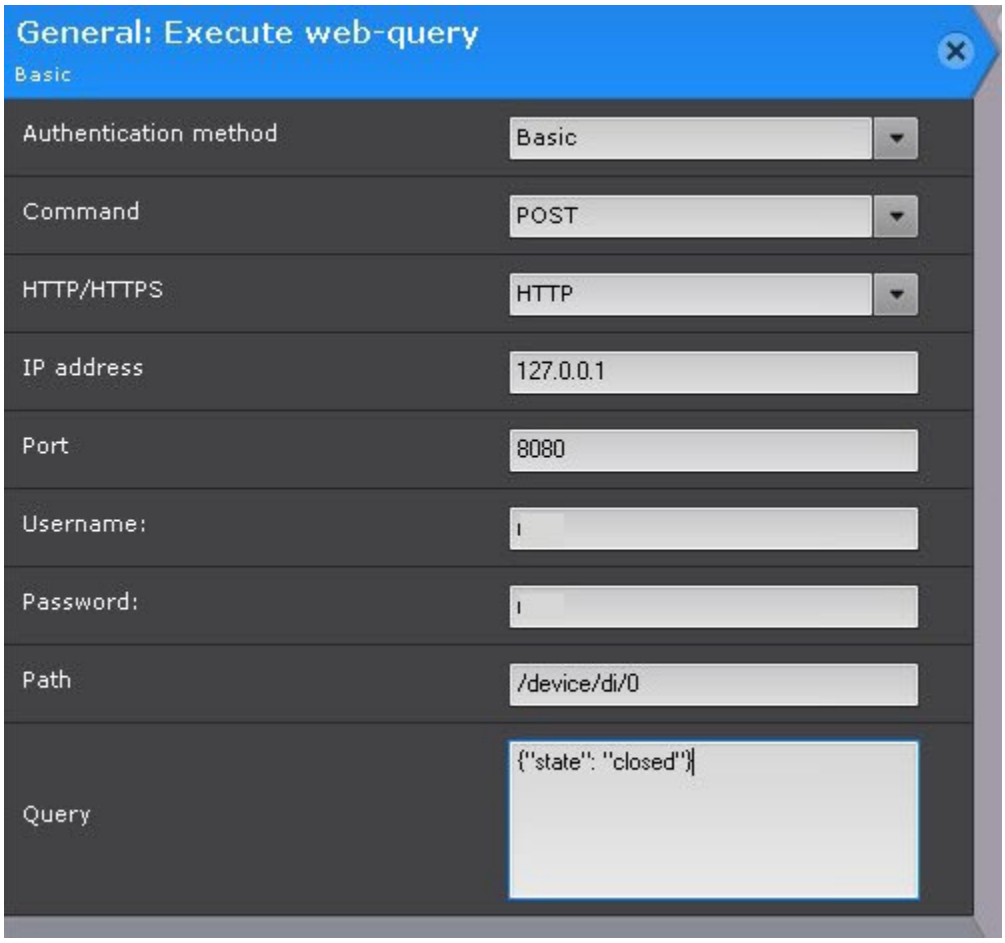


This setting is applied only after you disable and enable the input again.

Switching virtual inputs

To switch virtual inputs, the HTTP request is used (see Switch between virtual IP-device states (HttpListener)).

The requests can be handled by macros (see Executing a web query). Create 2 macros for each virtual input: to switch to **Closed** and to switch to **Opened**.



You can run macros and requests from Dialog board (see Configuring a Dialog Board).

Virtual inputs' status on map

You can add virtual inputs to maps just as you do with real ones (see Adding inputs and outputs).

Virtual inputs status is color-coded (see Displaying device status).

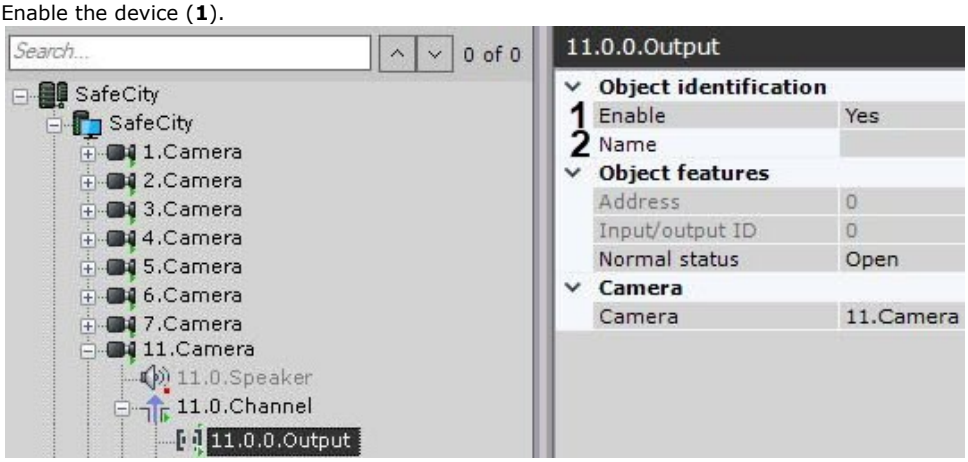
The Output Object

If a camera has a built-in or pluggable digital output, the **Output** object is displayed as a child object of the **Camera** in the object tree. The total number of **Output** objects for a camera corresponds to its number of pluggable digital outputs.

If a device is defined as an IP Server, a relay will be displayed as a child of a **Channel** object in the object tree (see The Channel object).

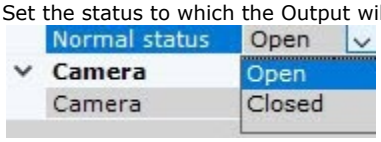
To configure a **Output** object, perform the following:

1. Select a **Output** object in the objects tree.
2. Enable the device (**1**).



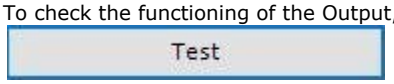
> **Note**
>
> If a output is a child of a **Channel** object, then:
>
> **a.** Turning on a output automatically enables its parent **Channel** object.
> **b.** Turning off all **Input** and **Output** child objects automatically disables their parent **Channel** object.

3. Enter the name of the Output (**2**).
4. Set the status to which the Output will be set when no alarm is present.

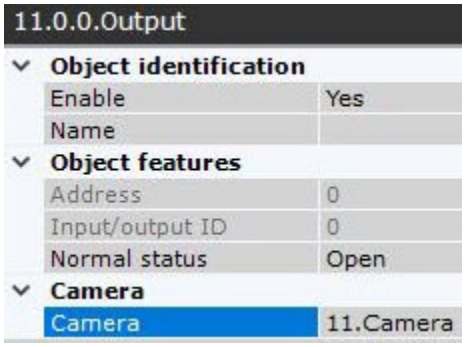


5. Click the **Apply** button.

The Output will then be switched to its assigned work mode.
To check the functioning of the Output, click the **Test** button**.** If the Output is configured correctly, its status will briefly change.



If a Output is part of an IP server, the sensor settings allow choosing the video camera of the IP server it will be matched to. When you do this, the **Output** object will appear as the child object of the specified camera in the object tree.



The Speaker object

On the page:

- General information
- Creating and configuring an object
- Checking the audio notification

General information

The **Speaker** object is used to configure audio notification that starts when a macro starts.

In *Axxon One,* you can create the following types of the **Speaker** objects:

1. **IP speaker device.** Created automatically if there is an audio outlet on an IP device.

   > **Note**
   >
   > One audio outlet on an IP device corresponds to one child **Speaker** of the **Camera** object.

2. **System speaker.** Created manually. Sound on the system speaker is played back using the Server's sound card.

A **Speaker** object can playback audio notification files with the extensions:

1. .ac3;
2. .amr;
3. .avi;
4. .aac;
5. .aiff;
6. .au;
7. .adts;
8. .caf;
9. .dts;
10. .flac;
11. .gsm;
12. .mkv;
13. .mp3;
14. .m4a;
15. .m4r;
16. .mp2;
17. .oga;
18. .ogg;
19. .opus;
20. .voc;
21. .w64;
22. .wav;
23. .wma;
24. .wv.

The following audio notification file encoding formats are supported:

1. MPEG AAC Audio;
2. MPEG-4 Video;
3. MPEG Audio layer 1/2;
4. Vorbis Audio;
5. Opus Audio;
6. PCM S16 LE;
7. PCM S16 BE;
8. twos;
9. FLAC (Free Lossless Audio Codec);
10. AMR narrow band;
11. DTS Audio;
12. GSM Audio;
13. WavPack;

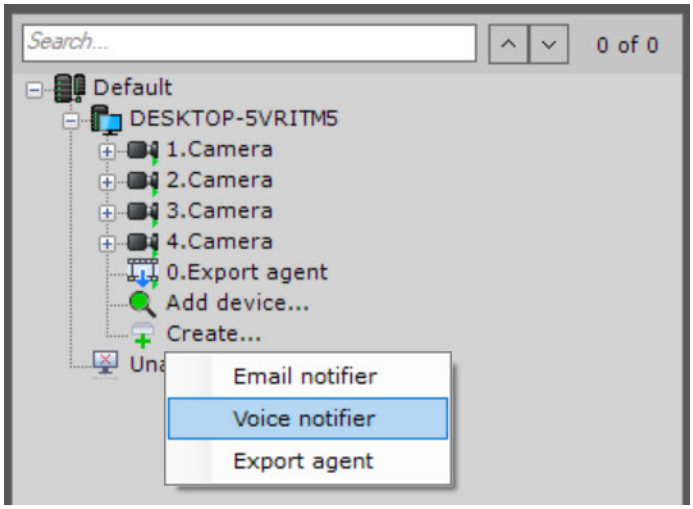
14. A52 Audio (aka AC3);
15. Yamaha ADPCM Audio;
16. ADTS.

The audio notification file must be stored on the computer corresponding to the **Server** object on the basis of which the **Speaker** object is registered.

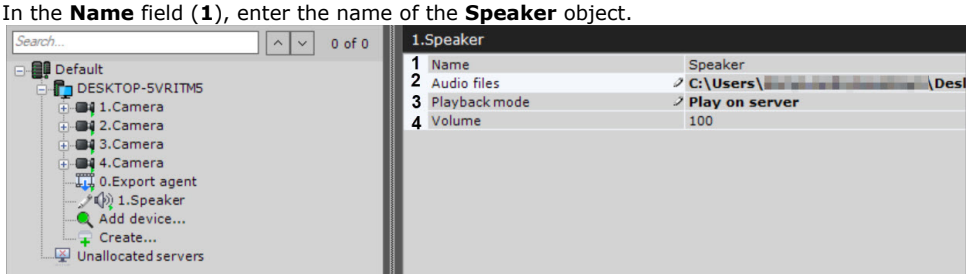
Creating and configuring an object

To create a **Speaker** system object, do the following:

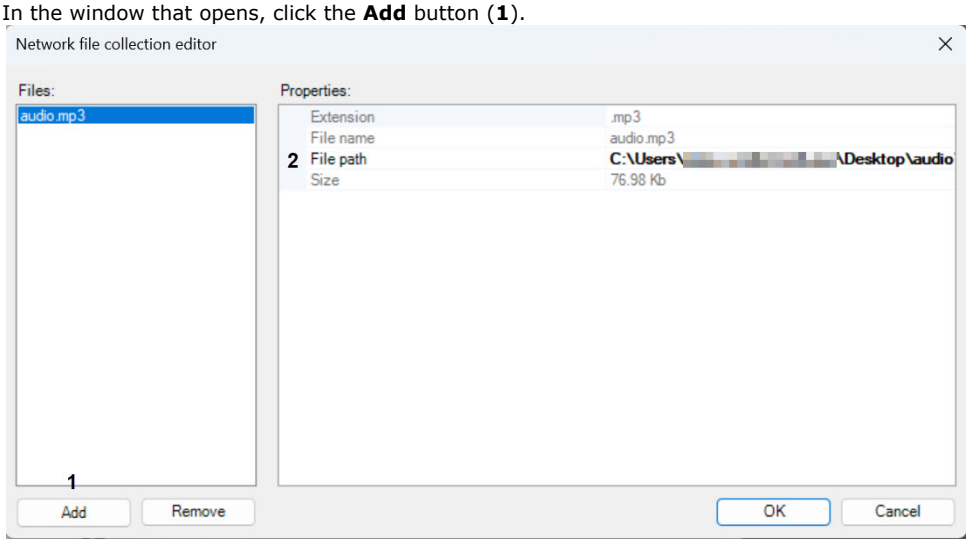
1. Click **Create** in the hardware tree and select **Voice notifier**.



2. In the **Name** field (**1**), enter the name of the **Speaker** object.



3. In the **Audio files** field (**2**), specify the path to the audio notification file in one of the following ways:
   - Enter the full path to the audio notification file in the **Audio files** field (**2**).
   - Select any already added file from the file collection.
   - Add a file using the file collection:
     a. Click the  button.
     b. In the window that opens, click the **Add** button (**1**).

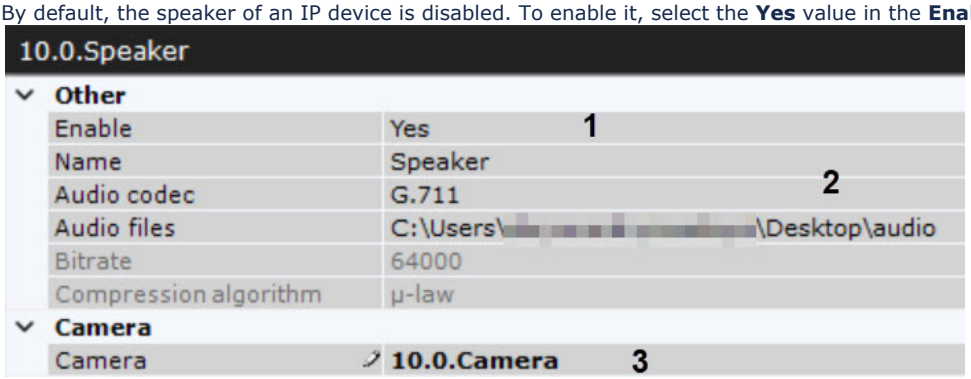


     c. Specify the path to the audio file (**2**). As a result, the remaining fields will display the selected audio file name, size and extension.

d. Click the **OK** button.
As a result, the path to the selected file will be displayed in the **Audio files** field.

> **Note**
>
> This parameter is mandatory.

4. Select the speaker playback mode: disabled, play of server, play on clients (**2**).
5. In the **Volume** field (**4**), enter the speaker volume level.
6. When configuring a speaker of an IP device:
   a. By default, the speaker of an IP device is disabled. To enable it, select the **Yes** value in the **Enable** parameter (**1**).

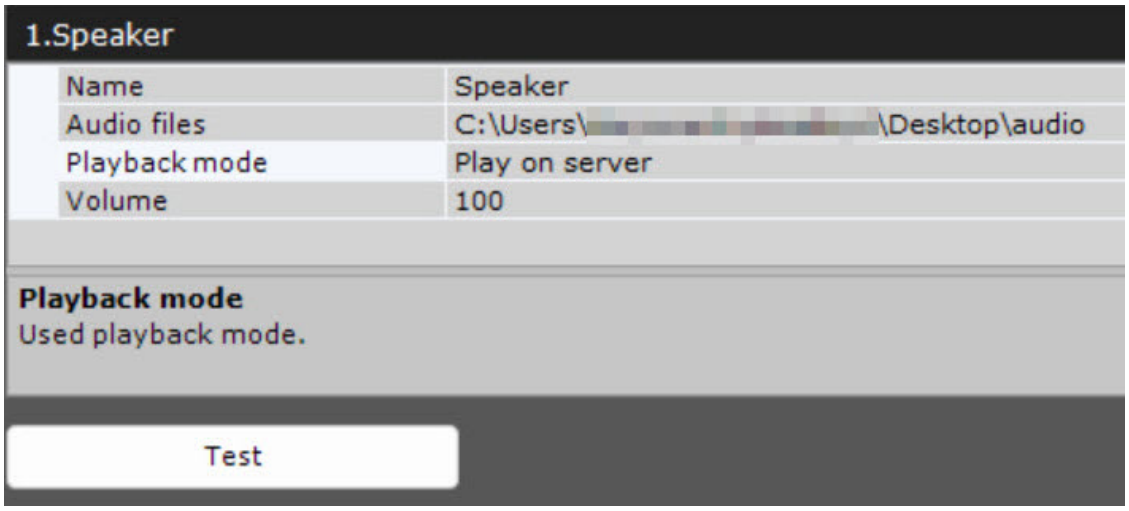


   b. When configuring the speaker of an IP device, you can specify other parameters as well, such as the compression algorithm for the audio signal sent to the speaker for playback, audio notification file (**2**). The list of the speaker parameters that you can configure is determined by the integration protocol of an IP device and *Axxon One*.
   c. Select a camera to which you want to assign this speaker (**3**). As a result of this operation, the selected camera becomes a parent object for the speaker.
7. Click the **Apply** button.

Configuration of the **Speaker** object is now complete.

Checking the audio notification

To check the **Speaker** object, click the **Test** button.



As a result, the audio notification file will be played back, the path to which you specified in the **Audio files** field (see the Creating and configuring an object section).

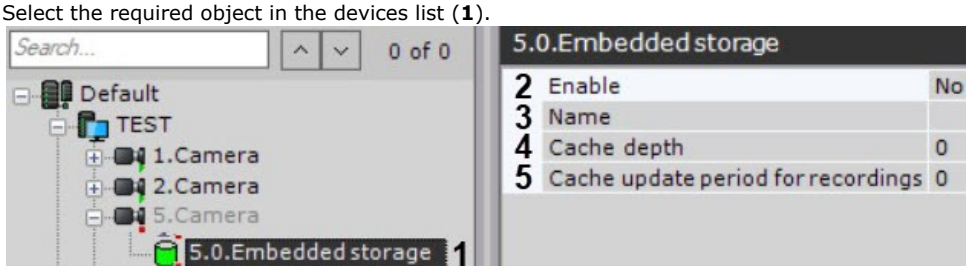
Playing back sound from Client microphone on camera speakers

The Embedded storage object

If a camera has on-board storage (SD card), the system will automatically create the corresponding object.

To configure on-board storage, do as follows:

1. Select the required object in the devices list (**1**).



2. Select **Yes** in the **Enable** field to activate the object (**2**).
3. If necessary, enter the name of the object (**3**).
4. If necessary, specify the **Cache depth** in days (**4**). The setting enables background caching of information about recording intervals in RAM. The value should be in the range [0; 365].
5. In the Cache update period for recordings, set the cache refresh period in seconds (**5**). The value should be in the range [0; 86400].
6. Click the **Apply** button.

You have configured on-board storage. You can view video from on-board storage (if enabled) and copy it to the archive (see Configuring data replication).

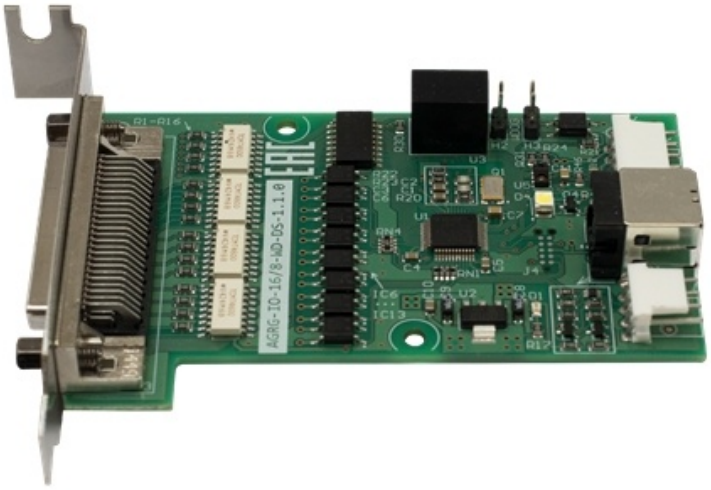
Particulars of Configuration of Devices

AGRG-IO-16/8-WD-DS Sensor-Relay cards

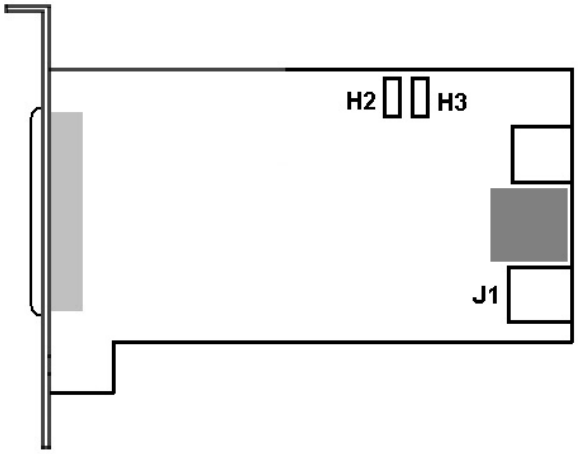
Connecting AGRG-IO-16/8-WD-DS Sensor-Relay cards

The *AGRG-IO-16/8-WD-DS Sensor-Relay* card is an interface of external sensors and external executive devices (relays) as a part of video surveillance and fire and security alarm systems.

The figure shows the appearance of *AGRG-IO-16/8-WD-DS* card.



The layout of card connectors:



The device is controlled via the USB interface. Electrical and technical specifications of the card are given in the Electrical and technical specifications of AGRG-IO-16/8-WD-DS devices section.

Connect the *AGRG-IO-16/8-WD-DS* card to the Server as follows:

1. Switch the computer power supply off. Remove the system cover.
2. Install the *AGRG-IO-16/8-WD-DS* card into a vacant motherboard slot and fix it in the casing.
3. Connect the loop (bundled with the distribution kit) to the **J1** connector and to a vacant USB connector on the motherboard of computer.
4. To activate the hardware control of the hang, connect the wires to the **H2 H3** connector.
5. To connect sensors and relays unsolder the connector bundled with the distribution kit.
    a. The connecting wires from the executive devices are soldered to the contacts marked as "Relay" (see the table below).

Connector	Application	Connector	Application
1	Relay 1 (+)	26	Sensor 5
2	Relay 1	27	Sensor 5

3	Relay 2	28	Sensor 6
4	Relay 2	29	Sensor 6
5	Relay 3	30	Sensor 7
6	Relay 3	31	Sensor 7
7	Relay 4	32	Sensor 8
8	Relay 4	33	Sensor 8
9	Relay 5	34	Sensor 9
10	Relay 5	35	Sensor 9
11	Relay 6	36	Sensor 10
12	Relay 6	37	Sensor 10
13	Relay 7	38	Sensor 11
14	Relay 7	39	Sensor 11
15	Relay 8	40	Sensor 12
16	Relay 8	41	Sensor 12

b. The connecting wires from the sensors are soldered to the contacts marked as "Sensor" (see the table below).

Connector	Application	Connector	Application
17	Sensor 1	42	Sensor 13
18	Sensor 1	43	Sensor 13
19	Sensor 2	44	Sensor 14
20	Sensor 2	45	Sensor 14
21	Sensor 3	46	Sensor 15
22	Sensor 3	47	Sensor 15
23	Sensor 4	48	Sensor 16
24	Sensor 4	49	Sensor 16
25	+ 12V (Output)	50	GND (Ground)

6. Fix the unsoldered connector in the casing bundled with the distribution kit.
7. Connect ready-for-use connector to external connector of the card in order to connect sensors and relays to the Server.

The *AGRG-IO-16/8-WD-DS* card is now connected.

Electrical and technical specifications of AGRG-IO-16/8-WD-DS devices

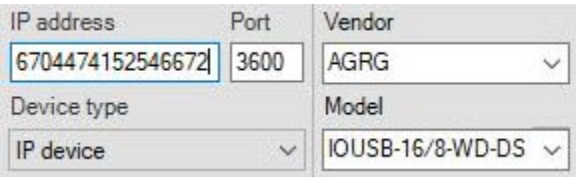
When connecting the AGRG-IO-16/8-WD-DS sensor-relay cards, the electrical and technical specifications shown in the table below should be considered.

Parameter	Specification
Galvanic isolation on inputs/outputs	3750 V
Inputs	Quantity - 16 Type - current loop Galvanic isolation - Yes Maximum voltage - 60 V Rated voltage - 12 V Maximum current - 60 mA
Outputs	Quantity - 8 Type - open collector Galvanic isolation - Yes Maximum voltage - 300 V Maximum current - 150 mA Minimum pick-up voltage - 1.0 V Minimum pick-up current - 5 mA
Reset Timer (Watchdog)	Customizable
Ping interval of all alarm inputs	100 ms for all contacts. Customizable
PC connection interface	USB 2.0, up to 5 meters
Power supply	500 mA consumption from USB port

Special features of configuring AGRG-IO-16/8-WD-DS card in Axxon One

The connected card is automatically detected in the IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).

If you add a device manually, enter the serial number of the device in the **IP address** field.



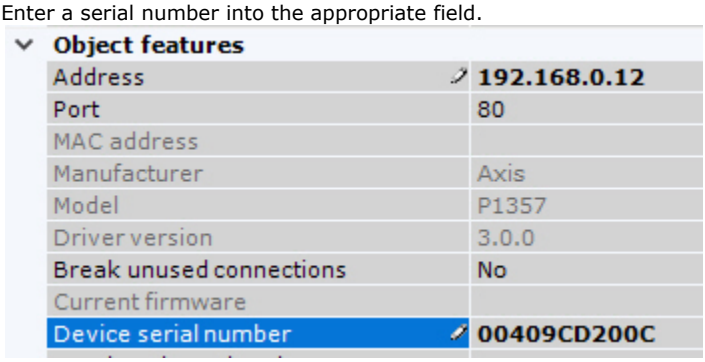
To read the serial number, use the manufacturer's utility.

Axis IP Devices

Serial number check

To check serial numbers of Axis IP devices, do the following:

1. Enter a serial number into the appropriate field.



2. Click **Apply**.
3. The device will be reconnected. Upon reconnection, the entered serial number will be checked against the real one. If numbers do not match, a separate event will be registered in the system Log.

Bonjour function

For Axis IP devices on which the Bonjour function is supported and enabled, changing the default value of the **Friendly name** paramet er is strongly discouraged. If an arbitrary **Friendly name** value is set for an Axis IP device, a search for connected equipment in the *Ax xon One* software package will give incorrect results for this IP device.

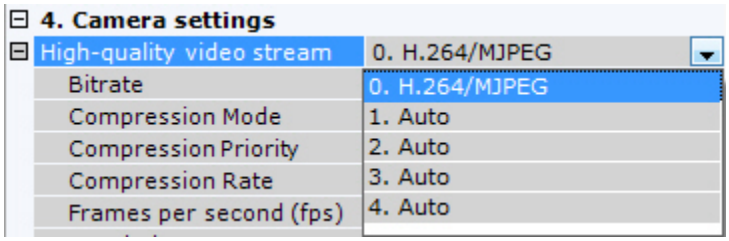
> **Note**
>
> - The **Friendly name** parameter is configured through the Web interface of the IP device: Setup -> System options -> Network -> Bonjour.
> - The default value of the **Friendly name** parameter is as follows: AXIS <model name> - <mac address>, where <model name> is the model of the Axis IP device and <mac address> is its MAC address (for example, AXIS 214 – 00408C7D2610).

Video streams

Axxon One can access the following video streams from Axis IP devices:

1. H.264/MJPEG video.
2–5. Streams matching the Quality, Balanced, Bandwidth, and Mobile profiles. These profiles are configured via the camera's Web interface.

In *Axxon One*, the Quality profile corresponds to stream **1. Auto**, Balanced is stream **2. Auto**, Bandwidth is stream **3. Auto**, and Mobile is stream **4. Auto** (see The Camera object).



CCTV Keyboards

General Information about CCTV Keyboards

Video surveillance control panels can be connected to *Axxon One* in two ways:

1. Connecting a panel via the Windows driver as an HID USB device. This method makes the panel immediately available for specifying hotkeys (see Assigning hot keys).

   > **Attention!**
   >
   > In HID mode, some control panel buttons may not work in *Axxon One*.

2. Connecting a panel via the *Axxon One* driver. Using this method, the panel is added to the system similarly to that of IP devices (see Searching, adding, configuring and removing IP devices).

   > **Attention!**
   >
   > To connect a control panel in this way, you need the *Axxon One* software to be installed in the **Server and Client** con figuration. It's not possible to operate a board as a remote client.

The following control panels are supported in the current version of *Axxon One*:

	Windows driver	***Axxon One* driver**
Axis T8310 (T8311, T8312, T8313)	+	+
Dahua DH-NKB1000	+	+
PELCO KBD5000	+	+
Videotec DCZ	+	+
Hikvision DS-1005KI	+	+
Hikvision DS-1100KI	-	+
Hikvision DS-1200KI	-	+
Hikvision DS-1600KI	-	+
UNIVIEW KB-1100	-	+

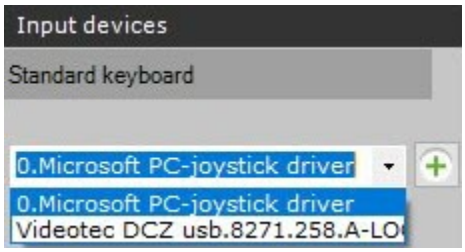
Axis T8310 specific configuration features

Setting up on a Server

To make a T8132 keyboard operate with Rev01 hardware, restart the *Axxon One* VMS server after you create the **IP Server** object (see Shutting down a Server, Starting a Server).

Setting up on a Client

You can use the Axis T8310 control board with remote Clients through the driver embedded into the *Axxon One* software. The panel is not added to the system as an IP device, and is immediately available for assigning hotkeys.



Various models differ in connected devices.

T8310	All devices
T8311	Joystick only
T8311 / T8312	Joystick and keypad
T8311 / T8313	Joystick and jog dial
T8312	Keypad only
T8312 / T8313	Keypad and jog dial
T8313	Jog dial only

Hikvision DS-1100KI specific configuration features

To work with the DS-1100KI network keyboard in *Axxon One*, power on the device and do as follows:

1. Switch the keyboard to **Server** mode.
2. Select **Third Platform Software**.
3. Enter the *Axxon One* Server's IP address and communication port number.
4. You have to use the same port to add the device to the *Axxon One* VMS.

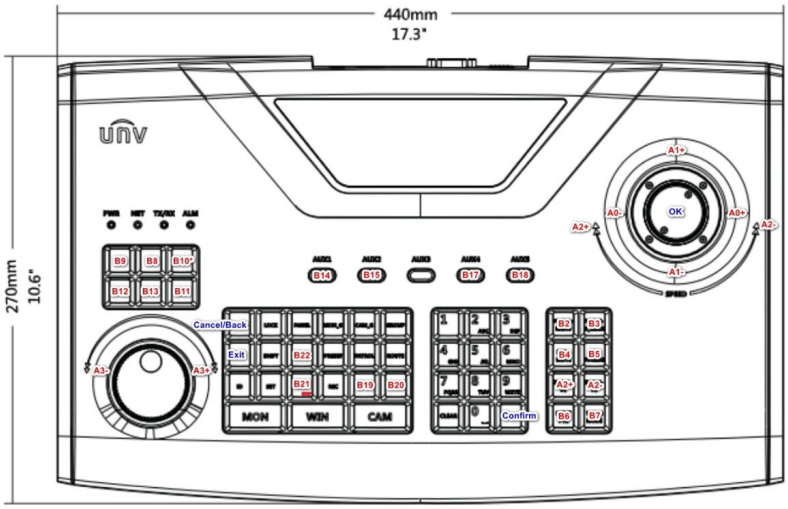
UNIVIEW KB-1100 specific configuration features

On page:

- General description of the UNIVIEW KB-1100 PTZ control device
- Configuring a remote control before adding it to Axxon One
- Configuring UNIVIEW KB-1100 in Axxon One

General description of the UNIVIEW KB-1100 PTZ control device

A schematic representation of the UNIVIEW KB-1100 PTZ control device is shown in the figure below.



The following physical controls are available on the device:

Joystick is a rotary control moving along three axes:

- Pan axis (panning: left or right deviation).
- Tilt axis (tilt: up or down deviation).
- Zoom axis (scaling: clockwise or counterclockwise deviation).

Acceleration along each of the three axes depends on the degree of deviation from the center. The movement is carried out until release. When released, the control returns to its original position.

Jog-Wheel (not integrated into the *Axxon One* software package!) is a rotary control rotating only around its axis. When released, the control returns to its original position. In the illustration it is located at the bottom left (outer ring).

Shuttle is a rotary control rotating only around its axis. Allows the intermittent movement in one of two directions. It has no initial position; when released, it remains in place. In the illustration it is located at the bottom left (inner ring).

Button is a push control element that can represent two states. Allows the call of one of two functions (the function for pressing and the function for releasing). When released, it returns to its original position ("not pressed" state).

Of all the push-button controls of the remote control, the following blocks are integrated:

- A block of playback control keys (6 keys on the left: the record button is triggered after pressing a button on the joystick).
- Block of keys for control of focus, zoom, aperture and PTZ presets (8 keys).

The following keys to manipulate the device interface are also available (not related to *Axxon One*):

- Pressing the button on the remote control joystick (OK) (equivalent to pressing the ENTER key).
- Cancel the action / return one step back in the remote control menu (equivalent to pressing the ESC key).
- Numbers / letters are entered from the numeric keyboard, the mode (upper/lower register, digits) is switched by the SHIFT key.
- Moving through the menu items and within the fields is carried out by deviating the remote control vertically / horizontally.

Configuring a remote control before adding it to Axxon One

Configure the network PTZ 4-dimensional Joystick Remote Control from Uniview (KB-1100) before you create the appropriate object in the *Axxon One* VMS. Proceed as follows:

1. Switch on the control device.
2. Enter username and password in the device display. The default credentials are as follows:
    a. Login: admin.
    b. Password: 123456.
3. Configure the device network configuration. To do this, in the Local Cfg -> Net Cfg menu, set the following settings:
    a. IP address.
    b. Mask.
    c. Gateway.
4. Add the *Axxon One* Server to the internal configuration of this CCTV joystick keyboard. To do this, in the Dev Manage -> Manual Cfg -> Add Dev menu, set the following settings:

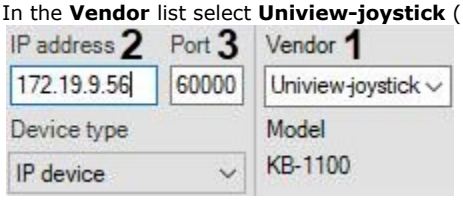
    a. ID – enter any number (range: 1-240, the number must not coincide with the ID of the remote control or other already added device).
    b. Name – enter a string (1-8 characters).
    c. DType – select VM (VideoManagementSystem, i.e. *Axxon One*).
    d. LType – select NetWork (the device is integrated for connecting to *Axxon One* via the network).
    e. After selecting LType, press the button on the joystick and enter the IP address of the *Axxon One* VMS Server and the port used (the default port is 60000).
5. Connect to *the Axxon One VMS*, added in the step above. To do this, enter the ID specified above in the FindDev -> Dev ID menu or select the found profile in the Dev Manage -> Search Dev menu.
6. If the device is found, information about it will be displayed on the device display.
7. Press on the ID field. This will onboard the remote control in the *Axxon One* VMS.

Setting up the UNIVIEW KB-1100 control device is completed.

Configuring UNIVIEW KB-1100 in Axxon One

Configure the UNIVIEW KB-1100 PTZ joystick control as follows:

1. Go to IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the **Vendor** list select **Uniview-joystick** (**1**).



3. In the **IP address** field, enter the IP address of the remote control (**2**).
4. In the **Port** field, enter the port number, as set in step 4 of the remote control settings configuration (**3**).
5. Click the  .
6. Enable the newly created **IP Server** and its **Channel** child object.

You have configured the UNIVIEW KB-1100 Joystick Remote Control and CCTV keyboard.

Hikvision DS-1200KI specific configuration features

On the page:

- Configuring the Hikvision DS-1200KI control device before adding it to Axxon One
- Features of the Hikvision DS-1200KI control device operation in Axxon One

Configuring the Hikvision DS-1200KI control device before adding it to *Axxon One*

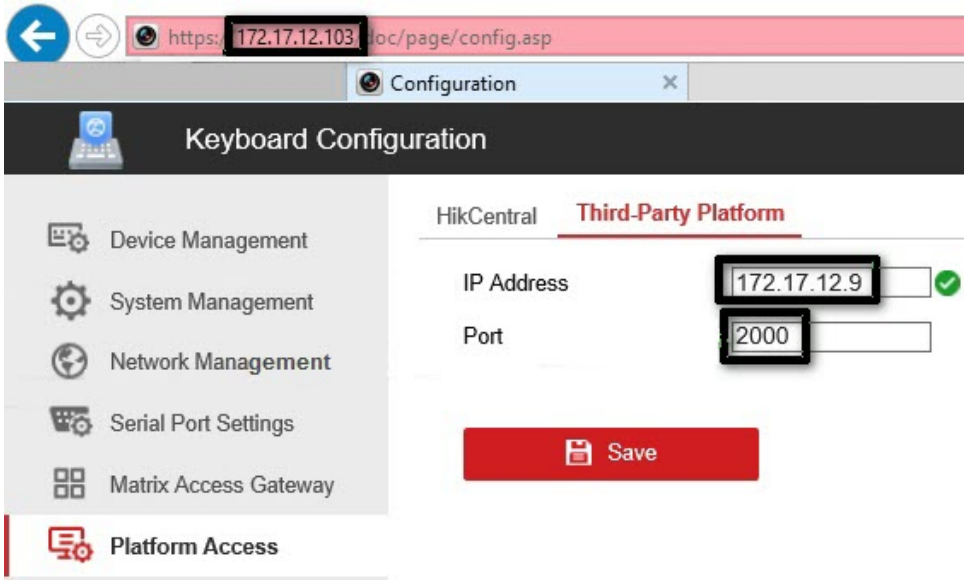
Configure the Hikvision DS-1200KI PTZ control device as follows before creating the corresponding object in *Axxon One*:

1. Set the control device address: **Select System – Network** in the device internal menu, then disable DHCP and set IP address and gateway.



2. Set the *Axxon One* server IP address and port on the device. Open the device Web interface by entering the above set IP address in the web browser, then select **Platform Access – Third-Party Platform**.

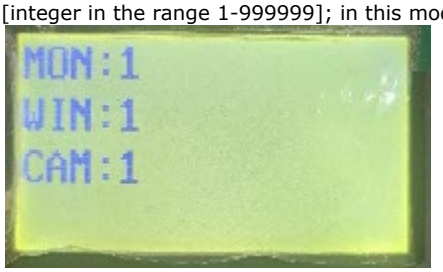
> **Note.**
>
> The Web interface is only available on https by default, so please use https prefix before the IP address.



3. Set the **8. Private VMS** mode in the device's internal interface.



4. Transfer the PTZ control device to operating mode by one of the following actions:
    a. Select any monitor MON (monitor) [integer in the range 1-9999], any camera CAM (camera) [integer in the range 0-999999]; in this mode all keys will work, including the WIN (subwindow of video wall) and MULT (layout size) keys for the monitor and camera.
    b. Select any camera CAM (camera) [integer number in the range 1-999999 (number 0 is available only when setting the monitor)]; the WIN, MULT and CAM-G keys will not work in this mode.
    c. Select any monitor MON (monitor) [integer in the range 1-9999] and any group of cameras CAM-G (camera group) [integer in the range 1-999999]; in this mode, only the MULT, OK keys and the rotations of the joystick axes will work.



> **Note.**
>
> To select these parameters, enter a number on the device keypad, then press the corresponding key (MON /WIN/CAM/CAM-G).
>
> If the the server IP address and/or port is not accessible from the PTZ control device, the "Connect failed" message will be displayed on the control device screen after pressing the MON/WIN/CAM/CAM-G keys.

The Hikvision DS-1200KI PTZ control device is now preconfigured.

Features of the Hikvision DS-1200KI control device operation in *Axxon One*

When the MULT, PRESET, PATROL, or PATTERN keys are pressed on the device, the following actions are performed:

- when entering a number in the range 1-99 and pressing MULT for each number, *Axxon One* receives a message about pressing the corresponding separate key with a number in the range 23-121 (B22-B120);
- when pressing PresetRec for the first time, *Axxon One* receives a message about pressing key 13 (B12), and the device displays **Record started**;
- after pressing PresetRec for the second time, *Axxon One* receives a message about pressing key 12 (B11), and **Record ended** appears on the device display;
- when entering a number in the range 1-65535 and pressing PresetRec, *Axxon One* receives a message about pressing key 22 (B21), and the device displays **PRESET:**;
- when entering a number in the range 1-65535 and pressing Patrol, *Axxon One* receives a message about pressing key 17 (B16), and the device displays **PATROL:**;
- when entering a number in the range 1-65535 and pressing PatternPlay, *Axxon One* receives a message about pressing key 18 (B17), and the device displays **PATTERN:**;
- when entering a number in the range 65536-999999 and press any of the PresetRec/Patrol/PatternPlay buttons, nothing happens: such numbers are not processed.

Dahua DH-NKB1000 specific configuration features

Keyboard operating modes

To work correctly with *Axxon One* VMS, the keyboard must be recognized by Windows OS as the KEYBOARD 1000 game device.

If the keyboard is recognized as an HID device, hold down the Shift key on the device to toggle its operating mode.

Specific OS settings

If Windows Device Manager recognizes the keyboard as BETTER_USB_HS, the device will not work.

In this case, roll back the device driver. For correct operation, Windows Device Manager has to recognize the keyboard as a HID-compatible game controller.

Specific *Axxon One* settings

The *Axxon One* VMS may recognize a Dahua DH-NKB1000 keyboard as a Hikvision-joystick DS-1005KI due to their shared device ID.

For correct operation, the keyboard has to be recognized as Dahua DH-NKB1000.

The Pattern button will not work in the *Axxon One* VMS.

CH VM-Desktop USB multifunction controller

For the controller to work properly in *Axxon One*, the controller must be connected before the *Axxon One* Client is started.

> **Note**
>
> To learn about connecting the device, consult the manufacturer's official documentation.

Controller keys cannot be remapped.

Use of the CH VM-Desktop USB multifunction controller in *Axxon One* is described in the corresponding section.

Configuring Vivotek Panoramic PTZ

Vivotek Panoramic PTZ is a technology for linking a fisheye camera to a PTZ camera.

This Vivotek technology allows simultaneously maintaining full situational awareness in the field of view of a fisheye camera, while maintaining the ability to carefully monitor a specific area in depth by using a PTZ unit.

Vivotek Panoramic PTZ is supported by the fisheye cameras Vivotek SF8172 and Vivotek SF 8172V and by the PTZ camera Vivotek SD8362E.

To use this technology in *Axxon One*:

1. Install and configure the cameras in accordance with the official Vivotek documentation.
2. Add the cameras to an *Axxon One* configuration.

Vivotek Panoramic PTZ support in *Axxon One* is implemented via the Areazoom (see Control using Areazoom) and Point&Click functions (see Control using Point&Click).

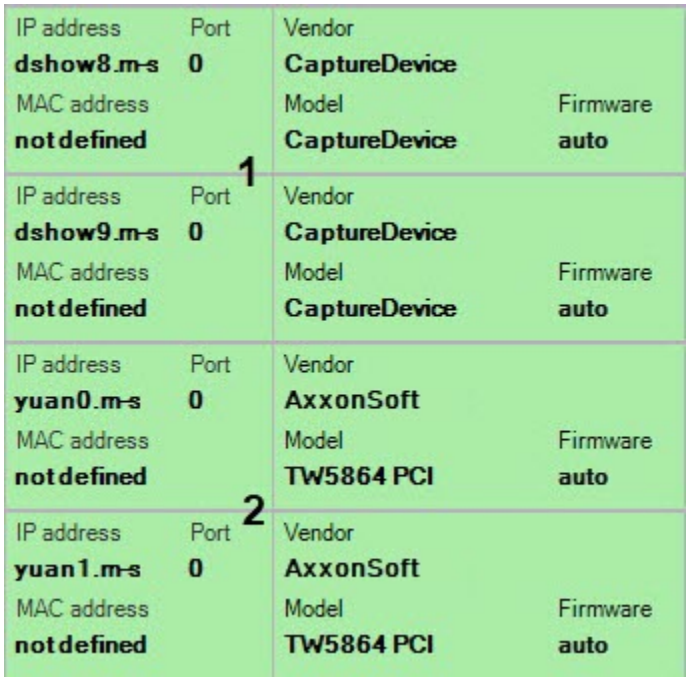
Video capture cards

Axxon One supports 3 PCIe and one USB video capture cards:

1. PCIe:
    a. Yuan SC300Q16.
    b. Yuan SC3C0N8.
    c. Yuan WS216.
2. USB: Yuan PD652.

WS-216 video capture cards

In *Axxon One*, each WS-216 video capture card corresponds to two devices: manufacturer **AxxonSoft**, model **TW5864 PCI** (driver **Yuan**, **2**) and manufacturer **CaptureDevice**, model **CaptureDevice** (driver **DShow**, **1**).



Note

If you have a WS-216 card added through the Yuan driver, in Windows Server OS you should activate: Desktop Experience Feature.

Cameras connected to *Axxon One* through the WS-216 card require the following configuration: add **AxxonSoft TW5864 PCI** device configuration (**2**) and select the checkbox **Send settings to device** (see The Camera object).

Note

Axxon One does not support receiving uncompressed video from WS-216 video capture cards.

For video cameras that are connected through WS-216 video capture cards, you can choose one of the two codecs for a video stream:

1. H.264 (configurable).

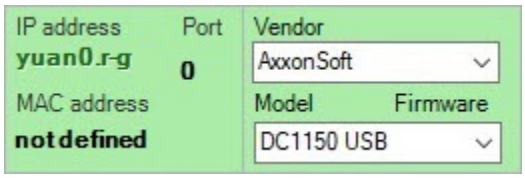
2. H.264 (minimum resolution, non-configurable).

YUAN PD652 cards

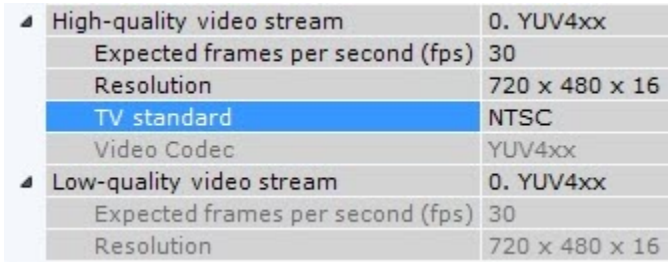
To work with the YUAN PD652 cards in *Axxon One*, do as follows:

> **Attention!**
>
> Please see the list of supported OS for the YUAN PD652 board on the official website of the manufacturer.

1. Disable the system check for the digital signature of the drivers and install the card driver.
2. Connect the camera to the card.
3. Create an IP device in *Axxon One*. The search result shows the camera connected through the YUAN PD652 card as follows.



4. In the IP device settings, select the TV standard supported by your camera.



Joysticks

Only joysticks that are detected in Windows as gaming input devices can be used in *Axxon One* for controlling PTZ cameras.

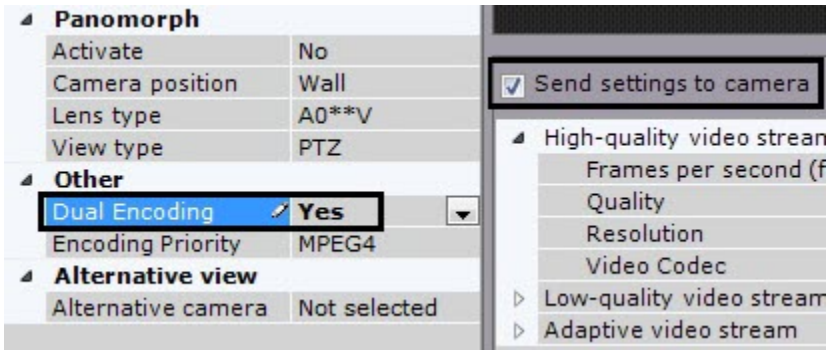
Information on how to view the status for a connected joystick is available in official Microsoft documentation.

> **Note**
>
> We recommend that you calibrate the joystick before you start working with *Axxon One*.

Sony IP Devices

Some Sony models support encoding of the video signal in two formats simultaneously. To use this option you must perform the following steps:

1. Select the **Send settings to camera** checkbox.
2. From the **Dual Encoding** list, select the codec which will take priority when dual encoding.

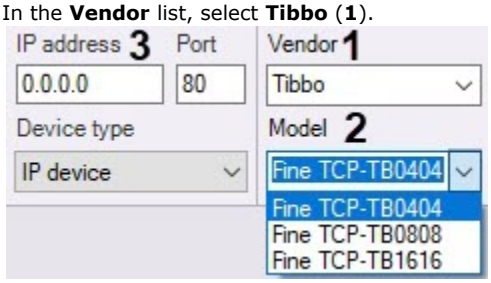


Setting up Tibbo relay/loop boards

Tibbo relay/loop boards allow monitoring air temperature and humidity on your premises.

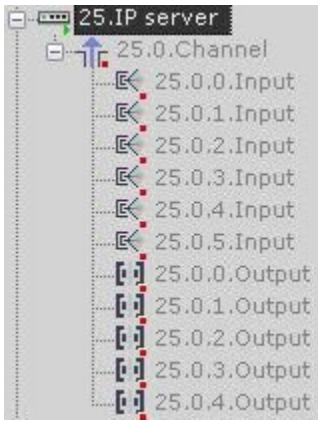
To add a board to the configuration, do the following:

1. Go to IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the **Vendor** list, select **Tibbo** (**1**).



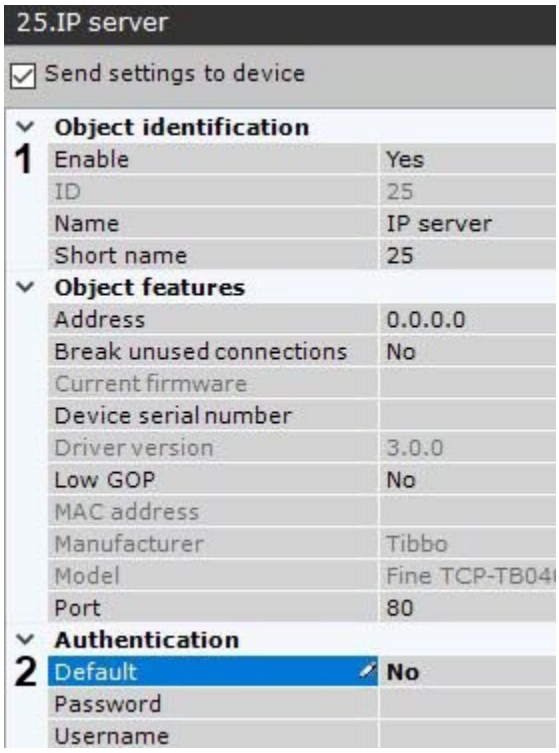
3. Select your board from the **Model** list (**2**).
4. Enter the IP address of the board (**3**).
5. Click the  button.

The parent **IP Server** object, and **Channel**, **Input** and child objects under it will be added.

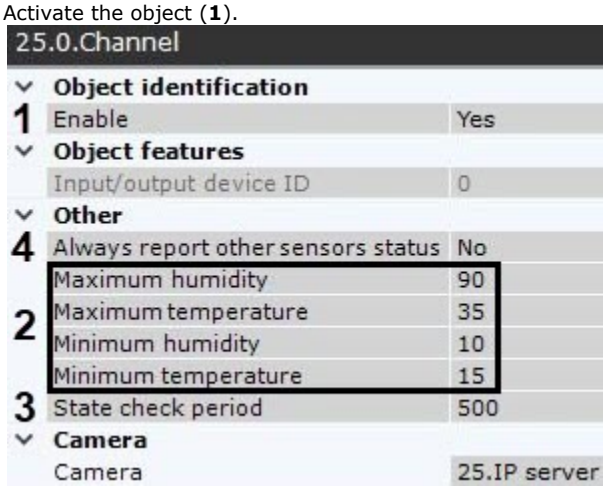


To configure the board, do the following:

1. Select the **IP Server**.



2. Activate the object (**1**).
3. In the **Authentication** parameter group, set **Default** to **No** (**2**).
4. Select a **Channel** object.
5. Activate the object (**1**).



6. Set permissible ranges for temperature (in centigrade) and relative humidity (in per cent) (**2**). If a reading falls out of the range, the corresponding Input (sensor) triggers an alarm.
7. Set the check period in milliseconds (**3**).
8. If you need to report sensors statuses when readings are within the range, set **Yes** for **Always report other sensors status** (4). In this case, the following records will appear in the log file in specified intervals of time (see paragraph 7):

```
Special humidity ray#16 changed status to: false ,Sensor value: 16,8 Correct range [15, 58]. Time: …..
Special temperature ray#17 changed status to: false ,Sensor value: 29,8 Correct range [20, 60]. Time: …..
```

9. Click **Apply**.

Now, the board is configured. Current temperature/humidity value will be displayed next to input's icon on the Map (see Displaying device status).

Configuring Tracking objects

Axxon One includes several features for tracking moving objects.

With Tag&Track Pro, an object can be tracked by a PTZ camera under the guidance of panoramic cameras.

> **Attention!**
>
> To use Tag&Track, make sure you have a PTZ camera in *Axxon One* that supports Absolute Positioning. The devices that support Tag&Track Pro are listed in the Drivers Pack documentation. If a PTZ camera does not meet the requirement, you should add it to the VMS via Onvif.

With Tag&Track Lite, the operator is alerted to the camera in front of which the moving object is most likely to appear next. The camera is predicted based on object trajectory and mapping of cameras to map locations.

For these functions to work, all video cameras involved must have an activated **Object tracker** or **Neurotracker** object (see General information on the standard detection sub-tools).

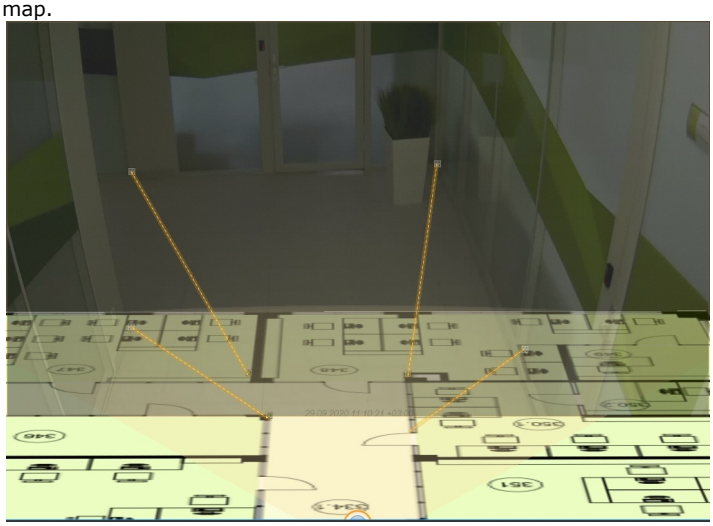
Configuring Tag&Track Lite

To follow objects with Tag&Track Lite, mount the cameras at the top of the scene, so that you can track motion across the plane (floor, ground) from above.

> **Attention!**
>
> The use of fish-eye cameras is not allowed.

To configure Tag&Track Lite, do as follows:

1. Create **Object tracker** or **Neurotracker** objects for all cameras.
2. Go to the Layout Editing mode (see Switching to layout editing mode).
3. Add video cameras to the map (see Adding video cameras).
4. Set the exact location of the video cameras, field of view and coverage areas shared with other video cameras (see Configuring a camera in standard map viewing mode). FoVs intersection – area, common for FoVs of two cameras – must be no less than triple footprint of the tracked object.
5. For each video camera:
    a. Switch to immersive mode (see Configuring cameras in immersion mode).
    b. Set 4 anchor point, that will correlate objects (door, corner, etc.) in the video image with their representation on the map.



6. Save the layout (see Exiting Layout Editing mode).

Configuring Tag & Track Pro

To configure Tag & Track Pro:

1. Link panoramic cameras to a PTZ camera (see Linking panoramic cameras to a PTZ camera).

   > ⚠ **Attention!**
   >
   > The use of fish-eye cameras is not allowed.

2. Calibrate cameras (see Matching the telemetry device positions with the overview cameras frame points (calibration)).
3. Set the PTZ mode (see Setting PTZ mode for Tag & Track Pro).

Camera requirements for Tag&Track Pro

Attention!

- To use Tag&Track Pro, make sure your PTZ camera supports Absolute Positioning. The devices that support Tag&Track Pro are listed in the Drivers Pack documentation.
- When connecting via the ONVIF protocol, Absolute Positioning support is also required. Contact camera vendor for Information on the Absolute Positioning support in the ONVIF protocol.
- The use of fish-eye cameras is not allowed.

For the Tag&Track Pro function to operate, the video cameras should be positioned on the top facing the flat surface (floor, ground) where the objects are moving.

The overview and the PTZ video cameras should be pointed in the same direction and be close to each other. If they are far from each other, they can interpret the scene differently. Because of this, sometimes the algorithm may not operate correctly.

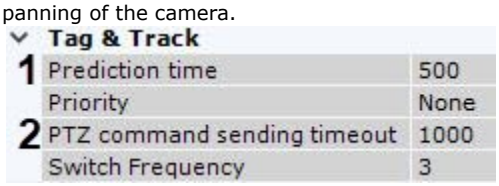
For all objects from the overview video camera, the corresponding pan coordinates should be in the range from 0° to 180°, or from −180° to 0°.

In addition, the overview video cameras should meet the following requirements: Video requirements for scene analytics detection tools.

Configuring Smooth Motion for PTZ cameras

To smooth panning of a PTZ camera while using Tag & Track Pro, you can configure:

1. The degree of prediction (**1**). This value should be in the range from 1 to 3000. The higher the value, the smoother is the panning of the camera.



2. The rate at which coordinates are sent in milliseconds (**2**). This value should be in the range from 100 to 3000.

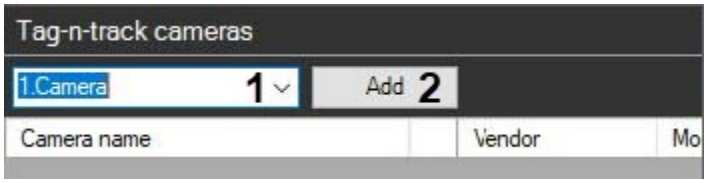
Linking panoramic cameras to a PTZ camera

To link panoramic cameras to a PTZ camera:

1. Go to the **PTZ** object of the relevant camera.
2. In the **Tag-n-track cameras** group, in the list (**1**), select the camera that you want to link to the PTZ camera. Click the **Add** b utton (**2**).

   > **Note**
   >
   > To search for a camera, enter its short name, the full or partial name in the **1** box.

   > **Note**
   >
   > You can add only those cameras for which the Object Tracking was created and activated.

3. Repeat this action for all cameras that you want to link to the PTZ. You can connect any number of panoramic cameras to a PTZ camera.

   > **Note**
   >
   > To remove a camera from the list of panoramic cameras, click the ×.

4. Click the **Apply** button.

Linking of panoramic cameras to the PTZ camera is now complete.

Matching the telemetry device positions with the overview cameras frame points (calibration)

For the precise tracking of the object under observation, you should calibrate the telemetry device by matching at least four telemetry device positions with the frame points of each overview camera.

> **Attention!**
>
> The recommended number of points that should be set is 4-10. If you add more points, the algorithm will be configured more precisely. However, this may increase the chance that some of the points are set up incorrectly, which may cause the decrease of the operation quality.
>
> The points set in the calibration setting should not be on the same line for both the overview and the PTZ camera. It is recommended to set the points for both cameras so that they evenly cover the entire frame.
>
> The calibration points should be set on the same surface (floor, ground). It is not recommended to set the points on different surfaces (for example, when some points are on the ground, and other points are on a tree, etc.).

To calibrate the telemetry device, do the following:

1. Select the overview camera from the list (see Linking panoramic cameras to a PTZ camera).
2. Focus the PTZ camera on any point. To do this, in the preview window click the button and change the orientation of the lens in one of the following ways:
    a. Left-click on the frame and holding the button, move the mouse cursor in the required direction.
    b. Use the Point&Click function (see Control using Point&Click).
3. Left-click to add a point to the frame of the overview camera to which the PTZ camera is currently oriented.



Attention!

The object under observation should be inside the frame of the PTZ camera.

4. Repeat the process to set at least 4 points.
5. Repeat the process for all overview cameras (select the camera by clicking in the list of the overview cameras).
6. Click the **Apply** button to save the calibration points.

Calibration of the telemetry device is complete.

It is recommended to perform a calibration check after calibration is complete. To do this, do the following:

1. Click the  button to the right of the preview window of the overview camera.
2. Click on different points in the image of the overview camera. If the PTZ camera is positioned correctly, the calibration is correct.

Note

To delete the calibration points, click the button.

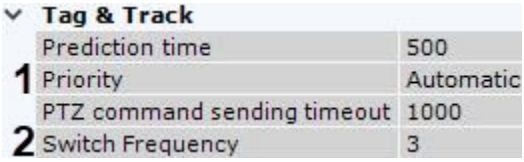
Setting PTZ mode for Tag & Track Pro

> **Attention!**
>
> The use of fish-eye cameras is not allowed.

Tag & Track Pro can be used in four PTZ modes:

1. **Manual** – in this mode, a PTZ camera starts tracking an object only after the user selects the object in the viewing tile.
2. **Automatic** – in this mode, a PTZ camera automatically initiates tracking of all active objects. The PTZ camera focus on each object in sequence based on the specified dwell interval.
3. **User priority** – in this mode, automatic mode is used unless the user manually selects an object for tracking. As soon as the user selects an object for tracking, manual mode is activated. When an object is no longer selected or disappears from the PTZ field of view, automatic mode is reactivated.
4. **Manual PTZ control** – in this mode, the operator can take control of the PTZ cameras at any time. If the user does not control the PTZ camera, then the **Automatic** mode is used.

Select a mode in the **Priority** list (**1**). The dwell time is specified in seconds in the corresponding field (**2**).



To save changes, click the **Apply** button.

Receiving Events from External Systems

Axxon One synchronizes the information from cash registers with the video from cameras pointed at the register area allowing you to monitor the process. In addition, *Axxon One* operators can receive events from any *Axxon PSIM* objects in real time and correlate the received information with the video. The event sources can be e.g.:

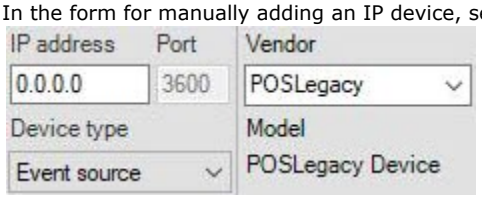
- Access control systems
- Security and fire alarm systems
- Perimeter security system

In *Axxon One*, information from external sources is superimposed on video from a selected camera.

Event source object

Axxon One uses the **Event source** object to get external events. To create the object, make sure that:

1. Run IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the form for manually adding an IP device, select **Event source** in the **Device type** drop-down list.



3. Click the  button.

The **Event source** object is added to the system.

> **Note**
>
> Once created, the **Event source** object is enabled by default. To disable, select **No** in the **Enable** field.

Configuring POS devices

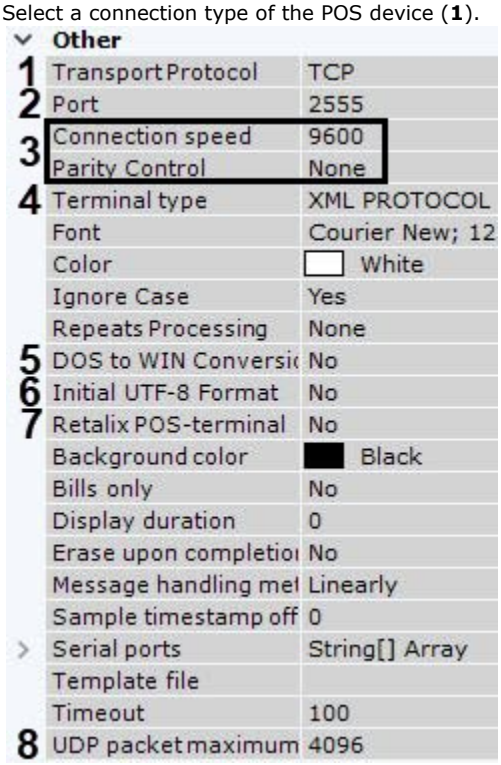
Axxon One can obtain data from POS devices and offers the following capabilities:

1. Show titles in live and recorded video.
2. Search titles in recorded video.

Connecting POS devices

To configure a POS device, do as follows:

1. Select the **Event source** object.
2. Select a connection type of the POS device (**1**).



3. Specify the Server connection port (**2**).
4. To connect via RS-232, select connection speed and parity check (**3**).
5. Select the type of your POS device (**4**).
6. Select **Yes** in the **DOS to WIN Conversion** field if the data from the POS device is DOS-encoded (**5**).
7. If the data is UTF-8 encoded, select **Yes** in the **Initial UTF-8 Format** to enable correct display of captions (**6**).
8. If a Retalix terminal is used, select **Yes** in the corresponding field (**7**).
9. Set the maximum size of UDP datagrams in bytes (**8**). Oversized packets will be ignored.
10. Click the **Apply** button.

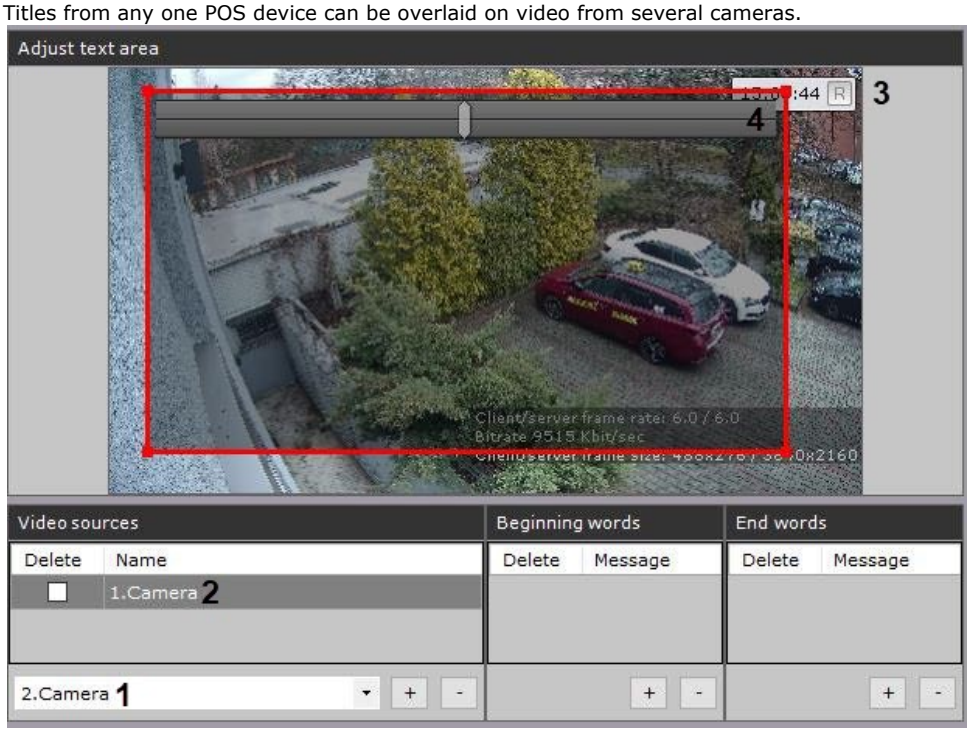
You have successfully connected your POS device.

Configuring titles view

You can configure the font and where you want the titles displayed on screen. The titles are displayed in a rectangular area superimposed on video.

To configure the titles view, do as follows:

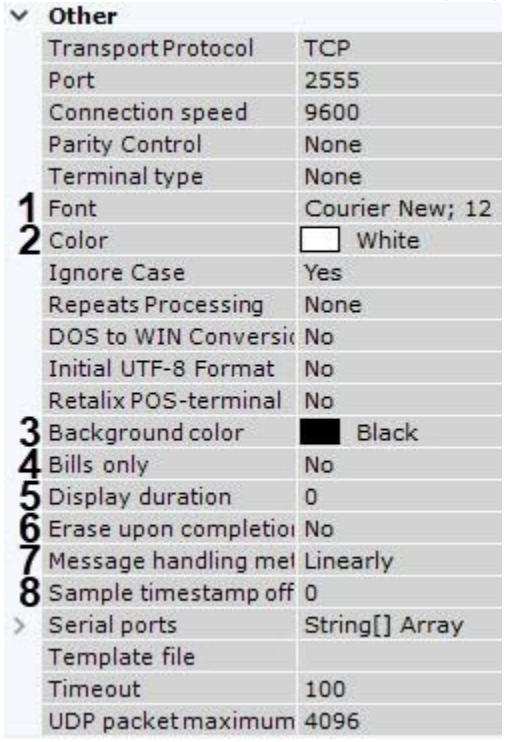
1. In the **Video sources** group, select a camera from the list and click the **+** button to add the camera for titles overlay (**1**). Titles from any one POS device can be overlaid on video from several cameras.



> **Note**
>
> To disable titles overlay for a camera, select the **Delete** checkbox and click the **−** button.

2. Select a camera in the **Video sources** group (**2**). The **Adjust text area** group shows video from the selected camera and the adjustable titles area (**3**).
3. You can configure the titles area: Resize it by moving the anchor points. Move it with Drag-and-drop.
4. Change transparency with the slider (**4**). Slide left for more transparency, slide right for less.

5. In the **Font** filed, click the [...] button and specify font settings in a standard Windows box (**1**).



6. Select font color (**2**).
7. Select captions font color in the camera window (**3**).
8. If you need to display only the lines contained between start and end markers of the receipt, **Yes** for the **Bills only** parameter ( ).
9. In the **Display duration** field, set the time in seconds for accumulated text rows on the screen (**5**). If you set **0**, captions will stay on the screen. New events replace old ones on a continuous basis.

> **Note**
>
> For shops where the checkout is never crowded, we recommend the captions display duration under 10 seconds.

10. If you don't need to display any lines following the end marker of the receipt, set **Yes** for the **Erase upon completion** parameter (**6**).
11. Select a method of processing incoming data (**7**):
    a. **PROCESS_LINEARLY** – incoming data is stored in a buffer until the next EOL is received, and only after that is transmitted to *Axxon One*.
    b. **PROCESS_EVENT** – each data portion is immediately transferred to *Axxon One*.
    c. **PROCESS_JSON** – not available in the current version.
12. By default, titles/captions are written to the database in sync with video. Though you may want to go to **Sample timestamp offset** and set up to 5 seconds time lag/jump in seconds in the range of [-5; 5] (**8**).
13. Click the **Apply** button.

You have configured the titles view.

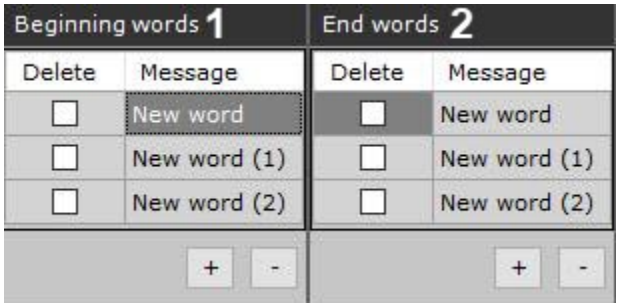
Configuring receipt beginning/end

The database stores only a full receipt. A receipt starts and ends with the configured phrases. If not configured, receipts contain 2000 lines. In this case, search will not work until the receipt is saved into the database (see Search by titles).

> **Attention!**
>
> It is strongly recommended that you configure this setting for shops with low-intensity events at the checkout. Otherwise, the accumulation of 2000 lines can take a long time.

To configure the beginning and the end of a receipt, do as follows:

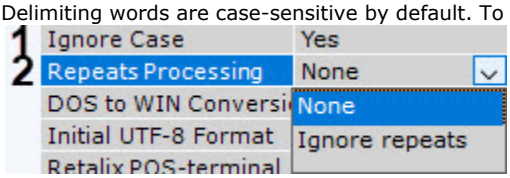
1. Populate the **Beginning words** (**1**) group. To add words, click the **+** button. To remove words, select their **Delete** check boxes and click the − button.



2. Populate the **End words** (**2**) group in the same manner.

> **Note**
>
> You can add any number of delimiting words. Double click a word to edit it.

3. Delimiting words are case-sensitive by default. To ignore case, select **Yes** in the corresponding field (**1**).



4. Select how to treat repetitions (**2**).
   a. Select **Ignore repeats** to skip repeating beginning words before the end words show up. When the end words show up, the next receipt starts with the beginning words.
   b. Select **None** to skip the end words and delimit receipts by the beginning words only.
5. Click the **Apply** button.

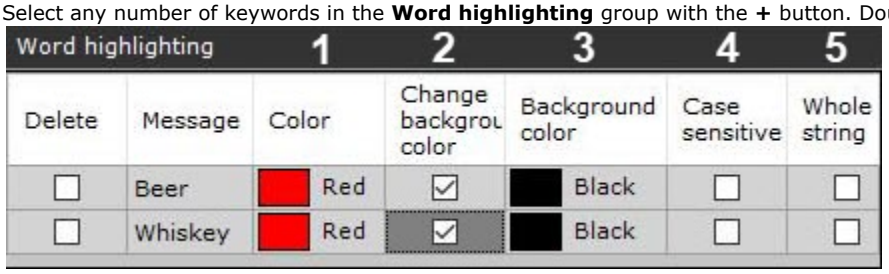
You have configured how receipts are delimited.

Configuring keywords

Keywords can be highlighted in the titles.

To configure keywords, do as follows:

1. Select any number of keywords in the **Word highlighting** group with the **+** button. Double click a keyword to edit it.



> **Note**
>
> To remove words, select their **Delete** check boxes and click the – button.

2. You can also configure these parameters:
   a. Highlighting color (**1**). In the appropriate column, click the button and choose a color.
   b. If you want to change the color of the background of the titles output in the camera window, select the corresponding check box (**2**) and select the required color (**3**) when this word appears.
   c. Select the **Case sensitive** check if you want (**4**).
   d. To highlight the whole line, select the **Whole string** checkbox (**5**).
3. Click the **Apply** button.

You have configured highlighting for keywords.

Importing parcers

A special parsing algorithm processes the receipts and adds data to the receipts database. This is an option for advanced settings.

The choice of parcers depends on POS data structure:

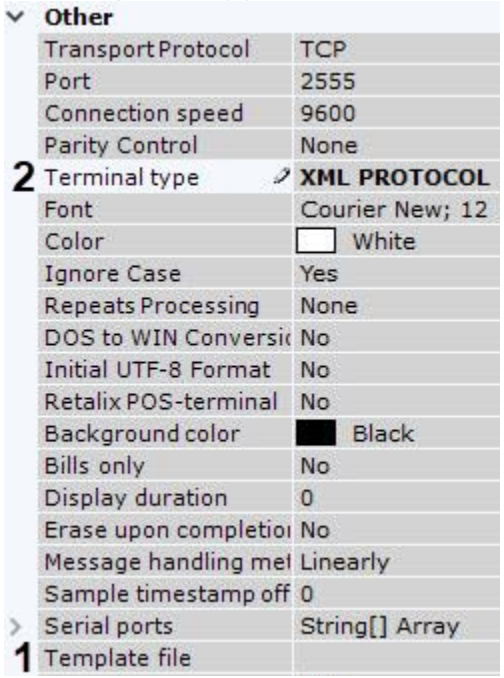
1. XML parcer for .txt files;
2. POS parcer for .prl files.

The XML parser specifies the rules for adding data to the receipts database if you have XML data from a POS terminal. The XML parser also validates the XML data against a schema.

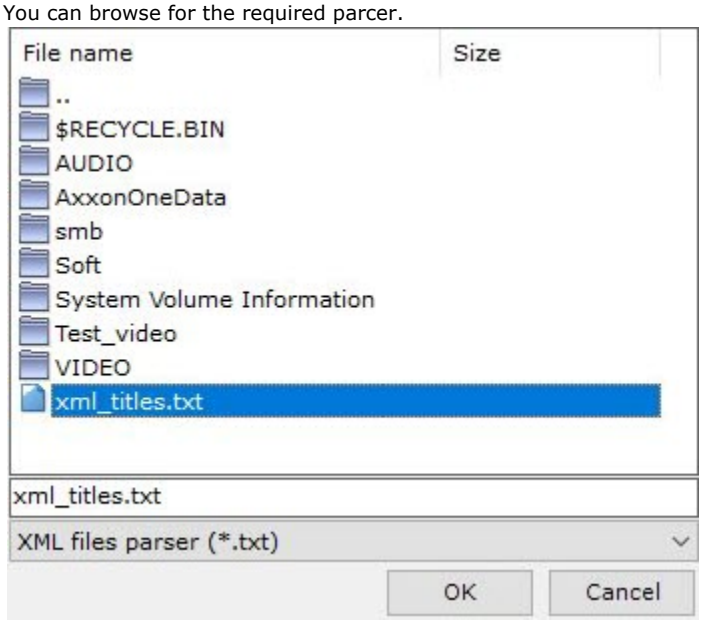
The POS parser specifies the rules for adding data to the receipts database if the data is from a POS terminal is other than XML. The parser depends on the POS terminal data structure.

To import a parcer, do as follows:

1. In the **Template file** (**1**) field, click the button.



You can browse for the required parcer.



2. Select the type of the parser and the file.
3. If you use an XML parser, select **XML PROTOCOL** in the **Terminal type** field (**2**).

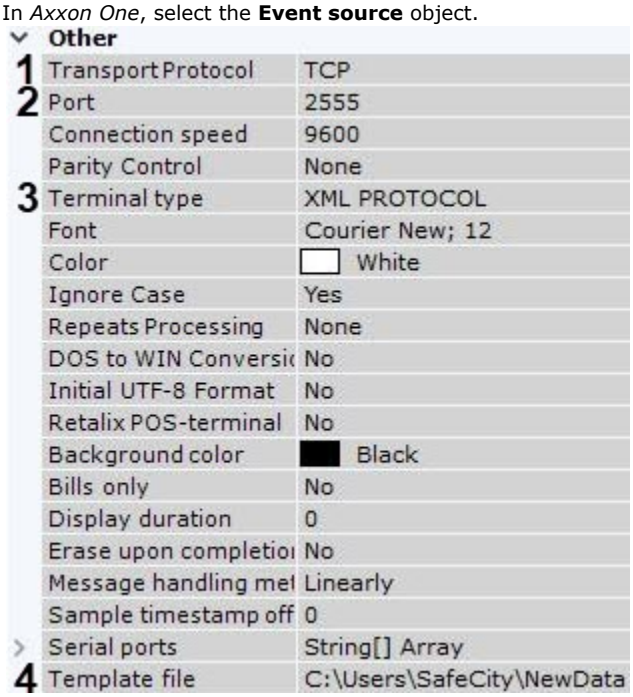
4. Click the **Apply** button.

You have imported the parcer.

Receiving Axxon PSIM Events

To be able to receive *Axxon PSIM* events, do as follows:

1. On the *Axxon PSIM* machine, configure a data transfer module.
2. In *Axxon One*, select the **Event source** object.



3. Select **TCP** in the **Transport Protocol** field (**1**).
4. Specify the connection port to *Axxon PSIM* (**2**).
5. Select **XML PROTOCOL** in the **Terminal type** field (**3**).
6. Select a preconfigured parser (**4**, see Configuring parser).
7. Configure the data output similar to that of the POS device (see Configuring titles view).
8. Configure keywords, if necessary (see Configuring keywords).
9. Click the **Apply** button.

If the setup procedure was done correctly, the events from specified objects will be displayed in the viewing tile on *Axxon PSIM* in the same way as POS device captions do (see Viewing titles from POS terminals).

Configuring Receiving Events from CommaxComplexServer

CommaxComplexServer events can be forwarded to the *Axxon One* VMS in two formats:

1. In JSON format using the **Event source** (see Configuring Commax Complex Server via Event Source).
2. As events from virtual inputs. This creates a virtual IP Server in the VMS (see Configuring Commax Complex Server via virtual IP server).

> **Note**
>
> CommaxComplexServer is smart apartment complex management software. It receives input from gates, doors, elevator call buttons etc.

Configure CommaxComplexServer before connecting to *Axxon One*.

Configuring Commax Complex Server via Event Source

Connect Commax Complex Server via **Event Source** as follows:

1. Run IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the field for manually adding an IP device, select **Event Source** in the **Device Type** drop-down list (**1**).



3. In the **Vendor** list select **Commax Complex Server** (**2**).
4. Enter the destination port name for Commax Complex Server events (**3**).
5. Click the button  .
   The **Event Source** object is added to the system.

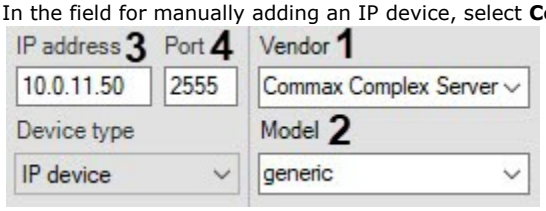
The Commax Complex Server connection is now configured.

> **Note**
>
> You can present information as caption (titles) superimposed on video in the Camera window. See POS configuration instructions for that (see Configuring POS devices).

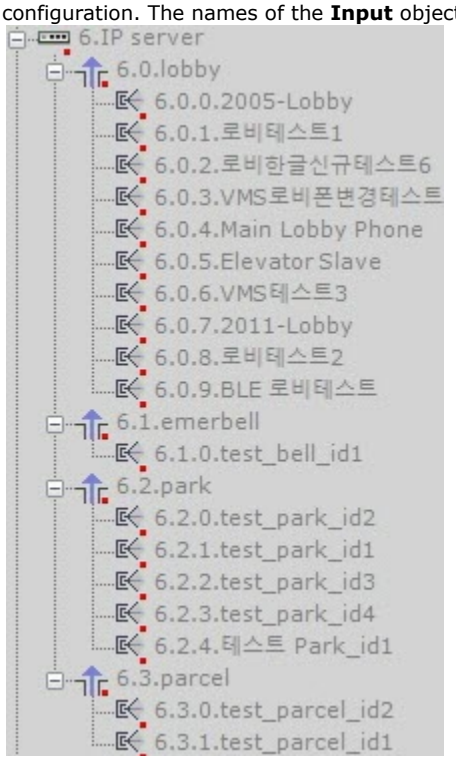
Configuring Commax Complex Server via virtual IP server

Connect to Commax Complex Server via virtual IP server as follows:

1. Run IP Device Discovery Wizard (see Searching, adding, configuring and removing IP devices).
2. In the field for manually adding an IP device, select **Commax Complex Server** in the **Vendor** drop-down list (**1**).



3. Select **generic** in the **Model** list (**2**).
4. Enter the IP address of the Commax Complex Server (**3**).
5. Enter the destination port name for Commax Complex Server events (**4**).
6. Click the button  .
   The parent **IP Server** object and **Channel** and **Input** objects under it are added according to Commax Complex Server configuration. The names of the **Input** objects in the VMS and Commax Complex Server are the same.

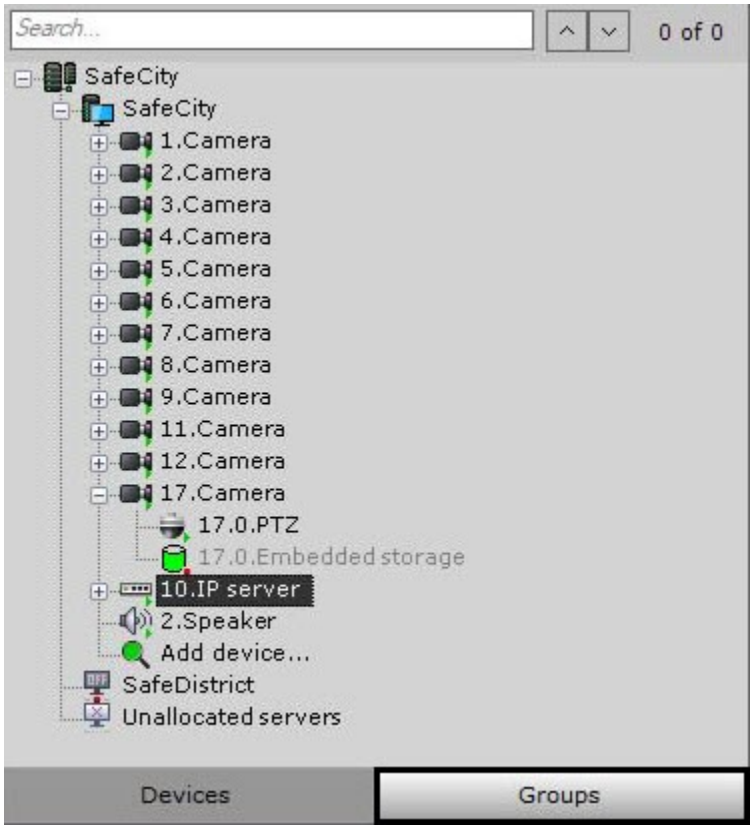


The Commax Complex Server connection is now configured.

Configuring video camera groups

Manual grouping of video cameras is designed to configure group access rights and quickly select the required video camera for display.

Video camera groups are configured through the interface using the **Devices** tab (under **Settings**). To configure device groups, you must have the appropriate permissions to configure devices.



Procedure for configuring video camera groups

Camera groups are configured in the following sequence:

1. Create **Group** objects.
2. Add video cameras created in the system to the **Group** objects.
3. Create a system of groups and subgroups.

Creating a Group object

To create a **Group** object, complete the following steps:

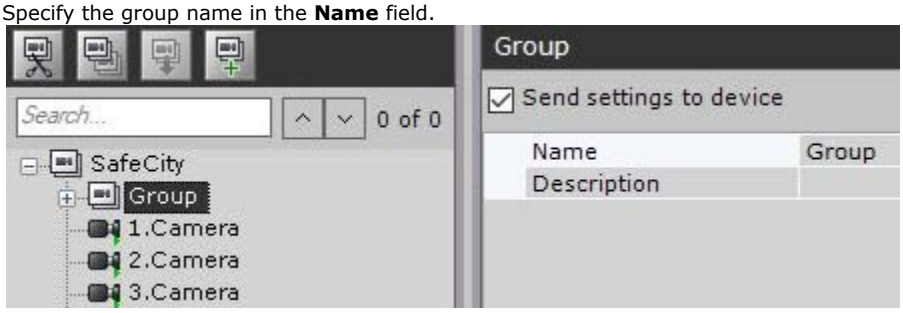
1. Go to the **Groups** tab.



2. To create a **Group** object, click the  button or select **Add group** in the context menu of the main group.

> **Note**
>
> By default, an object (whose name is the same as the Axxon-domain) is available, including all cameras that have been created in the system. This object is referred to here and elsewhere in the document as the "main group". This object cannot be deleted. Cameras in this group cannot be deleted.

3. Specify the group name in the **Name** field.



4. Enter a description of the group in the appropriate field.
5. Click the **Apply** button.

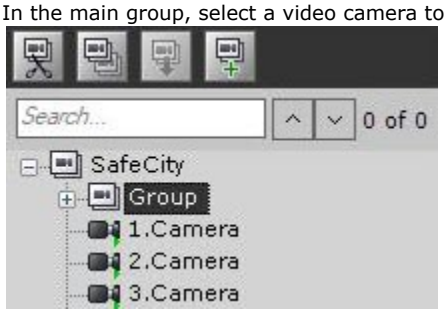
The **Group** object has now been created.

Adding video cameras created in the system to Group objects

To add video cameras to groups, complete the following steps:

> **Note**
>
> Video cameras are added to groups via management operations (see the section titled Managing Group and Video camera objects). The standard method for adding video cameras to groups is presented below.

1. In the main group, select a video camera to add to the selected group.



2. Click the  button or select **Copy** from the context menu of the selected video camera.
3. Select the **Group** object to which you need to add the video camera.
4. Click the  button or select **Paste** from the context menu of the selected group.
5. Fill the groups with the necessary video cameras (see steps 1-4).

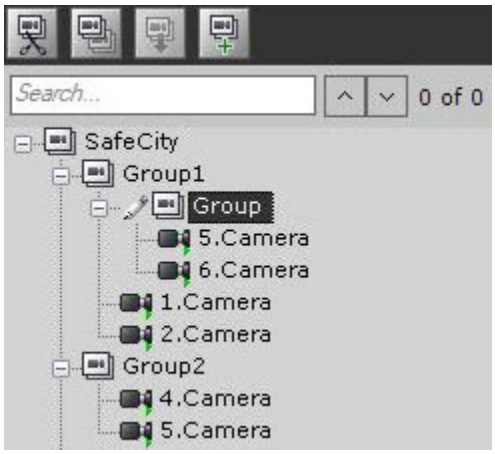
> **Note**
>
> One video camera can be assigned to multiple groups.

6. Click the **Apply** button.

Adding video cameras to groups is now complete.

Creating a system of groups and subgroups

Groups can be included within other groups, forming a system of groups and subgroups.

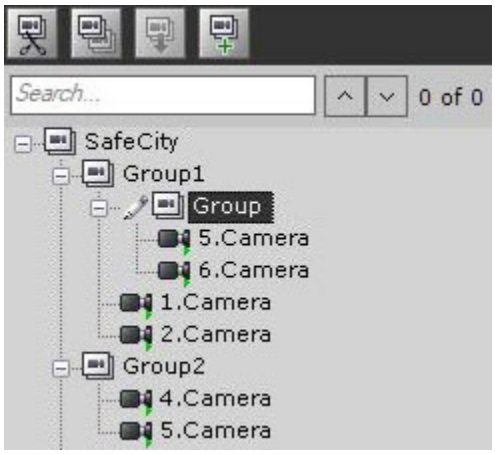


A system of groups and subgroups can be created via group management operations and video camera management operations (see the section titled Managing Group and Video camera objects).

Group objects can be moved or copied to other **Group** objects or to the main group.

Managing Group and Video camera objects

The main operations used to manage groups and video cameras are presented in table.



Action	Execution
Cut/Paste **Note** You can cut a **Video camera** object only from a **Group** object. You cannot cut a **Camera** object from the main group. It is also impossible to cut the main group.	**Using your mouse:** 1. Left-click and hold the **Video camera/Group** object. 2. Drag the object to the **Group** object (or to the main group if you are dragging a **Group** object). 3. Release the left mouse button.
	Using the toolbar: 1. Left-click the **Video camera/Group** object that you want to move. 2. On the toolbar, click  . 3. Left-click the **Group** object (or the main group, if one of the **Group** objects is being moved) to which you want to move the **Video camera/Group** object. 4. On the toolbar, click  .
	Using the keyboard: 1. Left-click the **Video camera/Group** object that you want to move. 2. Press the key combination **Ctrl+**X. 3. Left-click the **Group** object (or the main group, if one of the **Group** objects is being moved) to which you want to move the **Video camera/Group** object. 4. Press the key combination **Ctrl+V**.
Copy/Paste	**Using your mouse:** 1. Left-click and hold the **Video camera/Group** object while simultaneously holding down the **Ctrl** key. 2. Drag the selected object to the **Group** object (or to the main group, if the **Group** object is being copied). 3. Release the left mouse button.

	Using the toolbar: 1. Left-click the **Video camera/Group** object that you want to copy. 2. On the toolbar, click  . 3. Left-click the **Group** object (or the main group, if one of the **Group** objects is being copied) to which you want to copy the **Video camera/Group** object. 4. On the toolbar, click  .
	Using the keyboard: 1. Left-click the **Video camera/Group** object that you want to copy. 2. Press the key combination **Ctrl+C**. 3. Left-click the **Group** object (or the main group, if one of the **Group** objects is being copied) to which you want to copy the **Video camera/Group** object. 4. Press the key combination **Ctrl+V**.
Deletion **Note** You can delete a **Video camera** object only from a **Group** object. You cannot delete a **Camera** object from the main group.	1. Left-click the **Video camera/Group** object that you want to delete. 2. Press the **Delete** key.

Automatic copying of data from local Servers to a centralized Server

In *Axxon One*, it is possible to automatically copy archives (video, audio, alarms) and camera events from local Servers that are not combined into a single Axxon-domain with a centralized Server.

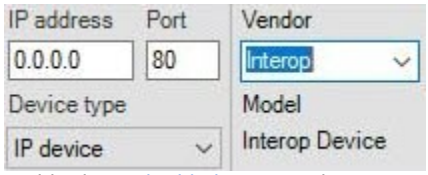
Note

This feature is useful, for example, in the following case:

- The video from a bus on the route network is recorded to a temporary archive on the local Server specific for each bus.
- When the bus arrives at the depot, the archive and camera events are automatically transferred to the centralized server.

To use this option, configure the centralized Server as follows:

1. Manually add the **Interop** IP device to the configuration (see Searching, adding, configuring and removing IP devices).



2. Enable the Embedded storage object.

Note

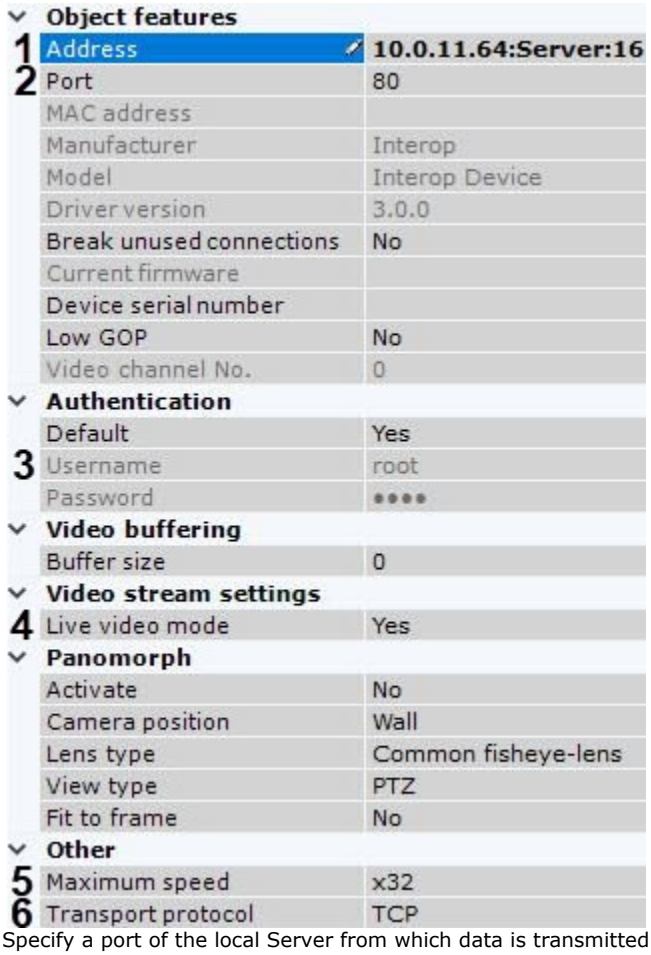
It is recommended to synchronize the time of the local Server with the time of the centralized Server.

3. To receive sound from video cameras, configure the Microphone object.
4. Specify the address of the device in the following format (**1**): <IP-address of local Server>:<name of local Server in Axxon-domain>:<ID of camera on Server>.

Attention!

The Server name is case-sensitive.

If the Server name is Server1, then if you enter server1 or SERVER1 there will be no connection.



5. Specify a port of the local Server from which data is transmitted (**2**). If you use TCP protocol (see step 9), specify the RTSP port number (554 by default, see Configuring an RTSP Server). If you use rtspoverhttp or rtspoverhttps protocol, specify the Web server's port (80 by default, Configuring the Web-Server).
6. Specify the user name and password (**3**). The user must have permissions to access the local server.
7. If you want to display live video from the local server when it is available, select **Yes** in the corresponding field (**4**).
8. Specify the maximum playback speed (**5**).
9. Select the data transfer protocol (**6**).
10. Click the **Apply** button.
11. Repeat the previous steps to add and configure all the necessary video cameras from all local Servers.
12. Configure automatic replication from the embedded storages of the added devices to the centralized server archive (see Configuring data replication).

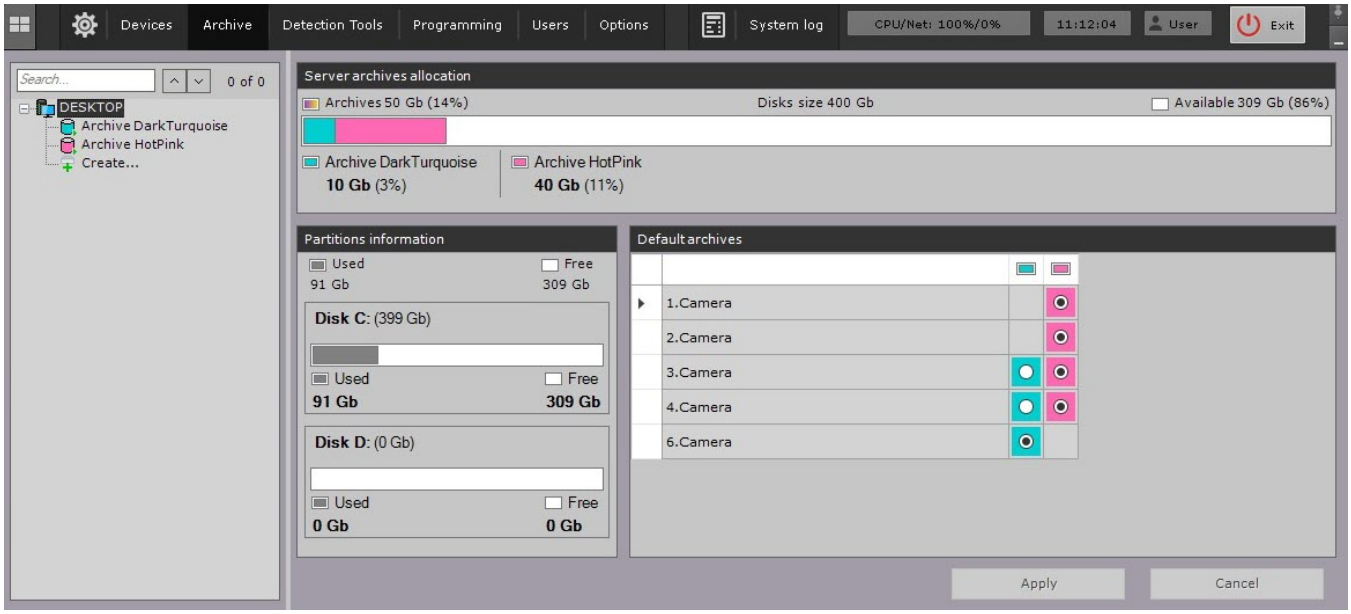
> ⚠ **Attention!**
>
> With a high network load, there may be gaps in the centralized server archive.

Automatic data copying from the local servers to the centralized server is configured.

Configuring archives

General information about configuring archives

You can configure archives using the interface of the **Archive** tab. To create archives, you must have the appropriate permissions. You can create an unlimited number of archives on the basis of one Server.



The archive can be stored:

- on local disks (see Creating a local archive);
- on remote disks (see Creating a remote archive);
- in cloud storages (see General information about the cloud archive).

Attention!

- For local or remote archives, it is not recommended to use the archive as a single large volume.
- It is more practical to split the archive into several volumes and locate them on different hardware devices.
- We recommend you to create an archive with volumes no larger than 30 TB each.

Features of archives:

Local archive	Remote archive	Cloud archive
The archive can be located on several logical disks of the Server	The archive can be stored in multiple remote storages	The archive can be stored in one cloud storage
On one logical disk for one archive, you can create only one volume, which occupies either a file of a set size or the entire partition (logical disk)	The archive can be stored only as a file of a specified size	The archive can contain several volumes of unlimited size. You can change the size of the archive without restarting ngp
The archive can contain multiple volumes, which may be in the form of a file or a partition		

Data from a local, remote, or cloud archive can be copied to other local, remote, or cloud archives (see Configuring data replication).

You can configure the archive as follows:

1. Create an archive (see Creating archives).
2. Configure recording streams from video cameras to archive (see Configuring recording to an archive).
3. Configure data replication, if necessary (see Configuring data replication).

You can also connect external archives—a set of video recordings with time links.

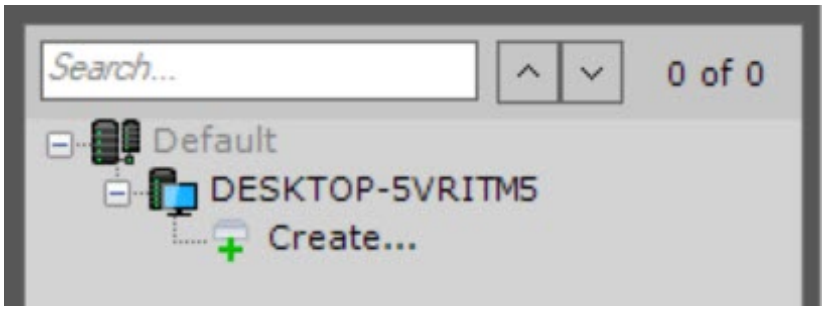
Video surveillance in archive mode

Creating archives

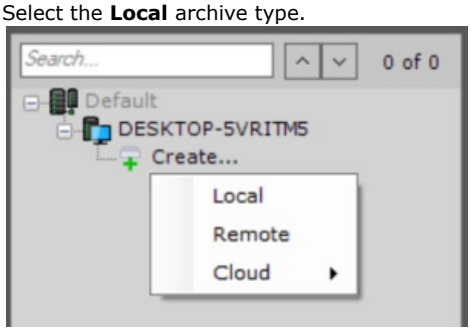
Creating a local archive

To create a local archive, do the following:

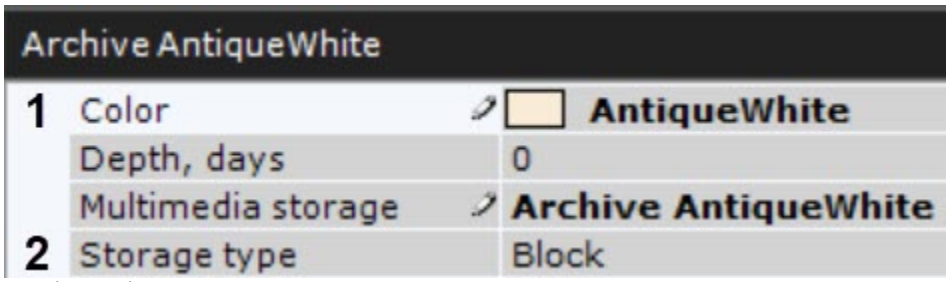
1. In the branch of the **Server** object corresponding to the computer on which you need to organize an archive, click the **Create** li nk.



2. Select the **Local** archive type.

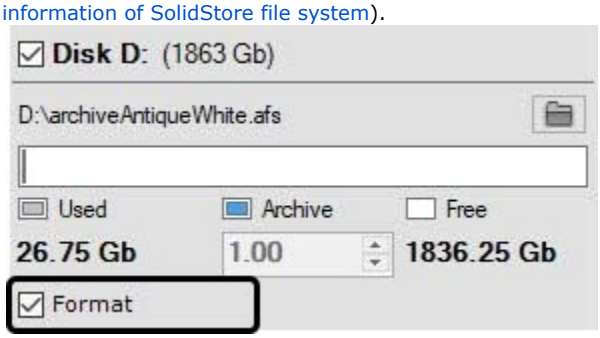


3. Specify the name and color of the archive (**1**).
4. Select the storage type (**2**):
   - block, if you need low latency and high performance in various situations. For example, for tasks with a large read and write load;
   - object, if you need to be able to change the size of the archive volume without restarting the system (see General information about the Round-robin algorithm).



5. Configure archive volumes.

   a. Set the checkboxes next to the disks that you want to include in the archive.
   b. If a disk does not have a file system, the disk can contain an archive volume in the form of a partition. In this case, set the **Format** checkbox. This will format the disk to the SolidStore file system developed by AxxonSoft (see General information of SolidStore file system).



Attention!

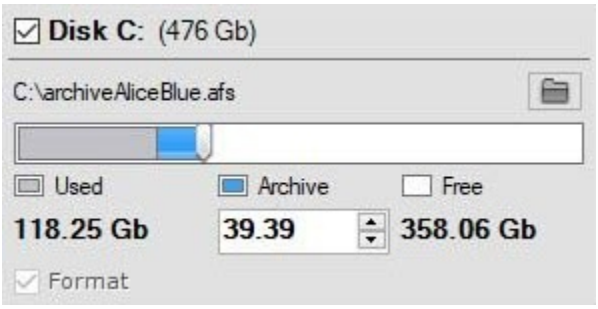
- When selecting the disk on which to place the archive volume, take into account its space. If the archive is completely full, the oldest data will be overwritten with new data.
- The file system on the disk can be erased by using the standard Disk Management utility in Windows. For the manual for starting and using the utility, see Microsoft website. Deleting the file system on the disk in the Disk Management utility consists of the following:
  - delete logical disk;
  - create a new disk in the resulting unallocated area;
  - assign a letter to the disk, but do not format it.

The system disk cannot be completely allocated for an archive.

- You cannot create an archive volume as a partition on a removable disk, since its partition cannot be erased through the Disk Management utility.

c. On disks that have a file system, you can store an archive volume in the form of a file.

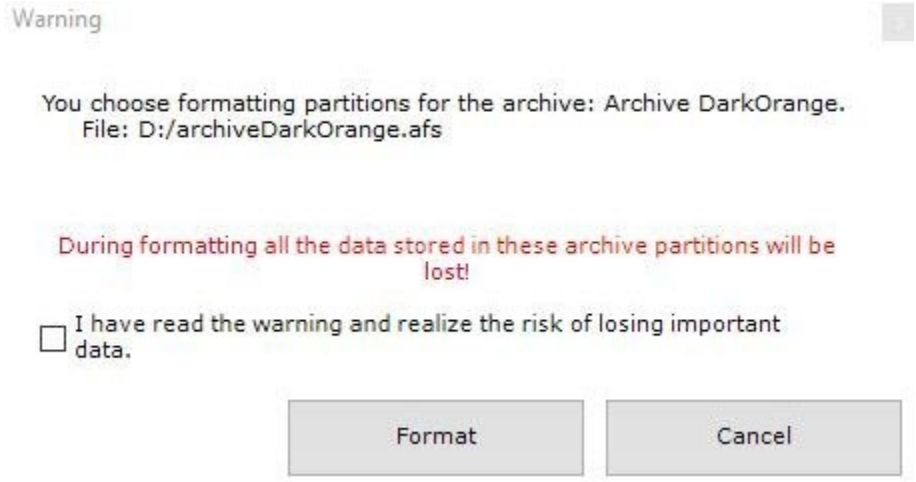
For this archive volume, you must enter a file size (in gigabytes) or set it by moving the slider. The size of the archive file must be greater than or equal to 1 GB. For the Fat32 file system, the maximum archive size is 4 GB.



Attention!

- If the archive is completely full, the oldest data will be overwritten with new data.
- By default, the file name will be the same as the name of the archive, and the file will be located at the root directory of the disk. To change the name and/or location of the file, click the button.

6. Click the **Apply** button.
If volumes are configured in the form of partitions, a dialog box will be displayed, warning about formatting of the relevant system disks.



7. Read through the list of partitions that will be formatted. If the list is correct, set the **I have read the warning and realize the risk of losing important data** checkbox, then click the **Format** button. Otherwise, click the **Cancel** button to return to the archive settings.

Creation of the local archive is now complete.

General information of SolidStore file system

Fragmented files accumulate over time in the Windows file system. This is due to the fact that the operating system sequentially fills the free disk space when writing files.

Free disk space, which appears when old files are deleted, can be located in different parts of the disk; therefore, each file can be split into many fragments.

When reading or writing such a file, the hard drive head must constantly move, which reduces the read/write speed and causes mechanical wear of the disc.

AxxonSoft has developed its own file system SolidStore especially for storing video archives. The system is installed on a blank physical or logical drive, which is fully allocated to Axxon One video archive (see Creating archives). In developing SolidStore, it was taken into account that recording will only be sequenced in one direction (looping mode), and the newest data is written in place of the oldest.

> ⚠ **Attention!**
>
> Loop recording (FIFO overwriting) should erase the earliest recordings, but in some cases selected recordings within 10% of the oldest ones may be compromised. This feature protects archive volumes from fragmentation.
>
> In such cases, these earliest 10% of videos in archive may have gaps.

By optimizing the reading/writing process we managed to minimize the travel of the hard disk head along its surface and to achieve three important advantages:

- Enable high read/write speeds, approaching the physical access speed limit of the hard disk.
- Increase the service life of the hard disk.
- Solve the problem of data fragmentation: as data is written only in looping mode, fragmentation is minimal and does not accumulate with time. This way, the read/write speed remains high throughout the operation of the video surveillance system.

SolidStore relieves the user from the need to periodically stop the video surveillance system and run the Disk Defragmenter tool. This significantly increases video surveillance uptime and the protected facilities remain under the watchful eyes of the security personnel.

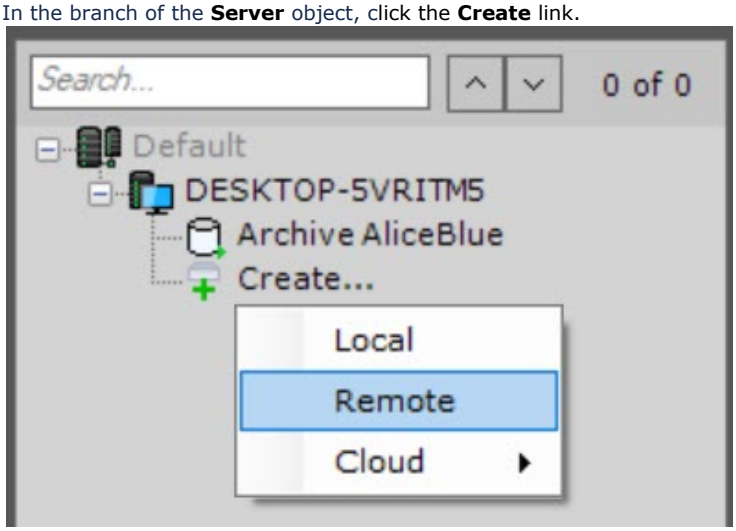
If it is not possible to allocate a separate disk for Axxon One video archive, it can be written as a regular file in the existing Windows file system.

Creating a remote archive

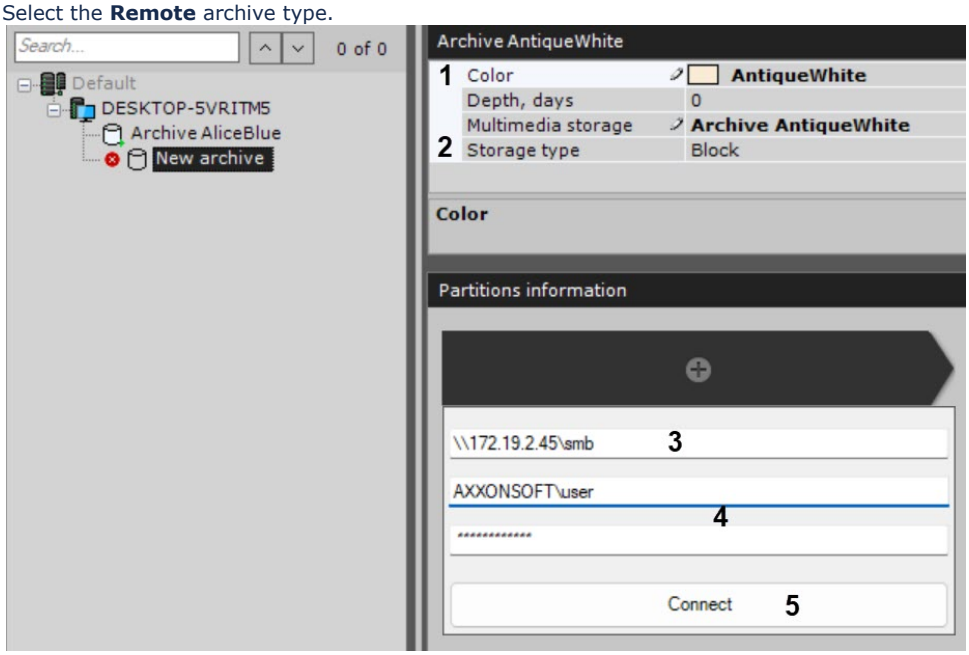
A remote archive can only be a file on one or several remote storages.

To create a remote archive, do the following:

1. In the branch of the **Server** object, click the **Create** link.



2. Select the **Remote** archive type.



3. Specify the name and color of the archive (**1**).
4. Select the storage type (**2**):
   - block, if you need low latency and high performance in various situations. For example, for tasks with a large read and write load;
   - object, if you need to be able to change the size of the archive volume without restarting the system (see General information about the Round-robin algorithm).
5. Enter a path to the remote storage where the archive must be located (**3**).

Attention!

If you plan to connect several users from this computer to the remote archive, do the following:

a. To the C:\Windows\System32\Drivers\etc\hosts file add the following string: "192.168.1.1 DNSname1", where 192.168.1.1 is the IP address of the remote storage, DNSname1 is the domain name of the remote storage.
b. When creating a remote archive, use the specified domain name in the address.

If you need to add several remote archives using different remote user accounts, do the following:

a. To the C:\Windows\System32\Drivers\etc\hosts file add the IP addresses and domain names of all remote storages.
b. When creating archives, use the specified domain names in the address.

In a failover system with a backup Server (see Setting up a configuration with the backup Server), the hosts file on the backup Server must include records from all Servers, if domain names differ on each Server.

6. Enter the username and password (**4**). The user must have permissions to access the remote storage.

Attention!

The username must be specified with a prefix of the domain (domainname\username) or name of the computer (computername\username) where this account is located.

7. Click the **Connect** button (**5**).
This will connect you to the remote storage. When you are connected, you will see a dialog box for configuring the archive parameters.

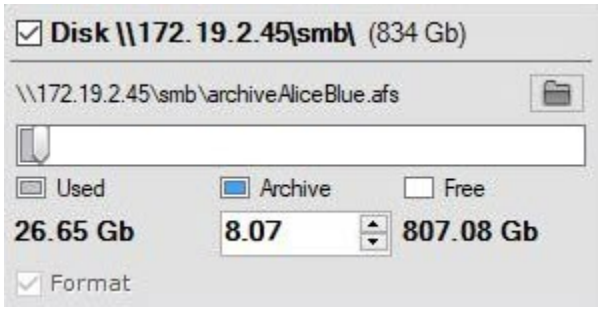
Attention!

Only one remote user can connect to the remote storage at a time. This is a limitation of Windows OS.

If this error occurs, disconnect the previous user in one of the following ways:

1. Run the net use /delete command.

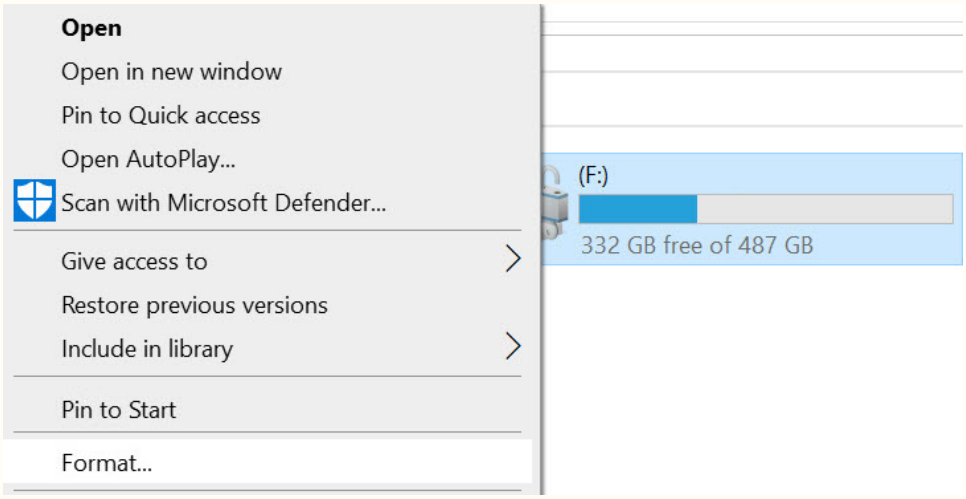
2. Use PsExec to open the command prompt as the LocalSystem user (psexec.exe -i -s cmd.exe) and run the same command.



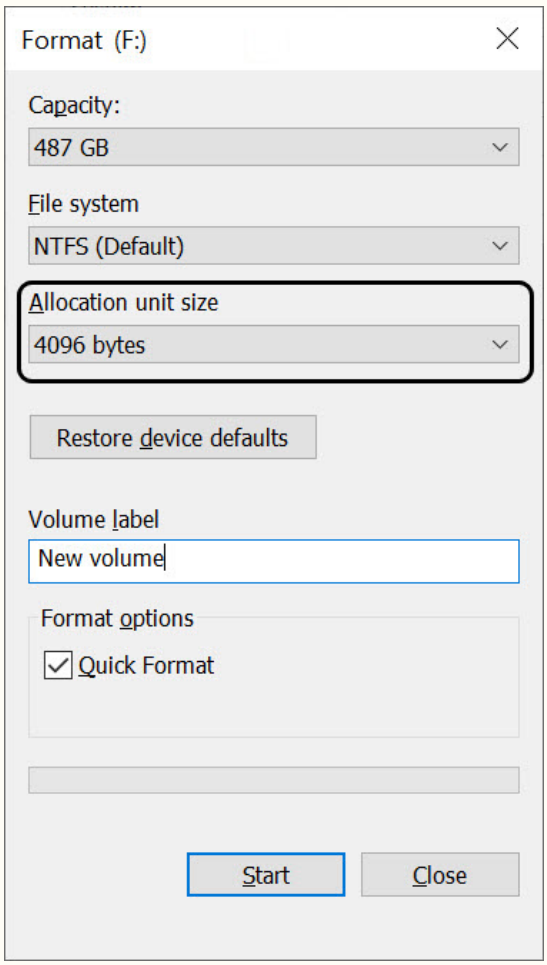
8. Enter the file size in GB or set it by moving the slider. The size of the archive file must greater than or equal to 1 GB. For the Fat32 file system, the maximum archive size is 4 GB.

Attention!

If you need to create an archive file larger than 16 TB, the cluster size for the NTFS file system should be set to a value greater than 4 KB when formatting the disk in Windows OS. To do this, right-click on the disk to which the archive file will be written, and in the menu that opens, select the **Format...** item.



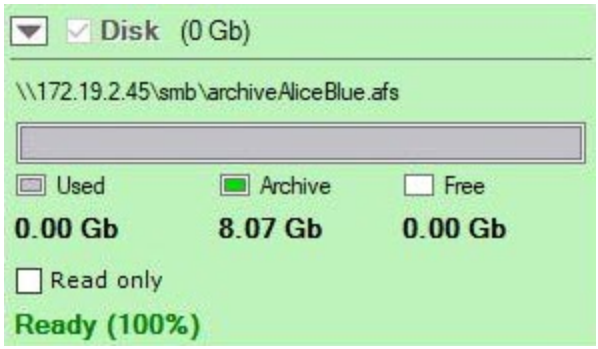
In the **Format** window that appears, from the **Allocation unit size** list, select a cluster size greater than 4 KB and click the **Start** button.



> **Note**
>
> To change the archive folder in the remote storage, click the button and select the required location.

9. If necessary, you can add other remote storages to the archive and configure their parameters.
10. Click the **Apply** button.

Creating a remote archive is complete. After the archive is created, the status of the remote storages, where the archive is located, will be displayed.

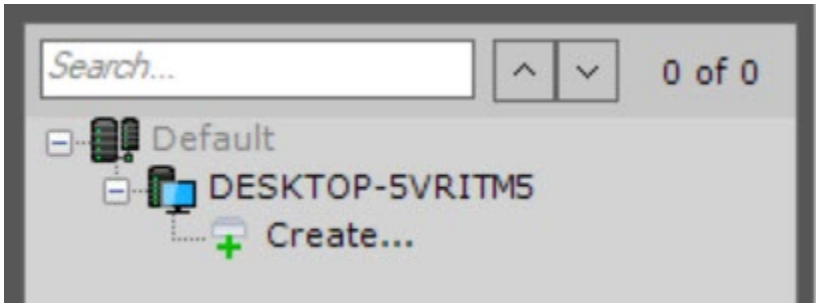


Creating a cloud archive

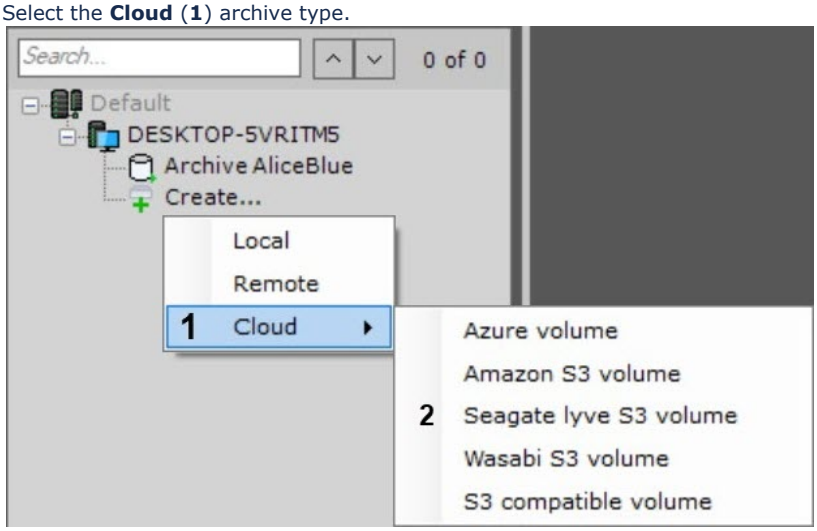
> **Attention!**
>
> It is not recommended to set a cloud archive lifecycle policy, as this may lead to complete loss of the archive.

You can create a cloud archive through the interface of archive creation. To do this, do the following:

1. In the branch of the **Server** object corresponding to the computer on which you need to organize an archive, click the **Create** link.



2. Select the **Cloud** (**1**) archive type.

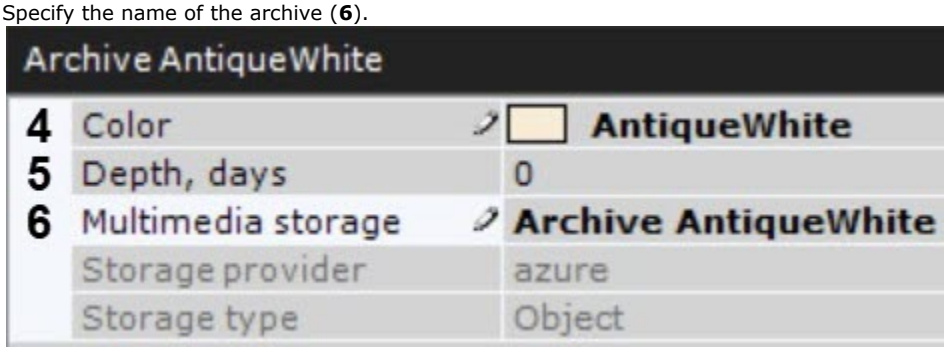


3. Select an archive from the suggested solutions (**2**).
4. Click the button (**3**) to create an archive volume.

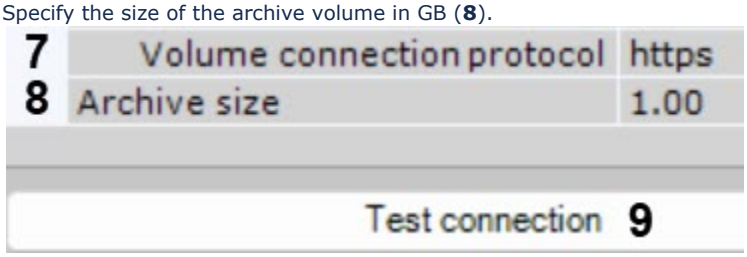


5. Specify general parameters for archive volumes:
    a. Specify the color of the archive (**4**).
    b. Specify the depth of the archive in days (**5**). If the value is set to **0**, the entire archive will be available for viewing.

c. Specify the name of the archive (**6**).



d. Specify the connection protocol: HTTP or HTTPS (**7**).
e. Specify the size of the archive volume in GB (**8**).



> **Note**
>
> Configuring the archive fields for different solutions is given on the corresponding pages.

6. To test the connection of the archive volume, click the **Test connection** button (**9**).
7. Click the **Apply** button.

As a result, a cloud archive and a volume will be created based on the selected solution.

Manage archives using gRPC API (ConfigurationService)

General information about the Round-robin algorithm

General information about the cloud archive

Cloud archive is an object file system for storing video archives in cloud storages

Benefits of using a cloud archive:

1. Integration with VSaaS.
2. Scalability.
3. High level of security.
4. Flexible pricing.
5. Data durability up to 99.999999999% according to Amazon.

Attention!

Before creating a cloud archive in *Axxon One*, you must preconfigure a cloud storage via the web interface of the corresponding provider.

In *Axxon One*, you can create archives based on the following solutions:

1. Amazon S3: https://aws.amazon.com/s3/.
2. Microsoft Azure: https://azure.microsoft.com/en-gb/services/storage/blobs/.
3. Wasabi: https://wasabi.com/.
4. Seagate Lyve Cloud: https://www.seagate.com/.
5. MinIO: https://min.io/. The RELEASE.2021-08-05T22-01-19Z version is tested by AxxonSoft.

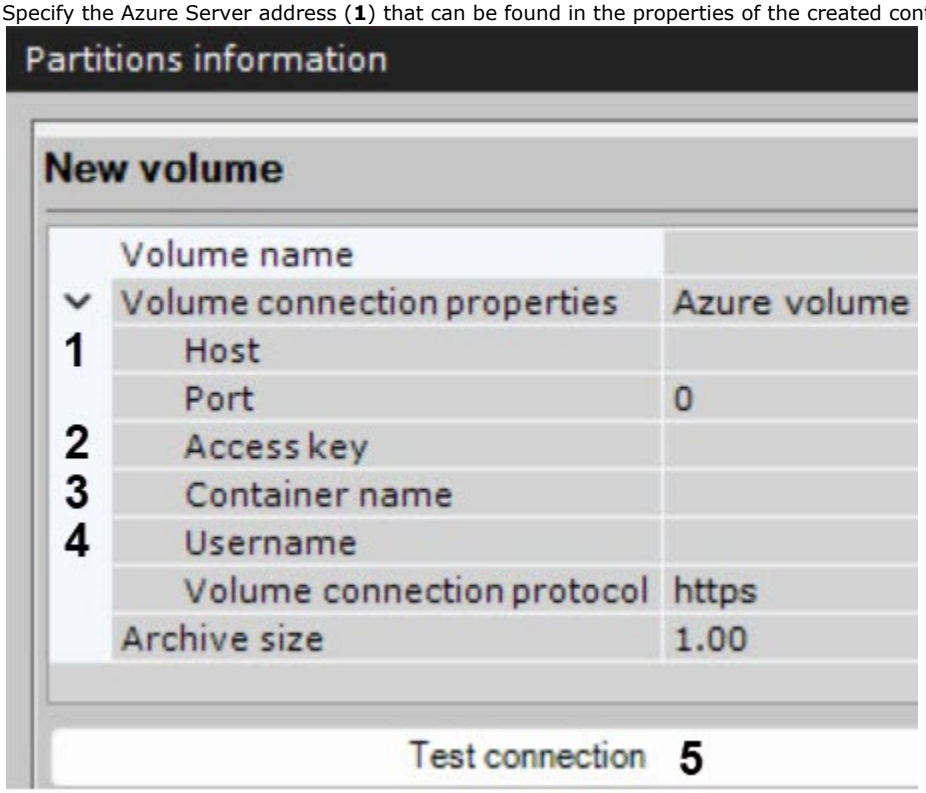
Creating a cloud archive

Configuring an archive volume based on the Microsoft Azure solution

General information about the cloud archive

You must fill in the following fields for an archive volume based on the Microsoft Azure solution:

1. Specify the general parameters for an archive volume (see Creating a cloud archive).
2. Specify the Azure Server address (**1**) that can be found in the properties of the created container.



3. Specify the access key (**2**) that can be found in the Access keys section.
4. Specify the Azure container (**3**) that can be found in the properties of the created container.
5. Specify the username (**4**) that can be found in the Access keys section (Storage account name).
6. To test the connection of the archive volume, click the **Test connection** button (**5**).
7. Click the **Apply** button.

Configuring an archive volume based on the Microsoft Azure solution is complete.

Example of configuring a volume of a cloud archive in Microsoft Azure:

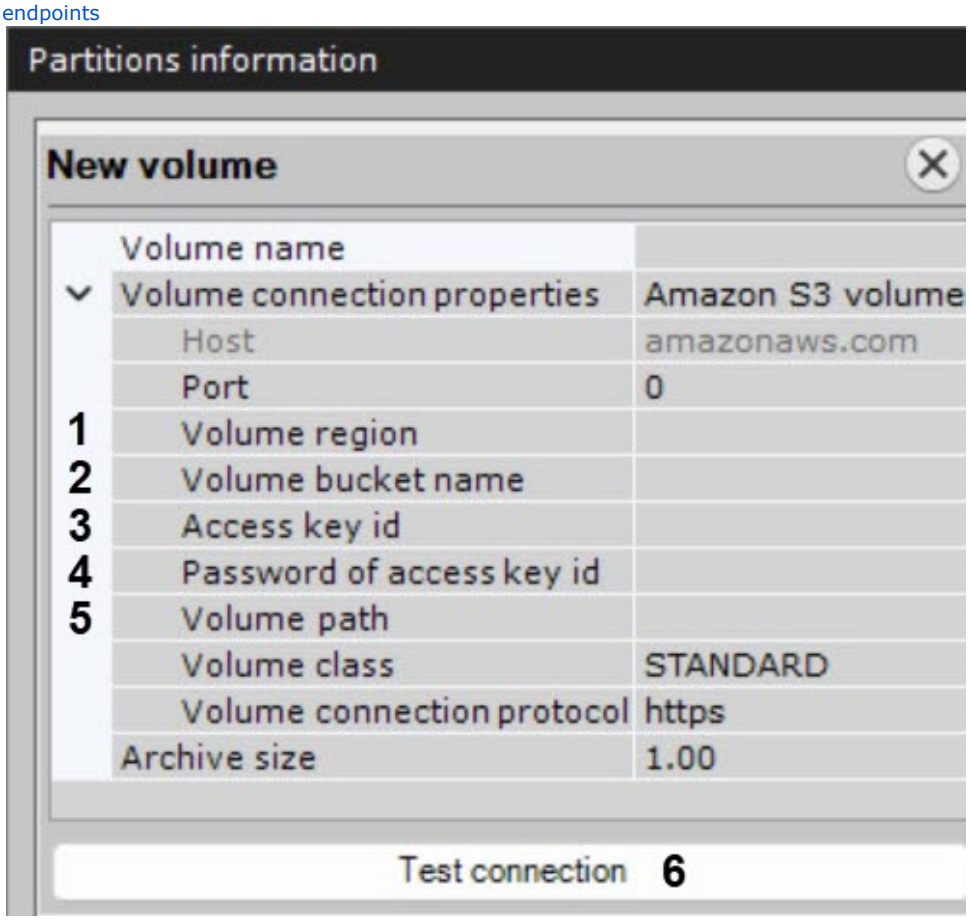
Parameter	Value
Host	axxonsoft.blob.core.windows.net
Access key	youraccesskey==
Container name	container
Username	axxonsoft

Configuring an archive volume based on the Amazon solution

General information about the cloud archive

You must fill in the following fields for an archive volume based on the Amazon solution:

1. Specify the general parameters for an archive volume (see Creating a cloud archive).
2. Specify the region of the archive volume storage (**1**) that is set when you create a cloud storage via Amazon web interface. To reduce delays when writing and reading the archive, it is necessary to specify the nearest region to the *Axxon One* Server in Amazon web interface. The list of possible regions—ttps://docs.aws.amazon.com/general/latest/gr/rande.html#regional-endpoints



3. Specify the name of the archive partition in the Amazon S3 (bucket) account (**2**). Different volumes can be located in different regions. On the Amazon S3 Server, the volume name must be unique and must be previously created by the user using the following rules to work in *Axxon One* (see https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html).
4. Specify the access key id (**3**). You must sign in to create access keys—https://console.aws.amazon.com/iam/home#/security_credentials$access_key.
5. Specify the password of the access key (**4**).

> **Note**
>
> The password is available after you create an access key.

6. Specify the path to the folder of the *Axxon One* volume inside the partition (bucket) (**5**).
7. To test the connection of the archive volume, click the **Test connection** button (**6**).
8. Click the **Apply** button.

Configuring an archive volume based on the Amazon solution is complete.

Example of configuring a volume of a cloud archive in Amazon:

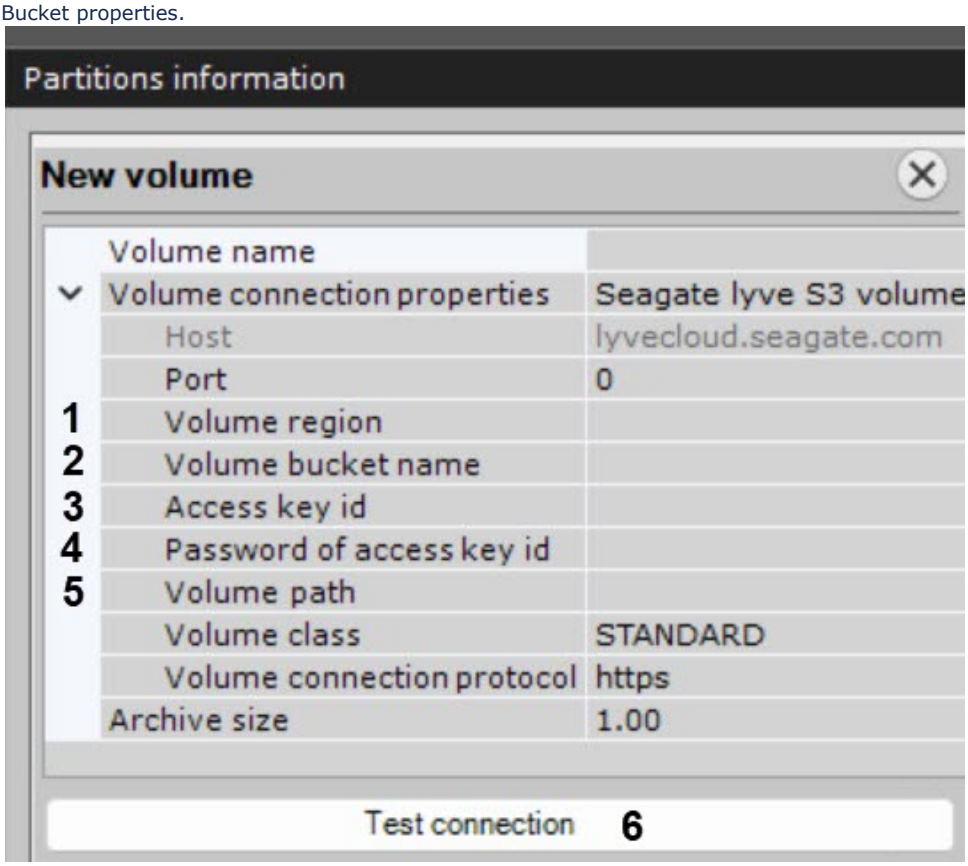
Parameter	Value
Volume region	us-west-1
Volume bucket name	axxonsoft-test
Access key id	youraccesskeyid
Password of access key id	yoursecretaccesskey
Volume path	path

Configuring an archive volume based on the Seagate Lyve Cloud solution

General information about the cloud archive

You must fill in the following fields for an archive volume based on the Seagate Lyve Cloud solution:

1. Specify the general parameters for an archive volume (see Creating a cloud archive).
2. Specify the region of the volume storage (**1**) that is set during its creation and corresponds to the Region parameter in the Bucket properties.



3. Specify the name of the archive partition (Bucket Name) previously set by the user (**2**). It corresponds to the Name parameter in the Bucket properties.
4. Specify the access key id that is generated when creating an account in the Create Service Account window (**3**).
5. Specify the password of the access key (**4**).

> **Note**
>
> The password is available after the access key is generated.

6. Specify the path to the folder created inside the archive volume (**5**).
7. To test the connection of the archive volume, click the **Test connection** button (**6**).
8. Click the **Apply** button.

Configuring an archive volume based on the Seagate Lyve Cloud solution is complete.

Example of configuring a volume of a cloud archive in Seagate Lyve Cloud:

Parameter	Value
Volume region	us-west-1
Volume bucket name	axxonsoft-test

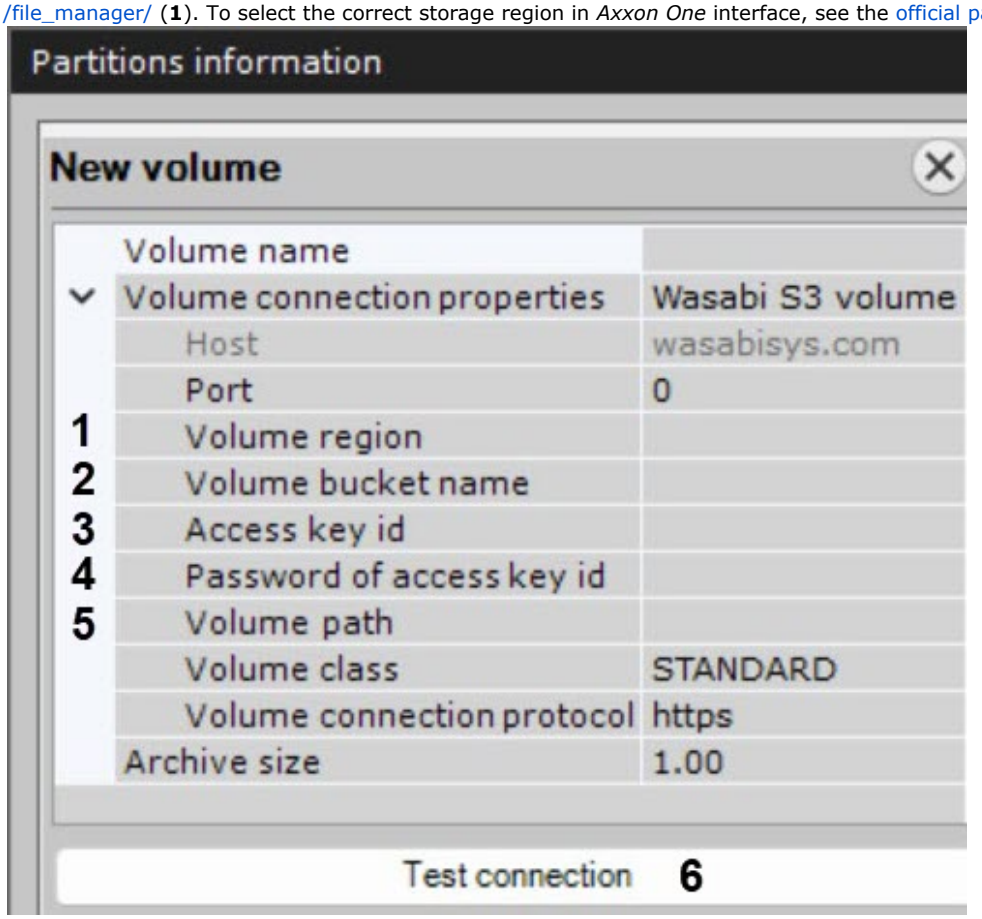
Access key id	youraccesskeyid
Password of access key id	yoursecretaccesskey
Volume path	path

Configuring an archive volume based on the Wasabi solution

General information about the cloud archive

You must fill in the following fields for an archive volume based on the Wasabi solution:

1. Specify the general parameters for an archive volume (see Creating a cloud archive).
2. Select the storage region of the corresponding volume that was previously set in https://console.wasabisys.com/#/file_manager/ (**1**). To select the correct storage region in *Axxon One* interface, see the official page on the Wasabi website.



3. Specify the name of the archive partition (Bucket Name) previously set by the user in https://console.wasabisys.com/#/file_manager/ (**2**).
4. Specify the access key id that you must create beforehand at https://console.wasabisys.com/#/access_keys (**3**).
5. Specify the password of the access key (**4**).

> **Note**
>
> The password is available after you create an access key.

6. Specify the path to the folder created inside the archive volume (the Folder object in Bucket) (**5**).
7. To test the connection of the archive volume, click the **Test connection** button (**6**).
8. Click the **Apply** button.

Configuring an archive volume based on the Wasabi solution is complete.

Example of configuring a volume of a cloud archive in Wasabi:

Parameter	Value
Volume region	us-central-1

Volume bucket name	axxontest-1
Access key id	youraccesskeyid
Password of access key id	yoursecretaccesskey
Volume path	path

Configuring an archive volume based on the MinIO solution

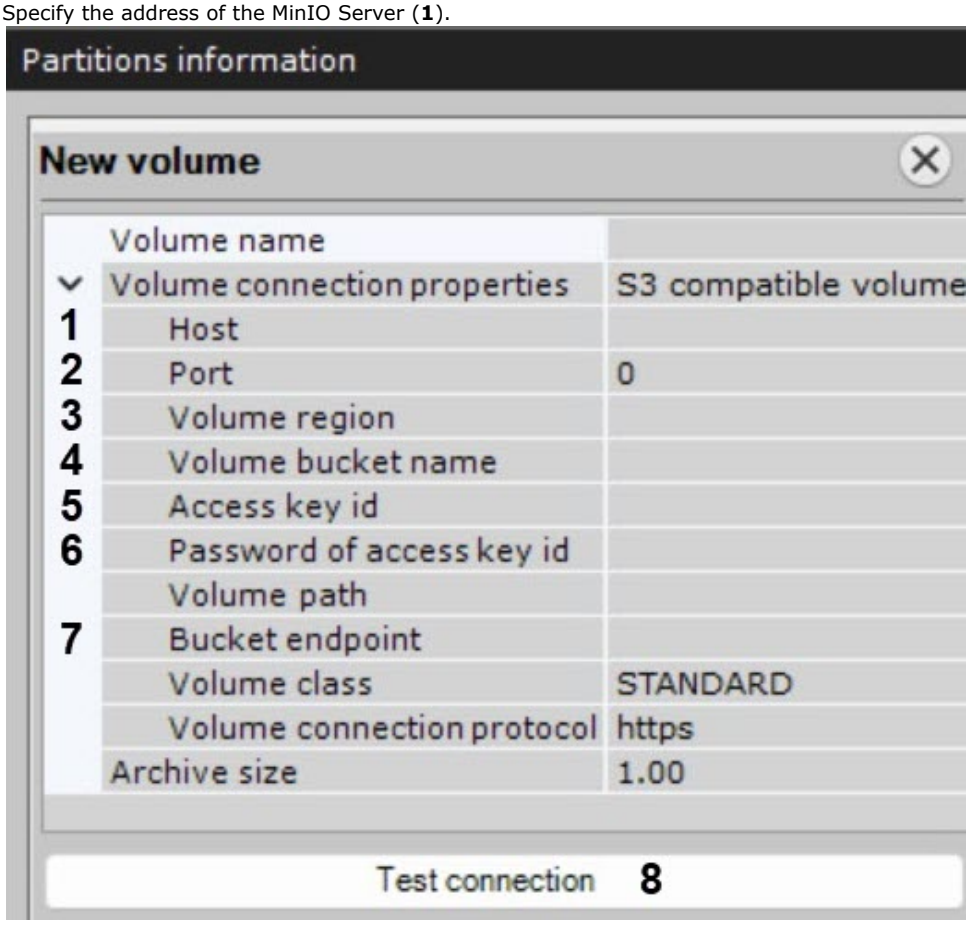
General information about the cloud archive

Note

The RELEASE.2021-08-05T22-01-19Z version of the MinIO object archive is tested by AxxonSoft.

You must fill in the following fields for an archive volume based on the MinIO solution:

1. Specify the general parameters for an archive volume (see Creating a cloud archive).
2. Specify the address of the MinIO Server (**1**).



3. Specify the port of the MinIO Server (**2**).
4. Specify the location region of the corresponding volume (**3**).
5. Specify the name of the archive partition (Bucket Name) previously set by the user. It corresponds to the Name parameter in the Bucket properties (**4**).
6. Specify the access key id (**5**).
7. Specify the password of the access key (**6**).

   Note

   The password is available after you create an access key.

8. Specify the full path to bucket endpoint (**7**).

> **Attention!**
>
> The parameter must only be used when using **MinIO** if the domain name of the **MinIO** Server is specified instead of the Server IP address.

Example: http://miniopoc1.agis.xh.ar:9000/
where

- http://miniopoc1.agis.xh.ar/—domain name of the **MinIO** Server.
- 9000—**MinIO** port.

9. To test the connection of the archive volume, click the **Test connection** button (**8**).
10. Click the **Apply** button.

Configuring an archive volume based on the MinIO solution is complete.

Example of configuring a volume of a cloud archive in MinIO:

Parameter	Value
Host	192.168.56.102
Port	9000
Volume region	us-east-1
Volume bucket name	bucket
Access key id	MINIOROOT
Password of access key id	MINIOPASS
Volume path	path

Example of configuring a volume of a cloud archive in MinIO using the full path to bucket endpoint:

Parameter	Value
Volume region	us-east-1
Volume bucket name	bucket
Access key id	MINIOROOT
Password of access key id	MINIOPASS
Bucket endpoint	http://miniopoc1.agis.xh.ar:9000/

General information about the Round-robin algorithm

If there are several volumes in the object archive, the archive records are distributed among all volumes by the Round-robin algorithm.

The archive records are distributed in a round-robin cycle: the first interval of the key frames of a record is transferred to the first volume of the archive, then the next interval is transferred to another volume, and so on until the last volume is reached. The cycle is repeated until all key frames of the archive record are completely distributed over the available volumes.

This algorithm allows increasing the writing speed of the archive, as well as preventing the loss of records for a certain period, in case there are problems with the archive volumes, i.e., if the archive volume is lost, the records for the previous period will be available with frame decimation. This behavior is ensured because the key frames of records are distributed evenly over all available volumes of the archive.

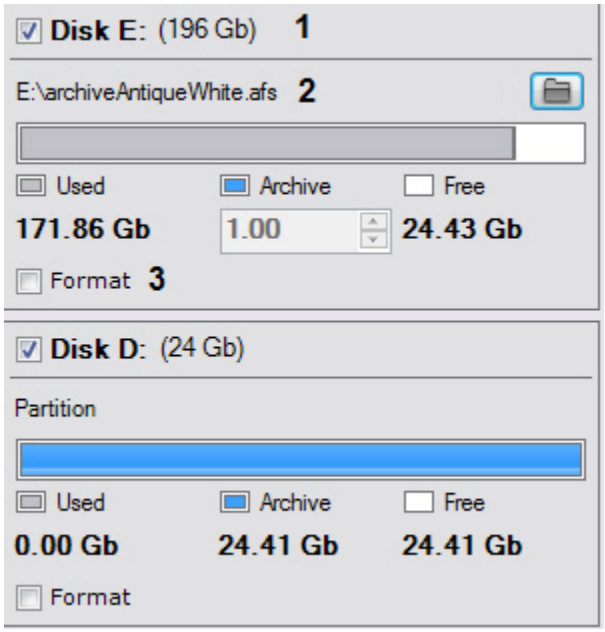
Creating an archive based on existing archive volumes

If an archive is created from an existing volume, it will be possible to extract saved video from the file only if the following conditions are met:

- The currently selected computer has the same name as the name of the Server or node on which the video has been saved to an existing Video Footage volume.
- The IDs of the video cameras from which the recordings were written to the existing archive volume are the same as the IDs of the current video cameras.

To create an archive based on an existing volume:

1. Create an archive (see Creating a local archive).
2. Select disks or network archives that contain existing volumes (by selecting check boxes, **1**).



> **Note**
>
> A new archive can contain volumes that previously belonged to different archives

3. If the volume is in file form, select the archive file to which recording was performed (**2**).
4. Clear the **Format** check box (**3**).

> **Note**
>
> If the **Format** check box is selected, the archive entries that are currently stored on the volume will be erased.

5. If necessary, create new archive volumes on free partitions.
6. Click the **Apply** button.

The archive is created and, if all requirements are met, the archive recordings are available.

Configuring recording to an archive

Video and audio streams are recorded synchronously.

You can configure recording to the archive both for one camera, and for several, using the same parameters.

To configure recording to the archive for one camera, do the following:

1. Select the created archive.
2. Set the checkbox next to the camera for which you want to configure the recording to the archive (**1**).



3. Configure the parameters for recording to the archive:
   a. From the **Constant recording** list (**2**), select the mode for recording to the archive.
      i. If **No** is selected, the video stream will be recorded to the archive only when an operator manually initiates an alarm or an automatic rule is run.
      ii. If **Always** is selected, video will be recorded to the archive non-stop.
      iii. If a time schedule is selected (see Configuring schedules), video will be recorded non-stop to the archive during the selected time period. Recording to the archive can also be initiated by the operator or an automatic rule.
   b. In the **Depth, days** field (**3**), specify the maximum archive depth of the given camera in days. If the **0** value is set, the archive depth is unlimited. As a result, the archive will only contain recordings within the specified depth. The recordings that are outside the specified archive depth won't be available for viewing.

> **Attention!**
>
> If you set an unlimited archive depth for one or several cameras, at some point the archive will become full, and FIFO based re-recording will be automatically started—the oldest recordings in the archive will be replaced with the new ones, regardless of the depth setting. In this case, the set archive depth for other cameras may not be maintained and be reduced
>
> Therefore, if you set an unlimited archive depth for at least one camera, limiting the archive depth for other cameras may be unnecessary.
>
> When you configure the archive depth for each camera, we recommend calculating the storage capacity of an archive (see Disk storage subsystem requirements) to avoid the situations when the archive is stored for fewer days than specified.
>
> When you specify the archive depth for a particular camera, note that the priority of the total archive depth is higher (see Configuring access restrictions to archive). If the archive depth of a camera is 20 days, and the total archive depth is 10 days, the archive depth of a camera won't exceed 10 days.
>
> Later, if you change the available archive depth of a camera upwards or to **0**, the setting will apply only to new recordings. Earlier recordings outside the initial archive depth don't become available.

   c. In the **Prerecord, sec** field (**4**), enter the prerecord time in seconds of a video stream. This value must be in the range [0; 30].

> **Attention!**
>
> Prerecord is a period of prerecording that will be added to the beginning of an alarm event recording.
>
> If a macro starts recording, the prerecord time may be longer, according to the specified settings (see Record to archive).

   d. If it is necessary to use decimation when recording to the archive, select the required value from the **Recording frame rate** list (**5**):
      - **By keyframes** (for all video streams except MJPEG);
      - **1** frame **per 240/120/60 seconds**;
      - specific value of frames per second (for MJPEG video stream).

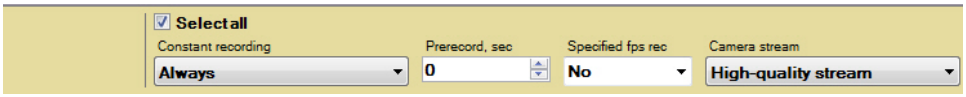
      Decimation reduces the size of the archive, but the video will be less "smooth".
   e. Select a stream for recording to the archive (**6**).

> **Note**
>
> This setting is relevant for cameras that support multistreaming.

4. Click the **Apply** button.

To configure recording to the archive for several cameras, do the following:

1. Set the checkboxes next to the cameras for which you want to configure recording to the archive. To select all cameras, set the **Select all** checkbox.



2. Configure the settings for recording to the archive for a group of cameras (marked with yellow). The specified settings will be automatically applied to all cameras.
3. Perform custom configuration of camera recording settings, if necessary.
4. Click the **Apply** button.

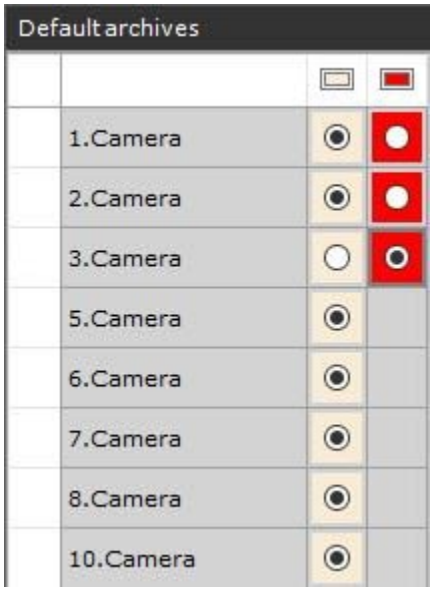
The camera is now bound to the archive.

Setting the default archive

The default archive of a video camera is the archive to which images from a given video camera are recorded during user-initiated alarms. For each video camera one and only one default archive must be set. The first archive to which recording of a video stream from a video camera was configured automatically becomes the default archive (see Configuring recording to an archive).

To switch the default archive for a camera:

1. Select a **Server** object.
   The **Default archives** form displays a list of cameras and archives, which are marked with the corresponding colors. If archive recording to at least one archive is enabled for a particular camera, the camera is visually marked as related to its default archive.



2. To change the default archive for a camera, move the designator to the relevant archive.
3. Click the **Apply** button.

Configuration of the default camera archive is now complete.

Configuring data replication

Replication of the archive data refers to copying of fixed-size blocks of information (video, audio, metadata) from one archive to another within the same Axxon-domain. The primary purpose of data replication is to ensure long-term storage and access to multimedia data on remote storage devices. Every archive can be both the sender and receiver of data.

Attention!

Replication is performed as blocks of information accumulate and only to the end of the archive. Blocks of information can be replicated to any part of the archive in the object archive.

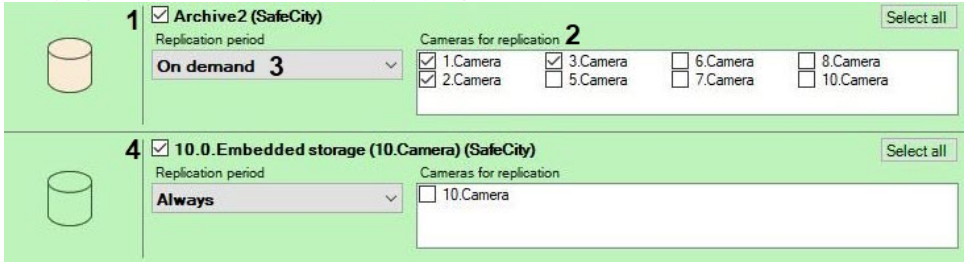
To transfer the old data from **Archive 1** to **Archive 2** and continue writing new data to **Archive 2**, do the following:

1. Replicate the data from **Archive 1** to **Archive 2**, while **Archive 2** cannot be written to.
2. Configure the camera to write to **Archive 2**.

The events indicating the start and successful completion of data replication will be generated in the system (see Event control). These events can be used in macros (see Configuring macros).

To configure data replication, do the following:

1. In the list of archives of the Axxon-domain, select the archive to which you want to copy data from other archives.
2. Select one or more archives form which you want to copy data (**1**). You can also replicate video from the embedded camera storage (**4**, see The Embedded storage object).



3. For each archive, select the cameras from which data will be copied to the replication archive (**2**). To select all cameras, click the **Select all** button.

Note

Data from a particular camera can be copied to the replication archive only from one archive. When you select a camera for replication from an archive, the camera becomes unavailable for replication from any other archive.

You cannot select cameras if they are already writing to the replication archive.

4. Select the replication period (**3**):
   a. **Always**—replication will be performed continuously.
   b. **Time schedule**—replication will be performed within the specified time schedule (see Creating schedules). For example, to distribute the CPU load, you can configure replication to run at night.
   c. **On demand**—replication will be started manually or using macros (see Manual Archive Replication, Start replication).

Attention!

If you change the replication period in an existing replication archive, the archive records for the previous period will be deleted.

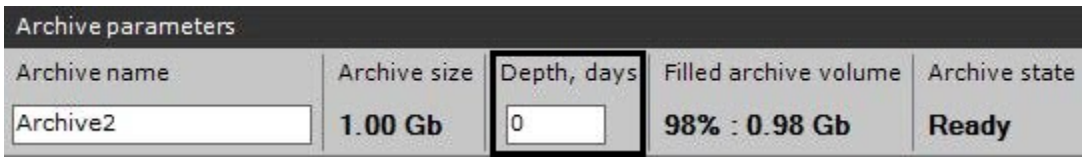
5. Click the **Apply** button.

Configuring data replication is complete. If the replication period was set to **Always**, data replication starts immediately after the settings are applied.

Configuring access restrictions to archive

You can limit the availability of the archive for viewing to the system users.

To do this, select the archive, specify the available archive depth in days in the corresponding field and click the **Apply** button.



Note

If the **0** value is set, the entire archive will be available for viewing.

As a result, only the recordings within the specified depth will be available. The recordings that are outside the specified archive depth won’t be available for viewing.

Attention!

Later, if you change the available archive depth of a camera upwards or to **0**, the setting will apply only to new recordings. Earlier recordings outside the initial archive depth don't become available.

Editing archives

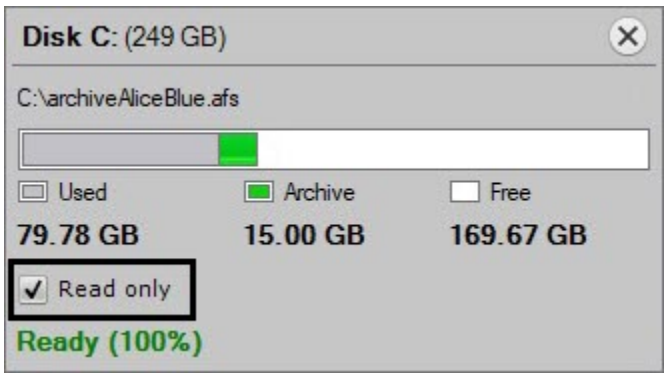
You can edit the archives that have been created in the system. You can do the following:

1. Rename an archive (see Creating archives).
2. Add new volumes. You can add new volumes in the same way as when creating an archive (see Creating archives).
3. Configure a write limit on the archive volume.
4. Delete and format archive volumes.
5. Change settings for archive recording (see Configuring recording to an archive).
6. Change replication settings (see Configuring data replication).

Configuring a write limit on the archive volume

You can stop writing on a certain volume of the archive. In this case, the data previously written to it will be available for viewing.

To do this, set the **Read only** checkbox and click the **Apply** button.



Note

This setting may be useful when you need to replace the disk if it has some bad sectors, but there shouldn’t be any "gaps" in the archive.

In this case, you should add a volume to the archive on a new disk and set the volume on the damaged disk to the **Read only** mode.

Protecting video footage from FIFO overwriting

In the *Axxon One* software package, data is being recorded cyclically (First In First Out). Normally, older video footage is overwritten by the newer.

You can protect selected videos from being overwritten. A macro copies protected recordings to another Video Footage.

To protect videos, do the following:

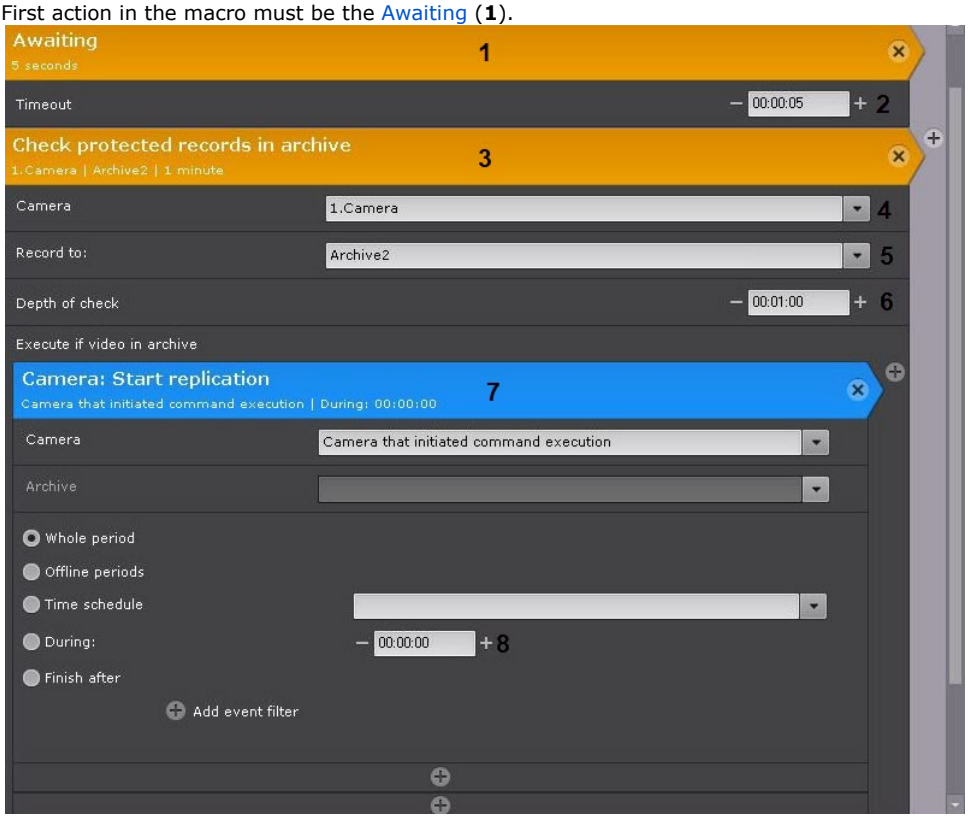
1. Configure on-demand replication (see Configuring data replication).
2. Configure a macro (see Setting up a macro for automatic copying of protected records).
3. Configure protection for necessary videos (see Setting up record protection).

You can further edit the list of protected recordings through the web client.

Setting up a macro for automatic copying of protected records

You have to create and set up a **cyclical** macro (see General information about the macros) as follows:

1. First action in the macro must be the Awaiting (**1**).



2. The timeout delay value sets the time interval for checking Video Footage for protected records (**2**).
3. The second action in the macro must be checking Video Footage for protected records (**3**). On this step, you have to:
    a. Select a camera or a group of cameras whose Video Footages have to be checked for protected records (**4**).
    b. If you select a particular camera, specify the archive to be checked (**5**). If a group of cameras was selected in the previous step, only default archive will be checked for each of them (see Setting the default archive).
    c. Specify the depth of the check in HH:MM:SS format (**6**). The time interval between checks is calculated as follows: [starting time of the earliest recording in archive, starting time of the earliest recording in archive + depth of the check].
    d. Add data replication as a conditional action upon discovery of protected records within the scanning interval (**7**, see Start replication).
    e. Select the Replication time for a time interval (**8**). The replication duration defines the time interval from which protected records have to be copied to another Video Footage. All protected intervals starting within the [starting time of the earliest recording in Video Footage; starting time of the earliest recording in Video Footage + replication duration] range will be copied to Video Footage for replication. Normally, the replication duration has to be equal to the depth of the check defined in Step 3c.

The screenshot shows settings that make the system scan once in a minute (**2**) for protected records in Camera 4's (**4**) archive AliceBlue (**5**) within the [starting time of the earliest recording in archive + 10 minutes] time interval (**6**). If this interval contains protected records, the replication will be launched to copy all protected records falling into [starting time of the earliest recording in archive; starting time of the earliest recording in archive + 10 minutes] **(8)** interval to archive specified for replication.

Setting up record protection

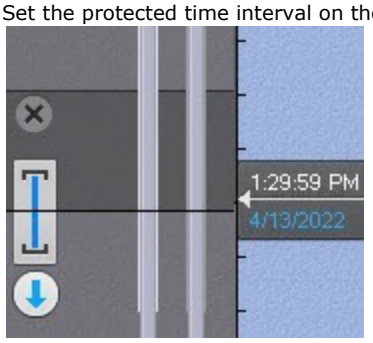
To protect a record, create a bookmark – a special case of the operator comment (see Operator comments).

To create a bookmark, do as follows:

1. Select the required camera on the layout and switch to the archive mode (see Switching to Archive Mode).

   > **Note**
   >
   > If you need to protect the same time interval in multiple camera archives, switch the necessary cameras to the archive mode.

2. Set the protected time interval on the timeline in the archive with the  and  buttons (see The Timeline).

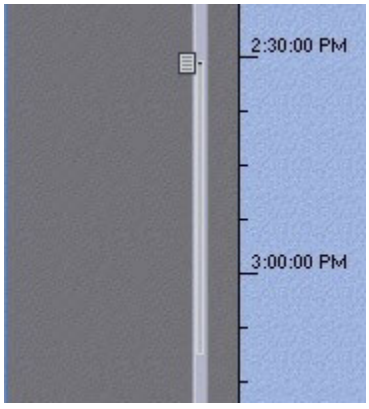


3. Click the  button in the video surveillance window.
4. Enter a comment (**1**).



5. Set the **Protect** checkbox (**2**)
6. Set the **All** (**3**) checkbox if it is necessary to protect the specified interval from all cameras currently in the archive mode.
7. Click the **Save** button (**4**).

The newly created bookmark will appear on the timeline.



The protected interval will be highlighted in light grey, and its beginning will be marked with  .

Click the  button to delete the specified protected interval in the archive.

Increasing capacity of an archive volume

You can increase the capacity of an archive volume.

Increasing capacity of an archive volume as a partition

You can increase volume capacity only with standard media. You cannot increase volume capacity on RAID array.

> ⚠ **Attention!**
>
> AxxonSoft cannot guarantee archive data integrity after this action is complete.

To increase volume capacity, do the following:

1. Stop the *Axxon One* Server (see Shutting down a Server).
2. Use the Windows disk management utility to increase volume capacity.
3. Start the Server (see Starting a Server).

Increasing capacity of an archive volume as a file

To increase volume capacity, use the -expand parameter in console utility for working with archives (see Console utility for working with archives).

Increasing capacity of an object archive volume

You can increase the capacity of an object archive volume using the **Archive size** parameter in the interface (see Creating a cloud archive), and via gRPC API (see Resize cloud archive using gRPC API methods).

Removing archive volumes

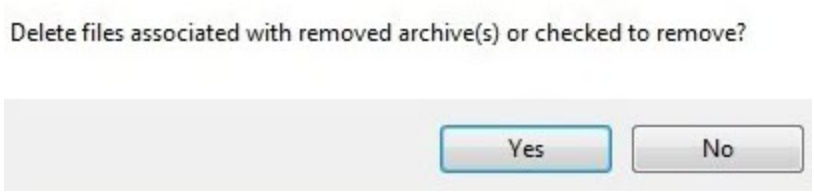
You can remove archive volumes.

To remove a volume, do the following:

1. Click the  button.

   > **Note**
   >
   > If there is only one volume in the archive, you cannot remove it.

2. Click the **Apply** button.
3. If necessary, you can remove archive files.



> **Attention!**
>
> If you remove the archive files, then all archive records that they contained will be lost.
>
> If you do not delete archive files, you can re-use them to create another archive (see Creating an archive based on existing archive volumes). You can also use a partition to re-create an archive.

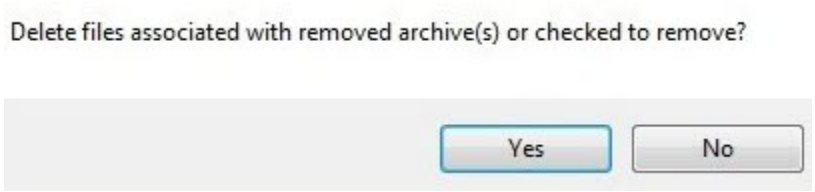
Removing an archive volume is complete.

Removing archives

To remove an archive from the system, do the following:

1. Select the archive that you want to remove in the archive list.
2. Click the **Remove** button.
3. Click the **Apply** button.

   If necessary, you can remove the archive files.



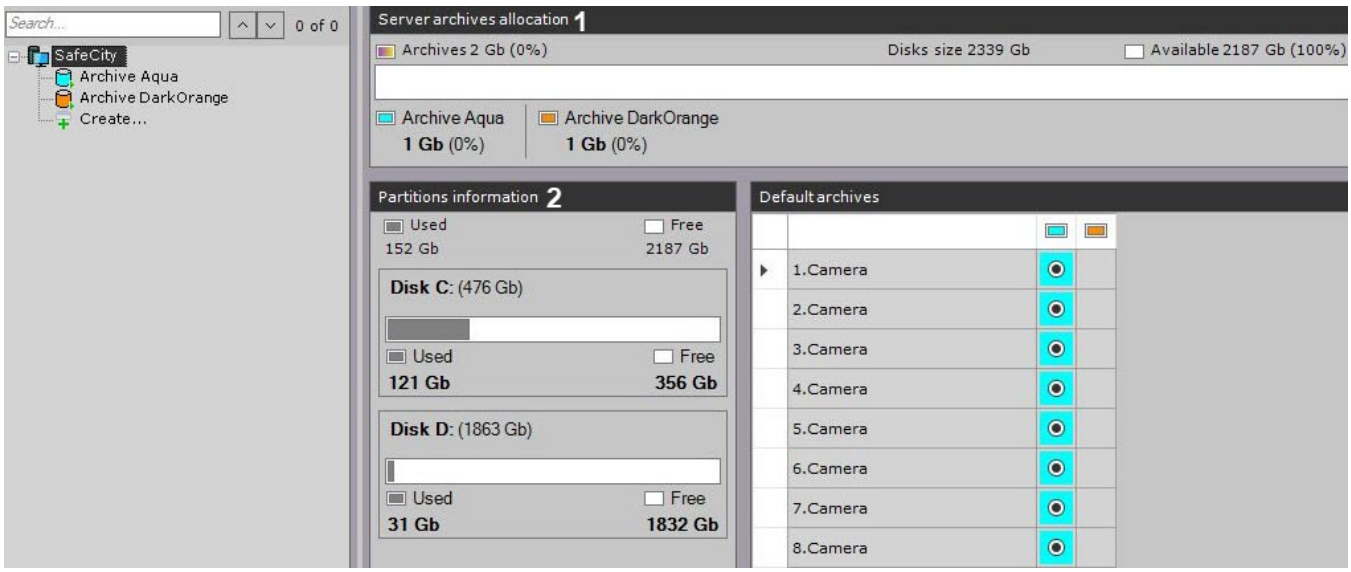
> **Attention!**
>
> If you remove the archive files, then all the video footage that they contained will be lost.
>
> If you do not remove the archive files, you can re-use them to create another archive (see Creating an archive based on existing archive volumes). You can as well use a partition to re-create an archive.

Removing an archive from the system is now complete.

Information about the filled archive volume

Selecting a **Server** object displays statistical information about the available Server disks and created archives.

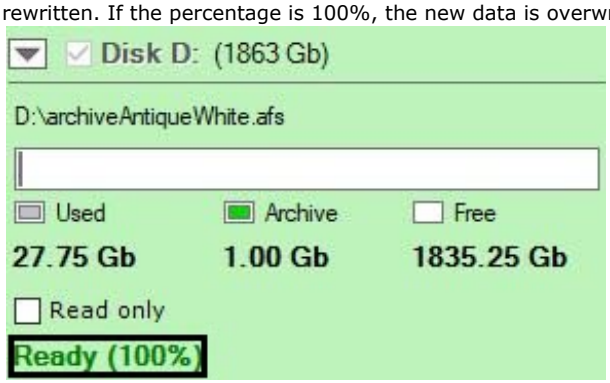
Figure (**1**) shows the overall balance of free disk space between the Server archives.



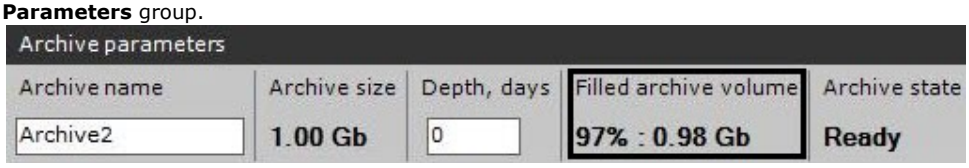
In addition, a list of disks is displayed, containing information about the total disk capacity, space used, and total free space (**2**).

When you select an archive, the following information is displayed:

1. The percentage of used space on each volume in the archive. This parameter indicates whether the volume's data is being rewritten. If the percentage is 100%, the new data is overwriting the old data.

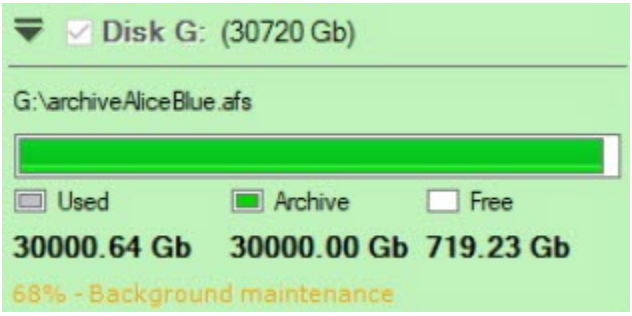


2. The approximate volume usage in percentage and gigabytes (**2**) is displayed in the **Filled archive volume** field of the **Archive Parameters** group.



When you update *Axxon One* or restart the Server, or create the archive based on the existing volume etc., the archive is reindexed.

Reindexing progress bar is displayed.

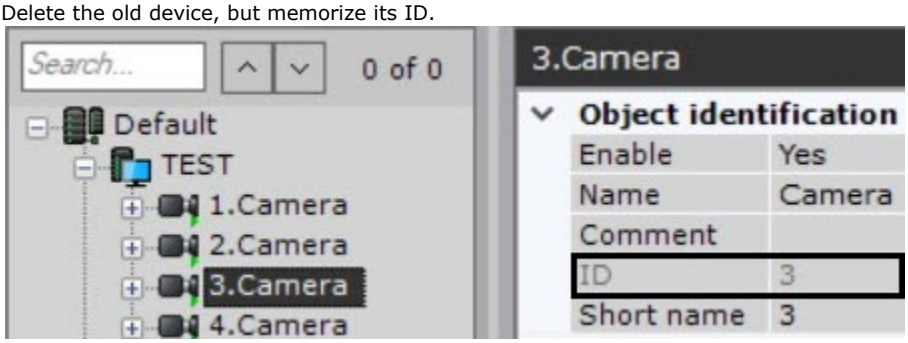

Disk G: (30720 Gb)
G:\archiveAliceBlue.afs
Used
Archive
Free
30000.64 Gb
30000.00 Gb
719.23 Gb
68% - Background maintenance

Saving the archive when replacing the video signal device

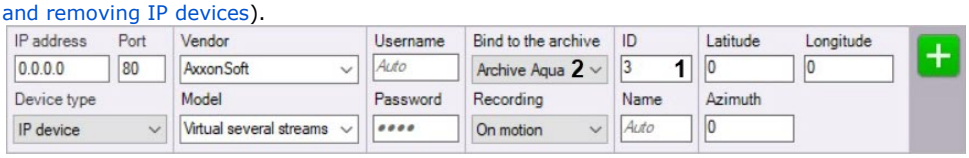
In *Axxon One*, you can save the archive in case you want to replace the camera, NVR, or any other source of video signal.

To do this, do the following:

1. Delete the old device, but memorize its ID.



2. Create a new device in the system with the same ID (**1**) and bind it to the old archive (**2**, see Searching, adding, configuring and removing IP devices).



> **Attention!**
>
> Device model, IP-address and any other device parameters may differ from the previous one.

If you replace NVR, the cameras must be connected to the same channels as before.

After creating a new device with the old ID, the archive recorded earlier will be available in the system.

Configuring detection tools

General information about detection tools and their sub-tools

Processors used for detection tools operation

Hardware requirements for GPU-based video decoding

Installing DetectorPack add-ons

Configuring detection tools and their sub-tools

General information on metadata

Neural analytics

- General information on neural analytics
- Hardware requirements for neural analytics operation
- Data collection requirements for neural network training
- Optimizing the operation of neural analytics on GPU in Windows OS
- Optimizing the operation of neural analytics on GPU in Linux OS

General settings of the detection tools

- Selecting Nvidia GPU when configuring detection tools
- Configuring the minimum and maximum size of detected objects
- Configuring a skip area
- Configuring a detection area
- Configuring perspective
- Configuring the scanning mode
- Displaying the number of detected objects

Standard detection sub-tools

- General information on the standard detection sub-tools
- Camera requirements for the standard detection sub-tools
- Configuring Line Crossing
- Configuring Loitering In Area
- Configuring Stop In Area
- Configuring Motion In Area
- Configuring Entrance In Area
- Configuring Exit From Area
- Configuring Multiple Objects
- Configuring Move From Area To Area

Category: Trackers

- Abandoned Objects Detection VI
  - Functions of the Abandoned Objects Detection VI
  - Video stream and scene requirements for the Abandoned Objects Detection VI
  - Image requirements for the Abandoned Objects Detection VI
  - Licensing of the software module for the Abandoned Objects Detection VI
  - Configuring the Abandoned Objects Detection VI
- Abandoned Objects Detection (Street) VI
  - Functions of the Abandoned Objects Detection (Street) VI
  - Video stream and scene requirements for the Abandoned Objects Detection (Street) VI
  - Image requirements for the Abandoned Objects Detection (Street) VI
  - Licensing of the software module for the Abandoned Objects Detection (Street) VI
  - Configuring the Abandoned Objects Detection (Street) VI
- Neurotracker
  - Functions of the Neurotracker
  - Video stream and scene requirements for the Neurotracker and its sub-tools
  - Image requirements for the Neurotracker and its sub-tools
  - Configuring the Neurotracker
- Object Tracker
  - Functions of the Object Tracker
  - Video stream and scene requirements for the Object Tracker and its sub-tools

    - Image requirements for the Object Tracker and its sub-tools
    - Recommendations for configuring the Object Tracker and its sub-tools
    - Configuring the Object Tracker
    - Abandoned Object detection
- Object Tracker VL
    - Functions of the Object Tracker VL
    - Video stream and scene requirements for the Object Tracker VL and its sub-tools
    - Image requirements for the Object Tracker VL and its sub-tools
    - Activating the license for the Object Tracker VL in Windows OS
    - Activating the license for the Object Tracker VL in Linux OS
    - Configuring the Object Tracker VL
        - Configuring the Object Tracker VL sub-tools
            - Configuring the Object Tracker VL standard detection sub-tools
- Stopped object detector
    - Functions of the Stopped object detector
    - Video stream and scene requirements for the Stopped object detector
    - Image requirements for the Stopped object detector
    - Configuring the Stopped object detector
- Motion detection
    - Functions of the Motion detection
    - Video stream and scene requirements for the Motion detection and its sub-tools
    - Image requirements for the Motion detection and its sub-tools
    - Configuring the Motion detection
- Privacy Masking
    - Functions of the Privacy Masking
    - Video stream and scene requirements for the Privacy Masking
    - Image requirements for the Privacy Masking
    - Configuring the Privacy Masking

Category: Face

- Face Detection VL
    - Functions of the Face Detection VL
    - Hardware requirements for the Face Detection VL and its sub-tools
    - Video stream and scene requirements for the Face Detection VL and its sub-tools
    - Image requirements for the Face Detection VL and its sub-tools
    - Activating the license for the Face Detection VL in Windows OS
    - Activating the license for the Face Detection VL in Linux OS
    - Configuring the Face Detection VL
- Face Detection VA
    - Functions of the Face Detection VA
    - Manual for switching from the Face Detection TV to Face Detection VA
    - Hardware requirements for the Face Detection VA and its sub-tools
    - Video stream and scene requirements for the Face Detection VA and its sub-tools
    - Image requirements for the Face Detection VA and its sub-tools
    - Optimizing the operation of the Face Detection VA on GPU
    - Configuring the Face Detection VA
- Masks Detection
- Configuring face recognition based on the created lists
- Configuring macros when working with face lists
    - Examples of macros used when working with face lists
- Configuring integration with FaceCube
- Face Detection TV
    - Functions of the Face Detection TV
    - Hardware requirements for the Face Detection TV and its sub-tools
    - Video stream and scene requirements for the Face Detection TV and its sub-tools
    - Image requirements for the Face Detection TV and its sub-tools
    - Optimizing the operation of the Face Detection TV on GPU
    - Configuring the Face Detection TV

Category: Vehicle

- Configuring vehicle license plate recognition based on the created lists
    - Configuring macros when working with vehicles lists
        - Examples of macros used when working with vehicles lists
- License Plate Recognition BRS
    - Camera requirements for License Plate Recognition BRS and its sub-tools
    - License Plate Recognition BRS features and specifications
    - Configuring License plate recognition BRS
- License Plate Recognition IV

    - License Plate Recognition IV features and specifications
    - Hardware requirements for License Plate Recognition IV
    - Camera requirements for License Plate Recognition IV and its sub-tools
        - Examples of correct and incorrect video images
    - Configuring License Plate Recognition IV
    - Activating the license for the License plate recognition IV in Linux OS
- License Plate Recognition RR and Vehicle Recognition RR
    - Functionality of License Plate Recognition RR and Vehicle Recognition RR
    - Hardware requirements for License Plate Recognition RR and Vehicle Recognition RR
    - Camera requirements for License Plate Recognition RR, Vehicle Recognition RR and their sub-tools
        - Recommendations for configuring the speed detection area
    - Optimizing the operation of License Plate Recognition RR and Vehicle Recognition RR on GPU
    - Configuring the License Plate Recognition RR detection tools
        - Configuring License Plate Recognition RR
        - Configuring License Plate Recognition RR—Parking
        - Configuring License Plate Recognition RR—Search In Archive
    - Configuring Vehicle Recognition RR
    - Parameters that specify the conditions for triggering macros when recognizing a vehicle
- License plate recognition VT
    - License plate recognition (VT) features and specifications
    - Hardware requirements for License Plate Recognition VT
    - Camera requirements for License plate recognition (VT)
    - Configuring License Plate Recognition VT
    - Fine-tuning the VT number plate detection tool
    - Licensing of the software module for License plate recognition (VT)
    - Licensing of the software module for the License plate recognition (VT) in Linux OS
- Vehicle Recognition XR
    - Functions of the Vehicle Recognition XR
    - Hardware requirements for the Vehicle Recognition XR
    - Video stream and scene requirements for the Vehicle Recognition XR
    - Image requirements for the Vehicle Recognition XR
    - Licensing of the software module for the Vehicle Recognition XR

Category: Poses

- Person-Based Privacy Masking
    - Functions of the Person-Based Privacy Masking
    - Video stream and scene requirements for the Person-Based Privacy Masking
    - Configuring the Person-Based Privacy Masking
- Pose Detection
    - Functions of the Pose Detection and its sub-tools
    - Video stream and scene requirements for the Pose Detection and its sub-tools
    - Image requirements for the Pose Detection and its sub-tools
    - Configuring the Pose Detection
    - Configuring the Pose Detection sub-tools
        - Configuring the Sitting Person Detection
        - Configuring the Person Down Detection
        - Configuring the Hands up detection
        - Configuring the Handrail holding detection
        - Configuring the People counter
        - Configuring the Close-standing people detection
        - Configuring the People masking
        - Configuring the standard detection sub-tools of the Pose Detection

Category: Production Safety

- Audio Analytics Detection IV
    - Functions of the Audio Analytics Detection IV
    - Audio data requirements for the operation of the Audio Analytics Detection IV
    - Configuring the Audio Analytics Detection IV
- Object Presence Detection
    - Functions of the Object Presence Detection
    - Video stream and scene requirements for the Object Presence Detection
    - Configuring the Object Presence Detection
- Fire Detection
    - Functions of the Fire Detection
    - Video stream and scene requirements for the Fire Detection
    - Configuring the Fire Detection
- Equipment detection (PPE)
    - Functions of the Equipment detection (PPE)

    - Video stream and scene requirements for the Equipment detection (PPE) and its sub-tools
    - Image requirements for the Equipment detection (PPE) and its sub-tools
    - Example of providing a list of valid equipment at the facility for the Equipment detection (PPE)
    - Configuring the Equipment detection (PPE)
- Smoke Detection
    - Functions of the Smoke Detection
    - Video stream and scene requirements for the Smoke Detection
    - Configuring the Smoke Detection
- Water Level Detection
    - Functions of the Water Level Detection
    - Video stream requirements for the Water Level Detection
    - Image requirements for the Water Level Detection
    - Configuring the Water Level Detection
- Glow detector
    - Functions of the Glow detector
    - Video stream and scene requirements for the Glow detector
    - Image requirements for the Glow detector
    - Configuring the Glow detector
- PPE detection VL
    - Functions of the PPE detection VL
    - Video stream and scene requirements for the PPE detection VL and its sub-tools
    - Image requirements for the PPE detection VL and its sub-tools
    - Example of providing a list of valid equipment at the facility for the PPE detection VL
    - Activating the license for the PPE detection VL in Windows OS
    - Activating the license for the PPE detection VL in Linux OS
    - Configuring the PPE detection VL

Category: Retail

- Barcode Detection
    - Functions of the Barcode Detection
    - Video stream and scene requirements for the Barcode Detection and its sub-tools
    - Image requirements for the Barcode Detection and its sub-tools
    - Configuring the Barcode Detection
    - Examples of macros for barcode detection
- Crowd Estimation VA
    - Functions of the Crowd Estimation VA
    - Video stream and scene requirements for the Crowd Estimation VA
    - Image requirements for the Crowd Estimation VA
    - Configuring the Crowd Estimation VA
- Neurocounter
    - Functions of the Neurocounter
    - Video stream and scene requirements for the Neurocounter operation
    - Image requirements for the Neurocounter operation
    - Configuring the Neurocounter
- Queue detection
    - Functions of the Queue detection
    - Video stream and scene requirements for the Queue detection
    - Image requirements for the Queue detection
    - Configuring the Queue detection
- Visitors Counter
    - Functions of the Visitors Counter
    - Video stream and scene requirements for the Visitors Counter
    - Image requirements for the Visitors Counter
    - Configuring the Visitors Counter

Category: Service

- Audio Loss
    - Functions of the Audio Loss
    - Configuring the Audio Loss
- Noise Detection
    - Functions of the Noise Detection
    - Configuring The Noise Detection
- Signal Detection
    - Functions of the Signal Detection
    - Configuring the Signal Detection
- Tampering Detection
    - Functions of the Tampering Detection
    - Video stream and scene requirements for the Tampering Detection

    - Image requirements for the Tampering Detection
    - Configuring the Tampering Detection

Scene Analytics detection tools

- Functions of Scene Analytics detection tools
- Video requirements for scene analytics detection tools
    - Video requirements for object tracker-based scene analytics detection tools
    - Video requirements for object tracker (with neural filter)-based scene analytics detection tools
    - Video requirements for VMD-based scene analytics detection tools
    - Camera requirements for abandoned objects detection
    - Camera requirements for neural filter operation
- Configuring Scene Analytics Detection Tools
    - Setting up Tracker-based Scene Analytics detection tools
        - Setting general parameters of Tracker-based Scene Analytics detection tools
            - Configuring detected objects
    - Setting up VMD-based Scene Analytics detection tools

Category: Embedded

- General information about embedded detection tools
- AxxonSoft Tracker in Axis devices
- Face Detection and Temperature Control with Mobotix M16 TR cameras
    - Functional parameters of the Face Detection and Temperature Control
    - Camera requirements for face detection and temperature control
    - Temperature screening protocol
    - Pre-configuration of the Mobotix M16 TR camera
    - Configuring Face Detection and Temperature Control
- Embedded vehicle speed measurement radar

Configuring Inputs

Checking the triggering of a detection tool

Automatic Rules

General information about detection tools and their sub-tools

Detection tool is a software object (part of the software environment) that represents an algorithm or a set of algorithms that allows you to analyze video and audio streams according to a predefined scenario and signal the analysis results by creating events within the software environment.

Detection sub-tool is a detection tool that processes the data received from the parent detection tool.

Attention!

- To configure detection tools and their sub-tools, you must have permissions to configure them (see Configuring user permissions).
- You can create detection tools and their sub-tools for the cameras connected to *Axxon One* (see The Camera object).
- You can configure detection tools and their sub-tools on the **Settings** tab **Detection Tools** (see Configuring detection tools and their sub-tools).

By default, no action is performed in the system when an event from a detection tool or sub-tool is received. To perform an action, you must create an automatic rule or macro (see Automatic Rules, Configuring macros).

All *Axxon One* detection tools and their sub-tools:

Installing DetectorPack add-ons

Category	Detection tools	Detection sub-tools
Category: Trackers	Motion detection	• Line Crossing • Loitering In Area • Stop In Area • Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area to Area • Abandoned object (for Object Tracker only)
	Neurotracker	
	Privacy Masking (doesn't have sub-tools)	
	Object Tracker	
	Object Tracker VL	
	Stopped object detector (doesn't have sub-tools)	
	Abandoned Objects Detection VI (doesn't have sub-tools)	
	Abandoned Objects Detection (Street) VI (doesn't have sub-tools)	
	Direction line	
	Direction area	
Category: Service	Audio Loss	NA
	Noise Detection	
	Signal Detection	
	Tampering detection	
Category: Face	Face Detection TV	• Line Crossing • Loitering In Area • Entrance In Area • Masks Detection
	Face Detection VL	
	Face Detection VA	
Category: Vehicle	License Plate Recognition BRS	• Line Crossing • Loitering In Area • Stop In Area
	License Plate Recognition IV	

	License Plate Recognition RR	• Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area to Area
	License Plate Recognition RR—Search In Archive	
	License Plate Recognition RR—Parking	
	License Plate Recognition VT	
	Vehicle Recognition RR	
Category: Poses	Person-Based Privacy Masking	NA
	Pose Detection	• Sitting Person Detection • Person Down Detection • Hands up detection • Handrail holding detection • People counter • Close-standing people detection • People masking • Line Crossing • Loitering In Area • Stop In Area • Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area to Area
Category: Production Safety	Audio Analytics Detection IV	For Equipment detection (PPE) and PPE detection VL only: • Line Crossing • Loitering In Area • Stop In Area • Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area to Area
	Fire Detection	
	Glow detector	
	Equipment detection (PPE)	
	Object Presence Detection	
	Smoke Detection	
	Water Level Detection	
	PPE detection VL	
Category: Retail	Barcode Detection	For Barcode Detection only: • Line Crossing • Loitering In Area • Stop In Area • Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area to Area
	Neurocounter	
	Queue detection	
	Visitors Counter	
	Crowd Estimation VA	
Category: Embedded	Embedded Motion Detection	NA
	Embedded Tampering detection	
	Embedded Audio detection	
	Embedded Face detection	
	Embedded Intrusion detection	
	Embedded Line crossing detection	
	Embedded Object Appearance in the Area	
	Embedded Disappearance in area	

Embedded Abandoned Object detection	
Embedded Object disappearance detection	
ROI compression	
Embedded GPS tracker	
Embedded License Plate Recognition	
Embedded temperature detection	Face Detection and Temperature Control
Embedded body temperature detection	NA
Tracker Analytics	• Line Crossing • Loitering In Area • Stop In Area • Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area to Area
Embedded analytics	

Also, the default detection tool list displays camera inputs (see Configuring Inputs) that you can use in an automatic rule.

Processors used for detection tools operation

> **Attention!**
>
> Starting with *Detector Pack* 3.10, working on VPU (Intel HDDL, Intel Movidius) isn't supported.

Refer to the following table to check the compatibility of detection tools and processors.

Category	Detection tool	Windows x64			Linux AMD64		
		CPU	GPU	VPU	CPU	GPU	VPU
Category: Trackers	Motion detection	✓	✓	–	✓	✓	–
	Neurotracker	✓	✓	✓	✓	✓	✓
	Privacy Masking	✓	✓	✓	✓	✓	✓
	Object Tracker	✓	–	–	✓	–	–
	Object Tracker VL	✓	✓	–	✓	–	–
	Stopped object detector	✓	✓	–	✓	✓	–
	Abandoned Objects Detection VI	✓	✓	–	✓	✓	–
	Abandoned Objects Detection (Street) VI	✓	✓	–	✓	✓	–
Category: Service	Tampering detection tool	✓	–	–	✓	–	–
	Audio Loss	✓	–	–	✓	–	–
	Noise Detection	✓	–	–	✓	–	–
	Signal Detection	✓	–	–	✓	–	–
Category: Face	Face Detection TV	✓	✓	–	✓	✓	–
	Face Detection VA	✓	✓	–	✓	✓	–
	Face Detection VL	✓	✓	–	✓	✓	–
Category: Vehicle	License Plate Recognition BRS	✓	–	–	✓	–	–
	License Plate Recognition IV	✓	✓	–	✓	✓	–
	License Plate Recognition RR	✓	✓	–	✓	✓	–
	License Plate Recognition RR—Search In Archive	✓	✓	–	✓	✓	–
	License Plate Recognition RR—Parking	✓	✓	–	✓	✓	–
	License plate recognition VT	✓	✓	✓	✓	–	✓
	Vehicle Recognition RR	✓	✓	–	✓	✓	–
Category: Poses	Person-Based Privacy Masking	✓	✓	✓	✓	✓	✓
	Pose Detection	✓	✓	✓	✓	✓	✓
Category: Production Safety	Audio Analytics Detection IV	✓	–	–	✓	–	–
	Fire Detection	✓	✓	✓	✓	✓	✓
	Glow detector	✓	–	–	✓	–	–
	Object Presence Detection	✓	✓	✓	✓	✓	✓
	Equipment detection (PPE)	✓	✓	✓	✓	–	–
	Smoke Detection	✓	✓	✓	✓	✓	✓
	PPE detection VL	✓	✓	✓	✓	–	–
	Water Level Detection without a neural network	✓	–	–	✓	–	–
	Water Level Detection with a neural network	✓	✓	✓	✓	✓	✓

Category: Retail	Barcode Detection	✓	✓	✓	✓	✓	✓
	Neurocounter	✓	✓	✓	✓	✓	✓
	Queue detection	✓	⊖	⊖	✓	⊖	⊖
	Visitors Counter	✓	⊖	⊖	✓	⊖	⊖
	Crowd Estimation VA	✓	✓	⊖	✓	✓	⊖

Hardware requirements for GPU-based video decoding

Hardware requirements

Processors used for detection tools operation

If detection tools use GPU for video decoding (see Processors used for detection tools operation), the following hardware requirements must be met:

For Nvidia GPUs	• CUDA 11.1–11.4. • Support for the required codec in NVDEC (see here). • Compute Capability 3.5–8.6. **Attention!** • CUDA is compatible with generations of computers with the following architectures: Kepler (partially), Maxwell, Pascal, Volta, Turing, Ampere (partially) (see CUDA). • You can check the GPU Compute Capability version on the manufacturer's website. • When using Nvidia GPUs, we recommend installing the latest driver from the official website. • To decode video in *Axxon One*, you can use up to four Nvidia GPUs (see Selecting Nvidia GPU when configuring detection tools) installed on the Server (Nvidia GPU 0, Nvidia GPU 1, Nvidia GPU 2, Nvidia GPU 3).
For the integrated Intel GPUs	• 6th generation CPU or higher. • Support for the required codec in Quick Sync Video

Installing DetectorPack add-ons

General information about detection tools and their sub-tools

By default, the *Axxon One* distribution package includes only the basic *DetectorPack* (see Installation, Installing Axxon One in Linux OS)

To install add-ons to the basic package, do the following:

1. Download the required packages from the official website.
2. Stop the Server (see Shutting down a Server).
3. Run the executable file and wait for the installation to complete.
4. Start the Server (see Starting a Server).

Attention!

Versions of the basic *DetectorPack* and the *DetectorPack* add-ons must be the same. If versions differ, you must update the version of the basic *DetectorPack,* so it matches the version of the *DetectorPack* add-ons.

All packages of the *DetectorPack* with detection tools and their sub-tools are described in the table:

Package	Detection tools	Detection sub-tools
Basic *DetectorPack*	• Motion detection • Object Tracker (without Neural filter) **Note** You need to install the Neuro Pack add-on for the Neural filter operation. • Tampering Detection • Audio Loss detection • Noise Detection • Signal Detection • Queue detection • Glow detector • Visitors Counter	• Line Crossing • Loitering In Area • Stop In Area • Motion In Area • Entrance In Area • Exit From Area • Multiple Objects • Move From Area To Area • Abandoned Objects Detection (for Object Tracker only)
Neuro Pack add-on	**Note** For the face and people masking function to work when exporting a video, you must install Neuro Pack add-on • Neurofilter • Neurotracker • Neurocounter • Pose Detection • Object Presence Detection • Stopped object detector • Smoke Detection • Fire Detection • Water Level Detection • Equipment detection (PPE) • Barcode Detection • Privacy Masking • Person-Based Privacy Masking	For Pose Detection only: • Sitting Person Detection • Person Down Detection • Hands up detection • Handrail holding detection • People counter • Close-standing people detection • People masking

<table>
<tr>
<td>VL Face Recognition Pack add-on</td>
<td>Face Detection VL

Attention!
For the Face Detection VL to work, you must install two packages from the DetectorPack:
VL Face Recognition Pack add-on;
SDK Pack.
You can install only one of the optional Face Recognition packs: VA Face Recognition Pack add-on, VL Face Recognition Pack add-on or TV Face Recognition Pack add-on. You cannot install several packs in the same system.</td>
<td>Masks Detection</td>
</tr>
<tr>
<td>VA Face Recognition Pack add-on</td>
<td>Face Detection VA

Attention!
You can install only one of the optional Face Recognition packs: VA Face Recognition Pack add-on, VL Face Recognition Pack add-on or TV Face Recognition Pack add-on. You cannot install several packs in the same system.
Face Recognition Pack is guaranteed to work on Linux Debian 11 and Ubuntu 20. Face Recognition Packs isn't guaranteed to work on Linux Debian 9/10, Ubuntu 18 and Ubuntu 19 (see Operating system requirements).</td>
<td>Masks Detection</td>
</tr>
<tr>
<td>TV Face Recognition Pack add-on</td>
<td>Face Detection TV

Attention!
You can install only one of the optional Face Recognition packs: VA Face Recognition Pack add-on, VL Face Recognition Pack add-on or TV Face Recognition Pack add-on. You cannot install several packs in the same system.
Face Recognition Pack is guaranteed to work on Linux Debian 11 and Ubuntu 20. Face Recognition Packs isn't guaranteed to work on Linux Debian 9/10, Ubuntu 18 and Ubuntu 19 (see Operating system requirements).</td>
<td>Masks detection</td>
</tr>
<tr>
<td>VL SDK Pack (must be installed when you install VL Face Recognition Pack and VL PPE)</td>
<td>Attention!
For the Face Detection VL to work, you must install two packages from the DetectorPack:
VL Face Recognition Pack add-on;
SDK Pack.
For the PPE detection VL to work, you must install two packages from the DetectorPack:
VL PPE add-on;
SDK Pack.</td>
<td>NA</td>
</tr>
<tr>
<td>RR LPR add-on</td>
<td>License Plate Recognition RR
License Plate Recognition—Parking RR
License Plate Recognition—Search in archive RR
Vehicle Recognition RR</td>
<td>NA</td>
</tr>
</table>

XR Vehicle Recognition add-on	Vehicle Recognition XR	NA
VT LPR add-on	License Plate Recognition VT	NA
IV Analytics Pack add-on	License Plate Recognition IV	NA
BRS LPR add-on	License Plate Recognition BRS	NA
VA Crowd Estimation Pack add-on	Crowd Estimation VA	NA
VL PPE add-on	PPE detection VL **Attention!** For the PPE detection VL to work, you must install two packages from the *DetectorPack*: • VL PPE add-on; • SDK Pack.	NA
IV Audio Analytics Pack add-on	Audio Analytics Detection IV	NA
VI Analytics Pack add-on	• Abandoned Objects Detection VI • Abandoned Objects Detection (Street) VI	NA
VL Analytics Pack add-on	Object Tracker VL **Attention!** For the Object Tracker VL to work, you must install two packages from the *DetectorPack*: • VL Analytics Pack add-on; • VL SDK Pack.	NA

Configuring detection tools and their sub-tools

On the page:

- General information
- Creating a detection tool
- Creating a sub-tool
- Removing a detection tool/sub-tool
- Bulk creation of detection tools/sub-tools of the same type for different cameras
- Bulk application of settings for detection tools/sub-tools of the same type
- Bulk removal of detection tools/sub-tools

General information

In *Axxon One*, you can create and configure detection tools and their sub-tools (child detection tools). Sub-tools process the data received from parent detection tools.

To create and configure detection tools, you must have permissions to do so (see Configuring user permissions).

Attention!

- You can create detection tools and sub-tools for enabled and disabled cameras if camera video streams are enabled (see Configuring video stream settings).
- You cannot create detection sub-tools if the parent detection tools don't have the settings applied (you must click the **Apply** button).

Several identical detection tools can operate on the same camera stream:

Detection tools	Number of identical detection tools for one camera
Motion detection, Neurotracker, Object Tracker, Neurocounter	10
Water Level Detection, Queue detection, Visitors Counter, Masks Detection	Unlimited

Attention!

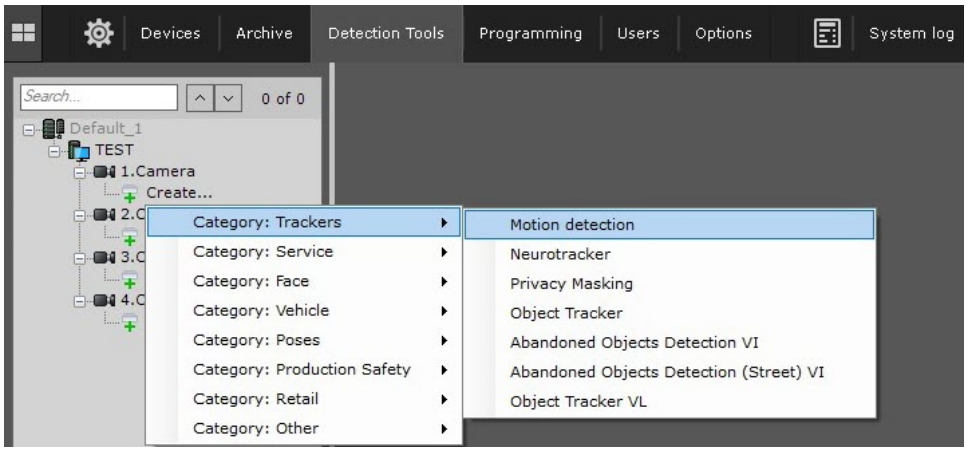
For other detection tools and their sub-tools, you cannot create identical detection tools and their sub-tools for one camera.

Creating a detection tool

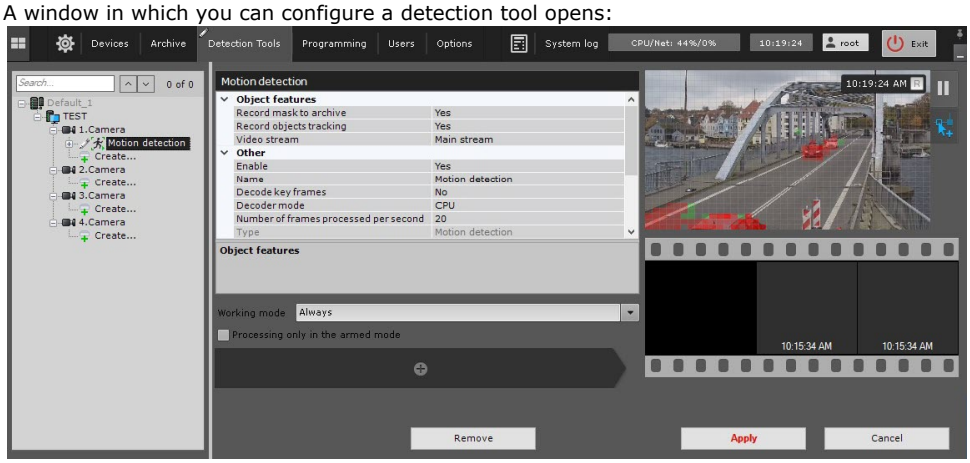
To create a detection tool, do the following:

1. Select the **Settings** tab **Detection Tools**.
2. Below the required camera, click **Create...**. The list of available categories of detection tools will be displayed (see General information about detection tools and their sub-tools).

3. Select a detection tool.



A window in which you can configure a detection tool opens:



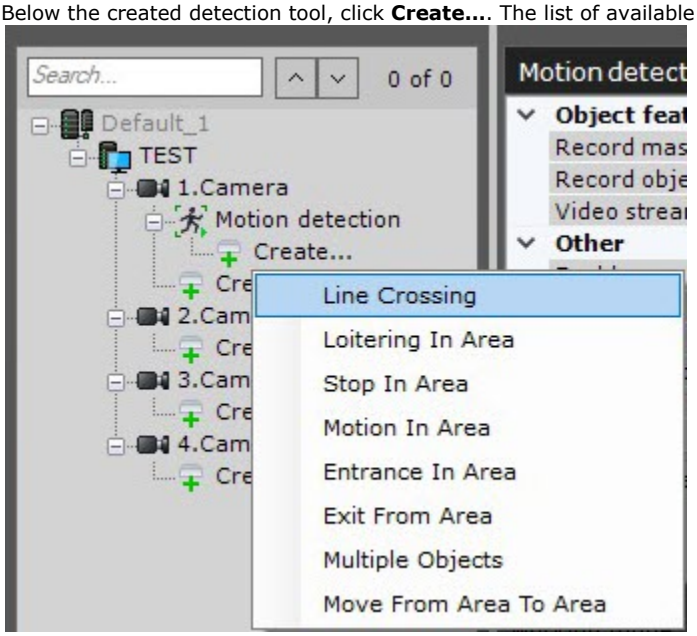
4. Click the **Apply** button.

Creation of a detection tool is complete. The detection tool is displayed below the selected camera in the objects tree.

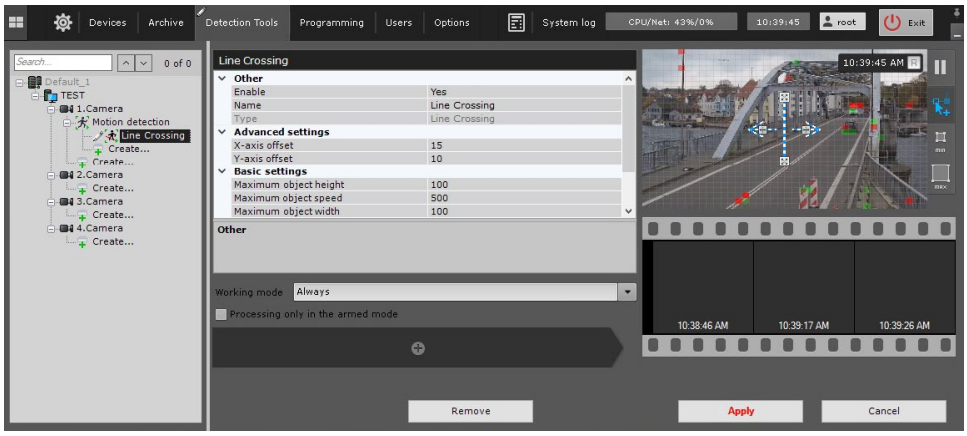
Creating a sub-tool

To create a sub-tool, do the following:

1. Create the required detection tool and specify its parameters (see General information about detection tools and their sub-tools).
2. Below the created detection tool, click **Create...**. The list of available sub-tools is displayed.



3. Select a sub-tool. A window in which you can configure a sub- tool opens.

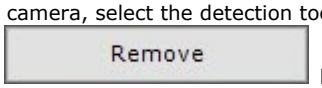


4. Click the **Apply** button.

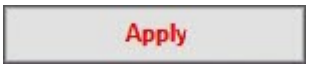
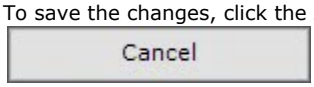
Creation of a sub-tool is complete. The sub-tool is displayed below the selected camera and below the detection tool in the objects tree.

Removing a detection tool/sub-tool

To remove a detection tool/sub-tool, do the following:

1. Select the **Settings** tab **Detection Tools**.
2. Below the required camera, select the detection tool/sub-tool.
3. Click the **Remove**  button.

> **Attention!**
>
> If you created sub-tools for the detection tool, they also will be removed from the existing configuration.

4. To save the changes, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Removing a detection tool/sub-tool is complete. The removed detection tool/sub-tool won't be displayed below the camera in the objects tree.

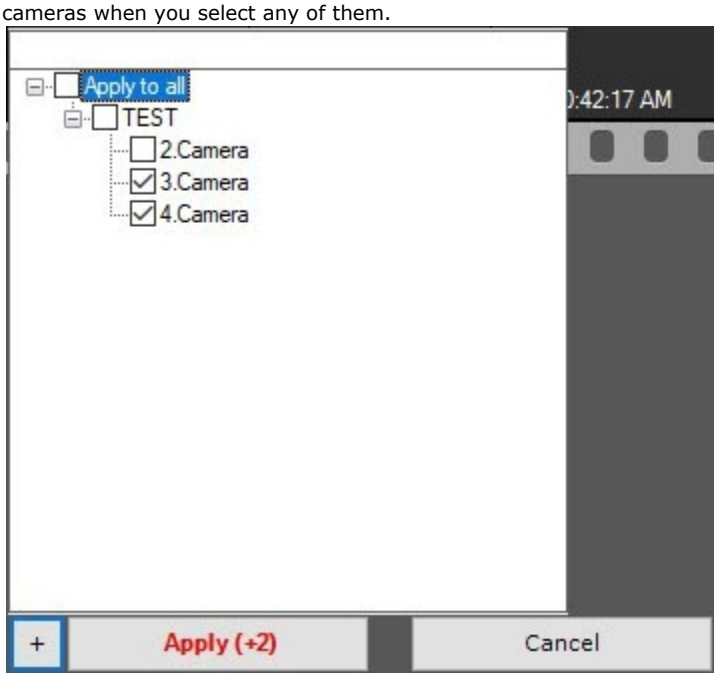
Bulk creation of detection tools/sub-tools of the same type for different cameras

To bulk create detection tools/sub-tools of the same type for different cameras, do the following:

1. Create and configure the required detection tool/sub-tool for one camera or select the existing detection tool/sub-tool in the objects tree.
2. Click the  button in the lower right corner.

> **Note**
>
> When you select a sub-tool, in the camera list, only those cameras that have the same parent detection tool will be available.

3. Set the checkbox next to the required cameras. To quickly select a large number of cameras, press the **Shift** key, select the first and the last cameras for which you want to create a detection tool/sub-tool. The checkbox will be set for all selected cameras when you select any of them.



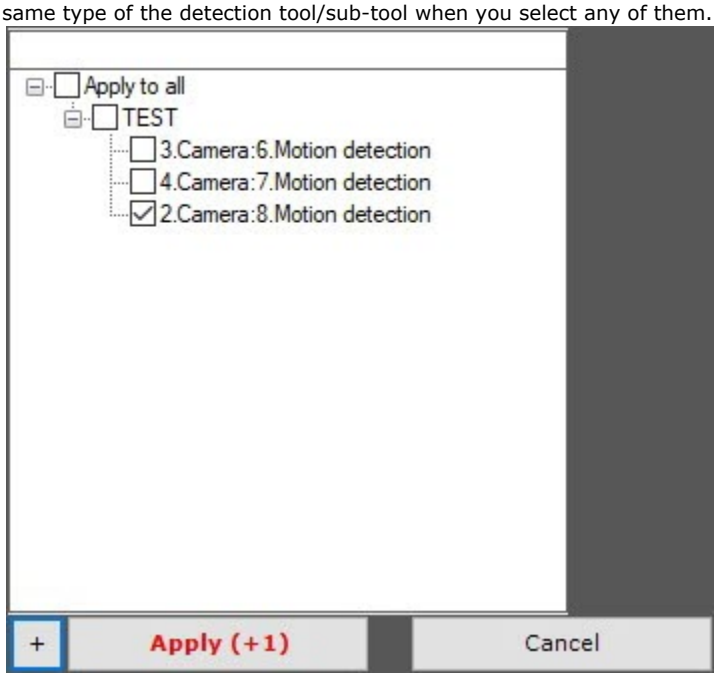
4. Click the **Apply** button. The number of cameras for which the detection tool/sub-tool is created is indicated in brackets.

Bulk creation of detection tools/sub-tools of the same type for different cameras is complete. The detection tools/sub-tools of the selected cameras will be displayed in the objects tree.

Bulk application of settings for detection tools/sub-tools of the same type

For bulk application of settings for detection tools/sub-tools of the same type, do the following:

1. Change the values of the parameters in the settings of one detection tool/sub-tool.
2. Click the  button in the lower right corner.
3. Set the checkbox next to the required cameras with the same type of the detection tool/sub-tool. To quickly select a large number of cameras with the same type of the detection tool/sub-tool, press the **Shift** key, select the first and the last cameras for which you want to change settings of a detection tool/sub-tool. The checkbox will be set for all selected cameras with the same type of the detection tool/sub-tool when you select any of them.



> **Attention!**
>
> You cannot bulk change detection areas (see Configuring a detection area) and ignore areas (see Configuring a skip area).

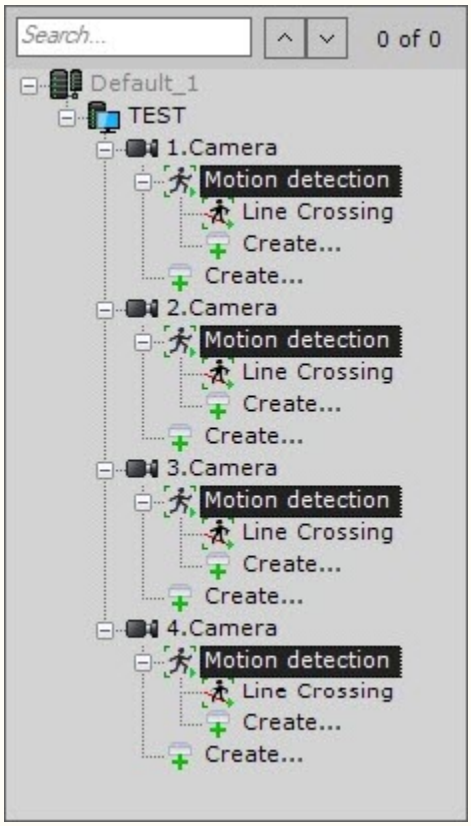
4. Click the **Apply** button. The number of cameras with the same type of detection tool/sub-tool for which the settings are applied is indicated in brackets.

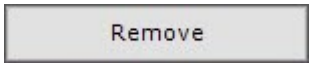
Bulk application of settings for detection tools/sub-tools of the same type is complete. In the settings of the detection tools/sub-tools, the selected cameras will have the same values of the parameters.

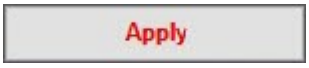
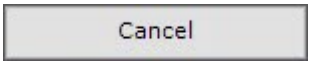
Bulk removal of detection tools/sub-tools

To bulk remove detection tools/sub-tools, do the following:

1. Select the **Settings** tab **Detection Tools**.
2. Use the **Ctrl** key to select the detection tools//sub-tools that you want to delete in the objects tree.

> **Attention!**
>
> You can select detection tools of one level only. For example, if you select **Motion detection**, you cannot select **Line Crossing** detection and vice versa.
>
> 
>

3. Click the **Remove**  button.

4. Click the **Apply**  button to save the changes. Click the **Cancel**  button to cancel the changes.

Bulk removal of detection tools/sub-tools is complete. The removed detection tools/sub-tools won't be displayed in the objects tree.

General information on metadata

Metadata is any accompanying data to any basic information. Metadata refers to additional information about the content or object. It reveals information about the attributes and properties that characterize an entity, allowing you to automatically search and manage it in large information flows.

In *Axxon One,* you can get metadata in two ways:

1. By analyzing video on the Server by detection tools (see General information about detection tools and their sub-tools).
2. By receiving ready metadata from the embedded camera analytics (see General information about embedded detection tools).

> **Attention!**
>
> To get metadata, video is decompressed and analyzed, which leads to a heavy load on the Server and limits the number of cameras that you can use on it.

Metadata are VMDADB files and are stored in the object tracks database. Path to the metadata folder: <Local directory of the Server selected when installing *Axxon One* (see Installation)>\vmda_db\VMDA_DB.0\vmda_schema.

> **Note**
>
> If necessary, you can place metadata in network storage (see Configuring storage of the system log and metadata).

The following tools are used for the Server-side analysis and metadata generation:

Detection tool	Possible information about an object contained in metadata from the detection tool
Neurotracker Object Tracker Object Tracker VL	• Object type • Object size • Object color • Position of an object in the frame • Object speed • Direction of movement of an object
Stopped object detector	• Object type • Object size • Position of an object in the frame
Motion detection	• Object type • Object color
Face Detection VA Face Detection TV Face Detection VL	• Face vector • Face bounding box • Gender • Age • Position of a face bounding box in the frame
License Plate Recognition BRS License Plate Recognition IV License Plate Recognition RR License Plate Recognition RR—Search In Archive License Plate Recognition RR—Parking	• Vehicle license plate • License plate bounding box • Position of a license plate bounding box in the frame • Direction of vehicle movement • Region • Country • License plate type • Vehicle manufacturer • Vehicle model • Vehicle color • Vehicle class

License plate recognition VT	• Vehicle bounding box • Position of a vehicle bounding box in the frame
Vehicle Recognition RR	• Vehicle manufacturer • Vehicle model • Vehicle color • Vehicle class • Vehicle bounding box • Position of a vehicle bounding box in the frame • Direction of vehicle movement
Pose Detection and its sub-tools: • Sitting Person Detection • Person Down Detection • Hands up detection • Handrail holding detection • People counter • Close-standing people detection • People masking	• Position of an object in the frame • Pose of an object in the frame
Equipment detection (PPE)	• Position of an object in the frame
PPE detection VL	
Barcode Detection	• Contents of a barcode in the frame

Metadata is used for the following system options to work:

Option	Required source of metadata
Standard detection sub-tools	• Object Tracker • Neurotracker • Object Tracker VL • Motion detection • General information about embedded detection tools
Forensic search MomentQuest	• Object Tracker • Neurotracker, • Motion detection • Face Detection TV • Face Detection VA • Face Detection VL • License Plate Recognition BRS • License Plate Recognition IV • License Plate Recognition RR • License Plate Recognition RR—Search In Archive • License Plate Recognition RR—Parking • License plate recognition VT • Pose Detection • Equipment detection (PPE) • PPE detection VL • General information about embedded detection tools
Face search	• Face Detection TV • Face Detection VA • Face Detection VL
Search by LPs	• Vehicle Recognition RR

Search by barcode	• Barcode Detection
TimeCompressor	• Object Tracker • Neurotracker • Motion detection • General information about embedded detection tools
Functions for tracking of moving objects	• Object Tracker • Neurotracker • Motion detection • General information about embedded detection tools
Object tracking	• Neurotracker • Object Tracker • Motion detection • Face Detection TV • Face Detection VA • Face Detection VL • License Plate Recognition BRS • License Plate Recognition IV • License Plate Recognition RR • License Plate Recognition RR—Search In Archive • License Plate Recognition RR—Parking • License plate recognition VT • Vehicle Recognition RR • Pose Detection • Equipment detection (PPE) • PPE detection VL • Barcode Detection • General information about embedded detection tools
Autozoom	• Neurotracker • Object Tracker • Motion detection • Face Detection TV • Face Detection VA • Face Detection VL • License Plate Recognition BRS • License Plate Recognition IV • License Plate Recognition RR • License Plate Recognition RR—Search In Archive • License Plate Recognition RR—Parking • License plate recognition VT • Vehicle Recognition RR • Pose Detection • Equipment detection (PPE) • PPE detection VL • Barcode Detection • General information about embedded detection tools

Neural analytics

General information on neural analytics

Hardware requirements for neural analytics operation

Neural analytics is a detection tool (see General information about detection tools and their sub-tools), the algorithms of which use neural networks.

Neural network is a mathematical model, as well as its software or hardware content, built on the principle of organization and functioning of biological neural networks (networks of neurons of a living organism). Within the context of the described software environment, neural networks are file models that have the .ann extension that you can use in the detection tools operation.

The table lists the detection tools that use neural networks in their operation:

Detection tool that uses neural network	Action of the neural network
Face Detection TV	Detection of faces
Face Detection VA	
Face Detection VL	
License Plate Recognition BRS	Detection of vehicle license plates
License Plate Recognition IV	
License Plate Recognition RR	
License Plate Recognition RR—Search In Archive	
License Plate Recognition RR—Parking	
License plate recognition VT	
Vehicle Recognition RR	Detection of vehicle attributes
Object Tracker with a neural network filter	Processes tracker results and filters out objects of no interest in a complex video image (foliage, glare, and so on)
Object Tracker VL	Detection of people in the frame
Stopped object detector	Detection of stopped objects in the frame
Abandoned Objects Detection VI	Detection of abandoned objects or objects that disappeared in the frame
Abandoned Objects Detection (Street) VI	
Neurotracker	Detection of the position of only the required objects in the frame
Neurocounter	Counts the number of objects in a specified area
Fire Detection	Detection of fire in the frame
Smoke Detection	Detection of smoke in the frame

Object Presence Detection	Neural network is trained to detect a specific object in the frame
Pose Detection and its sub-tools: • Sitting Person Detection • Person Down Detection • Hands up detection • Handrail holding detection • People counter • Close-standing people detection • People masking	Identifies each person's "skeleton" and detects poses that can represent a security threat
Equipment detection (PPE)	Detection of necessary equipment and personal protective equipment in the frame. Segmenting and classification neural networks are used for the operation of the Equipment detection (PPE) (see Functions of the Equipment detection (PPE))
PPE detection VL	
Person-Based Privacy Masking	Segmenting neural network breaks down the human body into zones
Privacy Masking	Detection and masking of moving and stationary objects
Water Level Detection	Increases the accuracy of water level detection in difficult conditions. For example, in scenes with clear water
Audio Analytics Detection IV	Recognizes different sounds: from a baby cry to the sound of a gunshot.
Crowd Estimation VA	Counts crowds of people in a specified area
Barcode Detection	Detection of a specific type of barcode in the frame

Hardware requirements for neural analytics operation

Hardware requirements

Hardware requirements for neural analytics (see General information on neural analytics) are the following:

1. Some NVIDIA SDK specific features allow neural analytics to work only on Windows Server 2019 and Windows 10.
2. Neural analytics can work on CPU, Nvidia GPU, VPU (Intel NCS, Intel HDDL).

   Attention!

   - To connect Intel NCS, insert the device into a USB port and make sure that it is recognized by Windows OS as a USB device with one of the following names: Movidius, Myriad X, or VSC Loopback Device. You can use Intel NCS on any computer that meets *Axxon One* hardware requirements (see Hardware requirements). We do not recommend using more than one Intel NCS device per Server.
   - You can use several Intel HDDL devices on one Server if they have the same revisions.
   - For Intel HDDL to work correctly with AMD processors, pre-install the OpenVINO™ toolkit version 2019.3.379 (see docs.openvino.ai).

3. If CPU or Intel GPU is used to run analytics, the following requirements must be met:

   a. Supported CPUs:
      i. 6th Generation Intel® Core™ processors and higher.

      Attention!

      When using a CPU lower than 6th Generation Intel® Core™ processors, the operation of the detection tools isn't guaranteed.

      ii. Intel® Xeon® v5 family and Intel® Xeon® v6 family.
      iii. Intel® Movidius™ Neural Compute Stick.
      iv. Intel® Neural Compute Stick 2.
      v. Intel® Vision Accelerator Design with Intel® Movidius™ VPUs.
   b. OpenVino must support the Intel CPU that you use (see software.intel.com).
   c. CPU must support the AVX2 or AVX512 instruction set (see ark.intel.com).
4. NVIDIA GeForce 1050 Ti grahics cardor higher. Requirements:
   a. At least 2 GB of memory;
   b. CUDA 11.1–11.4;
   c. Compute Capability 3.5–8.6.

   Attention!

   - CUDA is compatible with generations of computers with the following architectures: Kepler (partially), Maxwell, Pascal, Volta, Turing, Ampere (partially) (see CUDA).
   - You can check Compute Capability GPU version on the manufacturer's website.
   - If you use NVIDIA graphics cards, make sure to download the latest drivers from the manufacturer's website.

When you use a graphics card, a single neural network requires 500 MB of video memory, except for the neural network for Face Detection (see Hardware requirements for the Face Detection TV and its sub-tools) and License Plate Recognition RR (see Hardware requirements for License Plate Recognition RR and Vehicle Recognition RR). For example: a neural fire detection tool and a neural smoke detection tool, both with unlimited number of channels, require a 1 GB graphics card or higher. You can use multiple graphics cards in your system.

Attention!

For the correct operation of each detection tool, video image must meet a specified set of requirements. The requirements for each detection tool are listed in the corresponding sections (see Configuring detection tools).

Data collection requirements for neural network training

Description	To train neural networks, you must collect and submit to AxxonSoft videos and images from your actual cameras taken in the same resolution and in the same conditions as in your future application. For example, if you need your neural network to work outdoors, videos must contain all weather conditions (sun, rain, snow, fog, and so on) in different times of day (morning, afternoon, evening, night). If the collection requirements for the data submitted for training the neural network model are met, and if you operate the neural network in the conditions that are as similar as possible to the conditions in which the data was collected, we guarantee the overall accuracy (training in operating conditions) of neural network analytics from 90% to 97% and the percentage of false positives of 5-7%. For standard neural networks (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%. The standard neural networks are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. The requirements can be changed or added to at any time

General requirements for collected data	• When collecting data, specific requirements for object images, scene, angle, lighting, and video stream must be met for those detection tools that you plan to use (see Configuring detection tools).
	• If it is required to train neural network in different conditions of time of day, lighting, angle, object types, or weather, you must collect video data in equal proportions for each condition, that is, it must be balanced.
	
	Example. It is necessary to detect a person in the surveillance area at night and during the day.
	
	• **Data collected correctly**:
	  ○ four videos of the surveillance area, each five minutes long are submitted for training;
	  ○ the object of interest appears in the frame in each video;
	  ○ two videos were recorded in night conditions, two—in daytime conditions.
	• **Data collected incorrectly**:
	  ○ three videos of the surveillance area, each five minutes long are submitted for training;
	  ○ the object of interest appears in the frame in each video;
	  ○ two fragments were recorded in night conditions, one—in daytime conditions

Additional requirements for collected data for each neural analytics tool

Detection tool	Requirements
Neurofilter	At least 1000 frames containing different objects of interest in the given scene conditions, and the same number of frames containing no objects (noise frames)
Neurotracker	3–5 minutes of videos containing objects of interest in the given scene conditions. The more the number and variability of the situations in the scene, the better
Stopped object detector	
Pose Detection	10 seconds of video of a scene with no persons. At least 100 different persons in the given scene conditions. **Attention!** Different conditions mean, among others, different positions of a person in a scene (bending, different positions of body parts, and so on)
Equipment detection (PPE)	A list of all reference equipment with examples must be collected from the object and coordinated with the analytics manufacturer (see Example of providing a list of valid equipment at the facility for the Equipment detection (PPE)). 3-5 minutes of videos with personnel in the given scene conditions. Personnel must move and change position in the collected videos, as well as remove and put on equipment at intervals of 30 seconds. Since the equipment detection tools are designed for artificial constant lighting, videos in other lighting conditions aren't required
PPE detection VL	
Fire Detection	At least 1000 frames containing different objects of interest in the given scene conditions, and the same number of frames containing no objects (noise frames)
Smoke Detection	
Object Presence Detection	At least 1000 frames containing different objects of interest in the given scene conditions, and the same number of frames containing no objects (noise frames)

Optimizing the operation of neural analytics on GPU in Windows OS

On the page:

- General information
- Optimizing the operation of neural analytics on GPU
- Creating GPU neural network caches using parameters

General information

It can take several minutes to launch neural analytics algorithms on NVIDIA GPU after Server restart. At this time, the neural models are optimized for the current GPU type.

You can use the caching function to ensure that this operation is performed only once. Caching saves the optimization results on the hard drive and uses it for the subsequent analytics runs.

Starting with *DetectorPack* 3.9, a utility was added to the Neuro Pack add-ons (see Installing DetectorPack add-ons), which allows you to create GPU neural network caches without using *Axxon One*. The presence of the cache speeds up the initialization and optimizes video memory consumption.

Optimizing the operation of neural analytics on GPU

> ⚠ **Attention!**
>
> This function works in beta mode for all detection tools that use neural analytics (see General information on neural analytics), except Face Detection TV and Face Detection VA. To optimize the operation of Face Detection TV and Face Detection VA using the GPU_CACHE_DIR system variable, you need to perform additional actions (see Optimizing the operation of the Face Detection VA on GPU, Optimizing the operation of the Face Detection TV on GPU).

To optimize the operation of the neural analytics on GPU, do the following:

1. Stop the Server (see Shutting down a Server).

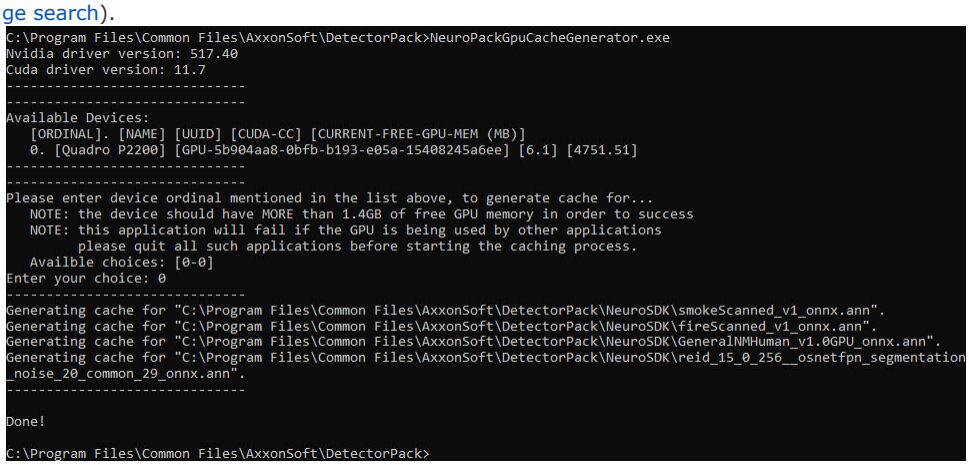
   > ⚠ **Attention!**
   >
   > If the system has the software running on GPU, it is necessary to stop its operation.

2. Create the GPU_CACHE_DIR system variable (see Appendix 10. Creating system variable) by specifying in the **Variable value** field the path to the cache location with an arbitrary folder name. For example, D:\GPU_cache. The specified directory will store the cache for all used detection tools and neural networks.
   The cache size depends on the number of neural networks used and their type,. The minimum size is 70 MB.
3. Run the command prompt as administrator.
4. To call the utility, in the command prompt, enter C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe.
5. Press **Enter**.
6. Specify the ID of the required GPU (see Selecting Nvidia GPU when configuring detection tools).
7. Press **Enter**.

Optimizing the operation of the neural analytics on GPU is complete. The utility will create the caches of four neural networks included in the Neuro Pack add-ons:

- GeneralNMHuman_v1.0GPU_onnx.ann—human;
- smokeScanned_v1_onnx.ann—smoke detection;
- fireScanned_v1_onnx.ann—fire detection;

- reid_15_0_256__osnetfpn_segmentation_noise_20_common_29_onnx.ann—search for the similar in the neurotracker (see Image search).



Attention!

The cache must be recreated in the following cases:

- if you update the Neuro Pack add-ons (see Installing DetectorPack add-ons),
- if you change the Nvidia GPU model,
- if you update the Nvidia GPU drivers.

Creating GPU neural network caches using parameters

1. **-p** is a parameter to create a cache for a particular neural network.
   Command example:

   ```
   C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe -p "<System
   disk>\<Neural network location directory>\Neural_network_name.ann"
   ```

   To create a cache for multiple neural networks, list the paths to the selected neural networks, separated by a space.
   Command example:

   ```
   C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe -p "<System
   disk>\<Neural network location directory>\Neural_network_name.ann" "C:\Program Files\Common
   Files\AxxonSoft\DetectorPack\NeuroSDK\WaterLevelRuleNet_origin_onnx.ann"
   ```

2. **-v** is a parameter to output the procedure log to the console during cache generation.
   Command example to automatically create caches of four neural networks included in the Neuro Pack add-ons with log output:

   ```
   C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe -v
   ```

   Command example:

   ```
   C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe -p "<System
   disk>\<Neural network location directory>\Neural_network_name.ann" -v
   ```

3. **--int8=1** is a parameter to create cache for those neural networks for which quantization is available. Neural networks for which the quantization mode is available are included in the Neuro Pack add-ons together with the *.info file. By default, the **--int8=0** parameter is disabled.
   Command example:

   ```
   C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe --int8=1
   ```

The neural networks for which the quantization mode is available (see Neurotracker, Stopped object detector, Neurocounter):

- GeneralNMCar_v1.0GPU_onnx.ann—Vehicle.
- GeneralNMHuman_v1.0GPU_onnx.ann—Person.
- GeneralNMHumanTopView_v0.8GPU_onnx.ann—Person (top-down view).

Starting with *DetectorPack* 3.11, the following neural networks were added:

- GeneralNMHumanAndVehicle_Nano_v1.0_GPU_onnx.ann—Person and vehicle (Nano).
- GeneralNMHumanAndVehicle_Medium_v1.0_GPU_onnx.ann—Person and vehicle (Medium).
- GeneralNMHumanAndVehicle_Large_v1.0_GPU_onnx.ann—Person and vehicle (Large).

Starting with *DetectorPack* 3.12, the following neural networks were added:

- GeneralNMHumanAndVehicle_Nano_v1.0_GPU_onnx.ann—Person (top-down view Nano).
- GeneralNMHumanAndVehicle_Medium_v1.0_GPU_onnx.ann—Person (top-down view Medium).
- GeneralNMHumanAndVehicle_Large_v1.0_GPU_onnx.ann—Person (top-down view Large).

Optimizing the operation of neural analytics on GPU in Linux OS

On the page:

- General information
- Optimizing the operation of neural analytics on GPU
- Creating GPU neural network caches using parameters

General information

It can take several minutes to launch neural analytics algorithms on NVIDIA GPU after Server restart. Meanwhile, the neural models are optimized for the current GPU type.

You can use the caching function to ensure that this operation is performed only once. Caching saves the optimization results on the hard drive and uses it for the subsequent analytics runs.

Starting with *DetectorPack* 3.11, a utility was added to the Neuro Pack add-ons (see Installing DetectorPack add-ons), which allows you to create GPU neural network caches without using *Axxon One*. The presence of the cache speeds up the initialization and optimizes video memory consumption.

Optimizing the operation of neural analytics on GPU

To optimize the operation of the neural analytics on GPU, do the following:

1. Stop the Server (see Starting and stopping the Axxon One Server in Linux OS).

   > **Attention!**
   >
   > If the system has the software running on GPU, it is necessary to stop its operation.

2. Login as **root** superuser:
   a. In the command prompt, run the command:

   ```
   sudo -i
   ```

   b. Enter the password for the **root** superuser.
3. Create a folder with a custom name to store the cache. For example:

   ```
   mkdir /opt/AxxonSoft/AxxonOne/gpucache
   ```

4. Change folder permissions:

   ```
   chmod -R 777 /opt/AxxonSoft/AxxonOne/gpucache
   ```

5. Create the **GPU_CACHE** system variable:
   a. Go to the **/opt/AxxonSoft/AxxonOne/** folder:

   ```
   cd /opt/AxxonSoft/AxxonOne
   ```

   b. Open the **instance.conf** file for editing:

   ```
   nano instance.conf
   ```

c. Add the following line to the file:

```
export GPU_CACHE_DIR="/opt/AxxonSoft/AxxonOne/gpucache"
```

d. Save the file using the **Ctrl+O** keyboard shortcut.
e. Exit file editing mode using the **Ctrl+X** keyboard shortcut.
f. Run the following command in the terminal:

```
export GPU_CACHE_DIR="/opt/AxxonSoft/AxxonOne/gpucache"
```

6. Go to the **/opt/AxxonSoft/DetectorPack/** folder:

```
cd /opt/AxxonSoft/DetectorPack
```

7. Run the following command:

```
./NeuroPackGpuCacheGenerator
```

> ⚠ **Attention!**
>
> If more than one NVIDIA GPU is available, you will be able to select one. To do this, specify a number from 0 to 3 which corresponds to the required device in the list.

Optimizing the operation of the neural analytics on GPU is complete. The utility will create the caches of four neural networks included in the Neuro Pack add-ons:

- GeneralNMHuman_v1.0GPU_onnx.ann—person;
- smokeScanned_v1_onnx.ann—smoke detection;
- fireScanned_v1_onnx.ann—fire detection;
- reid_15_0_256__osnetfpn_segmentation_noise_20_common_29_onnx.ann—search for the similar in the neurotracker (see Image search).

Creating GPU neural network caches using parameters

1. **-p** is a parameter to create a cache for a particular neural network.
Command example:

```
./NeuroPackGpuCacheGenerator -p /opt/AxxonSoft/DetectorPack/NeuroSDK/GeneralNMHumanAndVehicle_Nano_v1.
0_GPU_onnx.ann
```

2. **-v** is a parameter to output the procedure log to the console during cache generation.
Command example to automatically create caches of four neural networks included in the Neuro Pack add-ons with log output:

```
./NeuroPackGpuCacheGenerator -v
```

3. **--int8=1** is a parameter to create a quantized version of the cache for those neural networks for which quantization is available. By default, the **--int8=0** parameter is disabled.
Command example:

```
./NeuroPackGpuCacheGenerator -p /opt/AxxonSoft/DetectorPack/NeuroSDK/GeneralNMHumanAndVehicle_Nano_v1.
0_GPU_onnx.ann --int8=1
```

> ⚠ **Attention!**
>
> The neural networks for which the quantization mode is available are included in the Neuro Pack add-ons together with the *.info file.

The neural networks for which the quantization mode is available (see Neurotracker, Stopped object detector, Neurocounter):

- GeneralNMCar_v1.0GPU_onnx.ann—Vehicle.
- GeneralNMHuman_v1.0GPU_onnx.ann—Person.
- GeneralNMHumanTopView_v0.8GPU_onnx.ann—Person (top-down view).

Starting with *DetectorPack* 3.11, the following neural networks were added:

- GeneralNMHumanAndVehicle_Nano_v1.0_GPU_onnx.ann—Person and vehicle (Nano).
- GeneralNMHumanAndVehicle_Medium_v1.0_GPU_onnx.ann—Person and vehicle (Medium).
- GeneralNMHumanAndVehicle_Large_v1.0_GPU_onnx.ann—Person and vehicle (Large).

Starting with *DetectorPack* 3.12, the following neural networks were added:

- GeneralNMHumanAndVehicle_Nano_v1.0_GPU_onnx.ann—Person (top-down view Nano).
- GeneralNMHumanAndVehicle_Medium_v1.0_GPU_onnx.ann—Person (top-down view Medium).
- GeneralNMHumanAndVehicle_Large_v1.0_GPU_onnx.ann—Person (top-down view Large).

General settings of the detection tools

Selecting Nvidia GPU when configuring detection tools

When you configure detection tools, select Nvidia GPUs one by one.

Attention!

- If only one Nvidia GPU is installed, select **Nvidia GPU 0**.
- If several Nvidia GPUs are installed, select the graphics card on which you want to perform the detection process.
- If you select an uninstalled Nvidia GPU, detection isn't performed.

The table lists the parameter names and detection tools, configuring which you can select the required Nvidia GPU:

Parameter	Detection tool
Mode	Configuring the PPE detection VL Configuring the Neurocounter Configuring License Plate Recognition RR Configuring License Plate Recognition RR—Parking Configuring License Plate Recognition RR—Search In Archive Configuring the Smoke Detection Configuring the Fire Detection Configuring License Plate Recognition VT Configuring the Face Detection VA Configuring the Face Detection TV Configuring the Face Detection VL Configuring the Person-Based Privacy Masking Configuring the Object Presence Detection Configuring the Stopped object detector Configuring the Abandoned Objects Detection VI Configuring the Abandoned Objects Detection (Street) VI
Neural network mode	Configuring the Water Level Detection Configuring the Privacy Masking Configuring the Equipment detection (PPE)
Neurofilter mode	Configuring the Neurotracker
Neurotracker mode	
Detection mode	Configuring Vehicle Recognition RR
Moving object filter mode	Configuring the Object Tracker
Abandoned object filter mode	
Processing unit	Configuring License Plate Recognition IV

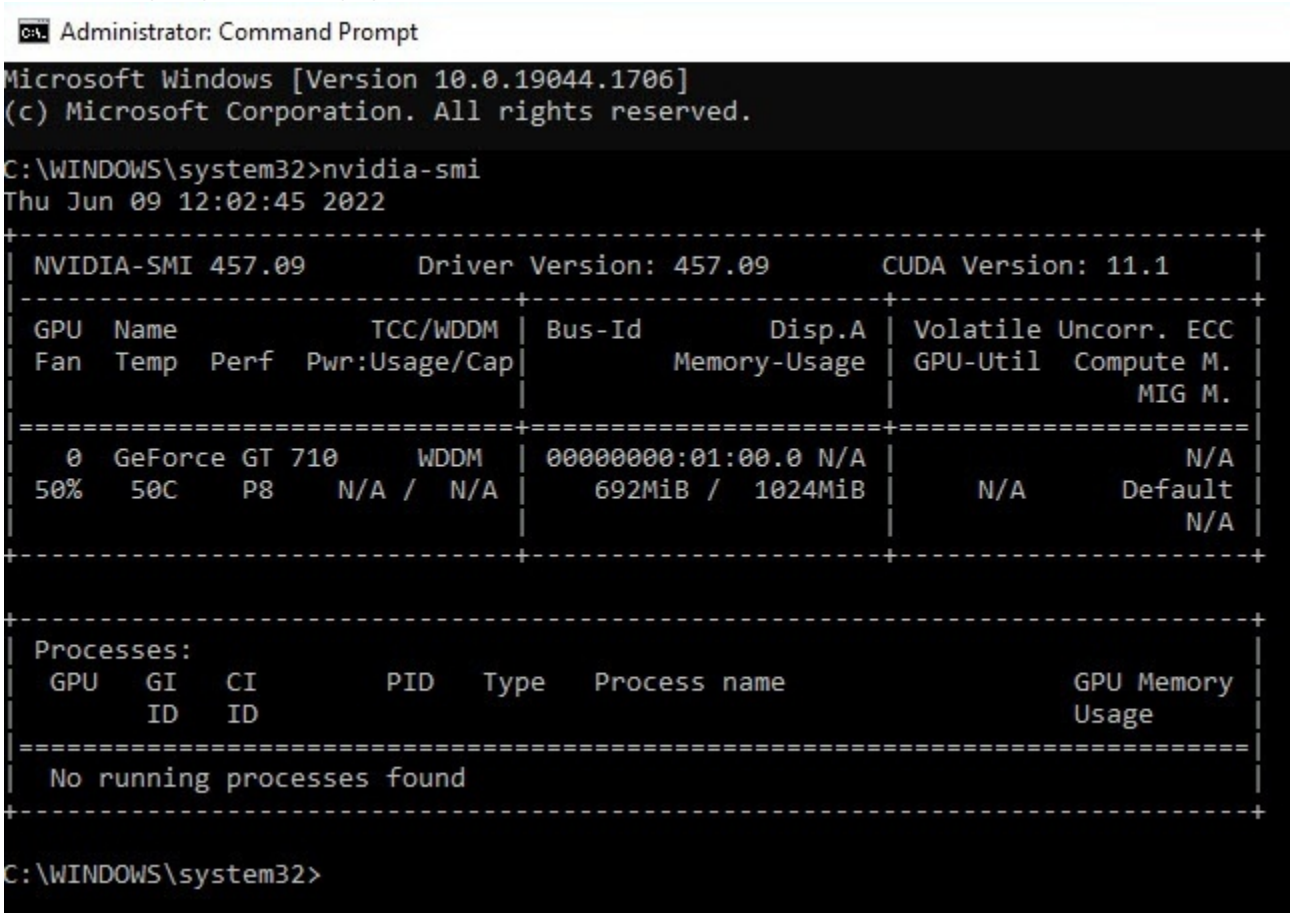
You can change the order of the Nvidia GPU display using the **CUDA_DEVICE_ORDER** system variable (see Appendix 9. Creating system variable) by specifying the required value:

1. The **FASTEST_FIRST** value numbers the GPUs from the most powerful card to the less powerful ones, that is, **Nvidia GPU 0** is the most powerful card.
2. The **PCI_BUS_ID** value numbers the GPUs according to the physical location of the cards in the PCI-E slots on the motherboard, that is, **Nvidia GPU 0** is the card in the highest slot.

To find out information about the availability, quantity and numbering of Nvidia GPUs, do the following:

1. Run the command prompt as administrator.
2. In the command prompt, enter the Nvidia-smi query.
3. Press **Enter**.

The command prompt window displays the information about the installed Nvidia GPUs.



Configuring the minimum and maximum size of detected objects

On the page:

- General information
- Specifying the size of objects numerically
- Specifying the size of objects visually

General information

You can specify the minimum and maximum size of detected objects both numerically and visually. Detection tool won't generate an event for larger or smaller objects.

Specifying the size of objects numerically

To specify the size of objects numerically, do the following:

1. Select the **Object Tracker**.
2. In the settings of the **Object Tracker** (see Configuring the Object Tracker), specify the values of the parameters:

Parameter	Value	Description
Max. object height	**100**	Specify the maximum height and width of the detected object as a percentage of the height/width of the frame. The values must be in the range [0.05, 100]
Max. object width		
Min. object height	**2**	Specify the minimum height and width of the detected object as a percentage of the height/width of the frame. The values must be in the range [0.05, 100]
Min. object width		

> **Attention!**
>
> If you enable the **Object calibration** parameter in the settings of the **Object Tracker** (see Configuring perspective), you must specify the minimum and maximum size of objects in **decimeters** and not as a percentage of the size of the frame side.

3. Click the **Apply** button. To cancel the changes, click the **Cancel** button.

Specifying the size of objects visually

To specify the size of objects visually, do the following:

1. Select the **Object Tracker**.

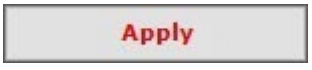
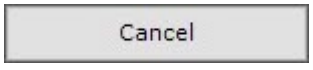
2. Click the **Min**  button and specify the minimum size of a detected object. To do this, move the anchor points of the display area.



3. Click the **Max**  button and specify the maximum size of a detected object.



> **Note**
>
> - By default, the maximum size is equal to the frame size, so that anchor points are located in the corners of the frame.
> - For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
> - If you click the **Min**  and **Max**  buttons again, the display area hides.

4. Click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuration of the minimum and maximum size of detected objects is complete. The size of objects are specified for all its detection sub-tools.

Configuring a skip area

By default, the entire frame is analyzed. If you want to exclude difficult areas in the camera FOV (foliage, water, and so on) from the analysis, you must specify one or more areas where detection and metadata generation won't be performed.

To do this, do the following:

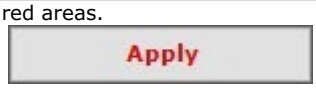
1. Select a detection tool and click the  button.
2. Set the anchor points of the closed area, within which the detection won't be performed.

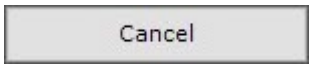


Note

- When you set anchor points, they are connected by a two-color dashed line outlining the border of the area.
- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- Once the area is closed, the  buttons are available on its borders between the anchor points. When you click them, a new anchor point is added, allowing you to specify the most precise areas possible.
- To delete a selected area, click the  button.

Action	Result
Left-click or right-click in the **Surveillance window**	Creates a new anchor point of the area
Right-click a created anchor point	Deletes an anchor point of the area
Hover the mouse cursor over an anchor point and, holding down the left mouse button, move the mouse	Moves an anchor point of the area

3. Specify all required areas.
4. Click the **Apply** 

button. To cancel the changes, click the **Cancel** 

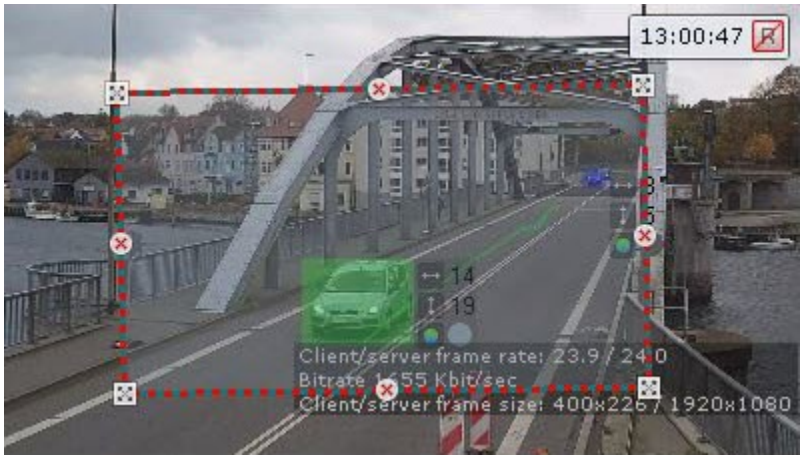
button.

Configuration of a skip area is complete. Skip areas will be relevant for all sub-tools created on the basis of the parent detection tool.

Configuring a detection area

For each standard detection sub-tool (except for Line Crossing, see Standard detection sub-tools), you can specify an area where detection and metadata generation will be performed.

After you create a detection tool, a rectangular detection area is displayed in bright color on the frame:



You can configure a detection area similar to a skip area (see Configuring a skip area).

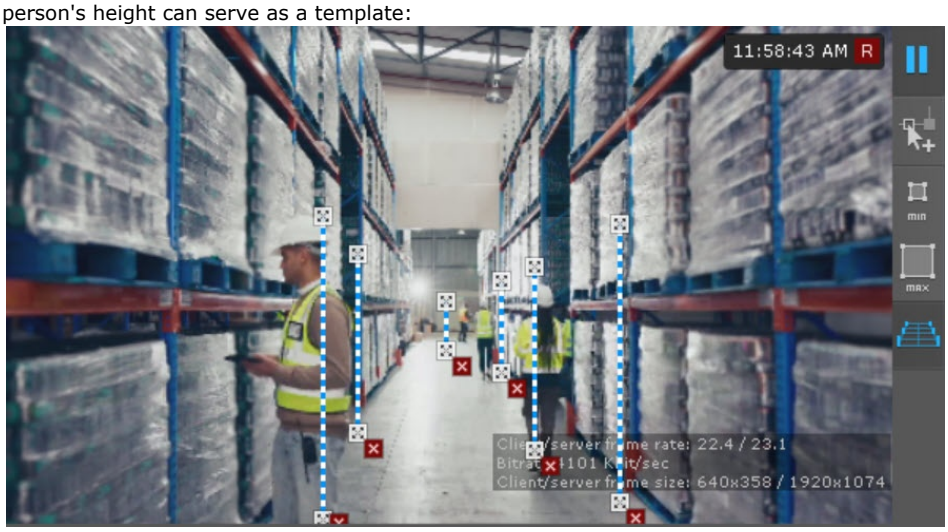
Configuring perspective

Perspective configuration enhances the performance of the detection tools and allows you to estimate the real size of objects based on a simplified calibration system.

> **Attention!**
>
> Correct operation of object calibration isn't possible if you use a camera with strong perspective distortion (for example, fisheye).

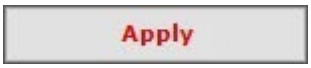
To configure perspective, do the following:

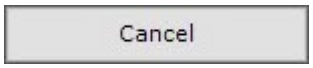
1. Select the **Object Tracker**.
2. In the settings of the **Object Tracker** (see Configuring the Object Tracker):
   a. Select the **Yes** value for the **Object calibration** parameter.
   b. In the **Leveling rod height** parameter, enter the height of the calibration object on the video image in **decimeters**.
3. In the preview window, click the  button.
4. Visually specify the size of the same object in different parts of the frame:
   - To create a leveling rod, add two anchor points by left-clicking the video image.
   - Set at least three leveling rods. The lower anchor points of any three rods must not be located on the same line (horizontal, vertical, slanting, and so on).
   - You can resize the rod by stretching its anchor points  , and move it on screen using drag-and-drop.
   - Rods must be exactly the same size as the object, which serves as a template for a leveling rod. For example, a person's height can serve as a template:



> **Attention!**
>
> When you configure leveling rods, the following requirements must be met:
>
> a. rods must be evenly distributed throughout the frame: the larger area they cover, the more accurate the calibration;
> b. rods that are equally distant from the camera lens must be the same size;
> c. all bases of the rods must be on the same plane (for example, floor);
> d. in complex scenes, we recommend adding more than three rods, but no more than 10-15 rods per frame.

> **Note**
>
> - For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
> - To delete a rod, click the  button.

5. Click the **Apply** button 

. To cancel the changes, click the **Cancel** 

button.

Perspective is now configured. These settings will apply for all detection sub-tools of the **Object Tracker**.

Configuring the scanning mode

On the page:

- General information
- Configuring the scanning mode
- Recommendations for configuring the scanning mode
- Example of configuring the scanning mode

General information

The scanning mode in *Axxon One* can improve detection of small objects or objects in areas far away from the camera. For example, when the camera is placed at a long distance and objects (such as people, smoke, fire) are small in the frame, scanning mode can improve detection.

In the scanning mode, the frame is divided into an arbitrary number of scanning windows for detection accuracy.

Scanning windows are parts of the frame that are analyzed separately and all together at the same time. Scanning windows allow the detection tool to receive more events, which improves the accuracy of detecting distant or small objects that might otherwise be missed.

> **Attention!**
>
> The scanning mode doesn't provide absolute detection accuracy, regardless of the number of windows.

The scanning mode is available for:

1. Fire Detection.
2. Smoke Detection.
3. Pose Detection.
4. Neurocounter.
5. Neurotracker.

Configuring the scanning mode

You can configure the scanning mode using the parameters of the corresponding detection tool. The list of required parameters and their values are presented in the table below.

Parameter	Value	Description
Scanning window	Yes	Select the **Yes** value to enable the scanning mode
	No	
Scanning window height	Numeric value (in pixels)	The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels
Scanning window width		
Scanning window step height		The scanning step determines the relative offset of the windows. If the step is equal to the height and width of the scanning window respectively, the segments will line up one after another. Reducing the height or width of the scanning step will increase the number of windows due to their overlapping each other with an offset. This will increase the detection accuracy, but will also increase the CPU load **Attention!** The height and width of the scanning step must not be greater than the height and width of the scanning window—the detection tool will not operate with such settings.

Scanning window step width		

Recommendations for configuring the scanning mode

1. Set the same values for the window height and scanning step, as well as the window width and scanning step.
2. Set the optimal number of scanning windows—from four to eight. The number of windows will depend on specific purposes, quality of the original frame, capabilities of devices. If the original frame is of low quality or small size, a large number of windows won't increase the detection accuracy, but can lead to false alarms or no detection. You must select the number of scanning windows experimentally.
3. If you didn't get the detection tool responses at the same values of window and step, you must experimentally reduce the scanning steps relative to the height or width.

Attention!

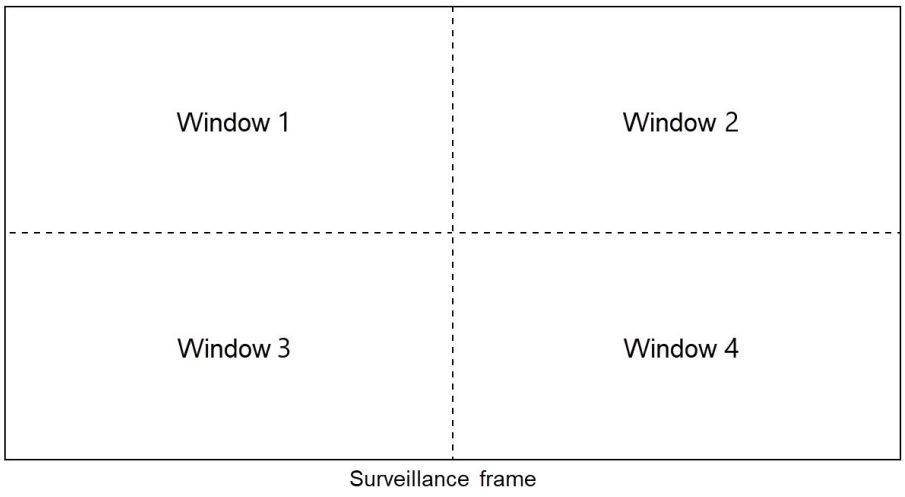
Increasing the number of windows increases the load on the device.

Example of configuring the scanning mode

It is necessary to configure the scanning mode for the smoke detection to detect smoke in the distance. If the actual frame size is 1920×1080 pixels, set the following values in the detection tool settings to divide the frame into four equal windows:

1. **Scanning window**—Yes.
2. **Scanning window height**—540.
3. **Scanning window width**—960.
4. **Scanning window step height**—540.
5. **Scanning window step width**—960.

As a result, the frame will be conditionally divided into four equal windows that will be analyzed separately and all together at the same time. If smoke is detected in any of these windows, the detection tool can trigger.



Displaying the number of detected objects

In the **Surveillance window**, on the layout, you can display the detection tool icon and the number of objects in the detection area (see Configuring a detection area). The number of detected objects can be displayed for the following detecttion tools:

1. Neurocounter.
2. People counter.
3. Crowd Estimation VA.

Configure the display of the number of detected objects as follows:

1. Go to layout editing mode with the selected camera (see Switching to layout editing mode).
2. Move the detection tool icon to an arbitrary location in the cell.
3. If necessary, adjust the font, click the T button.
4. To add text, click the gray area.
5. In an arbitrary place in the gray area, specify a template for displaying the number of objects in curly brackets:
   - {0}—integer;
   - {0.0}—fractional number with 1 digit after the point;

   > **Note**
   >
   > The template expands to {0.0000} to display the number with 4 digits after the point. If user text contains more digits after the point than received from the detection tool, the missing low-order digits are filled with zeros. If a template for displaying the number of objects is not added, then the number can be displayed as an integer or a fraction (with an accuracy of no more than 4 digits after the point).

6. If necessary, scale up/down the text and the sensor icon, click the button.
7. Save the layout (see Exiting Layout Editing mode).

After saving the layout, the detection tool icon and the number of objects will be displayed in the **Surveillance window**.

An example of configured display of the number of objects in the detection area based on the **People counter**:




2.Camera
Amount of people: {0}

Standard detection sub-tools

General information on the standard detection sub-tools

Hardware requirements for neural analytics operation

General information on metadata

The standard detection sub-tools generate events at certain actions of objects in the camera FOV:

Name of the detection sub-tool	Description
Line Crossing	Detection tool generates an event when an object track crosses a virtual line
Loitering In Area	Detection tool generates an event when an object stays in a specified area for a long period of time. The event stops when an object leaves the area or disappears inside the area
Stop In Area	Detection tool generates an event when an object stops moving in a specified area. The event stops when an object leaves the area or disappears inside the area
Abandoned Object	Detection tool generates an event when there is an abandoned object in a specified area
Motion In Area	Detection tool generates an event when an object starts moving in a specified area. The event stops when an object stops in the area, leaves the area, or disappears inside the area
Entrance In Area	Detection tool generates an event when an object enters a specified area
Exit From Area	Detection tool generates an event when an object leaves a specified area
Multiple Objects	Detection tool generates an event when the number of objects in a specified area exceeds the set value
Move From Area To Area	Detection tool generates an event when an object leaves one area and enters another area of the frame

To operate the standard detection sub-tools, you can use the metadata from the sources:

Category	Detection tool
Category: Trackers	• Motion detection • Neurotracker • Object Tracker • Object Tracker VL
Category: Face (reduced set of detection sub-tools: Line Crossing, Loitering In Area, Entrance In Area)	• Face Detection VA • Face Detection TV • Face Detection VL
Category: Vehicle	• License Plate Recognition BRS • License Plate Recognition IV • License Plate Recognition RR • License Plate Recognition RR—Search In Archive • License Plate Recognition RR—Parking • License plate recognition VT • Vehicle Recognition RR
Category: Poses	• Pose Detection

Category: Production Safety	• Equipment detection (PPE) • PPE detection VL
Category: Retail	• Barcode Detection

The standard detection sub-tools can operate on the basis of all of the above objects.

> **Note**
>
> You can track up to 25 objects at the same time.



Camera requirements for the standard detection sub-tools

For the standard detection tools to operate correctly, it is necessary to meet the camera requirements of the detection tools for which they are created.

- Video stream and scene requirements for the Motion detection and its sub-tools
- Video stream and scene requirements for the Neurotracker and its sub-tools
- Video requirements for object tracker-based scene analytics detection tools
- Video stream and scene requirements for the Object Tracker VL and its sub-tools
- Video stream and scene requirements for the Face Detection VA and its sub-tools
- Video stream and scene requirements for the Face Detection VL and its sub-tools
- Camera requirements for License Plate Recognition BRS and its sub-tools
- Camera requirements for License Plate Recognition IV and its sub-tools
- Camera requirements for License Plate Recognition RR, Vehicle Recognition RR and their sub-tools
- Camera requirements for License plate recognition (VT)
- Video stream and scene requirements for the Pose Detection and its sub-tools
- Video stream and scene requirements for the Equipment detection (PPE) and its sub-tools
- Video stream and scene requirements for the PPE detection VL and its sub-tools
- Video stream and scene requirements for the Barcode Detection and its sub-tools

Configuring Line Crossing

On the page:

- Configuring detection tool
- Configuring virtual line

Configuring detection tool

To configure the **Line Crossing**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create... Line Crossing**.

By default, the detection tool is enabled and set to generate events when an object crosses a virtual line.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Line Crossing**	Enter the detection tool name or leave the default name
Type	**Line Crossing**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Line Crossing**.

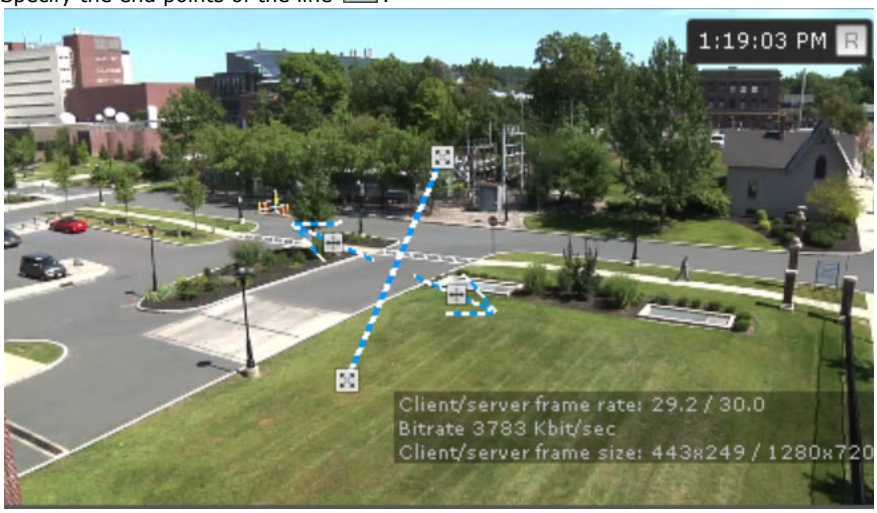
Maximum object speed	**500**	Specify the maximum object speed per second for the detection tool to trigger. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Line Crossing**.
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Line Crossing**.
Minimum object speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Line Crossing**.
Object class	**All classes** **Vehicle** **Person**	Select the object class that must generate an event. The default value is **All classes** **Note** • When you create the **Line Crossing** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Line Crossing** detection tool below the Category: Face and Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

Configuring virtual line

To configure a virtual line, do the following:

1. In the preview window:
   a. Specify the end points of the line :



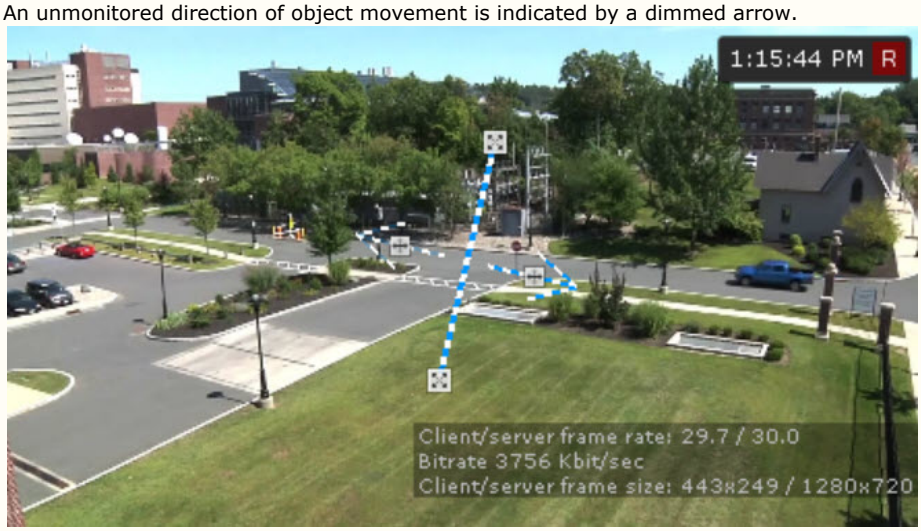
> **Note**
>
> - The end points are connected by a two-color dashed line. The directions of object movement through the line are indicated by dotted arrows.
> - For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
> - To hide the virtual line, click the button. To cancel the action, click this button again.

Action	Result
Hover the cursor over the end point and, holding down the left mouse button, move the mouse	Moving the end point of a line
Hover the cursor over the line and, holding down the left mouse button, move the mouse	Moving the line

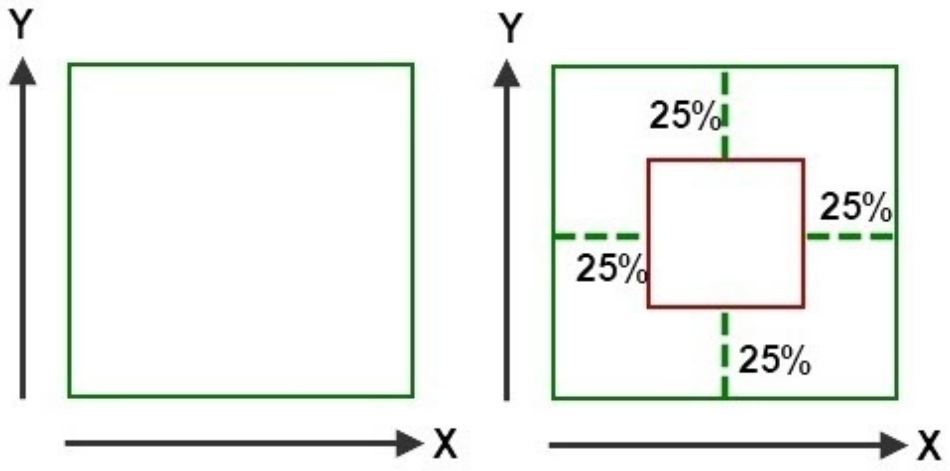
   b. By default, both directions of object movement through the line are detected. To stop the detection in the required direction, click the button corresponding to this direction.

Attention!

- You must select at least one direction for detection.
- An unmonitored direction of object movement is indicated by a dimmed arrow.

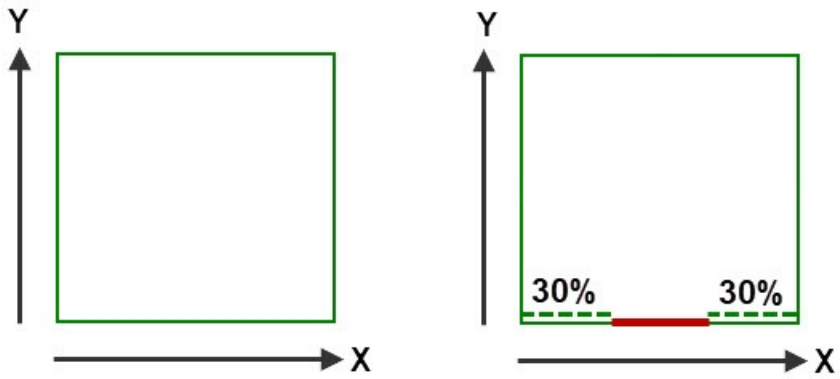


2. In the frame, there can be situations when one and the same object frequently moves near the virtual line, which can cause generation of excessive events. In this situation we recommend specifying the area of the object track that completely crosses the line to receive an event from the detection tool. For this, in the detection tool parameters, specify the X-axis and Y-axis offsets as a percentage of the track area width and height.
   Configuration of the X-axis and Y-axis offsets depends on the **Camera position** parameter of a detection tool below which the **Line Crossing** detection tool is created. For example, **Neurotracker** has the **Camera position** parameter (see Configuring the Neurotracker).
   a. The **Ceiling** camera position:
      For example, the green rectangle is the object track. If the X-axis and Y-axis offsets are set to 25%, an event will be generated only if the red rectangle completely crosses the line.



   b. The **Wall** camera position:
      For example, the green rectangle is the object track. If the X-axis offset is set to 30%, an event will be generated only

if the red segment completely crosses the line.



3. Click the **Apply** button. Click the **Cancel** button to cancel the changes.

Configuring Loitering In Area

To configure the **Loitering In Area**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create... Loitering In Area**.

By default, the detection tool is enabled and set to generate events when an object leaves the detection area after spending there some time.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Loitering In Area**	Enter the detection tool name or leave the default name
Event hold time (sec)	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This is the time period during which the detection tool waits for the next objects after the first object in the group is detected. If the specified number of objects (specified in the **Number of alarm objects** parameter) are detected within this time period, the detection tool generates an event. If no additional objects are detected within the specified time period, the detection tool doesn't generate an event. Specify the time period in seconds when events will be held when responding to a group of objects. The value must be in the range [0, 86400]
Type	**Loitering In Area**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Event duration to trigger detection (sec)	**30**	Specify the time of the object stay in the detection area in seconds. The value must be in the range [0, 86400]
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Loitering In Area**.

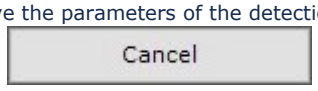
Maximum object speed	**500**	Specify the maximum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Loitering In Area**.
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Loitering In Area**.
Minimum object speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Loitering In Area**.
Number of alarm objects	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This number determines the minimum number of objects that are considered a group and can generate an event. Specify the number of objects that can cause the detection tool to generate an event. The value must be in the range [1, 100]
Object class	**All classes**	Select the object class that must generate an event. The default value is **All classes**

	Vehicle **Person**	**Note** • When you create the **Loitering In Area** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Loitering In Area** detection tool below the Category: Face and Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.
Time detection mode	**Specified time**	The detection tool generates an event after the object leaves the area after spending there the time specified in the **Event duration to trigger detection (sec)** parameter (default value)
	Longer than specified time	The detection tool generates an event after the object leaves the area after spending there more time than specified in the **Event duration to trigger detection (sec)** parameter. If an event has already been generated and the track is still in the area after an event, the event won't be generated again until the track leaves the area and enters it again
	Shorter than specified time	The detection tool generates an event after the object leaves the area after spending there less time than specified in the **Event duration to trigger detection (sec)** parameter
Trigger on group of objects	**Yes** **No**	The parameter is disabled by default. If you want the detection tool to generate an event only for a group of objects, select the **Yes** value **Note** • The group of objects that must cause the detection tool to generate an event is specified in the **Object class** parameter. • The number of objects that is considered a group is specified in the **Number of alarm objects** parameter. • Waiting time for the next objects after the first object from the group is detected is specified in the **Event hold time (sec)** parameter. For example, you select the **Person** object class, the **Number of alarm objects** is **3**, the **Event hold time (sec)** is **2** seconds, and the **Trigger on group of objects** parameter is enabled. If the detection tool detects the first person and detects the others within two seconds, these people are considered a group and the detection tool generates an event.

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring Stop In Area

To configure the **Stop In Area**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create... Stop In Area**.

By default, the detection tool is enabled and set to generate events when an object stops moving in the area and remains stationary for a specified time.

> **Note**
>
> Slight shaking of an object is allowed.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Stop In Area**	Enter the detection tool name or leave the default name
Event hold time (sec)	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This is the time period during which the detection tool waits for the next objects after the first object in the group is detected. If the specified number of objects (specified in the **Number of alarm objects** para meter) are detected within this time period, the detection tool generates an event. If no additional objects are detected within the specified time period, the detection tool doesn't generate an event. Specify the time period in seconds when events will be held when responding to a group of objects. The value must be in the range [0, 86400]
Type	**Stop In Area**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Stop In Area**.

Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Stop In Area**.
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Stop In Area**.
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Stop In Area**.
Number of alarm objects	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This number determines the minimum number of objects that are considered a group and can generate an event. Specify the number of objects that can cause the detection tool to generate an event. The value must be in the range [1, 100]
Object class	**All classes** **Vehicle** **Person**	Select the object class that must generate an event. The default value is **All classes** **Note** • When you create the **Stop In Area** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Stop In Area** detection tool below the Category: Face and Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.
Stop in area duration	**0**	Specify the time in seconds during which the object is stationary for the detection tool to generate an event. The value must be in the range [0, 3600] **Attention!** • The value of this parameter must be **less** than the value of the **Time of object in DB** parameter in the settings of the **Object Tracker** (see Configuring the Object Tracker). • If the detection tool uses the metadata from the Motion detection (see Configuring the Motion detection), the value of the **Stop in area duration** parameter must be **0**. Otherwise, the detection tool won't work.
Trigger on group of objects	**Yes**	The parameter is disabled by default. If you want the detection tool to generate an event only for a group of objects, select the **Yes** value

	No	**Note** • The group of objects that must cause the detection tool to generate an event is specified in the **Object class** parameter. • The number of objects that is considered a group is specified in the **Number of alarm objects** parameter. • Waiting time for the next objects after the first object from the group is detected is specified in the **Event hold time (sec)** parameter. For example, you select the **Person** object class, the **Number of alarm objects** is **3**, the **Event hold time (sec)** is **2** seconds, and the **Trigger on group of objects** parameter is enabled. If the detection tool detects the first person and detects the others within two seconds, these people are considered a group and the detection tool generates an event.

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring Motion In Area

To configure the **Motion In Area**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create... Motion In Area**.

By default, the detection tool is enabled and set to generate events when an object starts moving in the area.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

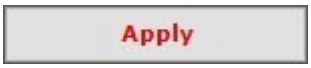
Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Motion In Area**	Enter the detection tool name or leave the default name
Type	**Motion In Area**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Motion In Area**.
Maximum object speed	**500**	Specify the maximum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Motion In Area**.

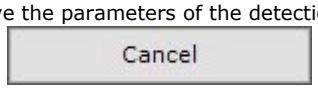
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Motion In Area**.
Minimum object speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Motion In Area**.
Number of alarm objects	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This number determines the minimum number of objects that are considered a group and can generate an event. Specify the number of objects that can cause the detection tool to generate an event. The value must be in the range [1, 100]
Object class	**All classes** **Vehicle** **Person**	Select the object class that must generate an event. The default value is **All classes** **Note** • When you create the **Motion In Area** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Motion In Area** detection tool below the Category: Face and Category : Vehicle detection tools, the **Object class** parameter must have the **All classes** value.
Trigger on group of objects	**Yes** **No**	The parameter is disabled by default. If you want the detection tool to generate an event only for a group of objects, select the **Yes** value **Note** • The group of objects that must cause the detection tool to generate an event is specified in the **Object class** parameter. • The number of objects that is considered a group is specified in the **Number of alarm objects** parameter.

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring Entrance In Area

To configure the **Entrance In Area**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create... Entrance In Area**.

By default, the detection tool is enabled and set to generate events when an object enters the detection area.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Entrance In Area**	Enter the detection tool name or leave the default name
Event hold time (sec)	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This is the time period during which the detection tool waits for the next objects after the first object in the group is detected. If the specified number of objects (specified in the **Number of alarm objects** parameter) are detected within this time period, the detection tool generates an event. If no additional objects are detected within the specified time period, the detection tool doesn't generate an event. Specify the time period in seconds when events will be held when responding to a group of objects. The value must be in the range [0, 86400]
Type	**Entrance In Area**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Entrance In Area**.

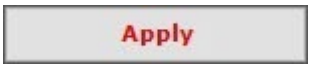
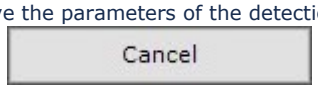
Maximum object speed	**500**	Specify the maximum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500]. **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** an d **Entrance In Area**.
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** an d **Entrance In Area**.
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Entrance In Area**.
Minimum speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Number of alarm objects	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This number determines the minimum number of objects that are considered a group and can generate an event. Specify the number of objects that can cause the detection tool to generate an event. The value must be in the range [1, 100]
Object class	**All classes**	Select the object class that must generate an event. The default value is **All classes**

	Vehicle **Person**	**Note** • When you create the **Entrance In Area** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Entrance In Area** detection tool below the Category: Face and Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.
Trigger on group of objects	**Yes** **No**	The parameter is disabled by default. If you want the detection tool to generate an event only for a group of objects, select the **Yes** value **Note** • The group of objects that must cause the detection tool to generate an event is specified in the **Object class** parameter. • The number of objects that is considered a group is specified in the **Number of alarm objects** parameter. • Waiting time for the next objects after the first object from the group is detected is specified in the **Event hold time (sec)** parameter. For example, you select the **Person** object class, the **Number of alarm objects** is **3**, the **Event hold time (sec)** is **2** seconds, and the **Trigger on group of objects** parameter is enabled. If the detection tool detects the first person and detects the others within two seconds, these people are considered a group and the detection tool generates an event.

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring Exit From Area

To configure the **Exit From Area**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create...** **Exit From Area**.

By default, the detection tool is enabled and set to generate events when an object leaves the detection area.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Exit From Area**	Enter the detection tool name or leave the default name
Type	**Exit From Area**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Event hold time (sec)	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This is the time period during which the detection tool waits for the next objects after the first object in the group is detected. If the specified number of objects (specified in the **Number of alarm objects** parameter) are detected within this time period, the detection tool generates an event. If no additional objects are detected within the specified time period, the detection tool doesn't generate an event. Specify the time period in seconds when events will be held when responding to a group of objects. The value must be in the range [0, 86400]
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Exit From Area**.

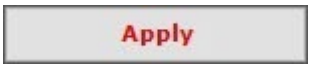
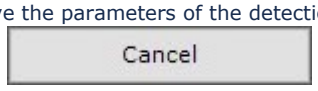
Maximum object speed	**500**	Specify the maximum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Exit From Area**.
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Exit From Area**.
Minimum object speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Exit From Area**.
Number of alarm objects	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This number determines the minimum number of objects that are considered a group and can generate an event. Specify the number of objects that can cause the detection tool to generate an event. The value must be in the range [1, 100]
Object class	**All classes**	Select the object class that must generate an event. The default value is **All classes**

	Vehicle **Person**	**Note** • When you create the **Exit From Area** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Exit From Area** detection tool below the Category: Face and Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.
Trigger on group of objects	**Yes** **No**	The parameter is disabled by default. If you want the detection tool to generate an event only for a group of objects, select the **Yes** value **Note** • The group of objects that must cause the detection tool to generate an event is specified in the **Object class** parameter. • The number of objects that is considered a group is specified in the **Number of alarm objects** parameter. • Waiting time for the next objects after the first object from the group is detected is specified in the **Event hold time (sec)** parameter. For example, you select the **Person** object class, the **Number of alarm objects** is **3**, the **Event hold time (sec)** is **2** seconds, and the **Trigger on group of objects** parameter is enabled. If the detection tool detects the first person and detects the others within two seconds, these people are considered a group and the detection tool generates an event.

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring Multiple Objects

To configure the **Multiple Objects**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create...** **Multiple Objects**.

By default, the detection tool is enabled and set to generate events when the number of objects in the detection area exceeds the value specified in the detection tool settings.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

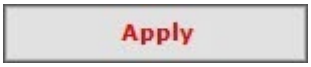
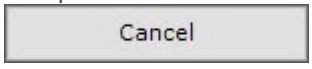
Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Multiple Objects**	Enter the detection tool name or leave the default name
Type	**Multiple Objects**	Name of the detection tool type (non-editable field)
Basic settings		
Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Multiple Objects**.
Maximum object speed	**500**	Specify the maximum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Multiple Objects**.
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Multiple Objects**.

Minimum object speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Multiple Objects**.
Number of alarm objects	**10**	Specify the number of objects for the detection tool to generate an event. The value must be in the range [1, 100]. When the specified number of objects is exceeded, the detection tool generates the **Triggering start** event. When the number of objects becomes less than the specified value, the **Triggering end** event is generated
Object class	**All classes** **Vehicle** **Person**	Select the object class that must generate an event. The default value is **All classes** **Note** • When you create the **Multiple Objects** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Multiple Objects** detection tool below the Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring Move From Area To Area

On the page:

- Configuring detection tool
- Configuring detection areas

Configuring detection tool

To configure the **Move From Area To Area**, do the following:

1. Create the required detection tool and specify its parameters (see Configuring detection tools and their sub-tools).
2. Below the created detection tool, click **Create... Move From Area To Area**.

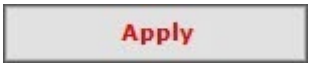
By default, the detection tool is enabled and set to generate events when an object leaves one area and enters another area.

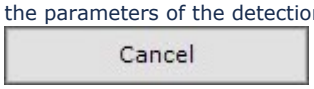
If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Move From Area To Area**	Enter the detection tool name or leave the default name
Type	**Move From Area To Area**	Name of the detection tool type (non-editable field)
Advanced settings		
X-axis offset	**15**	Specify the X-axis and Y-axis offsets as a percentage of the track area to receive events from the specified area. The values must be in the range [1, 40]
Y-axis offset	**10**	
Basic settings		
Event hold time (sec)	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This is the time period during which the detection tool waits for the next objects after the first object in the group is detected. If the specified number of objects (specified in the **Number of alarm objects** para meter) are detected within this time period, the detection tool generates an event. If no additional objects are detected within the specified time period, the detection tool doesn't generate an event. Specify the time period in seconds when events will be held when responding to a group of objects. The value must be in the range [0, 86400]

Maximum object height	**100**	Specify the maximum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object height must be equal in the settings of the **Object Tracker** and **Move From Area To Area**.
Maximum object width	**100**	Specify the maximum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the maximum object width must be equal in the settings of the **Object Tracker** and **Move From Area To Area**.
Maximum speed	**500**	Specify the maximum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).
Minimum object height	**0.1**	Specify the minimum object height as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object height must be equal in the settings of the **Object Tracker** and **Move From Area To Area**.
Minimum object width	**0.1**	Specify the minimum object width as a percentage of the frame size for the detection tool to generate an event. The value must be in the range [0.05, 100] **Attention!** The values of the minimum object width must be equal in the settings of the **Object Tracker** and **Move From Area To Area**.
Minimum speed	**0**	Specify the minimum object speed per second for the detection tool to generate an event. The value must be in the range [0, 500] **Note** • In *Axxon One*, speed is a conditional value that is calculated using values of different dimensions. The speed calculation algorithm takes into account both the frame width and its height. • For a visual understanding of the speed values, we recommend specifying the speed when searching the archive (see Configuring minimum and maximum object speed).

Number of alarm objects	**2**	**Note** The parameter is taken into account only if the **Trigger on group of objects** parameter is enabled. This number determines the minimum number of objects that are considered a group and can generate an event. Specify the number of objects that can cause the detection tool to generate an event. The value must be in the range [1, 100]
Object class	**All classes** **Vehicle** **Person**	Select the object class that must generate an event. The default value is **All classes** **Note** • When you create the **Move From Area To Area** detection tool below the **Object Tracker** and select the **Person** value, there won't be any events if the tracker detects the movement of several people nearby. • When you create the **Move From Area To Area** detection tool below the Category: Vehicle detection tools, the **Object class** parameter must have the **All classes** value.
Trigger on group of objects	**Yes** **No**	The parameter is disabled by default. If you want the detection tool to generate an event only for a group of objects, select the **Yes** value **Note** • The group of objects that must generate an event is specified in the **Object class** parameter. • The number of objects that is considered a group is specified in the **Number of alarm objects** parameter. • Waiting time for the next objects after the first object from the group is detected is specified in the **Event hold time (sec)** parameter. For example, you select the **Person** object class, the **Number of alarm objects** is **3**, the **Event hold time (sec)** is **2** seconds, and the **Trigger on group of objects** parameter is enabled. If the detection tool detects the first person and detects the others within two seconds, these people are considered a group and the detection tool generates an event.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

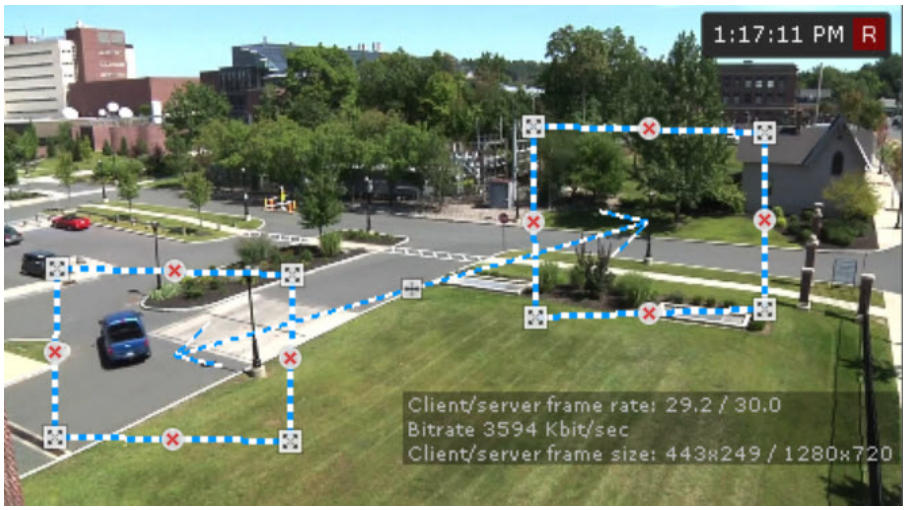
button.

Configuring detection areas

To configure detection areas, do the following:

1. In the preview window, specify two areas. The detection tool generates an event if any object moves from one area to the other in the specified direction.
   By default, the areas are located on the right side and the left side of the video image. The anchor points of each area are connected by a two-color dotted line. You can resize the area by dragging its anchor points  . To move the entire area, left click and drag its border. To add anchor points, click  .
2. In the preview window, specify the directions of the object movement. The direction of movement between the areas is indicated by a dotted arrow. To change the direction of movement, click  on the direction arrow. The available directions are:
   a. Left.
   b. Right.

c. Both directions.



3. Click the **Apply** button. To cancel the changes, click the **Cancel** button.

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

Category: Trackers

Abandoned Objects Detection VI

Functions of the Abandoned Objects Detection VI

Description	The **Abandoned Objects Detection VI** is used to automatically detect abandoned or disappeared objects that remain stationary for a certain period of time in the camera FOV. You can use the detection tool to detect abandoned/disappeared objects in a room
Licensing	To operate the detection tool, you need to contact an AxxonSoft manager and get a license file (see Types of licenses, Licensing of the software module for the Abandoned Objects Detection VI)
Add-ons	For the detection tool to work, you must install the VI Analytics Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Abandoned Objects Detection VI

Hardware requirements for neural analytics operation

Image requirements for the Abandoned Objects Detection VI

Requirements for the operation of the **Abandoned Objects Detection VI** are given in the table:

Camera	• Pitch angle of the camera optical axis relative to the horizontal plane:
	  ◦ at least 15 degrees (for the inclined method of placement);
	  ◦ from 80 to 100 degrees (for placement on ceiling).
	• Resolution is from 640x360 to 1920×1080 pixels. Resolution can be:
	  ◦ lower for close-up scenes (2–7 meters for cameras with standard focal length) without loss of recognition quality;
	  ◦ higher for scenes far from camera (from 10 meters).
	• FPS is at least 25
	• Color image only

Lighting	• Lighting in the scene is from 100 to 1000 lux
Scene and camera angle	• Shooting distance is from 5 to 30 meters • Density of people flow is no more than one person per square meter • Volume of the abandoned object is from 3 cubic decimeters • Background texture: moving, random and inhomogeneous background with contrast variations from 0.2 to 0.8

Image requirements for the Abandoned Objects Detection VI

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Abandoned Objects Detection VI

Requirements for the operation of the **Abandoned Objects Detection VI** are given in the table:

Object images	• For abandoned objects, the optimum density is 100 pixels per meter • Maximum signal-to-noise ratio (without the function of automatic signal amplification) is at least 42 dB • Image isn't noisy and isn't distorted by artifacts of the compression algorithm • Distortion is no more than 10% (at the edges of the frame—at a distance of one third from its center in width, height and diagonal)

Licensing of the software module for the Abandoned Objects Detection VI

On the page:

- Installing the environment for license keys
- License activation and update
- Deleting the license

Installing the environment for license keys

The Sentinel LDK Run-time environment is required for the operation of the license keys of the Abandoned Objects Detection VI. The environment is installed automatically with the VI Analytics Pack add-on (see Installing DetectorPack add-ons).

To install the Sentinel LDK Run-time environment manually, do the following:

1. Download the haspdinst_EOAWT.exe installer.
2. Run the command line as the system administrator.
3. Run the **haspdinst_EOAWT.exe -i -fi -fss** command.
4. Restart the Sentinel LDK License Manage service or restart the OS.

> **Note**
>
> When the environment is successfully installed, the Sentinel Admin Control Center web application opens in a web browser at http://127.0.0.1:1947/.

Installation of the Sentinel LDK Run-time environment is complete.

License activation and update

> **Attention!**
>
> Before installing the software key, you must install the Sentinel LDK Run-time environment.

To activate/update the license, do the following:

1. Open a browser and go to http://127.0.0.1:1947/checkin.html.
2. On the page that opens, in the **Select File** line, select the key with v2c extension.

   > **Attention!**
   >
   > To get the key with v2c extension, you need to contact an AxxonSoft manager.

3. Click **Apply File**.
4. If activation was successful, the key is displayed at http://127.0.0.1:1947/devices.html.

After activation, in the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK directory, the **installed** folder appears.

The license activation/update is complete.

Deleting the license

To delete the license, do the following:

1. Delete the license file with v2c extension from the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK\installed\ directory.
2. Restart the OS.

Note

- When you delete the license, only the key is deleted. All license restriction counters remain in the secure storage.
- If you return the key to the root directory, it will be fully restored. Its counters will continue counting license restrictions from the moment when they stopped when the license file with v2c extension was deleted. The validity time of the license continues to count down even when the key is missing.

The license deletion is complete.

When you delete the **installed** folder with licenses, you must restart the Sentinel LDK Run-time environment:

1. Press the **Win + R** keyboard shortcut.
2. In the window that opens, enter **services.msc** and press **Enter**.
3. In the **Services** window, find **Sentinel LDK License Manager**.
4. Right-click **Sentinel LDK License Manager** and select **Restart**.

The **Sentinel LDK License Manager** service will stop and then automatically start again.

Configuring the Abandoned Objects Detection VI

Licensing of the software module for the Abandoned Objects Detection VI

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Abandoned Objects Detection VI

Image requirements for the Abandoned Objects Detection VI

To configure the **Abandoned Objects Detection VI**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Abandoned Objects Detection VI**.

By default, the detection tool is enabled and set to detect abandoned objects.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Abandoned Objects Detection VI**	Enter the detection tool name or leave the default name
Background accumulation	**Yes**	By default, scene background accumulation is enabled. To disable, select the **No** value
	No	
Background override	**Yes**	By default, background override is disabled. Background override is used for PTZ cameras. For fixed cameras, the parameter must be disabled
	No	
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Detection area sensitivity	**Medium level**	Select the detection area sensitivity. The **Medium level** of sensitivity is selected by default. Additional neural network processing is applied in this area
	Low level	
Detection sensitivity	**70**	Specify the sensitivity level of the detection tool as a percentage. The value must be in the range [0, 100]

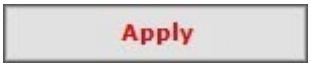
Event intersection time (sec)	**0.01**	Specify the time interval in seconds during which events won't be processed after successful detection when the event results match. The parameter determines the level of intersection between new and previous events. If the specified value is exceeded, it is considered that these events refer to the same real object. The parameter is necessary to reduce the total number of events, since the analysis is performed continuously and the duration of real events can be several seconds. You must select the required value empirically. The value must be in the range [0, 1]
Frame size change	**640**	Specify the size to which the video is compressed before analysis. The value must be in the range [480, 960]
Highlight and shadow filter	**0.15**	Specify the value of highlight and shadow filtering. The value must be in the range [0, 10]
Ignore time (sec)	**0**	Specify the time interval in seconds during which events won't be processed after successful detection. The parameter is necessary to reduce the total number of events, since the analysis is performed continuously and the duration of real events can be several seconds. You must select the required value empirically. The value must be in the range [0, 9999]
Maximum size of detected objects	**100**	Specify the maximum size of an object as a percentage to get an event from the detection tool. If objects are larger than specified, there won't be any events from the detection tool. The value must be in the range [0, 100]
Minimum size of detected objects	**0**	Specify the minimum size of an object as a percentage to get an event from the detection tool. If objects are smaller than specified, there won't be any events from the detection tool. The value must be in the range [0, 100]
Mode	**CPU**	Select the processor for the detection tool operation (see Selecting Nvidia GPU when configuring detection tools)
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	
	Nvidia GPU 3	
Monotony filter	**0.15**	Specify the value of monotonous/single-color events filtering (for example, spots on the floor). The value must be in the range [0, 10]
Number of execution threads	**4**	Specify the number of execution threads. The value must be in the range [0, 100]
Object filter	**Yes**	By default, the neural network object filter is disabled. To enable, select the **Yes** value
	No	
People flow intensity (%)	**99**	Specify the value as a percentage that is responsible for the detection tool ability to detect objects when the camera FOV is heavily overlapped by people walking by. The value must be in the range [0, 100]
Person filter	**Yes**	By default, objects near people aren't ignored. To ignore objects near people, select the **Yes** value
	No	
Saving background	**Yes**	By default, saving the scene background is enabled. To disable, select the **No** value
	No	
Sensitivity of slight changes in background (%)	**95**	Controls the sensitivity to object contrast. Specify the value as a percentage that is responsible for the detection tool ability to distinguish between objects that are less visible (that blend into the background). The higher the value, the less noticeable object can be detected. The value must be in the range [0, 100]

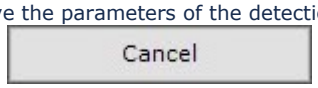
State saving interval	**0**	Specify the state saving interval in seconds. The value must be in the range [0, 9999]
Time for detection (sec)	**120**	Specify the time in seconds after which the object is considered abandoned. The value must be in the range [0, 9999]
Type	**Abandoned Objects Detection VI**	Name of the detection tool type (non-editable field)

In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button (see Configuring a detection area). To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Abandoned Objects Detection (Street) VI

Functions of the Abandoned Objects Detection (Street) VI

Description	The **Abandoned Objects Detection (Street) VI** is used to automatically detect abandoned or disappeared objects that remain stationary for a certain period of time in the camera FOV. You can use the detection tool to detect abandoned /disappeared objects in an area with changes in the scene due to weather conditions or unstable lighting
Licensing	To operate the detection tool, you need to contact an AxxonSoft manager and get a license file (see Types of licenses, Functions of the Abandoned Objects Detection (Street) VI)
Add-ons	For the detection tool to work, you must install the VI Analytics Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Abandoned Objects Detection (Street) VI

Hardware requirements for neural analytics operation

Image requirements for the Abandoned Objects Detection (Street) VI

Requirements for the operation of the **Abandoned Objects Detection (Street) VI** are given in the table:

Camera	• Pitch angle of the camera optical axis relative to the horizontal plane:
	  ◦ at least 15 degrees (for the inclined method of placement);
	  ◦ from 80 to 100 degrees (for placement on ceiling).
	• Resolution is from 640x360 to 1920×1080 pixels. Resolution can be:
	  ◦ lower for close-up scenes (2–7 meters for cameras with standard focal length) without loss of recognition quality;
	  ◦ higher for scenes far from camera (from 10 meters).
	• FPS is at least 25
	• Color image only

Lighting	• Lighting in the scene is from 100 to 1000 lux
Scene and camera angle	• Shooting distance is from 5 to 30 meters • Density of people flow is no more than one person per square meter • Volume of the abandoned object is from 3 cubic decimeters • Background texture: moving, random and inhomogeneous background with contrast variations from 0.2 to 0.8

Image requirements for the Abandoned Objects Detection (Street) VI

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Abandoned Objects Detection (Street) VI

Requirements for the operation of the **Abandoned Objects Detection (Street) VI** are given in the table:

Object images	• For abandoned objects, the optimum density is 100 pixels per meter • Maximum signal-to-noise ratio (without the function of automatic signal amplification) is at least 42 dB • Image isn't noisy and isn't distorted by artifacts of the compression algorithm • Distortion is no more than 10% (at the edges of the frame—at a distance of one third from its center in width, height and diagonal)

Licensing of the software module for the Abandoned Objects Detection (Street) VI

On the page:

- Installing the environment for license keys
- License activation and update
- Deleting the license

Installing the environment for license keys

The Sentinel LDK Run-time environment is required for the operation of the license keys of the Abandoned Objects Detection (Street) VI. The environment is installed automatically with the VI Analytics Pack add-on (see Installing DetectorPack add-ons).

To install the Sentinel LDK Run-time environment manually, do the following:

1. Download the haspdinst_EOAWT.exe installer.
2. Run the command line as the system administrator.
3. Run the **haspdinst_EOAWT.exe -i -fi -fss** command.
4. Restart the Sentinel LDK License Manage service or restart the OS.

> **Note**
>
> When the environment is successfully installed, the Sentinel Admin Control Center web application opens in a web browser at http://127.0.0.1:1947/.

Installation of the Sentinel LDK Run-time environment is complete.

License activation and update

> **Attention!**
>
> Before installing the software key, you must install the Sentinel LDK Run-time environment.

To activate/update the license, do the following:

1. Open a browser and go to http://127.0.0.1:1947/checkin.html.
2. On the page that opens, in the **Select File** line, select the key with v2c extension.

   > **Attention!**
   >
   > To get the key with v2c extension, you need to contact an AxxonSoft manager.

3. Click **Apply File**.
4. If activation was successful, the key is displayed at http://127.0.0.1:1947/devices.html.

After activation, in the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK directory, the **installed** folder appears.

The license activation/update is complete.

Deleting the license

To delete the license, do the following:

1. Delete the license file with v2c extension from the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK\installed\ directory.
2. Restart the OS.

Note

- When you delete the license, only the key is deleted. All license restriction counters remain in the secure storage.
- If you return the key to the root directory, it will be fully restored. Its counters will continue counting license restrictions from the moment when they stopped when the license file with v2c extension was deleted. The validity time of the license continues to count down even when the key is missing.

The license deletion is complete.

When you delete the **installed** folder with licenses, you must restart the Sentinel LDK Run-time environment:

1. Press the **Win + R** keyboard shortcut.
2. In the window that opens, enter **services.msc** and press **Enter**.
3. In the **Services** window, find **Sentinel LDK License Manager**.
4. Right-click **Sentinel LDK License Manager** and select **Restart**.

The **Sentinel LDK License Manager** service will stop and then automatically start again.

Configuring the Abandoned Objects Detection (Street) VI

Licensing of the software module for the Abandoned Objects Detection (Street) VI

Video stream and scene requirements for the Abandoned Objects Detection (Street) VI

Image requirements for the Abandoned Objects Detection (Street) VI

Hardware requirements for neural analytics operation

To configure the **Abandoned Objects Detection (Street) VI**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Abandoned Objects Detection (Street) VI**.

By default, the detection tool is enabled and set to detect abandoned objects.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Abandoned Objects Detection (Street) VI**	Enter the detection tool name or leave the default name
Background accumulation	**Yes**	By default, scene background accumulation is enabled. To disable, select the **No** value
	No	
Background sensitivity (%)	**100**	Controls the sensitivity to object contrast. Specify the value as a percentage that is responsible for the detection tool ability to distinguish the level of object contrast relative to the background. The higher the value, the object with less contrast can be detected. The value must be in the range [0, 100]
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei NPU	
Detection area sensitivity	**Medium level**	Select the detection area sensitivity. The **Medium level** of sensitivity is selected by default. Additional neural network processing is applied in this area
	Low level	

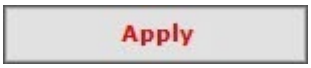
Detection sensitivity	**70**	Specify the sensitivity level of the detection tool as a percentage. The value must be in the range [0, 255]
Event intersection time (sec)	**0.01**	Specify the time interval in seconds during which events won't be processed after successful detection when the event results match. The parameter determines the level of intersection between new and previous events. If the specified value is exceeded, it is considered that these events refer to the same real object. The parameter is necessary to reduce the total number of events, since the analysis is performed continuously and the duration of real events can be several seconds. You must select the required value empirically. The value must be in the range [0, 1]
Frame size change	**640**	Specify the size to which the video is compressed before analysis. The value must be in the range [480, 960]
Ignore time (sec)	**5**	Specify the time interval in seconds during which events won't be processed after successful detection. The parameter is necessary to reduce the total number of events, since the analysis is performed continuously and the duration of real events can be several seconds. You must select the required value empirically. The value must be in the range [0, 9999]
Maximum brightness (%)	**255**	Specify the maximum brightness of an object as a percentage to get an event from the detection tool. The value must be in the range [0, 255]
Maximum object height (%)	**100**	Specify the minimum object size as a percentage of the frame height to get an event from the detection tool. If objects are smaller than specified, there won't be any events from the detection tool. The value must be in the range [0, 100]
Maximum object width (%)	**100**	Specify the maximum object width as a percentage of the frame width to get an event from the detection tool. If object width is larger than specified, there won't be any events from the detection tool. The value must be in the range [0, 100]
Minimum object area (%)	**0**	Specify the minimum object area as a percentage of the frame area to get an event from the detection tool. If object area is smaller, there there won't be any events from the detection tool. The value must be in the range [0, 100]
Mode	**CPU**	Select the processor for the detection tool operation (see Selecting Nvidia GPU when configuring detection tools)
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	
	Nvidia GPU 3	
Number of execution threads	**4**	Specify the number of execution threads. The value must be in the range [0, 100]
Object filter	**Yes**	By default, the neural network object filter is disabled. To enable, select the **Yes** value
	No	
Object frame intersection	**0**	Specify the percentage of the object frame intersection that must be merged into one object. The value must be in the range [0, 100]
Person filter	**Yes**	By default, objects near people aren't ignored. To ignore objects near people, select the **Yes** value
	No	
Ratio of object height to width	**90**	Specify the maximum level of object extension to get an event from the detection tool. The value must be in the range [0, 100]
Saving background	**Yes**	By default, saving the scene background is enabled. To disable, select the **No** value
	No	

Scene static (%)	**25**	Specify the scene static as a percentage. The higher the value of the parameter, the lower the scene dynamics. The value must be in the range [0, 100]
Scene update threshold (%)	**10**	Specify the scene update threshold as a percentage. If the percentage of changes in the frame exceeds the value of this parameter, the background is updated. The value must be in the range [0, 9999]
State saving interval	**0**	Specify the state saving interval in seconds. The value must be in the range [0, 9999]
Time for detection (sec)	**120**	Specify the time in seconds after which an object is considered abandoned. The value must be in the range [0, 9999]
Type	**Abandoned Objects Detection (Street) VI**	Name of the detection tool type (non-editable field)

In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Neurotracker

Functions of the Neurotracker

Description	The **Neurotracker** allows you to detect moving and static objects in the frame
Add-ons	For the **Neurotracker** to operate, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Neurotracker and its sub-tools

Image requirements for the Neurotracker and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Neurotracker** and its sub-tools are given in the table:

Camera	• Resolution must be at least 640x360 pixels. We also don't recommend using a resolution higher than 1920×1080, since higher resolution doesn't increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 • The frame rate per second in the video stream from the camera is at least 8 for solving typical tasks • Neurotracker-based analytics works with both colorless (gray) and color images. When you use a neurofilter, we recommend using color cameras. When you use black-and-white cameras, the recognition quality can be noticeably worse **Attention!** Correct operation of the **Neurotracker** isn't guaranteed when using a fisheye camera.
Lighting	• Lighting in the scene is at least 50 lux. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on) • The analyzed scene doesn't have reflective surfaces and sharp shadows from moving objects. If present, they must be masked • Camera shake doesn't result in image offsets greater than 1% of the frame size

Image requirements for the Neurotracker and its sub-tools

Video stream and scene requirements for the Neurotracker and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Neurotracker** and its sub-tools are given in the table:

Object images

- The detected object must be clearly distinguishable by the human eye
- Width and height of objects in the image must not exceed 75% of the frame size
- When you use a neurofilter, the minimum width or height of an object must be at least 5% of the width/height of the frame
- The image isn't noisy and not distorted by the artifacts of the compression algorithm
- The duration of the object visibility is at least six frames
- Between two frames, an object must move in the direction of a distance not exceeding its size. This condition is necessary for the correct calculation of the object track
- The minimum value of pixel density per meter is observed:

Image resolution	Object type	Minimum pixel density per meter (ratio of the object width in pixels to the object width in meters)	Minimum object size in pixels, width x height	Ratio of the object width to the frame width as a percentage
1920x1080	Human	55	~25x105	~3%
1280x720	Human	35	~17x70	~3%
640x360	Human	17	~10x42	~3%
1920x1080	Light vehicle (2 axles)	55	~354x300	~20%
1280x720	Light vehicle (2 axles)	35	~240x205	~20%
640x360	Light vehicle (2 axles)	17	~132x112	~20%

Configuring the Neurotracker

On the page:

- Configuring the detection tool
- Example of configuring Neurotracker for solving typical tasks

Video stream and scene requirements for the Neurotracker and its sub-tools

Image requirements for the Neurotracker and its sub-tools

Hardware requirements for neural analytics operation

Configuring the detection tool

To configure the **Neurotracker**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create...** **Category: Trackers** **Neurotracker**.

By default, the detection tool is enabled and set to detect moving people.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	By default, metadata are recorded into the database. To disable metadata recording, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Neurotracker**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei iNPU	
Neurofilter mode	**CPU**	Select a processing resource for neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools) **Attention!** • We recommend using the GPU. It may take several minutes to launch the algorithm on Nvidia GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS). • Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	

	Nvidia GPU 3 **Intel NCS (not supported)** **Intel HDDL (not supported)** **Intel GPU** **Huawei NPU**	• Starting with *Detector Pack* 3.12, the parameter is removed from the detection tool settings, and Neurofilter runs on the same processor as Neurotracker. If before *Detector Pack* update, you select a different processor in the **Neurofilter mode** parameter, after the update, the detection tool works without Neurofilter.
Number of frames processed per second	**6**	Specify the number of frames for the neural network to process per second. The higher the value, the more accurate the tracking, but the load on the CPU is also higher. The value must be in the range [0.016, 100]. ⚠ **Attention!** We recommend the value of at least 6 FPS. For fast moving objects (running individuals, vehicles), you must set the frame rate at **12** FPS or above.
Type	**Neurotracker**	Name of the detection tool type (non-editable field)
Advanced settings		
Camera position	**Wall** **Ceiling**	To sort out false events from the detection tool when using a fisheye camera, select the correct device location. For other devices, this parameter is irrelevant
Hide moving objects	**Yes** **No**	By default, the parameter is disabled. If you don't need to detect moving objects, select the **Yes** value. An object is considered static if it doesn't change its position more than 10% of its width or height during its track lifetime ⚠ **Attention!** If a static object starts moving, the detection tool will create a track, and the object will no longer be considered static.
Hide static objects	**Yes** **No**	By default, the parameter is disabled. If you don't need to detect static objects, select the **Yes** value. This parameter lowers the number false events from the detection tool when detecting moving objects. An object is considered static if it has not moved more than 10% of its width or height during the whole time of its track existence. ⚠ **Attention!** If a static object starts moving, the detection tool will create a track, and the object will no longer be considered static.
Minimum number of detection triggers	**6**	Specify the **Minimum number of detection triggers** for the Neurotracker to display the object's track. The higher the value, the longer the time interval between the detection of an object and the display of its track on the screen. Low values of this parameter can lead to false events from the detection tool. The value must be in the range [2, 100]
Model quantization	**Yes**	

	No	By default, the parameter is disabled. The parameter is applicable only to standard neural networks for Nvidia GPU. It allows you to reduce the consumption of computation power. The neural network is selected automatically depending on the value selected in the **Object type** parameter. To quantize the model, select the **Yes** value **Attention!** AxxonSoft conducted a study in which a neural network model was trained to identify the characteristics of the detected object with quantization. The following results of the study were obtained: model quantization can lead to both an increase in the percentage of recognition and a decrease. This is due to the generalization of the mathematical model. The difference in detection ranges within ±1.5%, and the difference in object identification ranges within ±2%. • The first launch of a detection tool with the **Model quantization** parameter enabled can take longer than a standard launch. • If GPU caching is used, next time the detection tool with quantization will run without delay.
Neural network file		If you use a custom neural network, select the corresponding file **Attention!** • To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training). • A trained neural network for a particular scene allows you to detect only objects of a certain type (for example, a person, a cyclist, a motorcyclist, and so on). • If the neural network file is not specified, the default file will be used, which is selected automatically depending on the selected object type (**Object type**) and the selected processor for the neural network operation (**Decoder mode**). If you use a custom neural network, enter a path to the file. The selected object type is ignored when you use a custom neural network. • To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. • If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%. The standard neural networks are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory.
Scanning window	**Yes** **No**	By default, the parameter is disabled. To enable the scanning mode, select the **Yes** value (see Configuring the scanning mode)
Scanning window height	**0**	The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels
Scanning window step height	**0**	The scanning step determines the relative offset of the windows. If the step is equal to the height and width of the scanning window respectively, the segments will line up one after another. Reducing the height or width of the scanning step will increase the number of windows due to their overlapping each other with an offset. This will increase the detection accuracy, but will also increase the CPU load. **Attention!** The height and width of the scanning step must not be greater than the height and width of the scanning window—the detection tool will not operate with such settings.
Scanning window step width	**0**	
Scanning window width	**0**	The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels

<table>
<tr><td>Selected object class</td><td></td><td>If necessary, specify the class of the detected object. If you want to display tracks of several classes, specify them separated by a comma with a space. For example, 1, 10.
The numerical values of classes for the embedded neural networks: 1—Human/Human (top-down view), 10—Vehicle.

a. If you leave the field blank, the tracks of all available classes from the neural network will be displayed (Object type, Neural network file).
b. If you specify a class/classes from the neural network, the tracks of the specified class/classes will be displayed (Object type, Neural network file).
c. If you specify a class/classes from the neural network and a class/classes missing from the neural network, the tracks of a class/classes from the neural network will be displayed (Object type, Neural network file).
d. If you specify a class/classes missing from the neural network, the tracks of all available classes from the neural network will be displayed (Object type, Neural network file)

Note
Starting with Detector Pack 3.10.2, if you specify a class/classes missing from the neural network, the tracks won’t be displayed (Object type, Neural network file).</td></tr>
<tr><td>Similitude search</td><td>Yes
No</td><td>By default, the parameter is disabled. To enable the search for similar persons, select the Yes value. If you enabled the parameter, it increases the processor load.

Attention!
The Similitude search works only on tracks of people.</td></tr>
<tr><td>Time of processing similitude track (sec)</td><td>0</td><td>Specify the time in seconds for the algorithm to process the track to search for similar persons. The value must be in the range [0, 3600]</td></tr>
<tr><td>Time period of excluding static objects</td><td>0</td><td>Specify the time in seconds after which the track of the static object is hidden. If the value of the parameter is 0, the track of the static object isn't hidden. The value must be in the range [0, 86 400]</td></tr>
<tr><td>Track retention time</td><td>0.7</td><td>Specify the time in seconds after which the object track is considered lost. This helps if objects in scene temporarily overlap each other. For example, when a larger vehicle completely blocks the smaller one from view. The value must be in the range [0.3, 1000]</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td>Detection threshold</td><td>30</td><td>Specify the Detection threshold for objects in percent. If the recognition probability falls below the specified value, the data will be ignored. The higher the value, the higher the detection quality, but some events from the detection tool may not be considered. The value must be in the range [0.05, 100]</td></tr>
<tr><td>Neurotracker mode</td><td>CPU
Nvidia GPU 0
Nvidia GPU 1
Nvidia GPU 2
Nvidia GPU 3
Intel NCS (not supported)</td><td>Select the processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

Attention!
• We recommend using the GPU. It may take several minutes to launch the algorithm on Nvidia GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS).
• If neurotracker is running on GPU, object tracks can be lagging behind the objects in the Surveillance window. If this happens, set the camera buffer size to 1000 milliseconds (see The Camera object).
• Starting with Detector Pack 3.11, Intel HDDL and Intel NCS aren’t supported.</td></tr>
</table>

	Intel HDDL (not supported)	
	Intel GPU	
	Huawei NPU	
Object type	**Person**	Select the recognition object. • **Nano**—low accuracy, low processor load. • **Medium**—medium accuracy, medium processor load. • **Large**—high accuracy, high processor load.
	Person (top-down view)	
	Person (top-down view Nano)	
	Person (top-down view Medium)	
	Person (top-down view Large)	
	Vehicle	
	Person and vehicle (Nano)	
	Person and vehicle (Medium)	
	Person and vehicle (Large)	
Neural network filter		
Neurofilter	**Yes**	By default, the parameter is disabled. To sort out parts of tracks, select the **Yes** value.
	No	For example: **Neurotracker** detects all freight trucks, and the neurofilter sorts out only the tracks that contain trucks with cargo door open

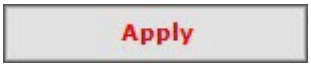
Neurofilter file		Select a neural network file **Attention!** Starting with *Detector Pack* 3.12, the neural network file of the Neurofilter must match the processor type specified in the **Neurotracker mode** parameter.

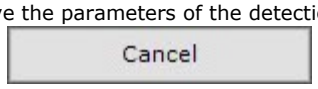
By default, the entire frame is a detection area. If necessary, in the preview window, set detection areas with the help of anchor points  (see Configuring a detection area).

Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

If necessary, you can create and configure the necessary detection sub-tools on the basis of Neurotracker (see Standard detection sub-tools).

Attention!

To get an event from the **Motion In Area** detection sub-tool on the basis of **Neurotracker**, an object must be displaced by at least 25% of its width or height in the frame.

Example of configuring Neurotracker for solving typical tasks

Parameter	Task: detection of moving people	Task: detection of moving vehicles
Other		
Number of frames processed per second	**6**	**12**
Neural network filter		
Neurofilter	**No**	**No**
Basic settings		
Detection threshold	**30**	**30**
Advanced settings		
Minimum number of detection triggers	**6**	**6**
Camera position	**Wall**	**Wall**

Hide static objects	**Yes**	**Yes**
Neural network file	Path to the *.ann neural network file. You can also select the **Object type** value. In this case, this field must be left blank	Path to the *.ann neural network file. You can also select the **Object type** value. In this case, this field must be left blank

Object Tracker

Functions of the Object Tracker

Description	The **Object Tracker** allows you to detect moving objects in the frame, on the basis of which their tracks are created
Add-ons	For the detection tool to work, you must install the Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Object Tracker and its sub-tools

Image requirements for the Object Tracker and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Object Tracker** and its sub-tools are given in the table:

Camera	• Resolution must be at least 640x360 pixels. We also don't recommend using a resolution higher than 800×600 **Attention!** Higher resolution doesn't increase the detection quality, but significantly increases the CPU and RAM load. • FPS is at least 6 • Tracker-based analytics works with both colorless (gray) and color images. If you use neurofilter, we recommend using color cameras. When you use black-and-white cameras, the recognition quality can be noticeably worse • Camera shake must not result in image offsets greater than 1% of the frame size
Lighting	• Moderate lighting. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting

Scene and camera angle	• Moving objects are visually separable from each other
	• The background is mostly static and doesn't change abruptly
	• Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on)
	• Analytics may not work correctly if:
	  ◦ the analyzed scene have reflective surfaces and sharp shadows from moving objects
	  ◦ there are extended monochromatic objects in the frame
	• When using the **Abandoned Object** detection tool, abandoned objects can be obscured by moving objects no more than 10% of the time

Image requirements for the Object Tracker and its sub-tools

Video stream and scene requirements for the Object Tracker and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Object Tracker** and its sub-tools are given in the table:

Object images	• Image isn't noisy and isn't distorted by artifacts of the compression algorithm
	• The width or height of objects in the image must not:
	  ○ be less than 1% of the frame size (at resolutions no less than 1920x1080 pixels) or 15 pixels (at lower resolutions)
	  ○ exceed 75% of the frame size
	• When you use a neurofilter, the minimum width or height of an object must be at least 5% of the width/height of the frame
	• When using the **Abandoned Object** detection tool:
	  ○ abandoned objects must be clearly visible in the image
	  ○ the width and height of objects in the image must not exceed 25% of the frame size
	• The speed of movement of objects in the image must not be less than 1 pixel per second
	• For the object to be detected, the duration of its visibility must be at least 8 frames
	• When the object moves between two adjacent frames in a certain direction, its distance of movement must not exceed its size. This condition is necessary for the correct calculation of the object's trajectory (track)

Recommendations for configuring the Object Tracker and its sub-tools

Configuring the Object Tracker

To avoid false positives from the sub-tools of the **Object Tracker**, the following recommendations must be met:

1. We recommend configuring the parameters of the **Object Tracker** empirically, checking the quality of its operation at each step.
2. Parameters that strongly influence the quality of operation:
    a. **Max. object height**, **Max. object width**, **Min. object height**, **Min. object width** (see Configuring the minimum and maximum size of detected objects):
        i. The values of the **Max. object height** and **Max. object width** parameters must be selected so that they are slightly lower than the size of a typical object in the image.
        ii. The values of the **Min. object height** and **Min. object width** parameters must be selected so that they are slightly larger than the size of a typical object in the image, taking into account its shadow.
    b. **Motion detection sensitivity, Abandoned object detection sensitivity** and **Auto sensitivity**:
        i. We recommend using the **Auto sensitivity** parameter that ensures the quality of the **Object Tracker** performance in highly variable lighting conditions.
        ii. If lighting is stable, we recommend selecting the values of the **Motion detection sensitivity** and **Abandoned object detection sensitivity** parameters empirically. For detection of objects with low contrast, the recommended sensitivity value is **35**, for contrast objects—**15**.
    c. If you decrease the value of the **Time of object in DB** parameter, generation of events on false static objects will be excluded. If you increase the value, in some cases the object track will be saved even when it temporarily disappears or overlaps with other objects.

If the requirements for the **Object Tracker** are met (see Video stream and scene requirements for the Object Tracker and its sub-tools , Image requirements for the Object Tracker and its sub-tools), the following performance parameters of the **Abandoned object** detection are guaranteed:

- out of 100 abandoned objects, the detection tool detects 92 objects;
- 80 detection events out of 100 will be caused by real abandoned objects, and 20 detection events will be caused by other changes in the monitored scene.

Configuring the Object Tracker

Video stream and scene requirements for the Object Tracker and its sub-tools

Image requirements for the Object Tracker and its sub-tools

Hardware requirements for neural analytics operation

To configure the **Object Tracker** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Object Tracker**.

By default, the detection tool is enabled and set to detect moving objects in the frame, on the basis of which their tracks are created.

Some parameters are set for all sub-tools of the **Object Tracker** simultaneously (see Recommendations for configuring the Object Tracker and its sub-tools).

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes** **No**	By default, metadata are recorded into the database. To disable metadata recording, select the **No** value. **Attention!** To obtain metadata, the video is decompressed and analyzed, which results in a heavy load on the Server and limits the number of video cameras that can be used on it.
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream allows you to reduce the Server load. **Attention!** To ensure the correct display of streams on a multi-stream camera, all video streams must have the same frame aspect ratio.
Other		
Enable	**Yes** **No**	By default, the parameter is enabled. To disable, select the **No** value
Name	**Object Tracker**	Enter the detection tool name or leave the default name
Decoder mode	**Auto** **CPU** **GPU** **Huawei NPU**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
Type	**Object Tracker**	Name of the detection tool type (non-editable field)
Neural network filter		
Enable filter	**Yes**	

<table>
<tr><td></td><td>No</td><td>By default, the neural network filter is disabled. To enable a neural network filter to filter out parts of tracks, set the value to Yes (see Hardware requirements for neural analytics operation). For example, a neural network filter can process the results of the tracker and filter out false positives on a complex video image (foliage, glare, etc.).

Attention!

A neural network filter can be used either only for the analysis of moving objects, or only for the analysis of abandoned objects. You cannot use two neural network filters simultaneously.</td></tr>
<tr><td rowspan="6">Moving object filter mode</td><td>CPU</td><td rowspan="14">Select the processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

Attention!

• If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
• It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS).</td></tr>
<tr><td>Nvidia GPU 0</td></tr>
<tr><td>Nvidia GPU 1</td></tr>
<tr><td>Nvidia GPU 2</td></tr>
<tr><td>Nvidia GPU 3</td></tr>
<tr><td>Intel GPU</td></tr>
<tr><td rowspan="6">Abandoned object filter mode</td><td>Huawei NPU</td></tr>
<tr><td>CPU</td></tr>
<tr><td>Nvidia GPU 0</td></tr>
<tr><td>Nvidia GPU 1</td></tr>
<tr><td>Nvidia GPU 2</td></tr>
<tr><td>Nvidia GPU 3</td></tr>
<tr><td>Intel GPU</td></tr>
<tr><td>Huawei NPU</td></tr>
<tr><td>Moving object filter file</td><td></td><td rowspan="2">Select the required neural network. To obtain a neural network, contact AxxonSoft technical support. If the neural network file is not selected or selected incorrectly, the filter will not work</td></tr>
<tr><td>Abandoned object filter file</td><td></td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td rowspan="2">Long-time abandoned object detection</td><td>Yes</td><td rowspan="2">By default, the parameter is disabled. To enable, select the Yes value.

Note

If you enable this and the Enable filter parameter, it can reduce the number of false positives during detection.</td></tr>
<tr><td>No</td></tr>
</table>

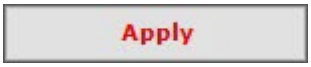
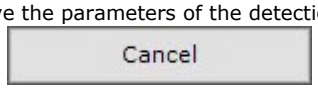
Abandoned object detection	**Yes** **No**	By default, the parameter is disabled. To enable, select the **Yes** value. **Note** Objects abandoned for 10 seconds or longer will be detected.
Max. object height	**100**	Set the maximum height and width of the detected object as a percentage of the frame size. The value must be in the range [0.05, 100].
Max. object width	**100**	**Attention!** If the **Object calibration** parameter is enabled in the tracker settings, then the maximum height and width of objects is set in decimeters, and not as a percentage of the frame size.
Alarm on object's max. idle time in area	**60**	Specify the time in seconds—if the object remains idle for the time longer than the specified, it will be detected. This value must be in the range [15, 1800]. **Note** This parameter is used only for the **Long-time abandoned object detection**. It is recommended to select the parameter value starting from **15**.
Min. object height	**2**	Set the minimum height and width of the detected object as a percentage of the frame size. The value must be in the range [0.05, 100].
Min. object width	**2**	**Attention!** If the **Object calibration** parameter is enabled in the tracker settings, then the minimum height and width of objects is set in decimeters, and not as a percentage of the frame size.
Motion detection sensitivity	**25**	Set the sensitivity of the motion detection sub-tools in percentage. The higher the sensitivity, the more subtle change in the frame will be detected. The value must be in the range [0, 100]
Abandoned object detection sensitivity	**9**	Set the sensitivity for abandoned object detection and long-time abandoned object detection in the range [1, 100]. **Note** This parameter depends on the lighting conditions and must be chosen empirically. It is recommended to select the parameter value starting from 20.
Advanced settings		
Auto sensitivity	**Yes** **No**	By default, the parameter is enabled. To disable automatic adjustment of the sensitivity of the **Object tracker** sub-tools, select the **No** value. **Note** It is recommended to enable this parameter if the lighting changes significantly in the video camera field of view (for example, if the camera operates in outdoors).
Time of object in DB	**3**	Set the time in seconds during which the object was present in the **Object tracker** database. If an object leaves the frame and returns within the set time, then it will be identified by the tracker as the same object (the same object id will be assigned)

Leveling rod height	**20**	Set the height of the calibration object in decimeters. The value must be in the range [1, 100]
Frame size change	**1280**	By default, during the analysis, the frame is compressed to the specified size (by default, 1280 pixels on the larger side). The following algorithm is used: • If the original resolution on the larger side of the frame is greater than the resolution specified in the **Frame size change** parameter, then it is divided in half. • If the resulting resolution becomes less than the specified one, then the algorithm stops and the resulting resolution will be used. • If the resulting resolution is still greater than the specified one, then it is divided in half again until it becomes less than the resolution specified in the **Frame size change** parameter. **Note** For example, the original video resolution is 2048x1536, the specified value is 1000. In this case, the original resolution will be divided in half (512x384) twice, because after the first division, the value on the larger side of the frame will be greater than the specified value (1024 > 1000). If a higher resolution stream is used for detection, and there are detection errors, it is recommended to reduce compression.
Object calibration	**Yes** **No**	By default, the parameter is disabled (see Configuring perspective). To estimate the real size of an object based on a simplified calibration system, select the **Yes** value
Camera position	**Wall** **Ceiling**	If you use a fish-eye camera, choose the correct location of the device to filter out false events. The default value is **Wall**. This parameter is not relevant for all other devices
Antishaker	**Yes** **No**	By default, the parameter is disabled. To reduce camera shake, select the **Yes** value. It is recommended to use this parameter only when there is significant camera shake

In the preview window, specify the detection area in which objects will be detected. The area is configured by moving the anchor points  (see Configuring a detection area). You can also configure the areas in which objects will not be detected (see Configuring a skip area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

The **Object tracker** detection tool is configured. General parameters will be set for all its sub-tools. If necessary, you can create and configure the necessary sub-tools on the basis of the **Object Tracker** (see Abandoned Object detection, Standard detection sub-tools).

Abandoned Object detection

Video stream and scene requirements for the Object Tracker and its sub-tools

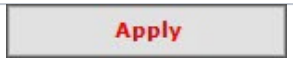
Attention!

The **Abandoned Object** detection can operate only with the **Object Tracker** detection tool.

Before you create and configure the **Abandoned Object** detection, do the following:

1. Create the **Object Tracker** detection tool and set its general parameters (see Configuring the Object Tracker).
2. Configure some parameters of the **Object Tracker** detection tool as follows:

Parameter	Value	Description
Auto sensitivity	**Yes**	If auto sensitivity is enabled, sensitivity adjustments for moving and abandoned objects are not applied. To apply manual sensitivity adjustments, it is necessary to disable the auto sensitivity
Long-time abandoned object detection	**Yes**	If you enable this and the **Enable filter** parameter (see Configuring the Object Tracker), it can reduce the number of false positives during detection
Abandoned object detection	**Yes**	Objects abandoned for 10 seconds or longer will be detected
Alarm on object's max. idle time in area	**60**	Specify the time in seconds—if the object remains idle for the time longer than the specified, it will be detected. This value must be in the range [15, 1800]. **Note** This parameter is used only for the **Long-time abandoned object detection**. It is recommended to select the parameter value starting from **15**.
Abandoned object detection sensitivity	**20**	For this parameter to work, it is necessary to first disable the **Auto sensitivity** parameter. Set the sensitivity for abandoned object detection and long-time abandoned object detection in the range [1, 100]. **Note** This parameter depends on the lighting conditions and must be chosen empirically. It is recommended to select the parameter value starting from 20.

3. Save the detection tool parameters by clicking the **Apply**  button.

To create the **Abandoned object** detection, below the **Object Tracker** detection tool, click **Create... Abandoned Object**.

By default, the detection tool is enabled and set to detect brought and abandoned objects.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	

Name	**Abandoned Object**	Enter a detection tool name or leave the default name
Type	**Abandoned Object**	Detection tool type name (non-editable field)
Basic settings		
Maximum object height	**100**	Set the maximum height of the object that must generate an event from the detection tool, as a percentage of the frame size. The value must be in the range [0.05, 100]
Maximum object width	**100**	Set the maximum width of the object that must generate an event from the detection tool, as a percentage of the frame size. The value must be in the range [0.05, 100]
Minimum object height	**0,1**	Set the minimum height of the object that must generate an event from the detection tool, as a percentage of the frame size. The value must be in the range [0.05, 100]
Minimum object width	**0,1**	Set the minimum width of the object that must generate an event from the detection tool, as a percentage of the frame size. The value must be in the range [0.05, 100]

Attention!

In the settings of the **Object Tracker** detection tool and the **Abandoned Object** sub-tool, the values of the maximum and minimum height and width of the object must be equal.

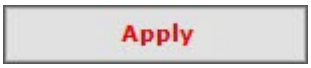
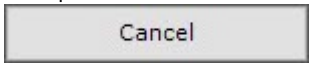
Object type	**Brought**	Select a value if it is necessary to detect an object that has disappeared from the observed area and crossed its boundaries
	Abandoned	
	Any	Select this value if it is necessary to detect both brought and abandoned objects

By default, the entire frame is a detection area. If necessary, in the preview window, set detection areas with the help of anchor points  (see Configuring a detection area).

Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

The **Abandoned Object** detection is now configured.

Object Tracker VL

Functions of the Object Tracker VL

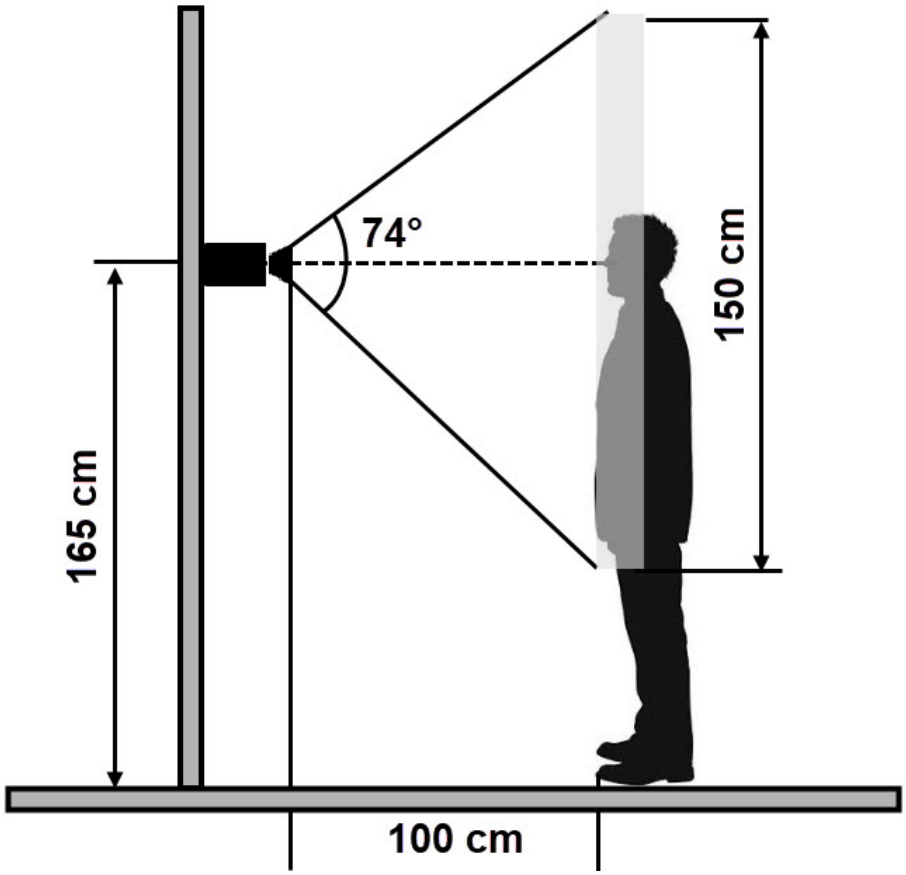
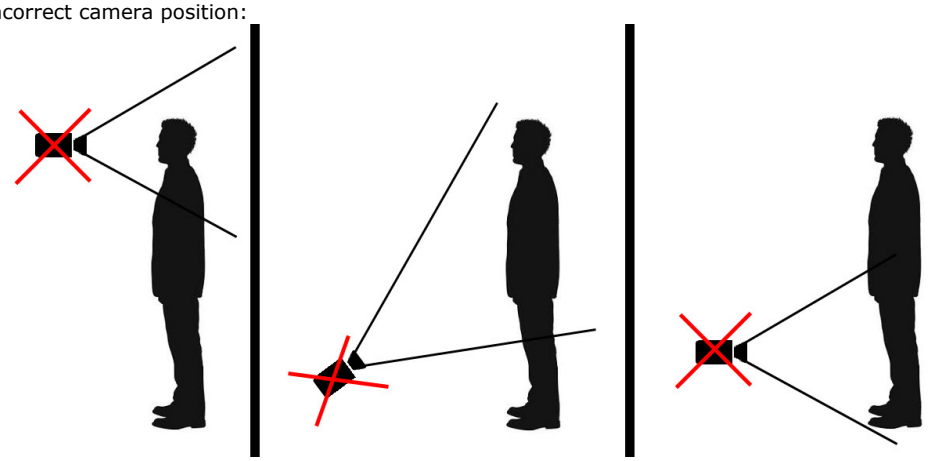
Description	The **Object Tracker VL** is used to detect people in the frame and generate events
Licensing	To operate the detection tool, you need to contact a manager of AxxonSoft and get a license file (see Types of licenses)
Add-ons	For the detection tool to work, you must install the VL SDK Pack and VL Analytics Pack add-ons (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Object Tracker VL and its sub-tools

Image requirements for the Object Tracker VL and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Object Tracker VL** and its sub-tools are given in the table:

Camera	• Resolution must be at least 640x360 pixels • Tracker-based analytics works with both colorless (gray) and color images. We recommend using color cameras. When you use black-and-white cameras, the recognition quality can be noticeably worse • The camera angle must be as horizontal as possible • Recommended camera tilt angle is from 0 (parallel to the ground) to 60 degrees • The camera position for human detection must be as shown in the image below:  Incorrect camera position: 
Lighting	• Lighting in the scene is at least 50 lux. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting

Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on) • The analyzed scene doesn't have reflective surfaces and sharp shadows from moving objects. If present, they must be masked • Camera shake doesn't result in image offsets greater than 1% of the frame size

Image requirements for the Object Tracker VL and its sub-tools

Video stream and scene requirements for the Object Tracker VL and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Object Tracker VL** and its sub-tools are given in the table:

Object images	• The person must be facing the camera
	• At least 60% of the person’s body (upper body) must be visible in the frame
	• No objects must obscure the human body in the frame
	• The image isn't noisy and not distorted by the artifacts of the compression algorithm
	• The analytics quality is decreased by the following factors:
	  ○ Non-standard poses (head tilt, splits, lying position, and so on)
	  ○ Camera position from above at a high angle

Activating the license for the Object Tracker VL in Windows OS

> **Attention!**
>
> Starting with *Detector Pack* 3.12, a demo license has been added to the VL Analytics Pack add-on (see Installing DetectorPack add-ons). Demo license is valid for 30 days after installation on one Server or a virtual machine.

To activate a license for the **Object Tracker VL** (see Configuring the Object Tracker VL), do the following:

1. Request **EID** and **ProductID** from the technical support.

   > **Attention!**
   >
   > **EID** and **ProductID** are linked with the MAC address of the Server. If the MAC address changes, you need to request **EID** and **ProductID** again.

2. Open the following file in a text editor: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
3. Enter the received **EID** and **ProductID**.

```
<param name="EID" type="Value::String" text="received EID"/>
<param name="ProductID" type="Value::String" text="received ProductID"/>
```

```
<?xml version="1.0"?>
<settings>
    <section name="Licensing::Settings">
        <param name="Server" type="Value::String" text="https://visionlabsbv.prod.sentinelcloud.com"/>
        <param name="EID" type="Value::String" text="[redacted]"/>
        <param name="ProductID" type="Value::String" text="[redacted]"/>
        <param name="Filename" type="Value::String" text="licenseFile.v2c"/>
        <param name="ContainerMode" type="Value::Int1" x="0"/>
    </section>
</settings>
```

4. Save the file: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
5. In the command line, run the following file as administrator: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\FingerprintViewer.exe. You will receive the **FingerPrint** data.

```
C:\Program Files\Common Files\[redacted]\DetectorPack\VLSdk\gpu>FingerprintViewer.exe
Using license file: ./data/license.conf
To run with default license file path:
        FingerprintViewer.exe
If you want to specify license file:
        FingerprintViewer.exe <path to license.conf>
[04.05.2023 09:28:42] [Debug] [createLicense] creation of the FitLicense license!
[04.05.2023 09:28:42] [Debug] [FitLicense Windows] deviceId = [redacted]
Fingerprint for the current device:
[redacted]
```

6. Go to the website.

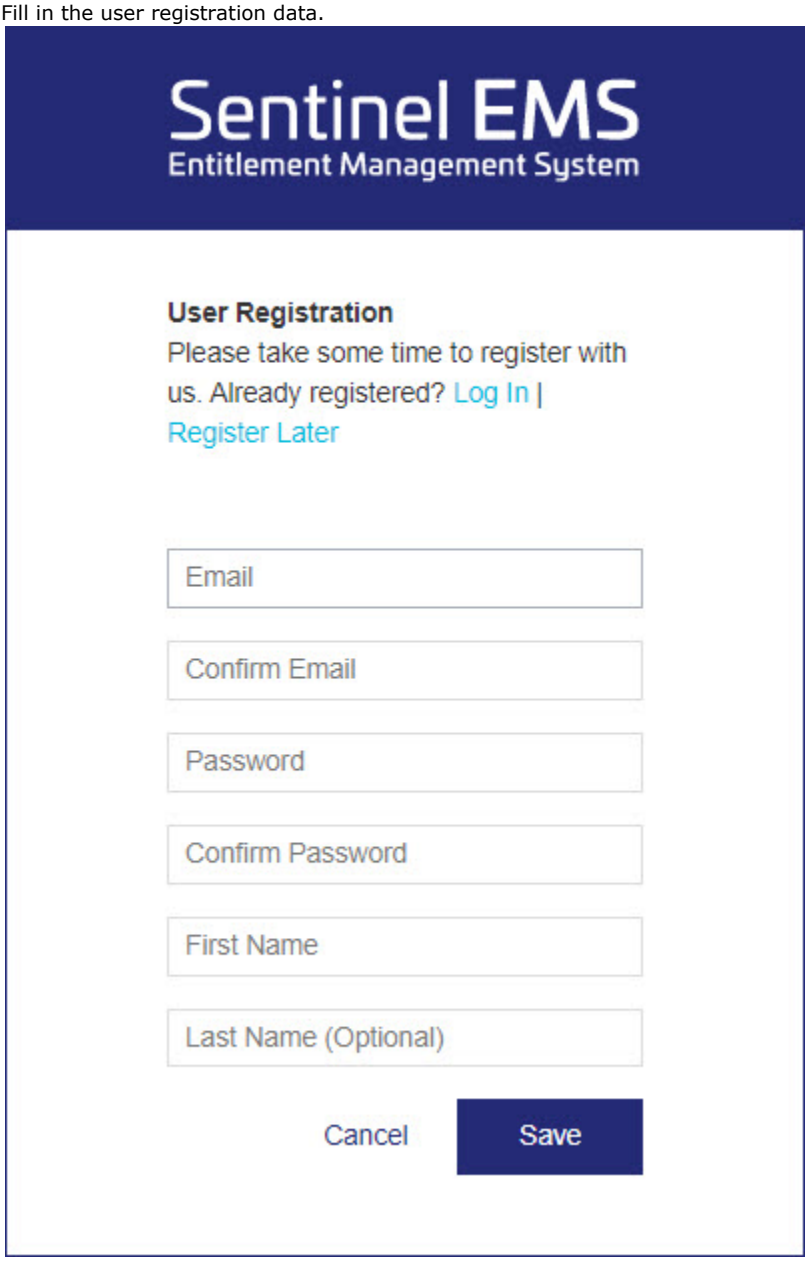
   > **Attention!**
   >
   > If you fail to log in to the website, contact the technical support.

   > Guide to the Sentinel EMS Customer Portal

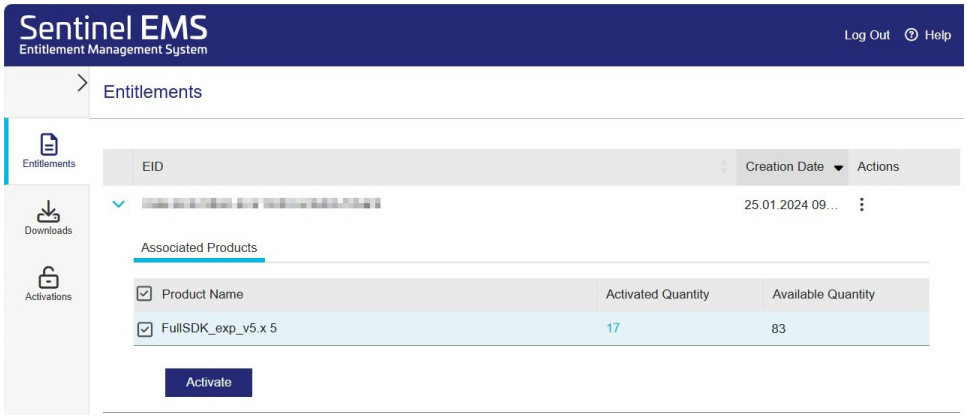
7. Log in using the received **EID**.



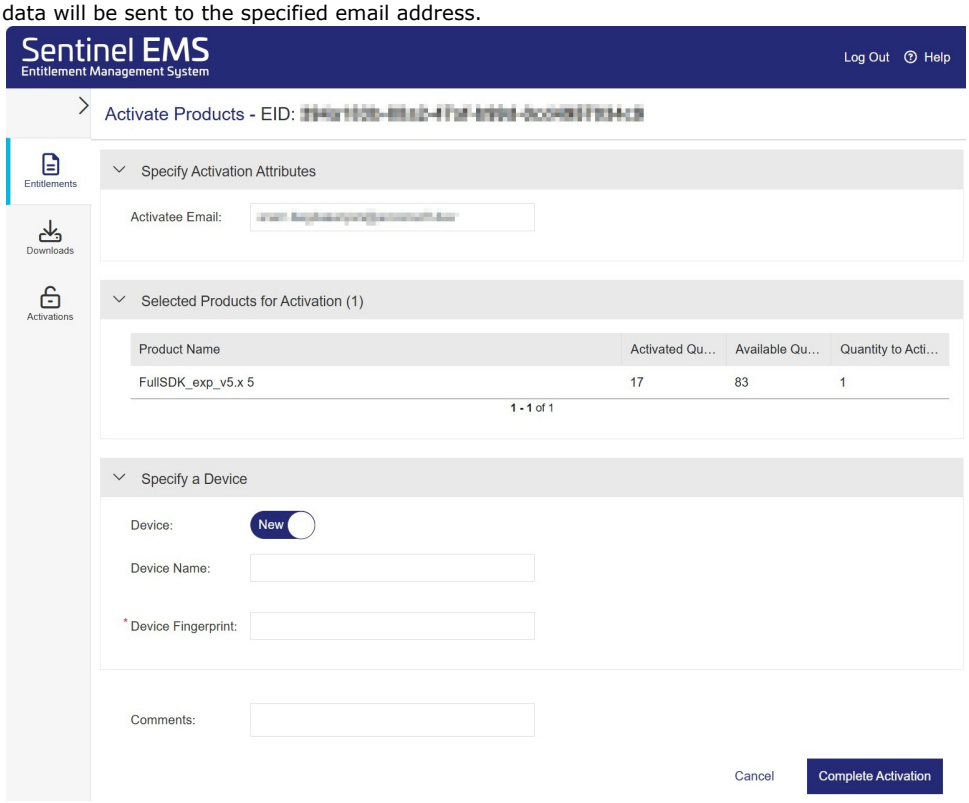
8. Fill in the user registration data.



9. Click the **Save** button.
10. Click the **Activate** button to activate the license.



11. In the **Activatee Email** field, specify the email address to confirm the license activation. The **licenseFile.v2c** file with license data will be sent to the specified email address.



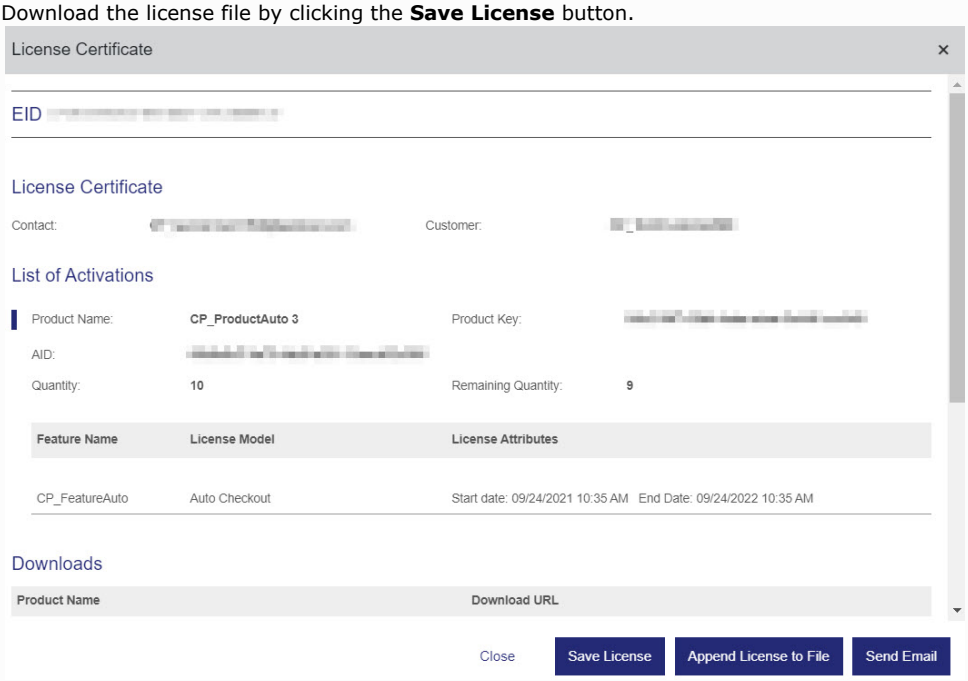
12. In the **Device FingerPrint** field, specify the **FingerPrint** data.
13. Click the **Complete Activation** button.
14. Place the downloaded **licenseFile.v2c** file on the Server in the folder: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\.
15. Make sure the license is successfully activated. If the Server is connected to the internet, the license will be checked automatically.

Note

If the Server doesn't have internet connection, do the following:

1. Do steps 2–5, 14 on the Server where the license will be used.
2. Do steps 1, 6–13, 15 on any computer connected to the internet.
3. Click the **View License Certificate** button.

4. Download the license file by clicking the **Save License** button.



The license is activated on the Server with no internet connection.

The **Object Tracker VL** license is activated.

Activating the license for the Object Tracker VL in Linux OS

> **Attention!**
>
> Starting with *Detector Pack* 3.12, a demo license has been added to the VL Analytics Pack add-on (see Installing DetectorPack add-ons). Demo license is valid for 30 days after installation on one Server or a virtual machine.

To activate a license for the **Object Tracker VL** (see Configuring the Object Tracker VL), do the following:

1. Request **EID** and **ProductID** from the technical support.

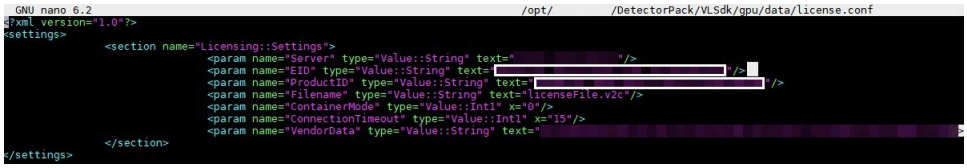
   > **Attention!**
   >
   > **EID** and **ProductID** are linked with the MAC address of the Server. If the MAC address changes, you need to request **EID** and **ProductID** again.

2. Open the **license.conf** file.

   ```
   sudo nano /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data/license.conf
   ```

3. Enter the received **EID** and **ProductID**.

   ```
   <param name="EID" type="Value::String" text="received EID"/>
   <param name="ProductID" type="Value::String" text="received ProductID"/>
   ```

4. Save the file.
5. Run the **FingerprintViewer** file. You will receive the **FingerPrint** data.

   ```
   sudo /opt/AxxonSoft/DetectorPack/VLSdk/gpu/FingerprintViewer
   ```

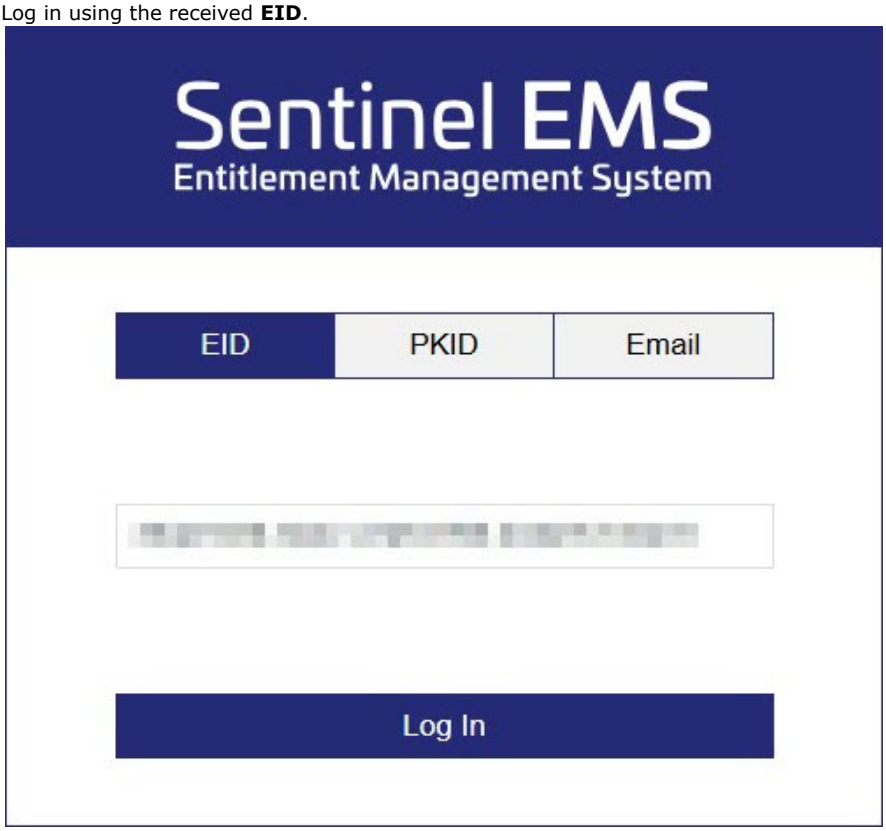
   

6. Go to the website.

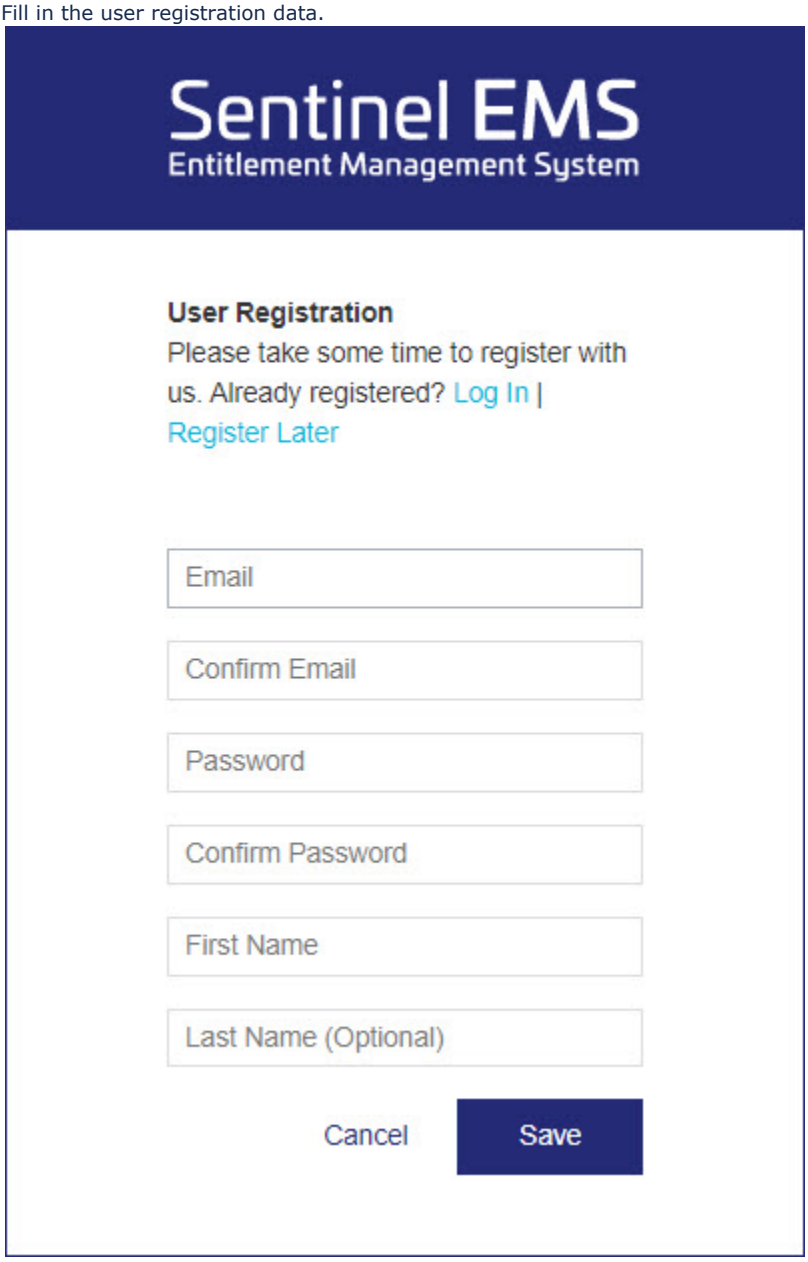
   > **Attention!**
   >
   > If you fail to log in to the website, contact the technical support.

> Guide to the Sentinel EMS Customer Portal

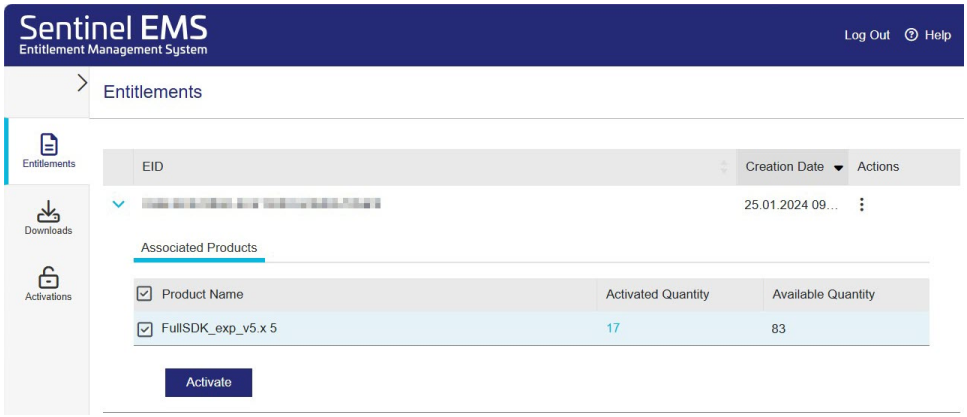
7. Log in using the received **EID**.



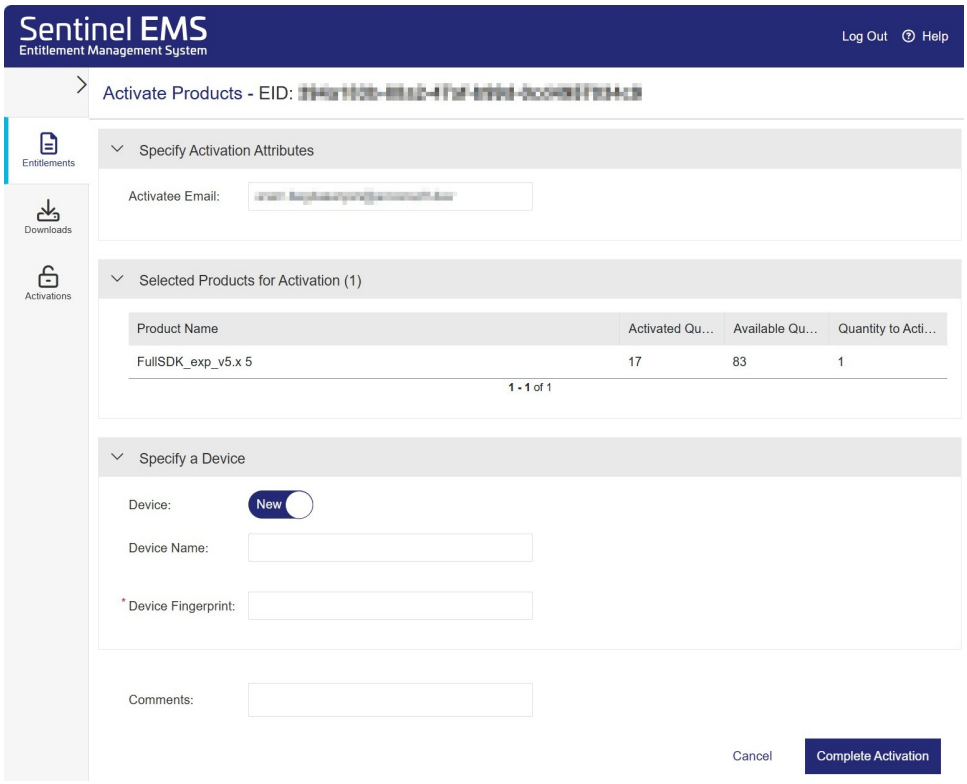
8. Fill in the user registration data.



9. Click the **Save** button.
10. Click the **Activate** button to activate the license.



11. In the **Activatee Email** field, specify the email address to confirm the license activation. The **licenseFile.v2c** file with license data will be sent to the specified email address.



12. In the **Device FingerPrint** field, specify the **FingerPrint** data.
13. Click the **Complete Activation** button.
14. Place the **licenseFile.v2c** in the required directory.

```
sudo cp /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data/licenses-archive/license.conf /opt/AxxonSoft
/DetectorPack/VLSdk/gpu/data/license.conf
```

15. Activate the license.

```
sudo /opt/AxxonSoft/DetectorPack/VLSdk/gpu/FingerprintViewer /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data
/license.conf
```

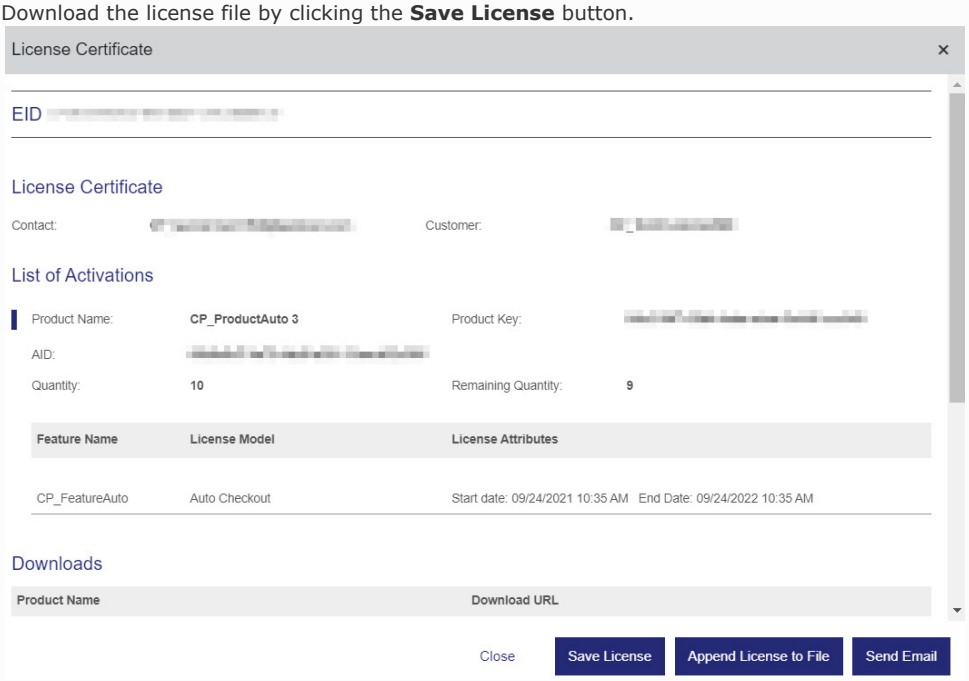
16. Make sure the license is successfully activated. If the Server is connected to the internet, the license will be checked automatically.

Note

If the Server doesn't have an internet connection, do the following:

1. Do steps 2–5, 14–15 on the Server where the license will be used.
2. Do steps 1, 6–13, 16 on any computer connected to the internet.
3. Click the **View License Certificate** button.

4. Download the license file by clicking the **Save License** button.



The license is activated on the Server with no internet connection.

The **Object Tracker VL** license is activated.

Configuring the Object Tracker VL

Video stream and scene requirements for the Object Tracker VL and its sub-tools

Image requirements for the Object Tracker VL and its sub-tools

Hardware requirements for neural analytics operation

Activating the license for the Object Tracker VL in Windows OS

Activating the license for the Object Tracker VL in Linux OS

To configure the **Object Tracker VL**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Object Tracker VL**.

By default, the detection tool is enabled and set to detect people in the frame and generate events.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

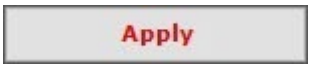
Parameter	Value	Description
Object features		
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. **Attention!** To ensure the correct display of streams on a multi-stream camera, all video streams must have the same frame aspect ratio.
Record objects tracking	**Yes** **No**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value. **Attention!** To obtain metadata, the video is decompressed and analyzed, which results in a heavy load on the Server and limits the number of video cameras that can be used on it.
Other		
Enable	**Yes** **No**	The **Object Tracker VL** detection tool is enabled by default. To disable the detection tool, select the **No** value
Name	**Object Tracker VL**	Enter the detection tool name or leave the default name
Decoder mode	**Auto** **CPU** **GPU** **HuaweiNPU**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
Type	**Object Tracker VL**	Name of the detection tool type (non-editable field)
Advanced settings		
Frame size	**640**	Select the resolution to which the video will be compressed before analysis

change	**960** **1280** **1920** **2560** **3840** **5120** **7680** **15360**	
Number of frames without detections	**18**	Specify the number of frames without objects detection. If no object is detected in the designated area, the neural network algorithm will continue to process the specified number of frames before it considers the track lost and terminated. The value must be in the range [1, 10 000]
Number of frames between detections	**7**	Specify the number of frames between detections. The lower the value, the higher the probability that the neural network algorithm will detect a new object as soon as it appears in the designated area. The value must be in the range [1, 10 000]
Minimum number of detections	**1**	Specify the minimum number of detections after which a track will be considered a detected object. The value must be in the range [1, 10 000]
Basic settings		
Minimum threshold of object authenticity	**60**	Specify the minimum threshold of object authenticity in percent, at which an object is considered detected. The higher the value, the fewer objects are detected, but the more reliable the detected objects are. The value must be in the range [1, 100]
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Huawei NPU**	Select a processor for the detection tool operation (see Selecting Nvidia GPU when configuring detection tools). **Attention!** If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.

If necessary, in the preview window, set an area of the frame, in which you want to detect objects. You can specify the area by moving the anchor points (see Configuring the Detection Zone).

Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- To hide detection area, click the button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

The **Object Tracker VL** is configured. If necessary, you can create and configure the necessary sub-tools on the basis of the **Object Tracker VL** (see Standard detection sub-tools).

Configuring the Object Tracker VL sub-tools

Configuring the Object Tracker VL standard detection sub-tools

Configuration of the standard detection sub-tools of the **Object Tracker VL** is described in the Standard detection sub-tools section.

Stopped object detector

Functions of the Stopped object detector

Description	The **Stopped object detector** is used to detect stopped objects in the camera FOV
Add-ons	For the detection tool to work, you must install the Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Stopped object detector

Image requirements for the Stopped object detector

Hardware requirements for neural analytics operation

Requirements for the operation of the **Stopped object detector** are given in the table:

Camera	• Resolution must be at least 640x360 pixels. We also don't recommend using a resolution higher than 1920×1080, since higher resolution doesn't increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 • The frame rate per second in the video stream from the camera is at least 8 for solving typical tasks • Stopped object detector-based analytics works with both colorless (gray) and color images. We recommend using color cameras. When you use black-and-white cameras, the recognition quality can be noticeably worse **Attention!** Correct operation of the **Stopped object detector** isn't guaranteed when using a fisheye camera.
Lighting	• Lighting in the scene is at least 50 lux. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on) • The analyzed scene doesn't have reflective surfaces and sharp shadows from moving objects. If present, they must be masked • Camera shake doesn't result in image offsets greater than 1% of the frame size

Image requirements for the Stopped object detector

Video stream and scene requirements for the Stopped object detector

Hardware requirements for neural analytics operation

Requirements for the operation of the **Stopped object detector** are given in the table:

Object images

- The detected object must be clearly distinguishable by the human eye
- Width and height of objects in the image must not exceed 75% of the frame size
- When you use a neurofilter, the minimum width or height of an object must be at least 5% of the width/height of the frame
- The image isn't noisy and not distorted by the artifacts of compression algorithm
- The duration of the object visibility is at least six frames
- Between two frames, an object must move in the direction of a distance not exceeding its size. This condition is necessary for the correct calculation of object track
- The minimum value of pixel density per meter is observed:

Image resolution	Object type	Minimum pixel density per meter (ratio of the object width in pixels to the object width in meters)	Minimum object size in pixels, width x height	Ratio of the object width to the frame width as a percentage
1920x1080	Human	55	~25x105	~3%
1280x720	Human	35	~17x70	~3%
640x360	Human	17	~10x42	~3%
1920x1080	Light vehicle (2 axles)	55	~354x300	~20%
1280x720	Light vehicle (2 axles)	35	~240x205	~20%
640x360	Light vehicle (2 axles)	17	~132x112	~20%

Configuring the Stopped object detector

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Stopped object detector

Image requirements for the Stopped object detector

To configure the **Stopped object detector**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Stopped object detector**.

By default, the detection tool is enabled and set to detect stopped objects.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes** **No**	By default, metadata are recorded into the database. To disable metadata recording, select the **No** value. **Attention!** To obtain metadata, video is decompressed and analyzed, which results in a heavy load on the Server and limits the number of cameras that you can use on it.
Video stream	**Main stream** **Second stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server
Other		
Enable	**Yes** **No**	By default, the detection tool is enabled. To disable, select the **No** value
Name	**Stopped object detector**	Enter the detection tool name or leave the default name
Decoder mode	**Auto** **CPU** **GPU** **Huawei NPU**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
Type	**Stopped object detector**	Name of the detection tool type (non-editable field)
Basic settings		
Detection threshold	**30**	Specify the **Detection threshold** for objects in percent. If the recognition probability falls below the specified value, the data will be ignored. The higher the value, the higher the accuracy, but some events from the detection tool may not be considered. The value must be in the range [1, 100]
Neurotracker mode	**CPU** **Nvidia GPU 0**	Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

	Nvidia GPU 1 **Nvidia GPU 2** **Nvidia GPU 3** **Intel GPU** **Intel HDDL (not supported)** **Huawei NPU**	**Attention!** • It may take several minutes to launch the algorithm on Nvidia GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS). • Starting with *Detector Pack* 3.11, Intel HDDL is not supported.
Object type	**Person** **Person (top-down view)** **Person (top-down view Nano)** **Person (top-down view Medium)** **Person (top-down view Large)** **Vehicle** **Person and vehicle (Nano)** **Person and vehicle (Medium)** **Person and vehicle (Large)**	Select the recognition object. • **Nano**—low accuracy, low processor load. • **Medium**—medium accuracy, medium processor load. • **Large**—high accuracy, high processor load
Advanced settings		
Wait time	**3**	Specify the waiting time for the reappearance of a disappeared stopped object in seconds. The value must be in the range [1, 60]
Stop time	**5**	Specify the time in seconds after which the object will be considered stopped. The value must be in the range [1, 60]

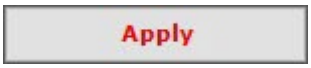
Selected object class		If necessary, specify the class of the detected object. If you want to display tracks of several classes, specify them separated by a comma with a space. For example, **1**, **10**. The numerical values of classes for the embedded neural networks: **1**—Human/Human (top-down view), **10**—Vehicle. *a.* If you leave the field blank, the tracks of all available classes from the neural network will be displayed (**Object type**, **Neural network file**). *b.* If you specify a class/classes from the neural network, the tracks of the specified class/classes will be displayed (**Object type**, **Neural network file**). *c.* If you specify a class/classes from the neural network and a class/classes missing from the neural network, the tracks of a class/classes from the neural network will be displayed (**Object type**, **Neural network file**). *d.* If you specify a class/classes missing from the neural network, the tracks of all available classes from the neural network will be displayed (**Object type**, **Neural network file**) **Note** Starting with *Detector Pack* 3.10.2, if you specify a class/classes missing from the neural network, the tracks won't be displayed (**Object type**, **Neural network file**).
Camera position	**Wall** **Ceiling**	To eliminate false events from the detection tool when using a fisheye camera, select the correct device location. For other devices, this parameter is irrelevant
Neural network file		If you use a custom neural network, select the corresponding file. **Attention!** • To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training). • A trained neural network for a particular scene allows you to detect only objects of a certain type (for example, a person, a cyclist, a motorcyclist, and so on). • If the neural network file is not specified, the default file will be used, which is selected automatically depending on the selected object type (**Object type**) and the selected processor for the neural network operation (**Decoder mode**). If you use a custom neural network, enter a path to the file. The selected object type is ignored when you use a custom neural network. • To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. • If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%. The standard neural networks are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory.

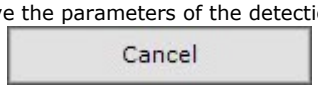
By default, the entire frame is a detection area. If necessary, in the preview window, set detection areas with the help of anchor points  (see Configuring a detection area).

Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

The **Stopped object detector** is configured.

Motion detection

Functions of the Motion detection

Description	The **Motion detection** is based on detecting differences between the current frame and the static background, and it generates an event when there is a movement in the camera FOV. You can use the metadata from the **Motion detection** to operate its sub-tools (see Standard detection sub-tools) **Attention!** • If you plan to use the metadata of the **Motion detection** for forensic search in archive (see Forensic Search for Fragments (MomentQuest)), you may need to update the license file. Contact a manager of AxxonSoft to get a detailed information and a license file. • You cannot determine the object type and color based on metadata from the **Motion detection**.

Video stream and scene requirements for the Motion detection and its sub-tools

Image requirements for the Motion detection and its sub-tools

Requirements for the operation of the **Motion detection** and its sub-tools are given in the table:

Camera	• Camera shake must not result in image offsets greater than 1% of the frame size
Lighting	• Moderate lighting. In conditions of insufficient (night) or excessive lighting (light-striking), the quality of analytics performance can decrease • No abrupt changes in lighting

Scene and camera angle	• Moving objects are visually separable from each other
	• The background is mostly static and doesn't change abruptly
	• Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on)
	• Analytics may not work correctly if:
	  ○ the analyzed scene have reflective surfaces and sharp shadows from moving objects
	  ○ there are extended monochromatic objects in the frame

Some requirements depend on whether you use the **Motion detection** only or its sub-tools (see Standard detection sub-tools). The difference in requirements is shown in the table:

Requirements	Motion detection	Motion detection sub-tools
Resolution in pixels	At least 320x240	At least 640x360
FPS	At least 1	At least 6
Work with image	Analytics only works with color images	Analytics works with both gray and color images

Image requirements for the Motion detection and its sub-tools

Video stream and scene requirements for the Motion detection and its sub-tools

Requirements for the operation of the **Motion detection** and its sub-tools are given in the table:

Object images	• Image isn't noisy and isn't distorted by artifacts of the compression algorithm • The speed of object movement in the image must not be less than 1 pixel per second • For the object to be detected, the duration of its visibility must be at least 8 frames • When the object moves between two adjacent frames in a certain direction, its distance of movement must not exceed its size. This condition is necessary for the correct calculation of the object's trajectory (track)

Some requirements depend on whether you use the **Motion detection** only or its sub-tools (see Standard detection sub-tools). The difference in requirements is shown in the table:

Requirements	Motion detection	Motion detection sub-tools
Size of objects in the image	The width and height of the objects in the image must be not less than 1% of the frame size (if resolution is over 704x576 pixels) or 15 pixels for lower resolution	The width or height of the objects in the image must be not less than 1% of the frame size (if resolution is over 1920x1080 pixels) or 15 pixels for lower resolution

Configuring the Motion detection

Video stream and scene requirements for the Motion detection and its sub-tools

Image requirements for the Motion detection and its sub-tools

To configure the **Motion detection**, do the following:

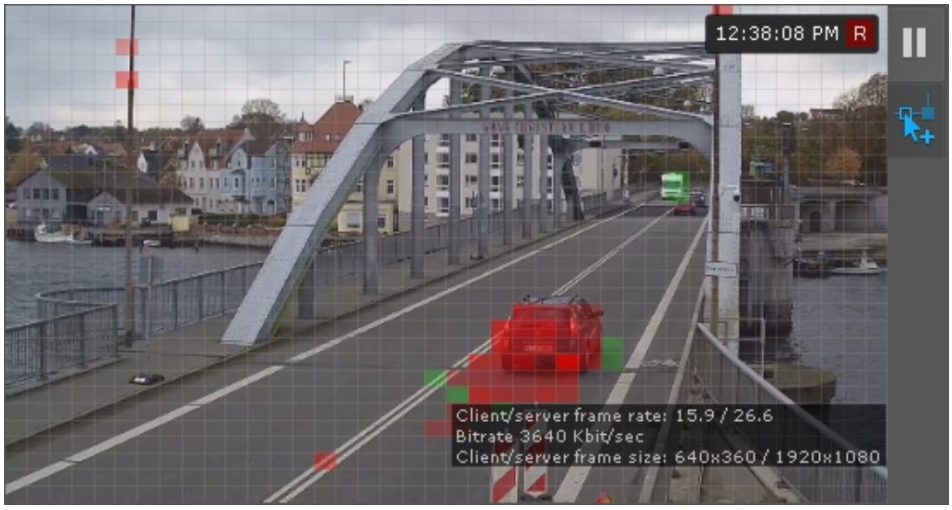
1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Motion detection**.

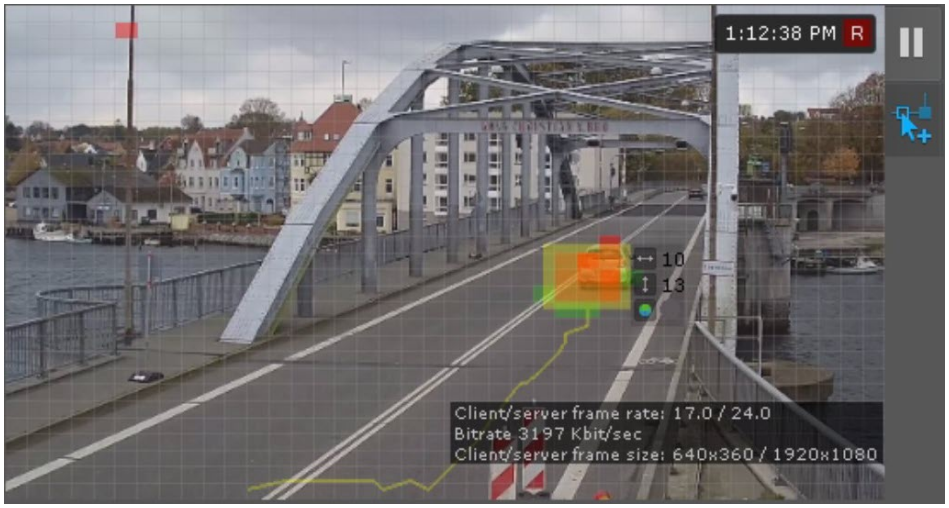
The **Motion detection** is based on detecting differences between the current frame and the static background, and it generates an event when there is a movement in the camera FOV.

You can set a number of parameters for all sub-tools of the **Motion detection** at the same time.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes** **No**	By default, mask is recorded to the archive. To disable the parameter, select the **No** value
Record objects tracking	**Yes** **No**	By default, object tracks are recorded to the database. To disable the parameter, select the **No** value. **Attention!** To obtain metadata, video is decompressed and analyzed, which results in a heavy load on the Server and limits the number of cameras that you can use on it.
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server. **Attention!** To ensure the correct display of streams on a multi-stream camera, all video streams must have the same frame aspect ratio.
Other		
Enable	**Yes** **No**	By default, the detection tool is enabled. To disable, select the **No** value
Name	**Motion detection**	Enter the detection tool name or leave the default name
Decode key frames	**Yes**	By default, the parameter is disabled. This parameter reduces the load on the Server, but at the same time the detection quality decreases. If you want to decode key frames only, select the **Yes** value. We recommend enabling this parameter for "blind" (without video image display) Servers, on which you want to perform detection. For the MJPEG codec decoding isn't relevant, as each frame is considered a key frame. **Attention!** The **Number of frames processed per second** and **Decode key frames** parameters are interrelated. If a local Client isn't connected to the Server, the following rules work for remote Clients:

	No	• If the key frame rate is less than the value specified in the **Number of frames processed per second** field, the detection tool will work by key frames. • If the key frame rate is greater than the value specified in the **Number of frames processed per second** field, the detection will be performed according to the set period. If a local Client is connected to the Server, the detection tool will always work according to the set period. After disconnecting the local Client, the above rules will be relevant again.
Decoder mode	**Auto** **CPU** **GPU** **Huawei NPU**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
Type	**Motion detection**	Name of the detection tool type (non-editable field)
Advanced settings		
Alarm end delay	**10**	Enter the time in seconds during which the generation of an event won't stop after the motion stops. If motion is detected again within the specified time, it will be considered as one event
Camera position	**Wall** **Ceiling**	To eliminate false events from the detection tool when using a fisheye camera (see Configuring fisheye cameras), select the correct device location
Motion mask	**Yes** **No**	By default, motion mask is enabled.  • If motion doesn't exceed the **Sensitivity: Contrast** and **Sensitivity: Size** parameters, the mask cells are colored green. • If motion generates an event, the cells are colored red. To disable the parameter, select the **No** value.
Object tracking	**Yes**	By default, the parameter is disabled. Select the **Yes** value to operate the detection sub-tools, and to display tracks and parameters (width and height as a percentage of the frame width or height and color) of tracking objects in the preview window:

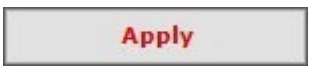
	No	
Basic settings		
Sensitivity: Contrast	**12**	Specify the values of sensitivity to contrast and object size depending on the scene in the frame: • **Sensitivity: Contrast**. The value must be in the range [0, 20] • **Sensitivity: Size**. The value must be in the range [0, 20] By default, the values of medium sensitivity are used. These values are recommended for most scenes: • **Sensitivity: Contrast**—**12**. • **Sensitivity: Size**—**9**. If objects are far away and small in size, the maximum sensitivity is required. Recommended values: • **Sensitivity: Contrast**—**16**. • **Sensitivity: Size**—**10**. If camera is located indoors with a distance to objects of about four meters, the minimum sensitivity is required. Recommended values: • **Sensitivity: Contrast**—**8**. • **Sensitivity: Size**—**8**.
Sensitivity: Size	**9**	

By default, the entire frame is a detection area. If necessary, you can specify one or more areas within which no detection will be performed (see Configuring a skip area).

Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuration of the **Motion detection** is complete. If necessary, you can create and configure the necessary sub-tools on the basis of the **Motion detection** (see Standard detection sub-tools).

Privacy Masking

Functions of the Privacy Masking

Description	The **Privacy Masking** allows you to hide moving objects in the video. When you use a neural network in the **Privacy Masking** operation, the accuracy of working with moving objects improves, and stationary objects are hidden as well
Add-ons	For the detection tool to work, you must install the Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Privacy Masking

Image requirements for the Privacy Masking

Hardware requirements for neural analytics operation

Requirements for the operation of the **Privacy Masking** are given in the table:

Camera	• Resolution is at least 320x240 pixels • FPS is at least 1 • Camera shake doesn't result in image offsets greater than 1% of the frame size
Lighting	• Moderate lighting. In conditions of insufficient (night) or excessive lighting (light-striking), the quality of analytics performance can decrease • No abrupt changes in lighting

Scene and camera angle	• Moving objects are visually separable from each other
	• Background is mostly static and doesn't change abruptly
	• Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on)
	• Analytics may not work correctly if:
	  ○ the analyzed scene have reflective surfaces and sharp shadows from moving objects
	  ○ there are extended monochromatic objects in the frame

Image requirements for the Privacy Masking

Video stream and scene requirements for the Privacy Masking

Hardware requirements for neural analytics operation

Requirements for the operation of the **Privacy Masking** are given in the table:

Object images	• Image isn't noisy and isn't distorted by artifacts of the compression algorithm
	• The width and height of objects in the image must not:
	  ◦ be less than 1% of the frame size (at resolutions no less than 1920x1080 pixels) or 15 pixels (at lower resolutions)
	  ◦ exceed 75% of the frame size
	• The speed of movement of objects in the image must not be less than 1 pixel per second
	• For the object to be detected, the duration of its visibility must be at least 8 frames

Configuring the Privacy Masking

Video stream and scene requirements for the Privacy Masking

Image requirements for the Privacy Masking

Hardware requirements for neural analytics operation

To configure the **Privacy Masking**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Trackers Privacy Masking**.

By default, the detection tool is enabled and set to hide stationary objects.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, mask is recorded to the archive. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server. **Attention!** To ensure the correct display of streams on a multi-stream camera, all video streams must have the same frame aspect ratio.
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Privacy Masking**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei iNPU	
Type	**Privacy Masking**	Name of the detection tool type (non-editable field)
Basic settings		
Detection threshold	**15**	Specify the **Detection threshold** for objects in percent. If the recognition probability falls below the specified value, the data will be ignored. The higher the value, the higher the sensitivity to recognizing and masking objects. The value must be in the range [5, 100]
Neural network mode	**CPU**	Select a processing resource for neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). **Attention!** • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
	Nvidia GPU 0	
	Nvidia GPU 1	

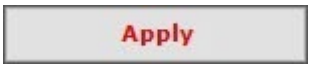
	Nvidia GPU 2 **Nvidia GPU 3** **Intel NCS (not supported)** **Intel HDDL (not supported)** **Intel GPU** **Huawei NPU**	• It may take several minutes to launch the algorithm on Nvidia GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS). • Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.
Neural network filter		
Neural network	**Yes** **No**	By default, the parameter is disabled. The detection tool works on the basis of an algorithm without neural network, ignoring the value specified in the **Neural network file** parameter. If the detection tool cannot correctly detect an object in the frame, select the **Yes** value. In the **Neural network file** parameter, select a custom neural network that is a privacy mask neural network. A detection tool with a neural network algorithm based on this neural network will be created
Neural network file		If you use a custom neural network, select the corresponding file. **Attention!** • To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training). • If the neural network file is not specified, the default file will be used that is selected automatically depending on the selected processor for the neural network operation (**Decoder mode**). If you use a custom neural network, enter a path to the file. • To ensure the correct operation of the neural network in Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. • If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%. The standard neural networks are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory.

By default, the entire frame is a detection area. If you want to exclude from analysis difficult areas in the camera FOV (foliage, water, and so on), specify one or more skip areas (see Configuring a skip area), within which detection won't be performed.

Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuration of the **Privacy Masking** is complete.



Attention!

Correct operation of the detection tool isn't guaranteed before 10 minutes from the moment of its creation or making any changes in the detection tool settings.

Category: Face

Face Detection VL

Functions of the Face Detection VL

Description	The **Face Detection VL** generates an event every time a face is captured in the frame. The *Axxon One* database stores all faces in binary form: 1. All captured faces are stored as biometric vectors (see Face search) in the **t_face_vector** table, and their corresponding capture events are stored in the **t_json_event** table. 2. All reference faces from the lists (see Lists of faces) are stored in the **t_face_listed** table. ⚠ **Attention!** When the number of faces in the database increases, the statistical error increases: the more faces in the database, the more often similar faces are recognized when searching in the archive. Accordingly, the degree of similarity when comparing the reference face with the captured face decreases. This error is relevant if: 1. The Video stream and scene requirements for the Face Detection VL and its sub-tools are met. 2. The database contains over a million faces. An example of the error calculation results: The mugshot dataset (good quality photo), 12 million faces in the database, and probability of false matching is 0.003%. With these initial data, the researchers obtained an identification error of 0.81%.
Licensing	To operate the detection tool, contact an AxxonSoft manager and get a license file (see Types of licenses)
Add-ons	For the **Face Detection VL** to work, you must install VL Face Recognition Pack and VL SDK Pack (see Installing DetectorPack add-ons). ⚠ **Attention!** You can install only one Face Recognition Pack: either VA Face Recognition Pack/TV Face Recognition Pack or VL Face Recognition Pack. You cannot install both packages in the same system.

Hardware requirements for the Face Detection VL and its sub-tools

Hardware requirements

Hardware requirements for neural analytics operation

The **Face Detection VL** and its sub-tools require a CPU supporting the AVX2.0 instruction set.

If the **Face Detection VL** runs on GPU, the following hardware requirements must be met:

1. The detection tool can run only on NVIDIA devices with at least 6 GB of video memory or more. We recommend 8 GB of video memory or more.
2. NVIDIA driver version is 452.39 or higher.
3. Compute Capability 6.1 or higher.

> **Note**
>
> You can check the GPU Compute Capability version on the manufacturer's website.

Video stream and scene requirements for the Face Detection VL and its sub-tools

Hardware requirements for the Face Detection VL and its sub-tools

Hardware requirements for neural analytics operation

Image requirements for the Face Detection VL and its sub-tools

Requirements for the operation of the **Face Detection VL** and its sub-tools are given in the table:

Camera	• FPS is at least 12. For face recognition at turnstiles, FPS is at least 6
Lighting	• Faces must be evenly illuminated with diffused light of at least 200 lux. Directional side lighting isn't allowed • Contrast of the captured faces must be over 64 grayscale • Insufficient or excessive lighting isn't allowed • There must be no backlighting and sharp gradients of light and shade
Scene and camera angle	• Maximum angle of frontal perspective of the photos of people’s faces received from cameras must not exceed +/- 15° • Mutual faces overlapping must be minimal **Note** You can specify the required distance between the camera and the face using a lens with the required focal length.

Image requirements for the Face Detection VL and its sub-tools

Hardware requirements for the Face Detection VL and its sub-tools

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Face Detection VL and its sub-tools

Requirements for the operation of the **Face Detection VL** and its sub-tools are given in the table:

Object images	• Photos of the captured faces received from cameras must be clear. Image blurring caused by motion isn't allowed • Distance between the pupils on the photos of people’s faces received from cameras must be at least 32 pixels

Activating the license for the Face Detection VL in Windows OS

> **Attention!**
>
> Starting with *Detector Pack* 3.11, a demo license has been added to the VL Face Recognition Pack add-on (see Installing DetectorPack add-ons). Demo license is valid for 30 days after installation on one Server or a virtual machine.

To activate a license for the **Face Detection VL** (see Configuring the Face Detection VL), do the following:

1. Request **EID** and **ProductID** from the technical support.

   > **Attention!**
   >
   > **EID** and **ProductID** are linked with the MAC address of the Server. If the MAC address changes, you need to request **EID** and **ProductID** again.

2. Open the following file in a text editor: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
3. Enter the received **EID** and **ProductID**.

```
<param name="EID" type="Value::String" text="received EID"/>
<param name="ProductID" type="Value::String" text="received ProductID"/>
```

```
<?xml version="1.0"?>
<settings>
    <section name="Licensing::Settings">
        <param name="Server" type="Value::String" text="https://visionlabsbv.prod.sentinelcloud.com"/>
        <param name="EID" type="Value::String" text="                                    "/>
        <param name="ProductID" type="Value::String" text="                                    "/>
        <param name="Filename" type="Value::String" text="licenseFile.v2c"/>
        <param name="ContainerMode" type="Value::Int1" x="0"/>
    </section>
</settings>
```

4. Save the file: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
5. In the command line, run the following file as administrator: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\FingerprintViewer.exe. You will receive the **FingerPrint** data.

```
C:\Program Files\Common Files\   \DetectorPack\VLSdk\gpu>FingerprintViewer.exe
Using license file: ./data/license.conf
To run with default license file path:
        FingerprintViewer.exe
If you want to specify license file:
        FingerprintViewer.exe <path to license.conf>
[04.05.2023 09:28:42] [Debug] [createLicense] creation of the FitLicense license!
[04.05.2023 09:28:42] [Debug] [FitLicense Windows] deviceId =
Fingerprint for the current device:
```

6. Go to the website.

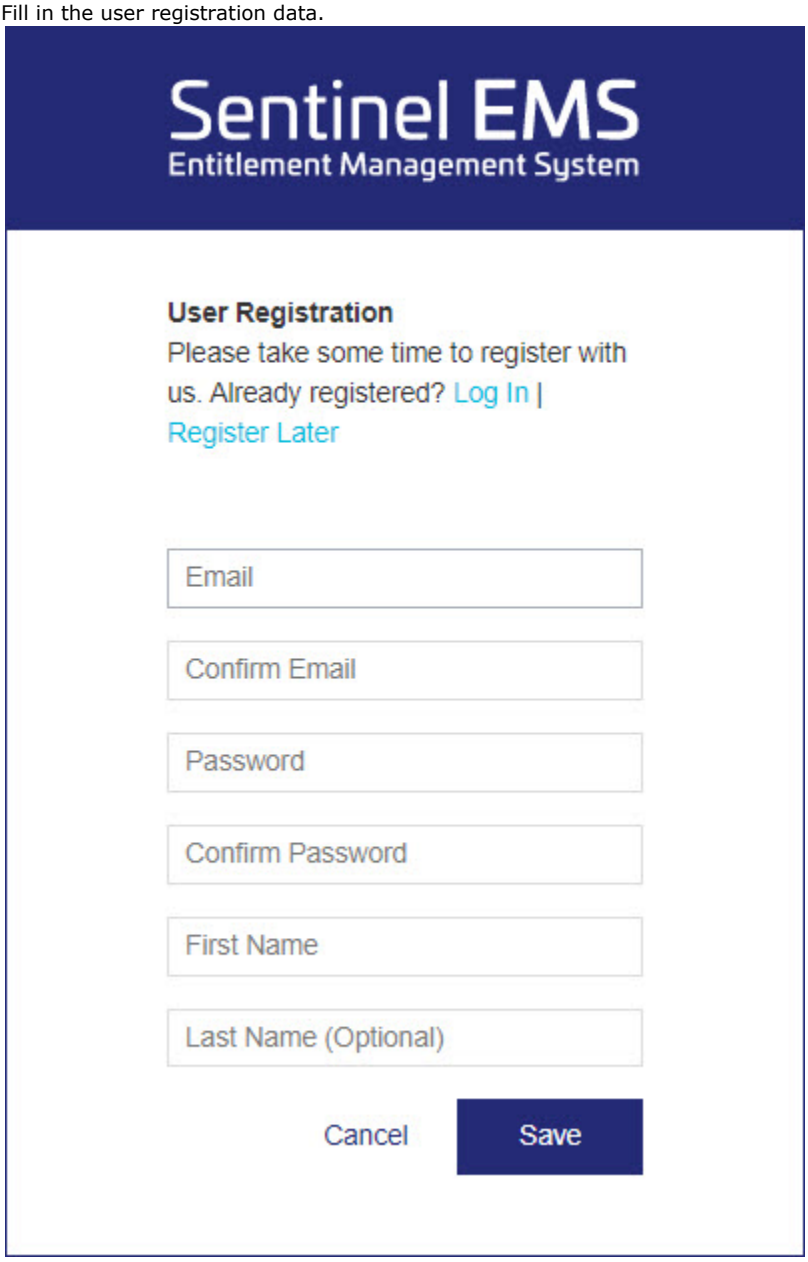
   > **Attention!**
   >
   > If you fail to log in to the website, contact the technical support.

   > Guide to the Sentinel EMS Customer Portal

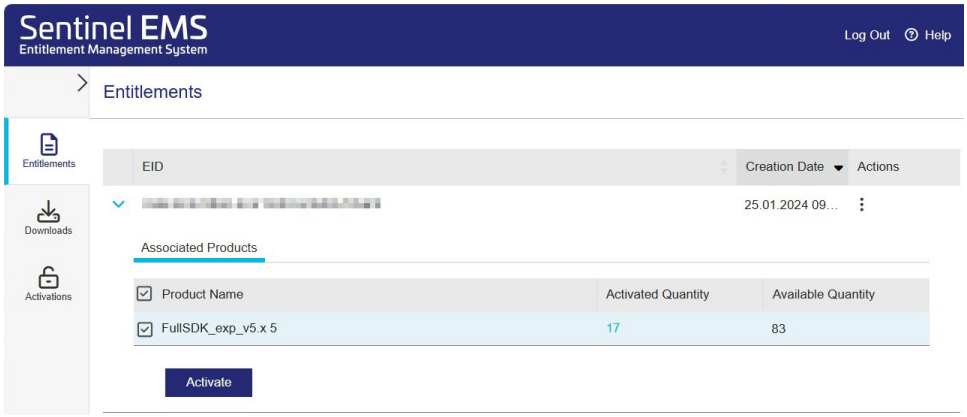
7. Log in using the received **EID**.



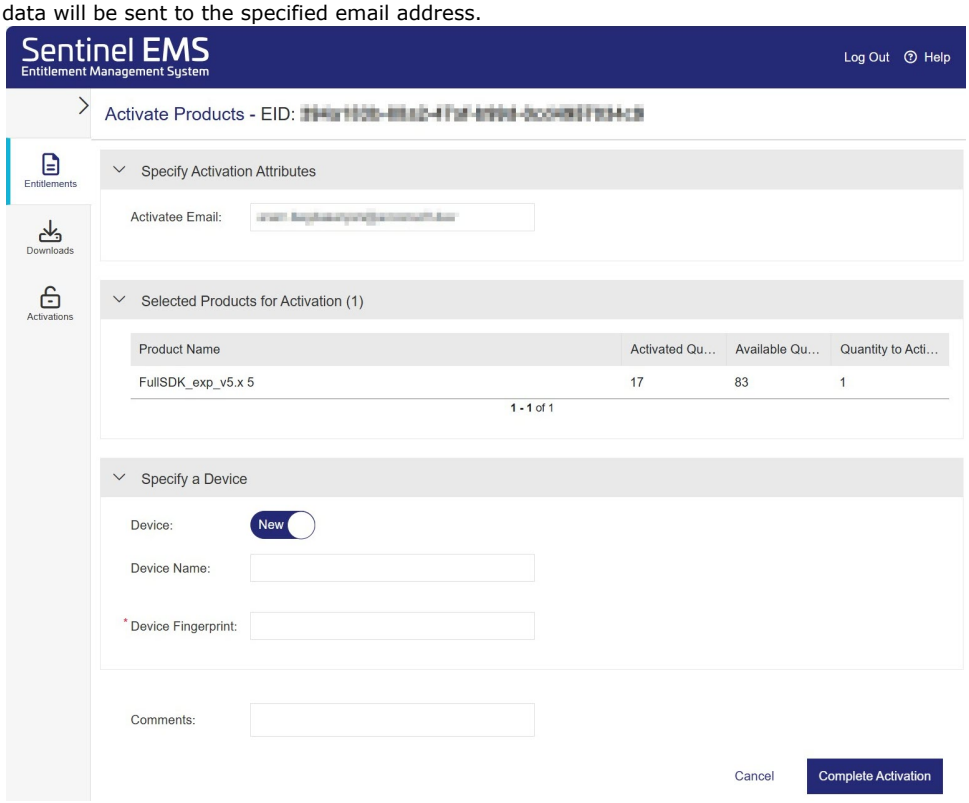
8. Fill in the user registration data.



9. Click the **Save** button .
10. Click the **Activate** button to activate the license.



11. In the **Activatee Email** field, specify the email address to confirm the license activation. The **licenseFile.v2c** file with license data will be sent to the specified email address.



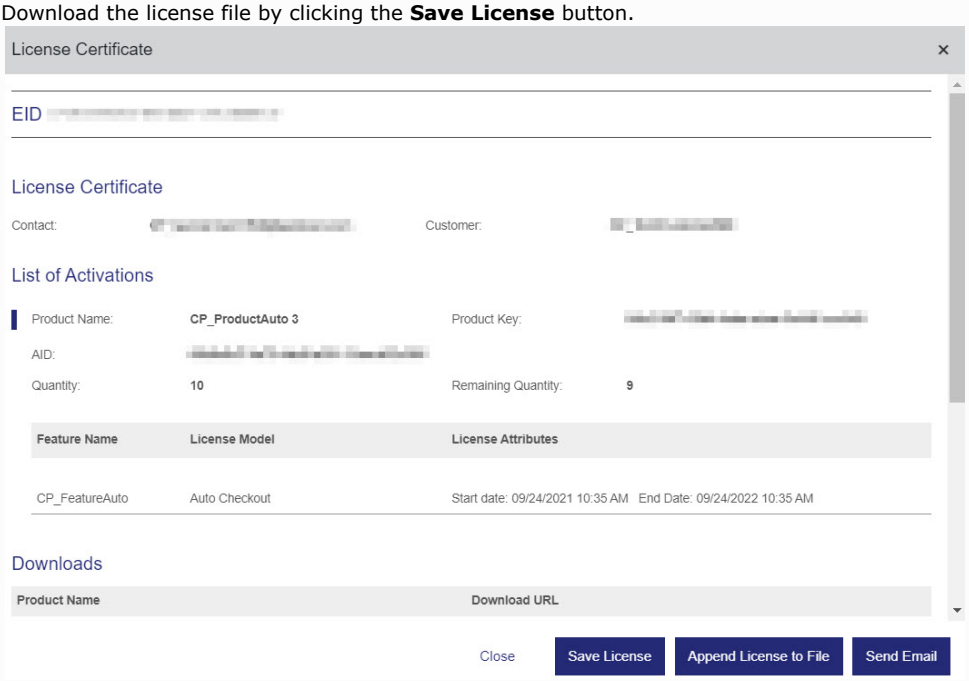
12. In the **Device FingerPrint** field, specify the **FingerPrint** data.
13. Click the **Complete Activation** button.
14. Place the downloaded **licenseFile.v2c** file on the Server in the folder: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\.
15. Make sure the license is successfully activated. If the Server is connected to the internet, the license will be checked automatically.

Note

If the Server doesn't have internet connection, do the following:

1. Do steps 2–5, 14 on the Server where the license will be used.
2. Do steps 1, 6–13, 15 on any computer connected to the internet.
3. Click the **View License Certificate** button.

4. Download the license file by clicking the **Save License** button.



The license is activated on the Server with no internet connection.

The **Face Detection VL** license is activated.

Activating the license for the Face Detection VL in Linux OS

> **Attention!**
>
> Starting with *Detector Pack* 3.11, a demo license has been added to the VL Face Recognition Pack add-on (see Installing DetectorPack add-ons). Demo license is valid for 30 days after installation on one Server or a virtual machine.

To activate a license for the **Face Detection VL** (see Configuring the Face Detection VL), do the following:

1. Request **EID** and **ProductID** from the technical support.

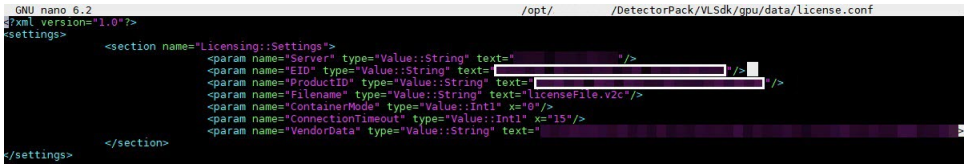
   > **Attention!**
   >
   > **EID** and **ProductID** are linked with the MAC address of the Server. If the MAC address changes, you need to request **EID** and **ProductID** again.

2. Open the **license.conf** file.

   ```
   sudo nano /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data/license.conf
   ```

3. Enter the received **EID** and **ProductID**.

   ```
   <param name="EID" type="Value::String" text="received EID"/>
   <param name="ProductID" type="Value::String" text="received ProductID"/>
   ```

4. Save the file.
5. Run the **FingerprintViewer** file. You will receive the **FingerPrint** data.

   ```
   sudo /opt/AxxonSoft/DetectorPack/VLSdk/gpu/FingerprintViewer /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data
   /license.conf
   ```

6. Go to the website.

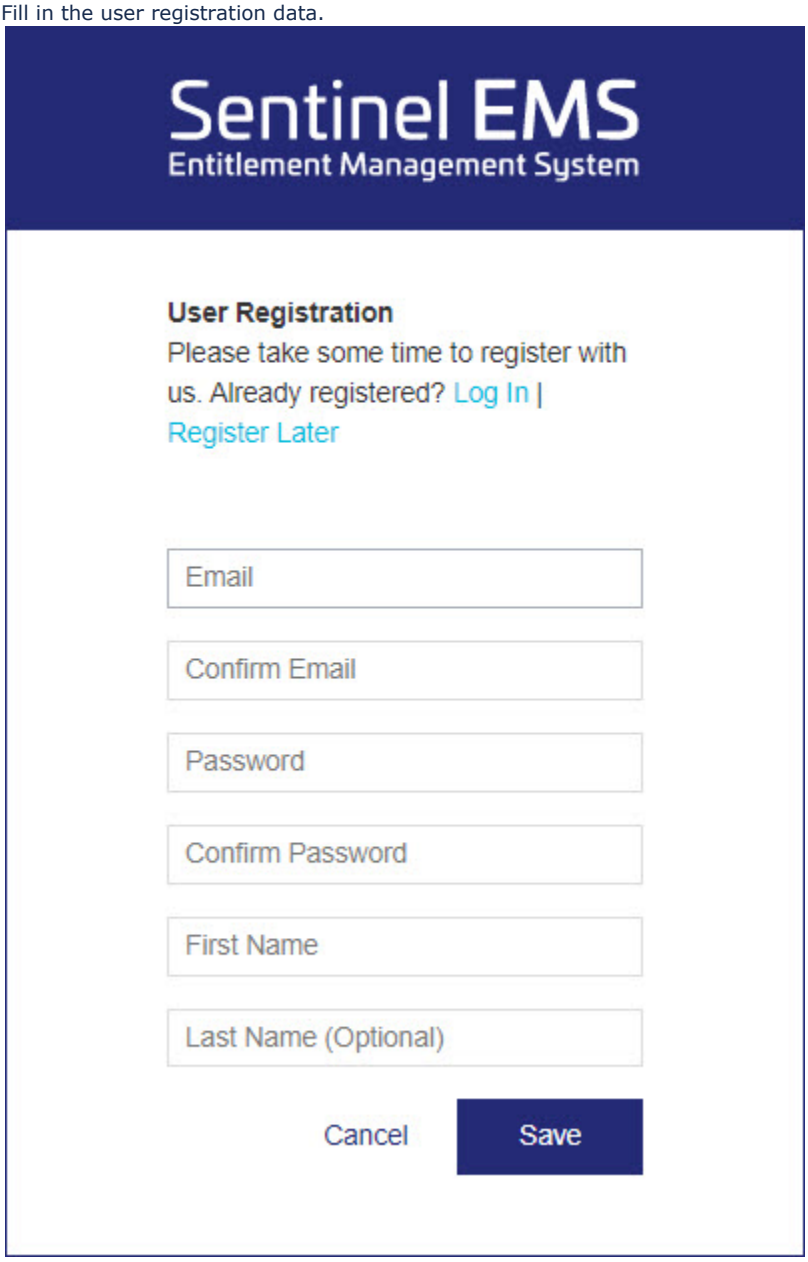
   > **Attention!**
   >
   > If you fail to log in to the website, contact the technical support.

   > Guide to the Sentinel EMS Customer Portal

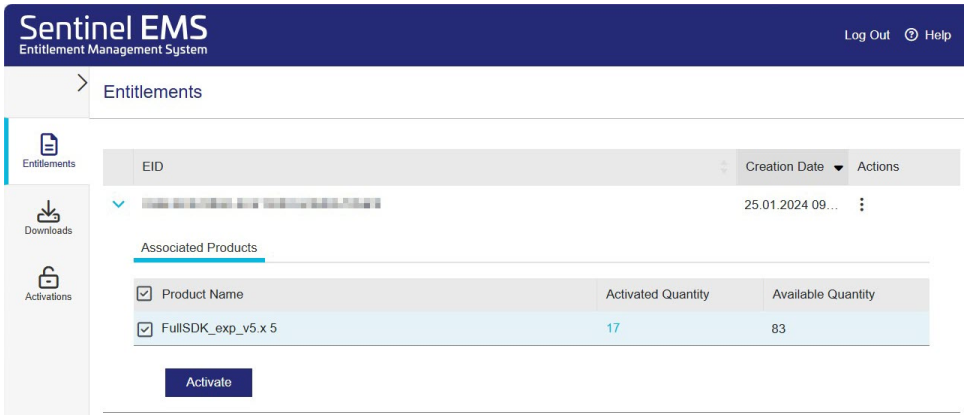
7. Log in using the received **EID**.



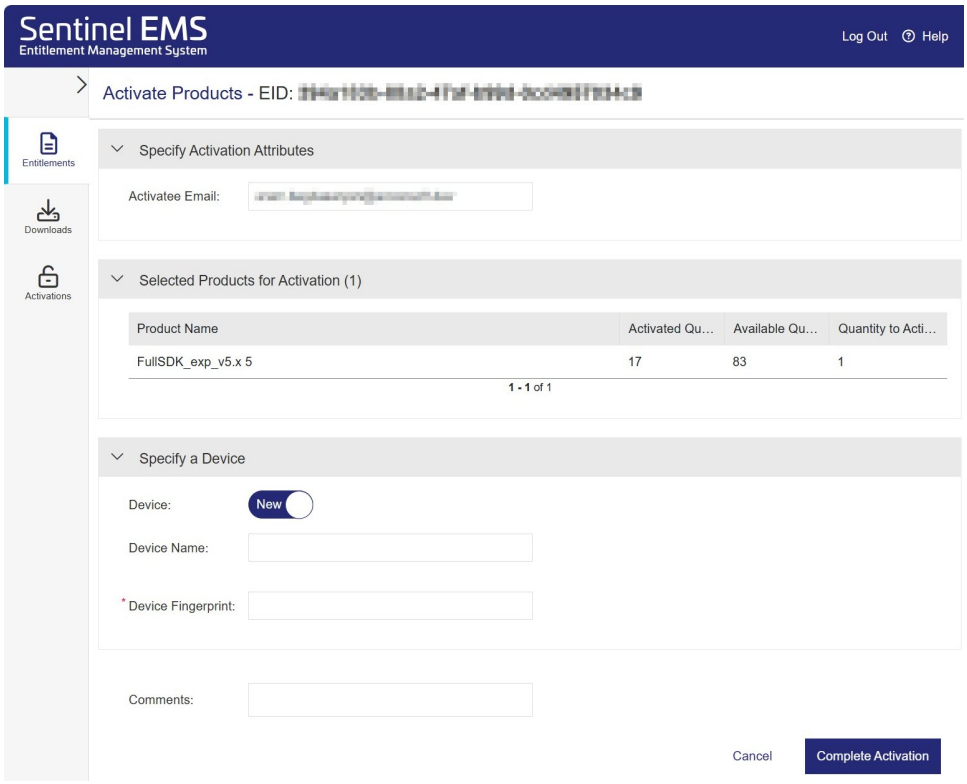
8. Fill in the user registration data.



9. Click the **Save** button.
10. Click the **Activate** button to activate the license.



11. In the **Activatee Email** field, specify the email address to confirm the license activation. The **licenseFile.v2c** file with license data will be sent to the specified email address.

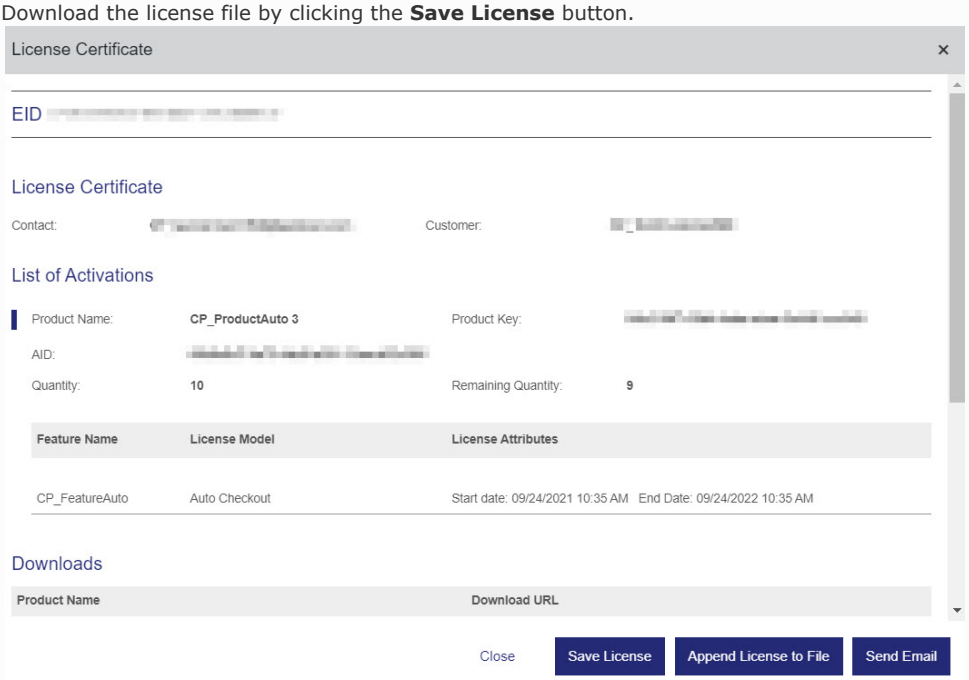


12. In the **Device FingerPrint** field, specify the **FingerPrint** data.
13. Click the **Complete Activation** button.
14. Place the **licenseFile.v2c** file in the required directory: /opt/AxxonSoft/DetectorPack/VLSdk/.
15. Make sure the license is successfully activated. If the Server is connected to the internet, the license will be checked automatically.

Note

If the Server doesn't have an internet connection, do the following:

1. Do steps 2–5, 14 on the Server where the license will be used.
2. Do steps 1, 6–13, 15 on any computer connected to the internet.
3. Click the **View License Certificate** button.
4. Download the license file by clicking the **Save License** button.



The license is activated on the Server with no internet connection.

The **Face Detection VL** license is activated.

Configuring the Face Detection VL

Hardware requirements for the Face Detection VL and its sub-tools

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Face Detection VL and its sub-tools

Image requirements for the Face Detection VL and its sub-tools

To configure the **Face Detection VL**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Face Face Detection VL**.

By default, the detection tool is enabled and set to detect faces.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes**	The **Check in lists** parameter is disabled by default. If you want to use this detection tool to check in lists of faces, select the **Yes** value (see Configuring face recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. For the correct operation of the **Face Detection VL**, we recommend using a high-quality video stream
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Face Detection VL**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	

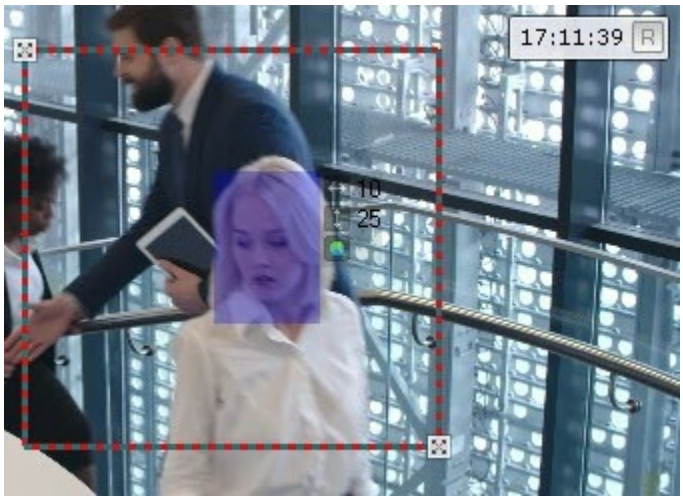
Frame size change	**640**	The analyzed frames are scaled down to a specified resolution (640 pixels on the longer side) by default. The value must be in the range [640, 10 000]. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to 1000. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
Type	**Face Detection VL**	Name of the detection tool type (non-editable field)
Use camera transform	**Yes** **No**	The **Use camera transform** parameter is disabled by default. If you use a XingYun bispherical lens (see Configuring fisheye cameras), by default the detection tool receives the image of two spheres of 180° each to analyze. In this case, the recognition quality can deteriorate. To send the dewarped image to the detection tool, select the **Yes** value. This parameter is also valid for other transformations
Advanced settings **Attention!** Advanced configuration of the detection tool must be performed only with the assistance of AxxonSoft technical experts.		
Analyze face rotation angle	**Yes** **No**	The **Analyze face rotation angle** parameter is disabled by default. If you want to detect the face rotation angle, select the **Yes** value. This parameter allows you to filter out results that have a rotation and tilt angle greater than the specified values in a search for a specific face (see Search for similar face)
Face recognition algorithm	**Algorithm 1** **Algorithm 2** **Algorithm 3**	Select the face recognition algorithm: • **Algorithm 1**—the recognition speed depends on the background and the number of faces in the frame. Works slower than **Algorithm 3**. • **Algorithm 2**—high speed, low accuracy. The recognition speed depends on the number of faces in the frame. • **Algorithm 3**—medium speed, high accuracy. The recognition speed depends on the resolution of the image. Optimal for most scenes
Face rotation pitch (°)	**45**	Specify the allowable face pitch angle in degrees. The value must be in the range [0, 90]
Face rotation roll (°)	**45**	Specify the allowable face roll angle in degrees. The value must be in the range [0, 90]
Face rotation yaw from (°)	**-45**	Specify the minimum allowable angle of face rotation to the right or left. The value must be in the range [-90, 90]
Face rotation yaw to (°)	**45**	Specify the maximum allowable angle of face rotation to the right or left. The value must be in the range [-90, 90]
Minimum image quality	**30**	Specify the minimum image quality for face detection. The value must be in the range [1, 100]

Minimum number of detections	**1**	Specify the minimum number of detections after which a track will be considered a detected face. The value must be in the range [1, 10 000]
Number of frames between detections	**3**	Specify the number of frames between detections. The lower the value, the higher the probability that TrackEngine will detect a new face as soon as it appears in the selected area. The value must be in the range [1, 10 000] **Note** TrackEngine doesn't perform face recognition. It tracks the position of one person's face in a sequence of frames, choosing the best frame and preparing the necessary data for external systems. TrackEngine is based on face detection and analysis methods provided by the FaceEngine library.
Send face images	**Yes** **No**	The **Send face images** parameter is disabled by default. If you want to send face images, select the **Yes** value
Track timeout	**2**	Specify the maximum time period in seconds after which the event will be sent. The value must be in the range [1, 10 000]
Basic settings		
Biometric data	**Yes** **No**	The **Biometric data** parameter is enabled by default. When searching for faces (see Face search), the search results will contain found faces that are similar to the attached photo or a track based on the specified minimum similarity level (percentage). If you want to keep the biometric data confidential, select the **No** value. When searching for faces (see Face search) by an attached photo or a track, there will be no results
Face attributes recognition	**Yes** **No**	The **Face attributes recognition** parameter is disabled by default. If you want to save the gender and age information for each captured face to the database, select the **Yes** value **Note** The average error in age recognition is 5 years.
Medical mask detection	**Yes** **No**	The **Medical mask detection** parameter is disabled by default. If you use mask detection, select the **Yes** value (see Masks Detection)
Minimum face size	**10**	Specify the minimum size of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum threshold of face authenticity	**60**	Specify the minimum level of face recognition accuracy for the creation of a track. You must select the relevant value empirically. We recommend specifying the value of not less than 90. The higher the value, the fewer faces are detected, while the recognition accuracy increases. The value must be in the range [1, 100]
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Huawei NPU**	Select a processor for the detection tool operation—CPU or Nvidia GPU (see Selecting Nvidia GPU when configuring detection tools) **Attention!** It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings.

Attention!

You can enable the advanced logging for SDK using the VL_SDK_VERBOSE_LOGGING=1 system variable (see Appendix 9. Creating system variable).

If necessary, in the preview window, set the rectangular area of the frame, in which you want to detect faces. You can specify the area by moving the anchor points .



Note

For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

If necessary, you can create and configure detection sub-tools on the basis of the **Face Detection VL** based on metadata (see General information on metadata):

1. Line Crossing—detection tool generates an event when a person moves across a line in the specified area of the frame and their face is detected.
2. Entrance In Area—detection tool generates an event when a person appears in the specified area of the frame and their face is detected.
3. Loitering In Area—detection tool generates an event when a person stays in the specified area of the frame for a long time and their face is detected.
4. Masks Detection—detection tool generates an event when it captures a face with or without a mask.

Face Detection VA

Functions of the Face Detection VA

Description	The **Face Detection VA** generates an event every time a face is captured in the frame. The *Axxon One* database stores all faces in binary form: 1. All captured faces are stored as biometric vectors (see Face search) in the **t_face_vector** table, and their corresponding capture events are stored in the **t_json_event** table. 2. All reference faces from the lists (see Lists of faces) are stored in the **t_face_listed** table. ⚠ **Attention!** When the number of faces in the database increases, the statistical error increases: the more faces in the database, the more often similar faces are recognized when searching in the archive. Accordingly, the degree of similarity when comparing the reference face with the captured face decreases. This error is relevant if: 1. The Video stream and scene requirements for the Face Detection VA and its sub-tools are met. 2. The database contains over a million faces. The mugshot dataset (good quality photo), 12 million faces in the database, and probability of false matching is 0.003%. With these initial data, the researchers obtained an identification error of 0.76%.
Licensing	To operate the detection tool, contact an AxxonSoft manager and get a license file (see Types of licenses)
Add-ons	For the **Face Detection VA** to work, you must install VA Face Recognition Pack (see Installing DetectorPack add-ons). ⚠ **Attention!** • You can install only one Face Recognition Pack: either VA Face Recognition Pack or VL Face Recognition Pack. You cannot install both packages in the same system. • Face Recognition Pack is guaranteed to work on Linux Debian 11 and Ubuntu 20. Face Recognition Packs isn't guaranteed to work on Linux Debian 9/10, Ubuntu 18 and Ubuntu 19 (see Operating system requirements).

Manual for switching from the Face Detection TV to Face Detection VA

Attention!

- Starting with *DetectorPack* 3.11.1, the **Face Detection TV** is no longer supported. We replaced it with the **Face Detection VA**. You cannot use the **Face Detection TV** and the **Face Detection VA** at the same time (see DetectorPack 3.11.1 Release Notes).
- After you switch from the **Face Detection TV** to the **Face Detection VA**, the results of the previously recognized persons will no longer be available. If you need to save the previously recognized persons, don't update the analytics package.
- You cannot use the previously created cache for optimizing the operation of the **Face Detection TV** on GPU. To optimize the operation of the **Face Detection VA** on GPU, you must create a new cache (see Optimizing the operation of the Face Detection VA on GPU).

To switch from the **Face Detection TV** to the **Face Detection VA**, do the following:

1. Contact an AxxonSoft manager to get a new license file with the **Face Detection VA** support.
2. Remove all previously created **Face Detection TV** tools from *Axxon One* (see Configuring detection tools and their sub-tools).
3. Go to **Control Panel Apps Apps & Features** and uninstall *DetectorPack Addon Face Recognition Pack*.
4. Install *DetectorPack: Add-ons VA Face Recognition Pack v.3.11.1* (see Installing DetectorPack add-ons).
5. Create cache for the **Face Detection VA** (see Optimizing the operation of the Face Detection VA on GPU).
6. Create and configure the required number of the **Face Detection VA** tools in *Axxon One* (see Configuring the Face Detection VA).

Switching from the **Face Detection TV** to the **Face Detection VA** is complete.

Hardware requirements for the Face Detection VA and its sub-tools

Hardware requirements

Hardware requirements for neural analytics operation

The **Face Detection VA** and its sub-tools require a CPU supporting the SSE4.2, FMA3, or AVX2.0 instruction set.

If the **Face Detection VA** runs on GPU, the following hardware requirements must be met:

1. The detection tool can run only on NVIDIA devices with at least 6 GB of video memory or more.
2. NVIDIA driver version is 418.39 or higher.
3. Compute Capability 6.0 or higher.

> **Note**
>
> You can check the GPU Compute Capability version on the manufacturer's website.

Video stream and scene requirements for the Face Detection VA and its sub-tools

Hardware requirements for the Face Detection VA and its sub-tools

Hardware requirements for neural analytics operation

Image requirements for the Face Detection VA and its sub-tools

Requirements for the operation of the **Face Detection VA** and its sub-tools are given in the table:

Camera	• FPS is at least 12. For face recognition at turnstiles, FPS is at least 6
Lighting	• Faces must be evenly illuminated with diffused light of at least 200 lux. Directional side lighting isn't allowed • Contrast of the captured faces must be over 64 grayscale • Insufficient or excessive lighting isn't allowed • There must be no backlighting and sharp gradients of light and shade
Scene and camera angle	• Maximum angle of frontal perspective of the photos of people’s faces received from cameras must not exceed +/- 15° • Mutual faces overlapping must be minimal **Note** You can specify the required distance between the camera and the face using a lens with the required focal length.

Image requirements for the Face Detection VA and its sub-tools

Hardware requirements for the Face Detection VA and its sub-tools

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Face Detection VA and its sub-tools

Requirements for the operation of the **Face Detection VA** and its sub-tools are given in the table:

Object images	• Photos of the captured faces received from cameras must be clear. Image blurring caused by motion isn't allowed • Distance between the pupils on the photos of people’s faces received from cameras must be at least 32 pixels

Optimizing the operation of the Face Detection VA on GPU

Configuring the Face Detection VA

The VA Face Recognition Pack add-on (see Installing DetectorPack add-ons) includes a utility that allows you to create GPU neural network caches without using *Axxon One*. The presence of the cache speeds up the initialization, optimizes video memory consumption and ensures the start and correct operation of the **Face Detection VA** on GPU.

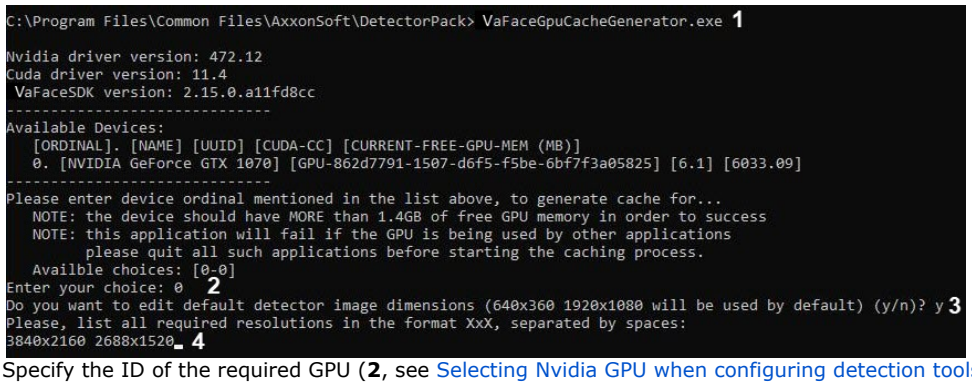
To optimize the operation of the **Face Detection VA** on GPU, do the following:

1. Stop the Server (see Shutting down a Server).

   Attention!

   If the system has the software running on GPU, it is necessary to stop its operation.

2. Create the GPU_CACHE_DIR system variable (see Appendix 9. Creating system variable) by specifying in the **Variable value** field the path to the cache location in Latin characters only. For example, D:\GPU_cache. The specified directory will store the cache for all used detection tools and neural networks.
3. Run the command line as administrator.
4. To call the utility, enter in the command line: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VaFaceGpuCacheGenerator.exe (**1**).
5. Press **Enter**.



6. Specify the ID of the required GPU (**2**, see Selecting Nvidia GPU when configuring detection tools.
7. Press **Enter**.
8. If you want to change the resolution of the video stream for the **Face Detection VA**:

   a. Enter **y** (**3**).
   b. Specify the required resolution (**4**). GPU uses the default video stream resolutions. Changing the resolution of the video stream from 1920*1080 and higher, increases the percentage of face detection.
9. Press **Enter**. The cache creation process starts. The cache creation is successful, if the result value is "0".

Optimizing the operation of the **Face Detection VA** on GPU is complete.

Attention!

The cache must be recreated in the following cases:

- if you update the VA Face Recognition Pack add-on (see Installing DetectorPack add-ons),
- if you change the Nvidia GPU model,
- if you update the Nvidia GPU drivers.

Configuring the Face Detection VA

Hardware requirements for the Face Detection VA and its sub-tools

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Face Detection VA and its sub-tools

Image requirements for the Face Detection VA and its sub-tools

Optimizing the operation of the Face Detection VA on GPU

Attention!

To start and correctly operate the **Face Detection VA** on GPU, you must create cache beforehand (see Optimizing the operation of the Face Detection VA on GPU).

To configure the **Face Detection VA**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Face Face Detection VA**.

By default, the detection tool is enabled and set to detect faces.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

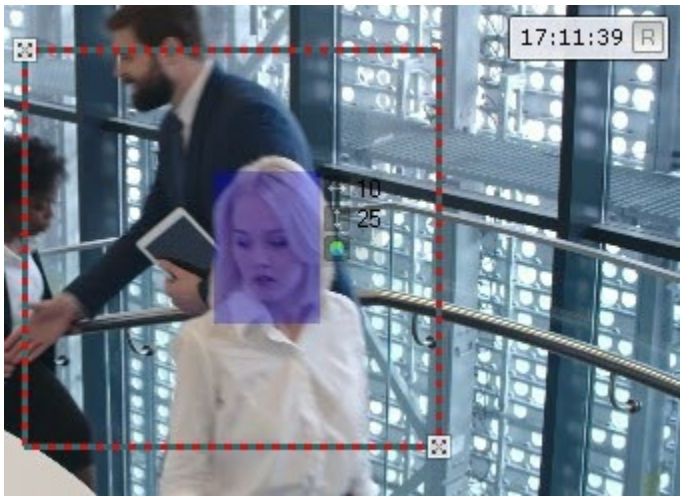
Parameter	Value	Description
Object features		
Check in lists	**Yes**	The **Check in lists** parameter is disabled by default. If you want to use this detection tool to check in lists of faces, select the **Yes** value (see Configuring face recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. For the correct operation of the **Face Detection VA**, we recommend using a high-quality video stream
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Face Detection VA**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Liveness detection	**Yes**	The **Liveness detection** parameter is disabled by default. Liveness detection is used when there is a photo of a face instead of an alive person. If you want to save to the database the information about whether each captured face is a photo (Yes/No), select the **Yes** value
	No	

Liveness threshold	**30**	Specify the threshold value in percent at which a face is defined as "not alive". The higher the value, the fewer captured faces will be detected as a photo. At the same time, the quality of recognizing whether the captured face is a photo (Yes/No) will be higher. You must select the relevant value empirically. The value must be in the range [1, 100]
Type	**Face Detection VA**	Name of the detection tool type (non-editable field)
Use camera transform	**Yes** **No**	The **Use camera transform** parameter is disabled by default. If you use a XingYun bispherical lens (see Configuring fisheye cameras), by default the detection tool receives the image of two spheres of 180° each to analyze. In this case, the recognition quality can deteriorate. To send the dewarped image to the detection tool, select the **Yes** value. This parameter is also valid for other transformations
Advanced settings **Attention!** Advanced configuration of the detection tool must be performed only with the assistance of AxxonSoft technical experts.		
Analyze face rotation angle	**Yes** **No**	The **Analyze face rotation angle** parameter is disabled by default. If you want to detect the face rotation angle, select the **Yes** value. This parameter allows you to filter out results that have a rotation and tilt angle greater than the specified values in a search for a specific face (see Search for similar face)
Face detection algorithm	**ALG1 (high speed, low accuracy)** **ALG2 (medium speed, medium accuracy)** **ALG3 (low speed, high accuracy)**	Select the face detection algorithm
Face detection period (msec)	**250**	Specify the time in milliseconds between face search operations in a frame. The larger the value, the less load on the Server, but some faces may not be recognized. The value must be in the range [1, 10 000]
Face rotation pitch (°)	**45**	Specify the allowable face pitch angle in degrees. The value must be in the range [0, 90]
Face rotation roll (°)	**45**	Specify the allowable face roll angle in degrees. The value must be in the range [0, 90]
Face rotation yaw from (°)	**-45**	Specify the minimum allowable angle of face rotation to the right or left. The value must be in the range [-90, 90]
Face rotation yaw to (°)	**45**	Specify the maximum allowable angle of face rotation to the right or left. The value must be in the range [-90, 90]
	Yes	

False mask detections filtering	**No**	The **False mask detections filtering** parameter is enabled by default. If you don't need to use the parameter, select the **No** value
Filter false alarms	**Yes** **No**	In some cases, the detection tool may mistake other objects for a face. The **Filter false alarms** parameter is enabled by default. If the parameter is enabled, false results of the face recognition will appear in the detection feed (see Face recognition and search), but they will be ignored when searching for faces in the archive. This parameter filters out objects that are not faces at the stage of face vector construction and its recording to the metadata database. If you don't need to use this parameter, select the **No** value
Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The value must be in the range [640, 10 000]. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to 1000. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
Ignore repeated recognitions	**Yes** **No**	The **Ignore repeated recognitions** parameter is disabled by default. If you want to ignore repeated recognitions of the same face, select the **Yes** value
Minimum face masking threshold	**70**	Specify the minimum threshold for recognizing the mask on the face. You must select the relevant value empirically. We recommend specifying the value of not less than 70. The value must be in the range [1, 100]
Minimum face quality for face mask detection	**30**	Specify the minimum quality of the face image when recognizing masks (see Masks Detection). You must select the relevant value empirically. We recommend specifying the value of not less than 30. The value must be in the range [1, 100]
Minimum face recognition quality	**50**	Specify the minimum quality of the face image when recognizing faces without masks. You must select the relevant value empirically. We recommend specifying the value of not less than 50. The value must be in the range [1, 100]
Minimum filtering threshold	**50**	If you enable the **Filter false alarms** parameter, specify the minimum percentage at which the additional algorithm considers the track to be a person's face. If the algorithm considers the track to be a face with a lower probability, this track will be disregarded. You must select the relevant value empirically. We recommend specifying the value of not less than 50. The value must be in the range [1, 100]
Minimum filtering threshold for face mask detection	**30**	Specify the minimum percentage at which the additional algorithm considers the track to be a person's face with a mask. If the algorithm considers the track to be a face with a mask with a lower probability, this track will be disregarded. You must select the relevant value empirically. We recommend specifying the value of not less than 30. The value must be in the range [1, 100]
Period of ignoring repeated recognitions	**2**	Specify the period in minutes during which new recognized faces will be compared with the previous ones to detect similarities. To adjust this parameter, you must enable the **Ignore repeated recognitions** parameter. The value must be in the range [2, 30]
Process color frames	**Yes** **No**	A black and white frame is processed by default. If you want the detection tool to use a color frame for processing, select the **Yes** value

Repeated recognitions similarity threshold	**85**	Specify the similarity threshold of the face to the previously recognized faces in percent. If the similarity threshold is lower than the specified value, the face will be recognized as a new one. To adjust this parameter, you must enable the **Ignore repeated recognitions** parameter. The value must be in the range [1, 100]
Send face images	**Yes** **No**	The **Send face images** parameter is disabled by default. If you want to send face images, select the **Yes** value
Track loss time	**500**	Specify the time in milliseconds after which the track of the captured face is considered to be lost. This parameter applies when a captured face moves in the frame and gets hidden behind an obstacle for some time. If this time is less than the specified value, the face will be recognized as the same. The value must be in the range [1, 10 000]
Basic settings		
Age and gender	**Yes** **No**	The **Age and gender** parameter is disabled by default. If you need to save age and gender information for each captured face in the database, select the **Yes** value **Note** The average error in age recognition is 5 years.
Biometric data	**Yes** **No**	The **Biometric data** parameter is enabled by default. When searching for faces (see Face search), the search results will contain found faces that are similar to the attached photo or a track based on the specified minimum similarity level (percentage). If you want to keep the biometric data confidential, select the **No** value. When searching for faces (see Face search) by an attached photo or a track, there will be no results
Face mask detection	**Yes** **No**	The **Face mask detection** parameter is disabled by default. If you use mask detection, select the **Yes** value (see Masks Detection)
Maximum face height	**100**	Specify the maximum height of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Maximum face width	**100**	Specify the maximum width of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum face height	**5**	Specify the minimum height of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum face width	**5**	Specify the minimum width of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum threshold of face authenticity	**90**	Specify the minimum level of face recognition accuracy for the creation of a track. You must select the relevant value empirically. We recommend specifying the value of not less than 90. The higher the value, the fewer faces are detected, while the recognition accuracy increases. The value must be in the range [1, 100]
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Huawei NPU**	Select a processor for the detection tool operation—CPU or Nvidia GPU (see Selecting Nvidia GPU when configuring detection tools). **Attention!** It may take several minutes to launch the algorithm on Nvidia GPU after you apply the settings.

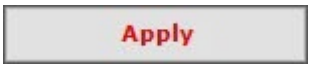
If necessary, in the preview window, set the rectangular area of the frame, in which you want to detect faces. You can specify the area by moving the anchor points  .



Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

If necessary, you can create and configure detection sub-tools on the basis of the **Face Detection VA** based on metadata (see General information on metadata):

1. Line Crossing—detection tool generates an event when a person moves across a line in the specified area of the frame and their face is detected.
2. Entrance In Area—detection tool generates an event when a person appears in the specified area of the frame and their face is detected.
3. Loitering In Area—detection tool generates an event when a person stays in the specified area of the frame for a long time and their face is detected.
4. Masks Detection—detection tool generates an event when it captures a face with or without a mask.

Masks Detection

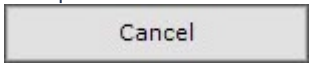
To configure the **Masks Detection**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera:
    a. in the settings of the **Face Detection VA**/**Face Detection TV** (see Configuring the Face Detection VA, Configuring the Face Detection TV), enable the **Face mask detection** parameter.
    b. in the settings of the **Face Detection VL** (see Configuring the Face Detection VL), enable the **Medical mask detection** parameter.
3. Below the **Face Detection VA**/**Face Detection VL**/**Face Detection TV**, click **Create... Masks Detection**.

By default, the detection tool is enabled and set to detect faces without masks.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

<table>
<tr><th>Parameter</th><th>Value</th><th>Description</th></tr>
<tr><td colspan="3">Other</td></tr>
<tr><td>Enable</td><td>Yes</td><td rowspan="2">The detection tool is enabled by default. To disable the detection tool, select the No value</td></tr>
<tr><td>No</td></tr>
<tr><td>Name</td><td>Masks Detection</td><td>Enter the detection tool name or leave the default name</td></tr>
<tr><td>Type</td><td>Masks Detection</td><td>Name of the detection tool type (non-editable field)</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td rowspan="3">Full face masking</td><td>Presence</td><td rowspan="10">Depending on a particular task, specify the parameters values according to the table:
<table>
<tr><th rowspan="2">Triggering event</th><th colspan="3">Value</th></tr>
<tr><th>Full face masking</th><th>Lower face part masking</th><th>No mask</th></tr>
<tr><td>No mask of any kind</td><td>Absence</td><td>Absence</td><td>Presence</td></tr>
<tr><td>No medical mask</td><td>Presence</td><td>Absence</td><td>Presence</td></tr>
<tr><td>No balaclava</td><td>Absence</td><td>Presence</td><td>Presence</td></tr>
<tr><td>Any mask present</td><td>Presence</td><td>Presence</td><td>Absence</td></tr>
<tr><td>Medical mask present</td><td>Absence</td><td>Presence</td><td>Absence</td></tr>
<tr><td>Balaclava present</td><td>Presence</td><td>Absence</td><td>Absence</td></tr>
</table></td></tr>
<tr><td>Not selected</td></tr>
<tr><td>Absence</td></tr>
<tr><td rowspan="3">Lower face part masking</td><td>Presence</td></tr>
<tr><td>Not selected</td></tr>
<tr><td>Absence</td></tr>
<tr><td rowspan="3">No mask</td><td>Presence</td></tr>
<tr><td>Not selected</td></tr>
<tr><td>Absence</td></tr>
<tr><td>Number of consecutive mask detections</td><td>2</td><td>Specify the minimum number of frames in which the detection tool must detect a mask in order to generate an event. The value must be in the range [0, 100]</td></tr>
<tr><td rowspan="3">Other types of masks</td><td>Presence</td><td rowspan="3">Note
The Other types of masks parameter isn't supported in this software version.</td></tr>
<tr><td>Not selected</td></tr>
<tr><td>Absence</td></tr>
</table>

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring face recognition based on the created lists

In *Axxon One*, you can configure macros to run the automatic system reactions based on the created face lists (see Lists of faces (*AxxonNet*), Face lists in Axxon Datacenter (*Axxon Datacenter*), Face lists in AxxonData (*AxxonData*)), when:

- the recognized face is present in the selected list;
- the recognized face is absent in the selected list;
- it is necessary to recognize the presence of the specific face from a list;
- it is necessary to recognize the absence of the specific face from a list;
- the recognized face is absent in all created lists.

To do this, do the following:

1. Connect Axxon-domain to *AxxonNet*/*AxxonData*/*Axxon Datacenter* (see Configuring a domain in AxxonNet, Configuring a domain in AxxonData, Configuring a domain in Axxon Datacenter).
2. Create one or more face lists in *AxxonNet*/*AxxonData*/*Axxon Datacenter* (see Lists of faces, Face lists in AxxonData, Face lists in Axxon Datacenter).
3. Create a face detection tool (see Category: Face).
4. Enable the **Check in lists** parameter in the face detection tool settings (see Configuring the Face Detection VL, Configuring the Face Detection VA, Configuring the Face Detection TV).
5. Select the condition to start the automatic system reaction (see Configuring start conditions for event-driven macros, Configuring macros when working with face lists).
6. Select one or more actions for the automatic system reaction (see Settings specific to actions).
7. If necessary, configure information boards to display the information from the automatic system reaction (see Examples of macros used when working with face lists, Configuring an Event Board, Configuring a Dialog Board).

Configuring macros when working with face lists

When working with face lists, you can configure the macro to trigger (see General information about the macros), when:

- the recognized face is present in the selected list;
- the recognized face is absent in the selected list;
- it is necessary to recognize the presence of the specific face from a list;
- the recognized face is absent in all created lists.

Presence of the recognized face in the selected face list

In this case, the parameters for starting the macro are the following:

1. The required list (**1**) is selected in the **Start conditions** field in the **Face recognition** list.

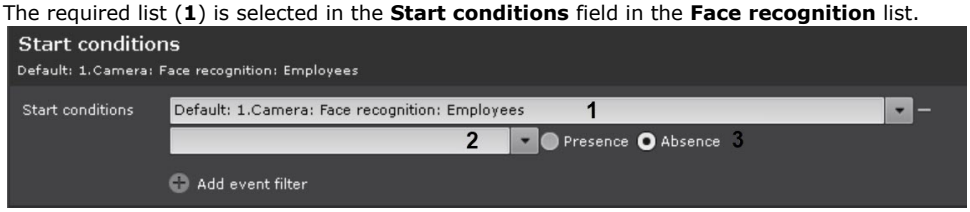


2. The field **2** is empty.
3. The **Presence** radio button is set (**3**).

Absence of the recognized face in the selected face list

In this case, the parameters for starting the macro are the following:

1. The required list (**1**) is selected in the **Start conditions** field in the **Face recognition** list.

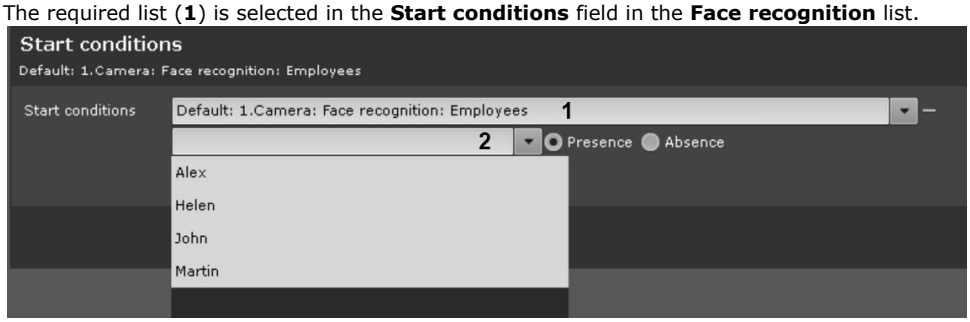


2. The field **2** is empty.
3. The **Absence** radio button is set (**3**).

Recognition of the presence of a specific face from the face list

In this case, the parameters for starting the macro are the following:

1. The required list (**1**) is selected in the **Start conditions** field in the **Face recognition** list.

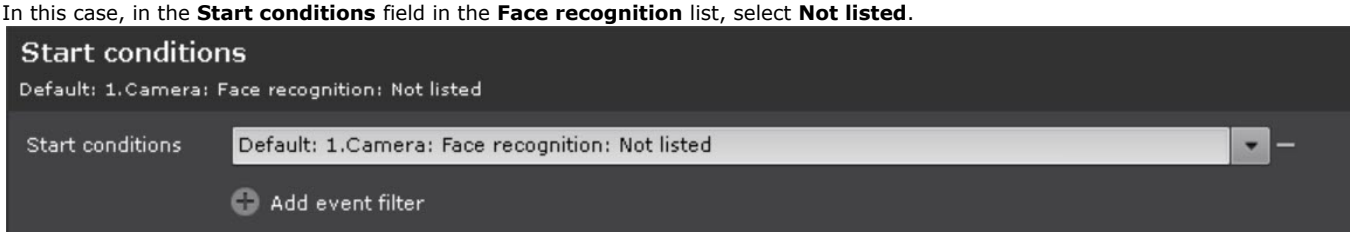


2. A specific person is selected in the field **2**.

> **Note**
>
> To select another person, clear the field **2** and re-open the list.

Absence of the recognized face in all created face lists

In this case, in the **Start conditions** field in the **Face recognition** list, select **Not listed**.



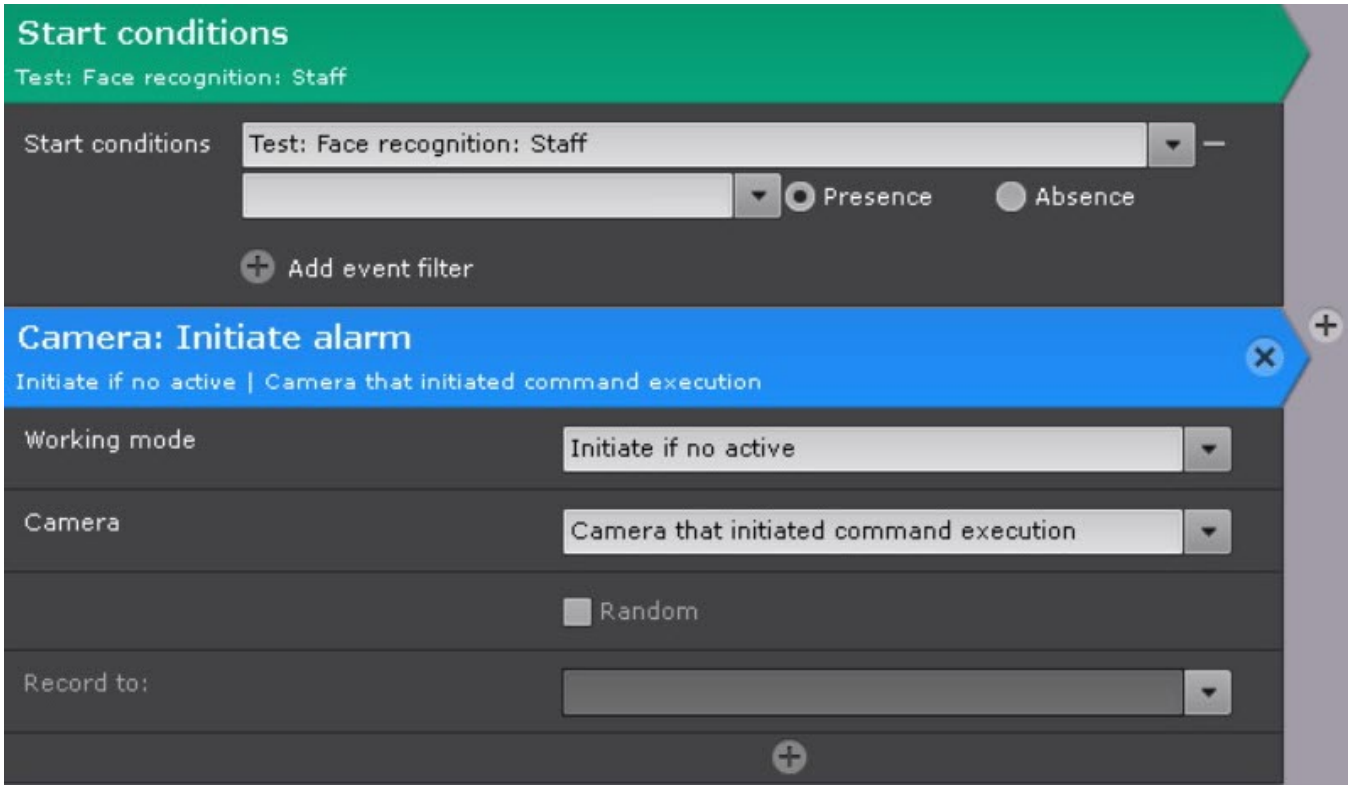
Examples of macros used when working with face lists

Examples of macros used when working with face lists

On this page:

- Alarm initiation
- Switching the output on for the authorized persons
- Sending an e-mail
- Starting export

Alarm initiation



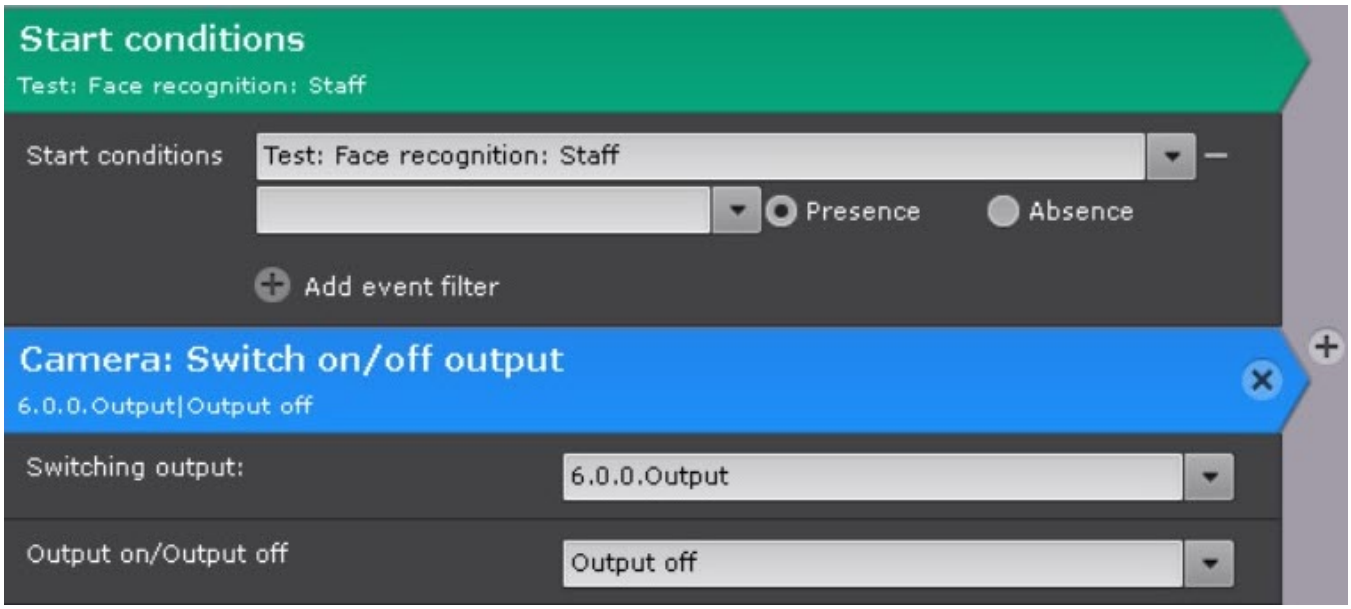
You can use this macro together with the Dialog Board (see Configure the Dialog Board).

If the Dialog Board is configured to display an alarm and linked with a camera (see Linking cells), then when a face from the list is recognized, the following information will be displayed on the Dialog Board:

- reference photo from the face list;
- an enlarged image of the recognized face in the frame;
- the name of the recognized person, the comment in quotation marks, the name of the face list in square brackets, and the percentage of similarity with the reference face in parentheses (see Lists of faces).

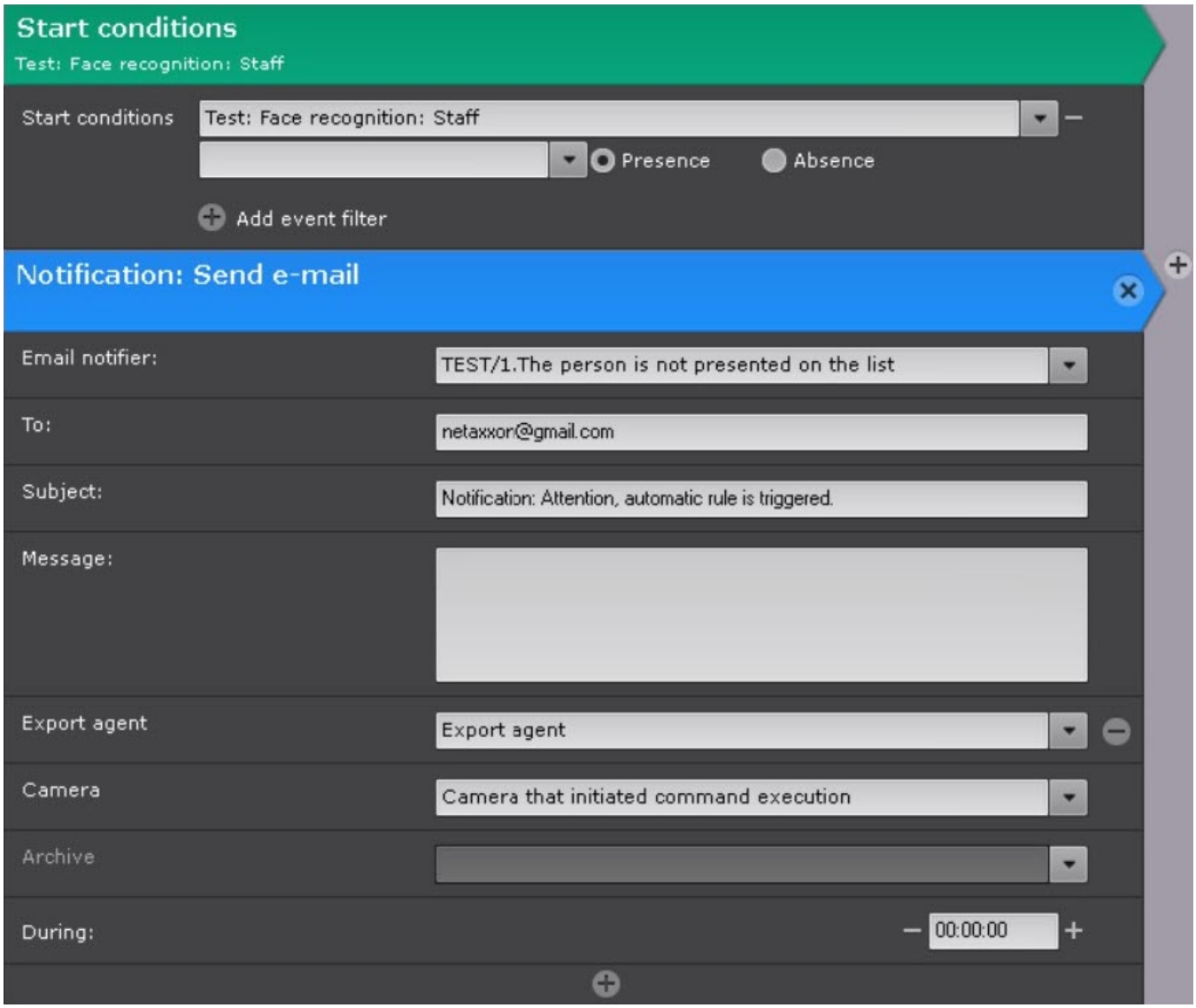


Switching the output on for the authorized persons



If only an authorized list of persons has access to the room, the system will trigger an automatic reaction if the recognized face is in the authorized list.

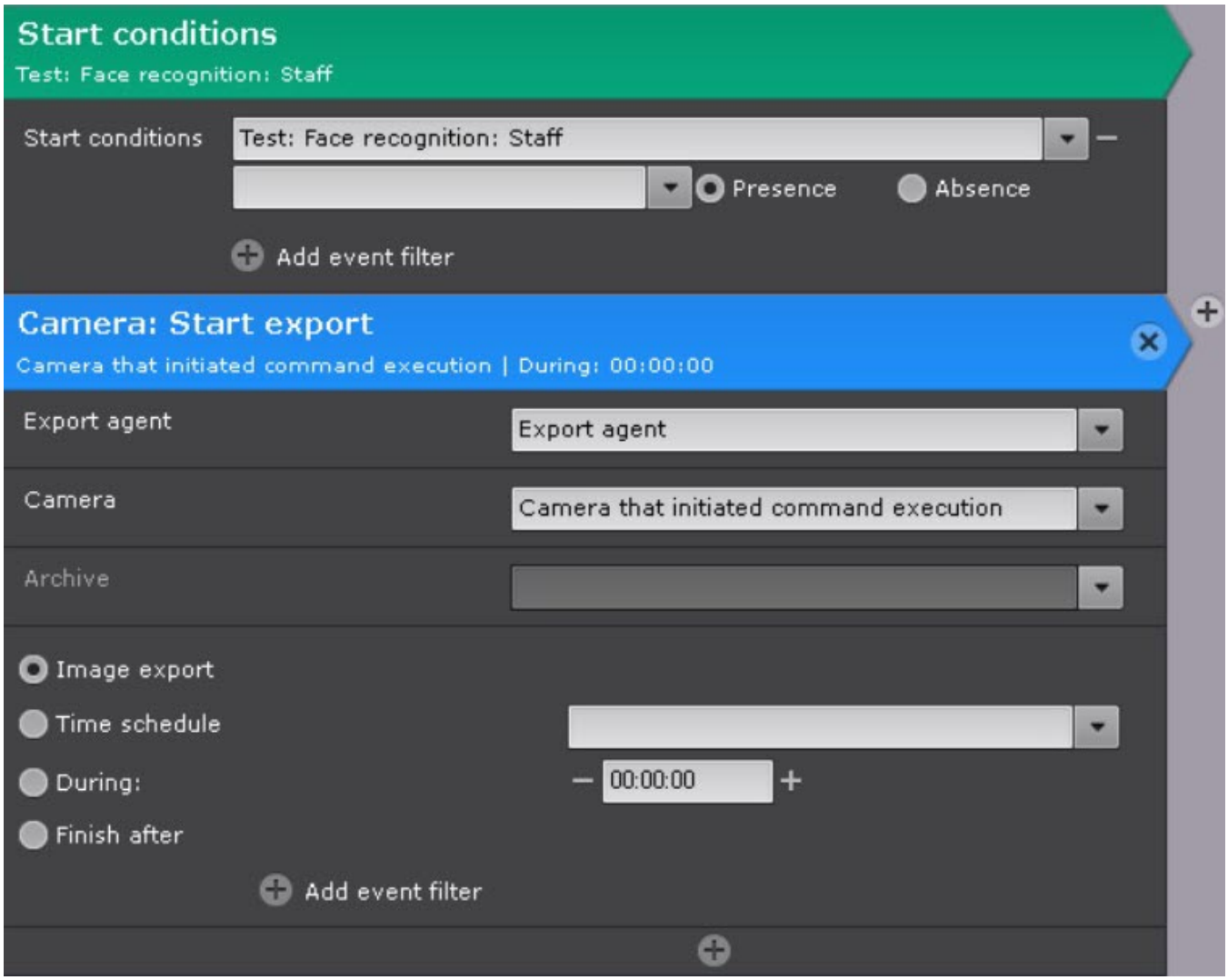
Sending an e-mail



If the e-mail is sent via the SMTP Server (see The Email notifier object), then three files will be attached to the message:

- full frame at the moment of face recognition;
- reference photo from the face list;
- an enlarged image of the recognized face in the frame.

Starting export



As with the e-mail message, three files will be exported when exporting an image upon face recognition event:

- full frame at the moment of face recognition;
- reference photo from the face list;
- an enlarged image of the recognized face in the frame.

Configuring integration with FaceCube

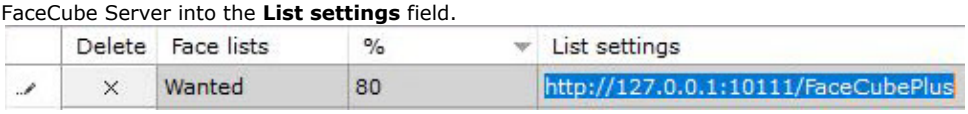
Axxon One supports the FaceCube facial recognition Server.

FaceCube works as follows:

1. *Axxon One* recognizes a face, then sends it to the FaceCube Server.
2. The FaceCube Server checks the face with reference faces in its own database.
3. If a match is found, the FaceCube Server sends the information to *Axxon One* (see Face recognition and search).

To configure integration with FaceCube, do the following:

1. Configure the FaceCube Server and add reference faces to it.
2. In *Axxon One,* in the **Server** object (see The Server Object), create a face list (see Lists of faces) and enter the address of the FaceCube Server into the **List settings** field.



3. Enable the **Check in lists** and **Send face images** parameters in the face detection settings (see Configuring the Face Detection VL, Configuring the Face Detection VA, Configuring the Face Detection TV).
4. Configure macros (see Configuring macros when working with face lists).

Face Detection TV

Functions of the Face Detection TV

Description

> **Attention!**
>
> Starting with *DetectorPack* 3.11.1, the **Face Detection TV** is no longer supported. We replaced it with the **Face Detection VA**. You cannot use the **Face Detection TV** and the **Face Detection VA** at the same time (see Manual for switching from the Face Detection TV to Face Detection VA).

The **Face Detection TV** generates an event every time a face is captured in the frame.

The *Axxon One* database stores all faces in binary form:

1. All captured faces are stored as biometric vectors (see Face search) in the **t_face_vector** table, and their corresponding capture events are stored in the **t_json_event** table.
2. All reference faces from the lists (see Lists of faces) are stored in the **t_face_listed** table

> **Attention!**
>
> When the number of faces in the database increases, the statistical error increases: the more faces in the database, the more often similar faces are recognized when searching in the archive. Accordingly, the degree of similarity when comparing the reference face with the captured face decreases.
>
> This error is relevant if:
>
> 1. The Video stream and scene requirements for the Face Detection TV and its sub-tools are met.
> 2. The database contains over a million faces.
>
> The mugshot dataset (good quality photo), 12 million faces in the database, and probability of false matching is 0.003%. With these initial data, the researchers obtained an identification error of 0.76%.

Licensing

To operate the detection tool, contact an AxxonSoft manager and get a license file (see Types of licenses)

Add-ons

For the **Face Detection TV** to work, you must install TV Face Recognition Pack add-on (see Installing DetectorPack add-ons).

> **Attention!**
>
> - You can install only one Face Recognition Pack: either TV Face Recognition Pack or VL Face Recognition Pack. You cannot install both packages in the same system.
> - Face Recognition Pack is guaranteed to work on Linux Debian 11 and Ubuntu 20. Face Recognition Packs isn't guaranteed to work on Linux Debian 9/10, Ubuntu 18 and Ubuntu 19 (see Operating system requirements).

Hardware requirements for the Face Detection TV and its sub-tools

Hardware requirements

Hardware requirements for neural analytics operation

The **Face Detection TV** and its sub-tools require a CPU supporting the SSE4.2, FMA3, or AVX2.0 instruction set.

If the **Face Detection TV** runs on GPU, the following hardware requirements must be met:

1. The detection tool can run only on NVIDIA devices with at least 6 GB of video memory or more.
2. NVIDIA driver version is 418.39 or higher.
3. Compute Capability 6.0 or higher.

Note

You can check the GPU Compute Capability version on the manufacturer's website.

Video stream and scene requirements for the Face Detection TV and its sub-tools

Hardware requirements for the Face Detection TV and its sub-tools

Hardware requirements for neural analytics operation

Image requirements for the Face Detection VA and its sub-tools

Requirements for the operation of the **Face Detection TV** and its sub-tools are given in the table:

Camera	• FPS is at least 12. For face recognition at turnstiles, FPS is at least 6
Lighting	• Faces must be evenly illuminated with diffused light of at least 200 lux. Directional side lighting isn't allowed • Contrast of the captured faces must be over 64 grayscale • Insufficient or excessive lighting isn't allowed • There must be no backlighting and sharp gradients of light and shade
Scene and camera angle	• Maximum angle of frontal perspective of the photos of people’s faces received from cameras must not exceed +/- 15° • Mutual faces overlapping must be minimal **Note** You can specify the required distance between the camera and the face using a lens with the required focal length.

Image requirements for the Face Detection TV and its sub-tools

Hardware requirements for the Face Detection TV and its sub-tools

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Face Detection TV and its sub-tools

Requirements for the operation of the **Face Detection TV** and its sub-tools are given in the table:

Object images	• Photos of the captured faces received from cameras must be clear. Image blurring caused by motion isn't allowed • Distance between the pupils on the photos of people’s faces received from cameras must be at least 32 pixels

Optimizing the operation of the Face Detection TV on GPU

Attention!

Starting with *DetectorPack* 3.11.1, the **Face Detection TV** is no longer supported. We replaced it with the **Face Detection VA**. You cannot use the **Face Detection TV** and the **Face Detection VA** at the same time (see Manual for switching from the Face Detection TV to Face Detection VA).

Configuring the Face Detection TV

The TV Face Recognition Pack add-on (see Installing DetectorPack add-ons) includes a utility that allows you to create GPU neural network caches without using *Axxon One*. The presence of the cache speeds up the initialization, optimizes video memory consumption and ensures the start and correct operation of the **Face Detection TV** on GPU.

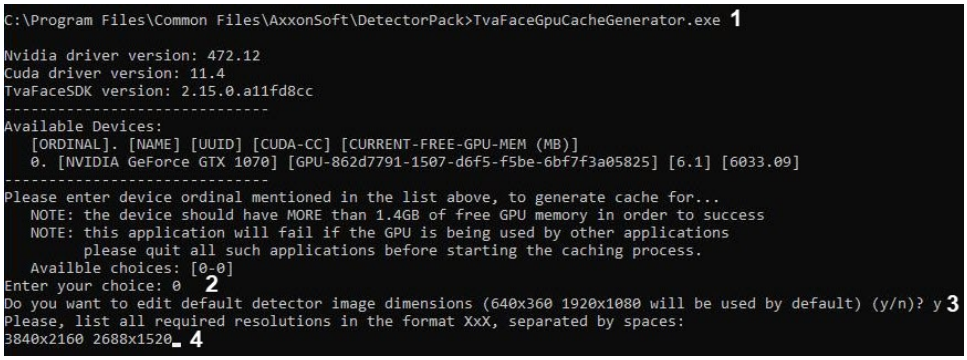
To optimize the operation of the **Face Detection TV** on GPU, do the following:

1. Stop the Server (see Shutting down a Server).

   Attention!

   If the system has the software running on GPU, it is necessary to stop its operation.

2. Create the GPU_CACHE_DIR system variable (see Appendix 9. Creating system variable) by specifying in the **Variable value** field the path to the cache location in Latin characters only. For example, D:\GPU_cache. The specified directory will store the cache for all used detection tools and neural networks.
3. Run the command line as administrator.
4. To call the utility, enter in the command line: C:\Program Files\Common Files\AxxonSoft\DetectorPack\TvaFaceGpuCacheGenerator.exe (**1**).
5. Press **Enter**.



6. Specify the ID of the required GPU (**2**, see Selecting Nvidia GPU when configuring detection tools).
7. Press **Enter**.
8. If you want to change the resolution of the video stream for the **Face Detection TV**:
   a. Enter **y** (**3**).
   b. Specify the required resolution (**4**). GPU uses the default video stream resolutions. Changing the resolution of the video stream from 1920*1080 and higher, increases the percentage of face detection.
9. Press **Enter**. The cache creation process starts. The cache creation is successful, if the result value is "0".

Optimizing the operation of the **Face Detection TV** on GPU is complete.

Attention!

The cache must be recreated in the following cases:

- if you update the TV Face Recognition Pack add-on (see Installing DetectorPack add-ons),
- if you change the Nvidia GPU model,
- if you update the Nvidia GPU drivers.

Configuring the Face Detection TV

Hardware requirements for the Face Detection TV and its sub-tools

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Face Detection TV and its sub-tools

Image requirements for the Face Detection TV and its sub-tools

Optimizing the operation of the Face Detection TV on GPU

Attention!

- Starting with *DetectorPack* 3.11.1, the **Face Detection TV** is no longer supported. We replaced it with the **Face Detection VA**. You cannot use the **Face Detection TV** and the **Face Detection VA** at the same time (see Manual for switching from the Face Detection TV to Face Detection VA).
- To start and correctly operate the **Face Detection TV** on GPU, you must create cache beforehand (see Optimizing the operation of the Face Detection TV on GPU).

To configure the **Face Detection TV**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Face Face Detection TV**.

By default, the detection tool is enabled and set to detect faces.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

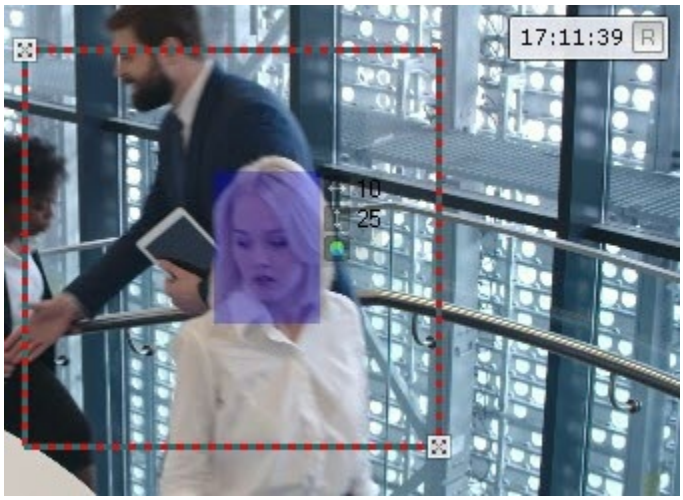
Parameter	Value	Description
Object features		
Check in lists	**Yes**	The **Check in lists** parameter is disabled by default. If you want to use this detection tool to check in lists of faces, select the **Yes** value (see Configuring face recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. For the correct operation of the **Face detection TV**, we recommend using a high-quality video stream
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Face Detection TV**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei iNPU	
Liveness detection	**Yes**	The **Liveness detection** parameter is disabled by default. Liveness detection is used when there is a photo of a face instead of an alive person. If you want to save to the database the information about whether each captured face is a photo (Yes/No), select the **Yes** value

	No	
Liveness threshold	**30**	Specify the threshold value in percent at which a face is defined as "not alive". The higher the value, the fewer captured faces will be detected as a photo. At the same time, the quality of recognizing whether the captured face is a photo (Yes/No) will be higher. You must select the relevant value empirically. The value must be in the range [1, 100]
Type	**Face Detection TV**	Name of the detection tool type (non-editable field)
Use camera transform	**Yes** **No**	The **Use camera transform** parameter is disabled by default. If you use a XingYun bispherical lens (see Configuring fisheye cameras), by default the detection tool receives the image of two spheres of 180° each to analyze. In this case, the recognition quality can deteriorate. To send the dewarped image to the detection tool, select the **Yes** value. This parameter is also valid for other transformations
Advanced settings **Attention!** Advanced configuration of the detection tool must be performed only with the assistance of AxxonSoft technical experts.		
Analyze face rotation angle	**Yes** **No**	The **Analyze face rotation angle** parameter is disabled by default. If you want to detect the face rotation angle, select the **Yes** value. This parameter allows you to filter out results that have a rotation and tilt angle greater than the specified values in a search for a specific face (see Search for similar face)
Face detection algorithm	**ALG1 (high speed, low accuracy)** **ALG2 (medium speed, medium accuracy)** **ALG3 (low speed, high accuracy)**	Select the face detection algorithm
Face detection period (msec)	**250**	Specify the time in milliseconds between face search operations in a frame. The larger the value, the less load on the Server, but some faces may not be recognized. The value must be in the range [1, 10 000]
Face rotation pitch (°)	**45**	Specify the allowable face pitch angle in degrees. The value must be in the range [0, 90]
Face rotation roll (°)	**45**	Specify the allowable face roll angle in degrees. The value must be in the range [0, 90]
Face rotation yaw from (°)	**-45**	Specify the minimum allowable angle of face rotation to the right or left. The value must be in the range [-90, 90]
Face rotation yaw to (°)	**45**	Specify the maximum allowable angle of face rotation to the right or left. The value must be in the range [-90, 90]

False mask detections filtering	**Yes** **No**	The **False mask detections filtering** parameter is enabled by default. If you don't need to use the parameter, select the **No** value
Filter false alarms	**Yes** **No**	In some cases, the detection tool may mistake other objects for a face. The **Filter false alarms** parameter is enabled by default. If the parameter is enabled, false results of the face recognition will appear in the detection feed (see Face recognition and search), but they will be ignored when searching for faces in the archive. This parameter filters out objects that are not faces at the stage of face vector construction and its recording to the metadata database. If you don't need to use this parameter, select the **No** value
Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The value must be in the range [640, 10 000]. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to 1000. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
Ignore repeated recognitions	**Yes** **No**	The **Ignore repeated recognitions** parameter is disabled by default. If you want to ignore repeated recognitions of the same face, select the **Yes** value
Minimum face masking threshold	**70**	Specify the minimum threshold for recognizing the mask on the face. You must select the relevant value empirically. We recommend specifying the value of not less than 70. The value must be in the range [1, 100]
Minimum face quality for face mask detection	**30**	Specify the minimum quality of the face image when recognizing masks (see Masks Detection). You must select the relevant value empirically. We recommend specifying the value of not less than 30. The value must be in the range [1, 100]
Minimum face recognition quality	**50**	Specify the minimum quality of the face image when recognizing faces without masks. You must select the relevant value empirically. We recommend specifying the value of not less than 50. The value must be in the range [1, 100]
Minimum filtering threshold	**50**	If you enable the **Filter false alarms** parameter, specify the minimum percentage at which the additional algorithm considers the track to be a person's face. If the algorithm considers the track to be a face with a lower probability, this track will be disregarded. You must select the relevant value empirically. We recommend specifying the value of not less than 50. The value must be in the range [1, 100]
Minimum filtering threshold for face mask detection	**30**	Specify the minimum percentage at which the additional algorithm considers the track to be a person's face with a mask. If the algorithm considers the track to be a face with a mask with a lower probability, this track will be disregarded. You must select the relevant value empirically. We recommend specifying the value of not less than 30. The value must be in the range [1, 100]
Period of ignoring repeated recognitions	**2**	Specify the period in minutes during which new recognized faces will be compared with the previous ones to detect similarities. To adjust this parameter, you must enable the **Ignore repeated recognitions** parameter. The value must be in the range [2, 30]
Process color frames	**Yes** **No**	A black and white frame is processed by default. If you want the detection tool to use a color frame for processing, select the **Yes** value

Repeated recognitions similarity threshold	**85**	Specify the similarity threshold of the face to the previously recognized faces in percent. If the similarity threshold is lower than the specified value, the face will be recognized as a new one. To adjust this parameter, you must enable the **Ignore repeated recognitions** parameter. The value must be in the range [1, 100]
Send face images	**Yes** **No**	The **Send face images** parameter is disabled by default. If you want to send face images, select the **Yes** value
Track loss time	**500**	Specify the time in milliseconds after which the track of the captured face is considered to be lost. This parameter applies when a captured face moves in the frame and gets hidden behind an obstacle for some time. If this time is less than the specified value, the face will be recognized as the same. The value must be in the range [1, 10 000]
Basic settings		
Age and gender	**Yes** **No**	The **Age and gender** parameter is disabled by default. If you need to save age and gender information for each captured face in the database, select the **Yes** value. **Note** The average error in age recognition is 5 years.
Biometric data	**Yes** **No**	The **Biometric data** parameter is enabled by default. When searching for faces (see Face search), the search results will contain found faces that are similar to the attached photo or a track based on the specified minimum similarity level (percentage). If you want to keep the biometric data confidential, select the **No** value. When searching for faces (see Face search) by an attached photo or a track, there will be no results
Face mask detection	**Yes** **No**	The **Face mask detection** parameter is disabled by default. If you use mask detection, select the **Yes** value (see Masks Detection)
Maximum face height	**100**	Specify the maximum height of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Maximum face width	**100**	Specify the maximum width of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum face height	**5**	Specify the minimum height of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum face width	**5**	Specify the minimum width of the captured faces as a percentage of the frame size. The value must be in the range [1, 100]
Minimum threshold of face authenticity	**90**	Specify the minimum level of face recognition accuracy for the creation of a track. You must select the relevant value empirically. We recommend specifying the value of not less than 90. The higher the value, the fewer faces are detected, while the recognition accuracy increases. The value must be in the range [1, 100]
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Huawei NPU**	Select a processor for the detection tool operation—CPU or Nvidia GPU (see Selecting Nvidia GPU when configuring detection tools) **Attention!** It may take several minutes to launch the algorithm on Nvidia GPU after you apply the settings.

If necessary, in the preview window, set the rectangular area of the frame, in which you want to detect faces. You can specify the area by moving the anchor points  .



Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

If necessary, you can create and configure detection sub-tools on the basis of the **Face Detection TV** based on metadata (see General information on metadata):

1. Line Crossing—detection tool generates an event when a person moves across a line in the specified area of the frame and their face is detected.
2. Entrance In Area—detection tool generates an event when a person appears in the specified area of the frame and their face is detected.
3. Loitering In Area—detection tool generates an event when a person stays in the specified area of the frame for a long time and their face is detected.
4. Masks Detection—detection tool generates an event when it captures a face with or without a mask.

Category: Vehicle

Configuring vehicle license plate recognition based on the created lists

In *Axxon One*, you can configure macros to run the automatic system reactions based on the created license plate lists (see Lists of vehicle numbers), when:

- the recognized license plate is present in the selected list;
- the recognized license plate is absent in the selected list;
- it is necessary to recognize the presence of the specific license plate from a list;
- it is necessary to recognize the absence of the specific license plate from a list;
- the recognized license plate is absent in all created lists.

To do this, do the following:

1. Connect Axxon-domain to *AxxonNet*/*AxxonData* (see Connecting Axxon-domain to AxxonNet, Configuring a domain in AxxonData).
2. Create one or more lists of license plates in *AxxonNet*/*AxxonData* (see Lists of vehicle numbers, Lists of vehicle numbers in AxxonData).
3. Create a license plate recognition tool (see Category: Vehicle).
4. Enable the **Check in lists** parameter in the license plate recognition tool settings (see Configuring License Plate Recognition VT, Configuring License Plate Recognition IV, Configuring License Plate Recognition RR).
5. Select the condition to start the macro (see Configuring start conditions for event-driven macros, Configuring macros when working with vehicles lists).
6. Select one or more actions to start the macro (see Settings specific to actions).
7. If necessary, configure information boards to display the information from the macro (see Examples of macros used when working with vehicles lists, Configuring an Event Board, Configuring a Dialog Board).

Configuring macros when working with vehicles lists

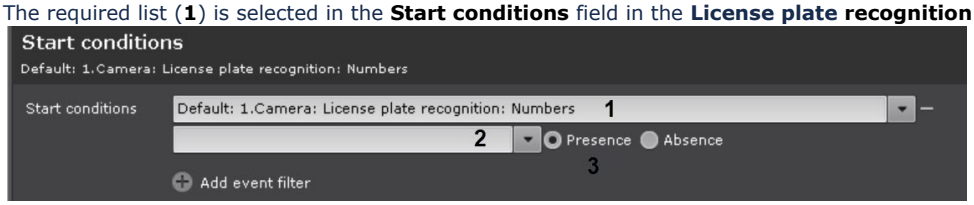
When working with vehicle license plate lists, you can configure the macro (see General information about the macros) to trigger when:

- the recognized license plate is present in the selected list;
- the recognized license plate is absent in the selected list;
- it is necessary to recognize the presence of the specific license plate from a list;
- the recognized license plate is absent in all created lists.

Presence of the recognized license plate in the selected list

In this case, the parameters for starting the macro are the following:

1. The required list (**1**) is selected in the **Start conditions** field in the **License plate recognition** list.

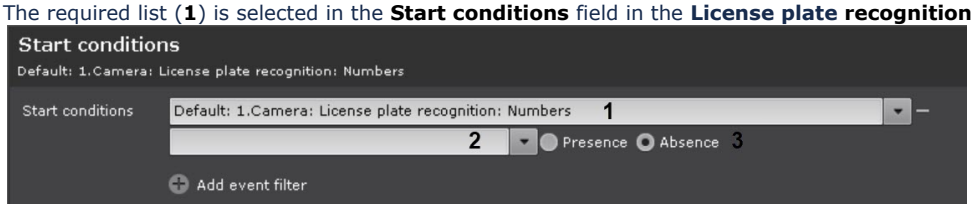


2. The field **2** is empty.
3. The **Presence** radio button is set (**3**).

Absence of the recognized license plate in the selected list

In this case, the parameters for starting the macro are the following:

1. The required list (**1**) is selected in the **Start conditions** field in the **License plate recognition** list.

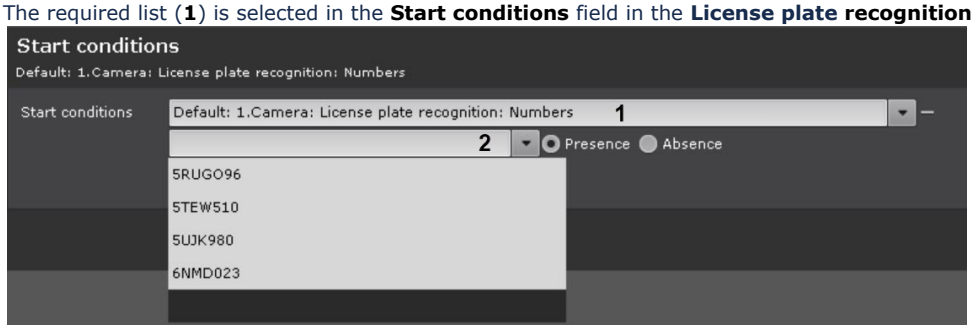


2. The field **2** is empty.
3. The **Absence** radio button is set (**3**).

Presence of the specific license plate from the selected list

In this case, the parameters for starting the macro are the following:

1. The required list (**1**) is selected in the **Start conditions** field in the **License plate recognition** list.

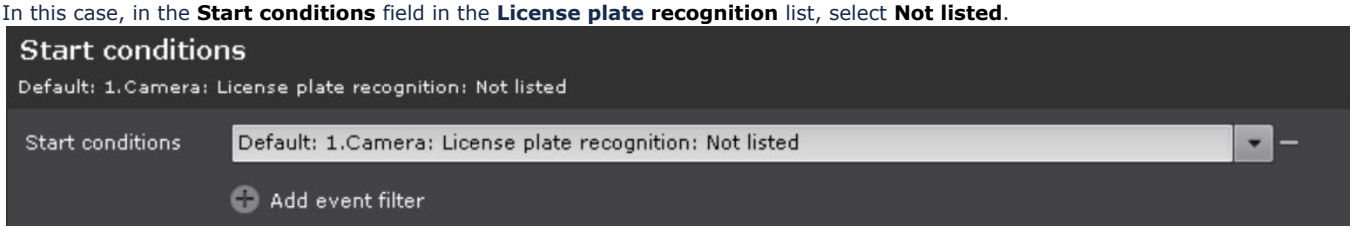


2. A specific license plate is selected in the field **2**.

> **Note**
>
> To select another license plate, clear the field **2** and re-open the list.

Absence of the recognized license plate in all created lists

In this case, in the **Start conditions** field in the **License plate recognition** list, select **Not listed**.



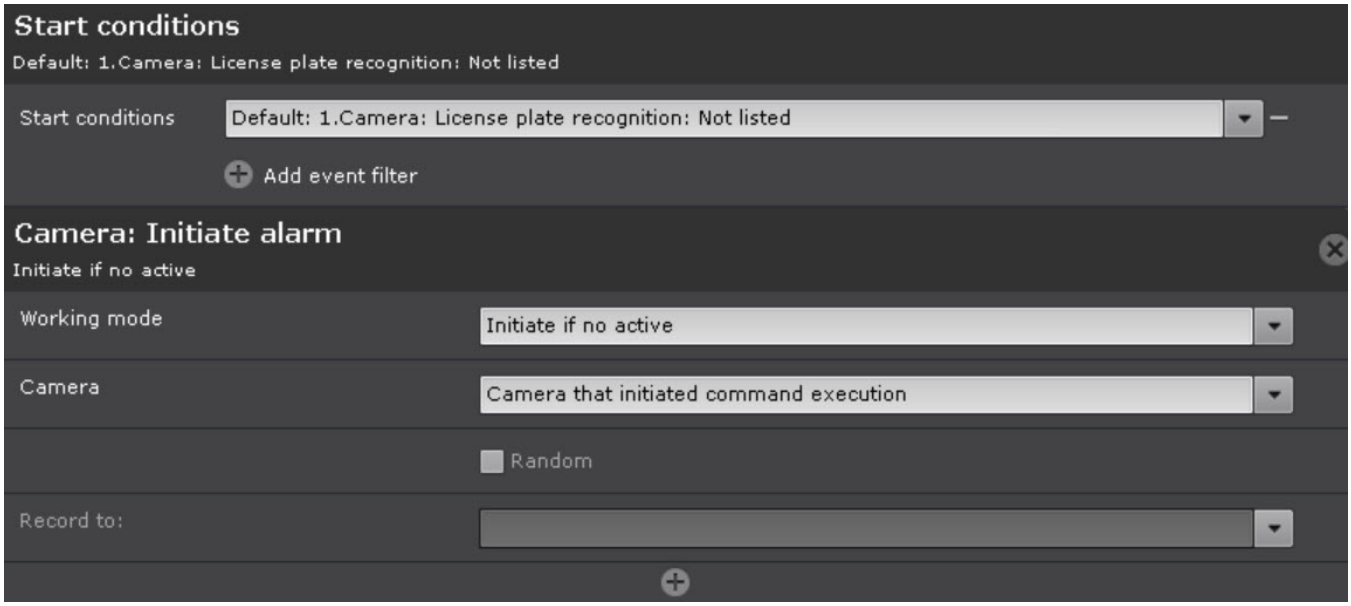
Examples of macros used when working with vehicles lists

Examples of macros used when working with vehicles lists

On this page:

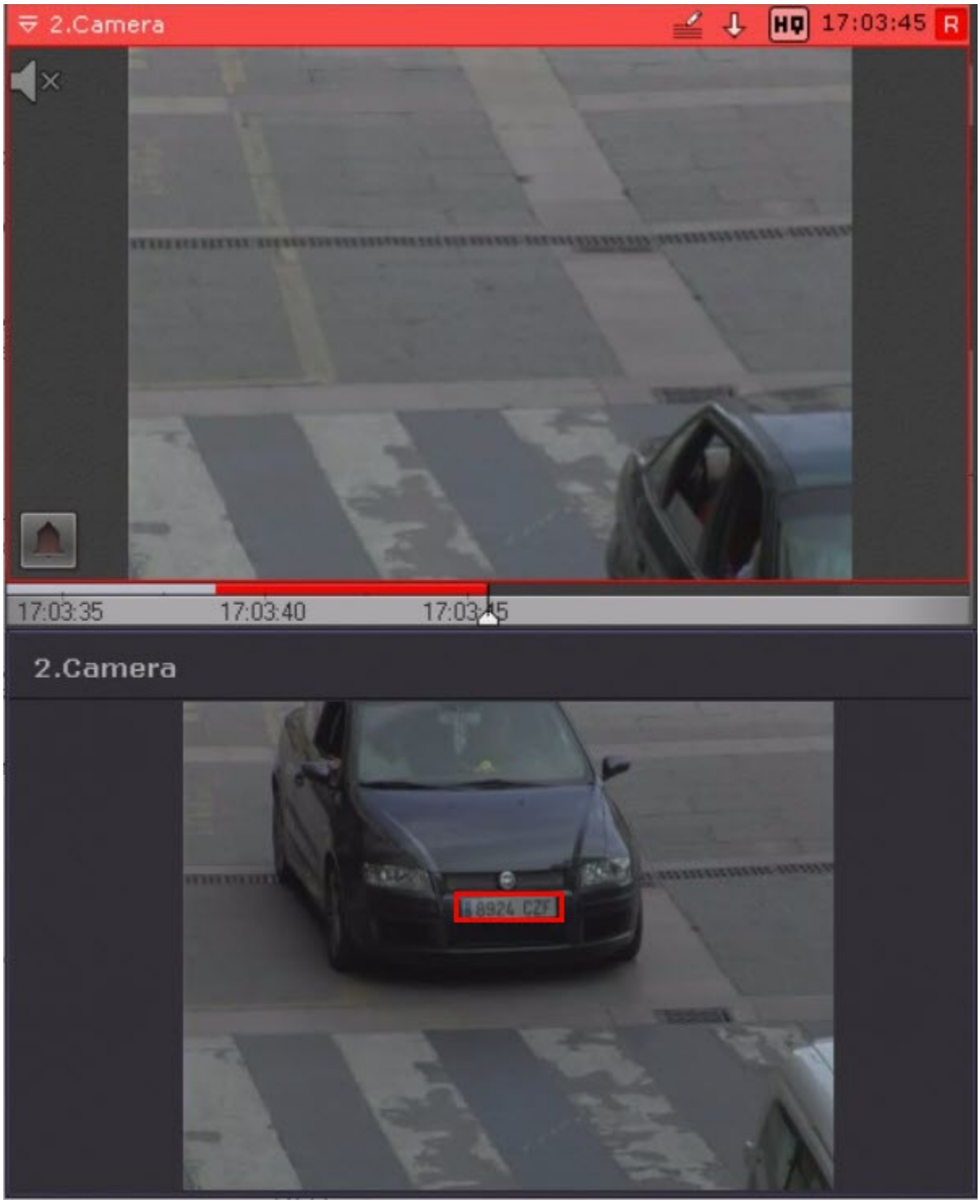
- Alarm initiation
- Switching the output on for the authorized license plates
- Sending an E-mail
- Starting export

Alarm initiation

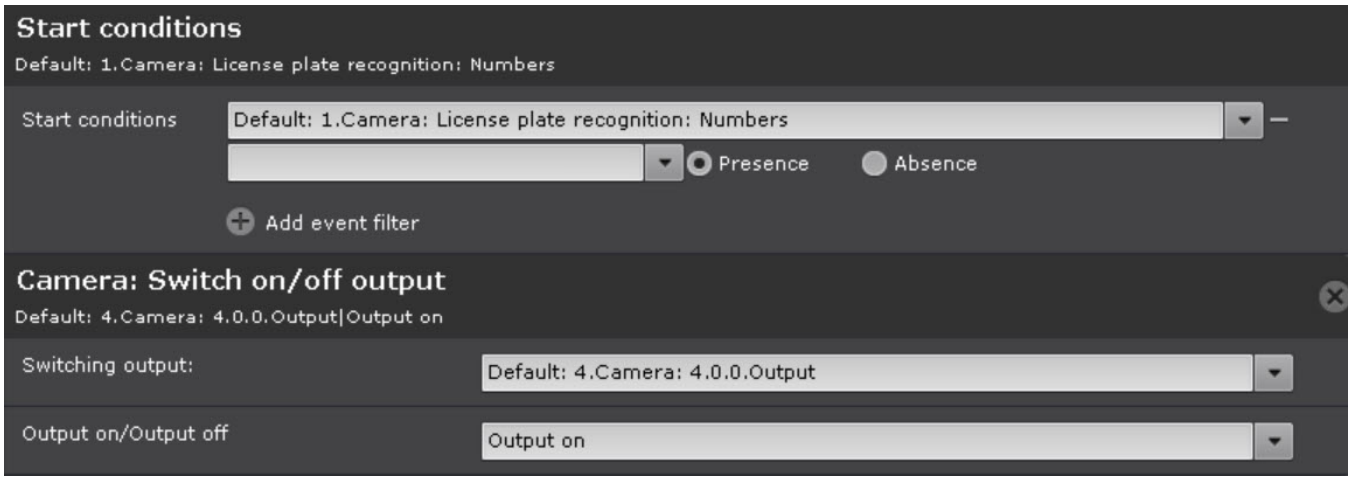


This macro can be used together with the Dialog Board (see Configuring a Dialog Board).

If the Dialog Board is configured to display an alarm and linked with a video camera (see Linking cells), then when not listed license plate is recognized, the board will display the recognized license plate highlighted in a red frame.

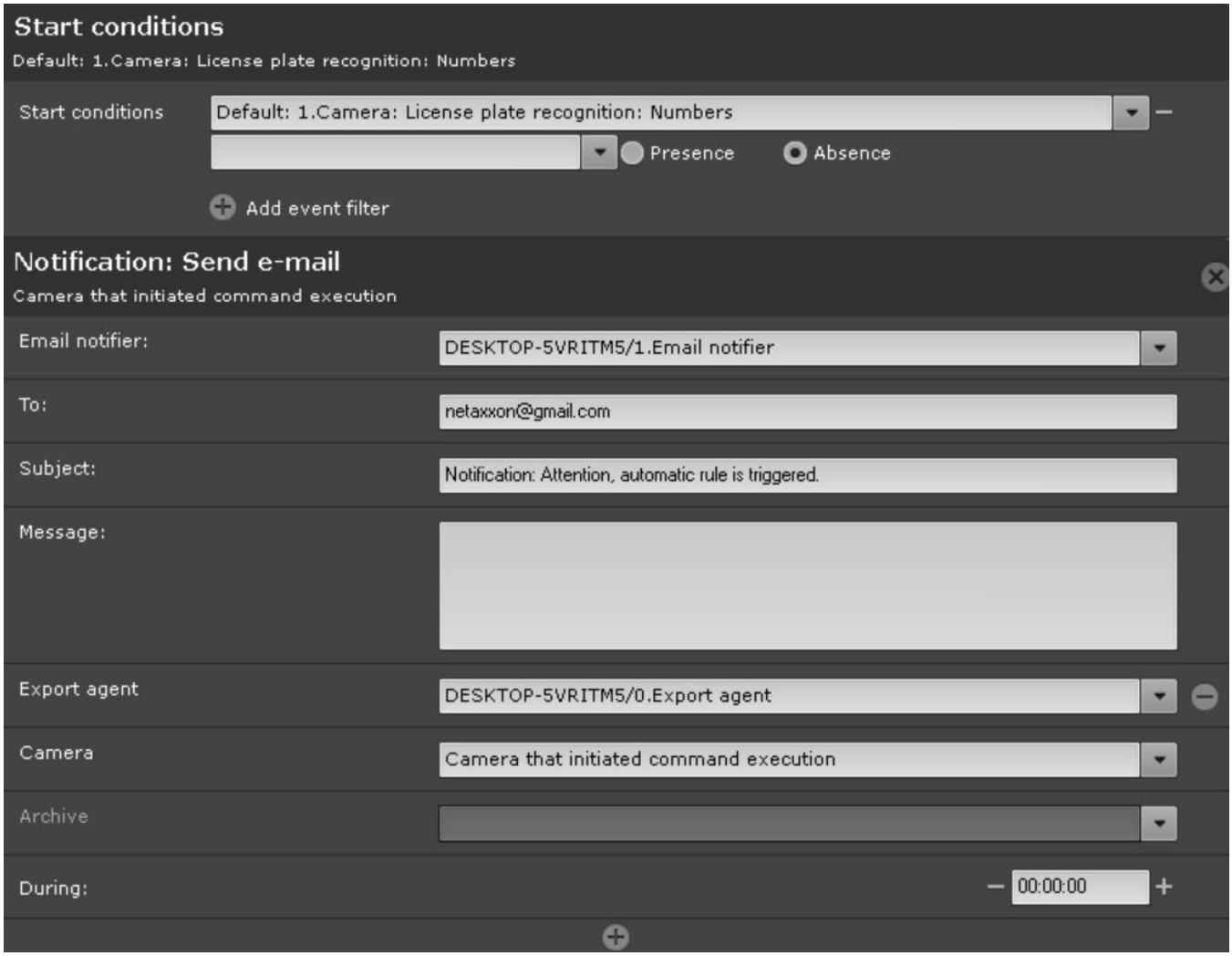


Switching the output on for the authorized license plates



If only an authorized list of license plates has access to the facility, the system will trigger an automatic reaction if the recognized license plate is in the authorized list.

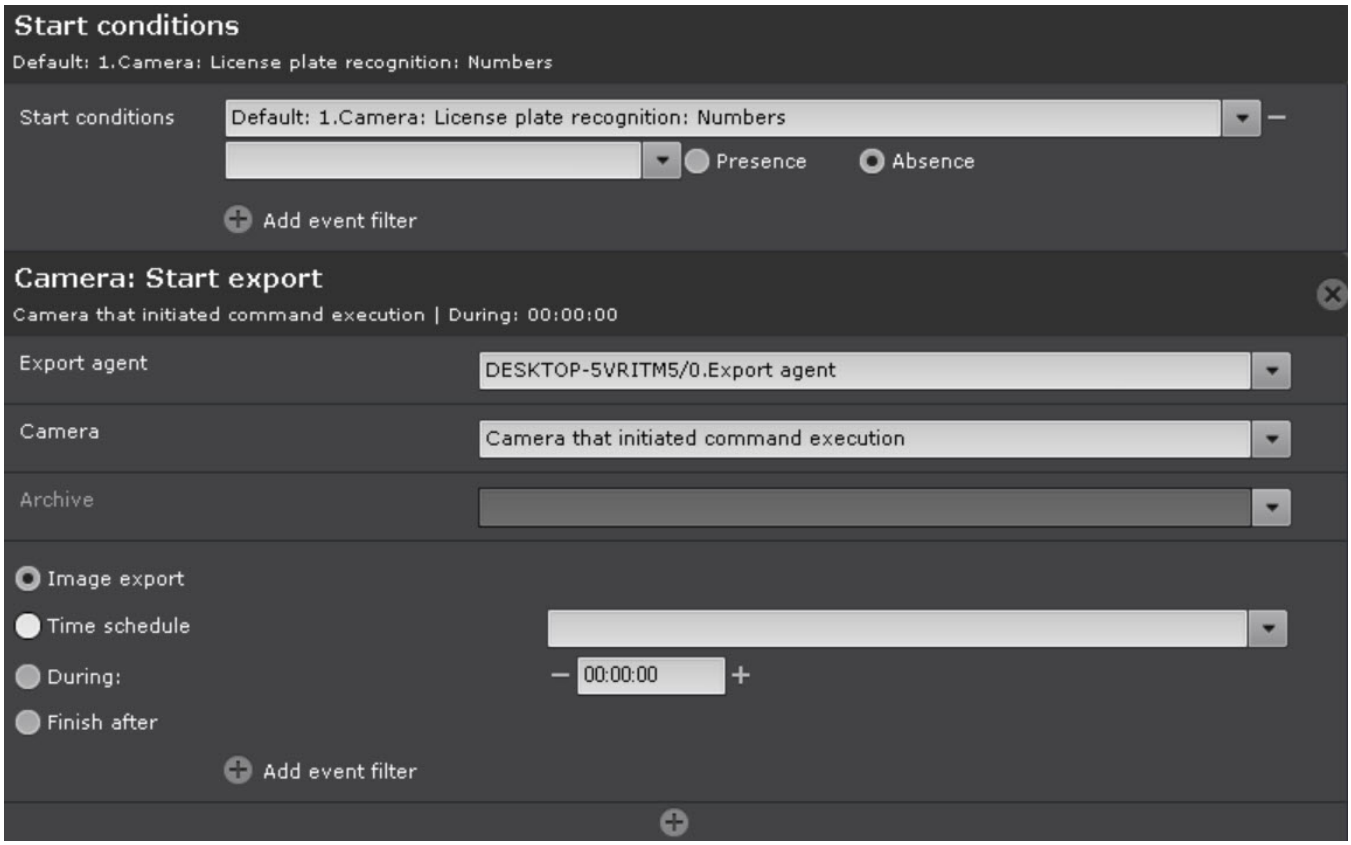
Sending an E-mail



If the E-mail is sent via the SMTP Server (see The Email notifier object), then two files will be attached to the message:

- full frame at the moment of license plate recognition;
- an enlarged image of the recognized license plate.

Starting export



As with the E-mail message, two files will be exported when exporting an image upon license plate recognition event:

- full frame at the moment of license plate recognition;
- an enlarged image of the recognized license plate.

License Plate Recognition BRS

Camera requirements for License Plate Recognition BRS and its sub-tools

To ensure the recognition of state license plates with **License plate recognition (BRS)**, it is necessary to install and configure the cameras to meet the following requirements:

Camera	• Minimum video resolution is 640*480, recommended resolution is 720p or 1080p • Minimum frame rate is 15 FPS, recommended frame rate is 25–30 FPS • Autofocus and zoom would be useful for making small adjustments after configuring the detection tool • Auto white balance • IR for night mode with good contrast of license plate images • HDR or WDR • In order to recognize state license plates on high-speed roads, the camera must have the Global Shutter mode
Video	• Video image must be clear, contrasting, without distortion, not blurred • Video image must have minimum noise in low light conditions • Size of the license plate must be 15–70% of the total size of the image • License plate must contain no more than two rows of characters
Camera installation	• Video camera must be mounted at 0.6–2.4 meters above the ground • Angle formed by the lower line of the license plate and the horizon line must be from 0 to 20 degrees

License Plate Recognition BRS features and specifications

Description	**License plate recognition (BRS)** is used to implement the following functions: 1. Recognize license plates of vehicles. List of supported countries: Hong Kong, China, Taiwan. 2. Write a recognized license plate to a database. 3. Check the recognized license plates of vehicles on the lists of license plates
Add-ons	For the **License plate recognition (BRS)** operation, you must install the License Plate Recognition BRS add-on (see Installing DetectorPack add-ons)

Configuring License plate recognition BRS

To configure the **License plate recognition BRS** detection tool, do the following:

1. Submit to the technical support the MAC address of the Server on which you will use the detection tool.

   > **Attention!**
   >
   > The detection tool won't operate on the Server with a different MAC address.

2. Copy the license received from technical support into the C:\Program Files\Common Files\AxxonSoft\DetectorPack\BioirisSDK\License.txt file.
3. Restart the Server (see Shutting down a Server, Starting a Server).

To create the **License plate recognition BRS** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle License plate recognition BRS**.

By default, the detection tool is enabled and set to recognize vehicle license plates.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes**	The parameter is disabled by default. If you want to use this detection tool to check in lists of vehicle license plates, select the **Yes** value (see Configuring vehicle license plate recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**License plate recognition BRS**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Type	**License plate recognition BRS**	Name of the detection tool type (non-editable field)
Advanced settings		

Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (**1920** pixels on the longer side) by default. The following algorithm is used: a. If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. b. If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. c. If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. I n this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
GDPR policy	**-**	By default, on the layout and in the archive, the characters of a license plate are completely hidden "GDPR ON". To display the characters of a license plate, you must enter a value: "**-**"—hide all characters (default value), " (blank field of a parameter value)"—show all characters, "**N-**"—hide the first N characters, "**-N**"—hide the last N characters, where **N** is the number of characters
Minimum recognition quality, in %	**80**	Specify the minimum quality of license plates recognition as a percentage. The higher the minimum recognition quality, the fewer false alarms. The value must be in the range [0, 100]
Event timeout	**3**	Specify the time in seconds after which the alarm must be generated after recognizing a license plate in the frame. The value must be in the range [1, 3600]. If the value is **0**, the alarm will be generated after the track with a license plate is lost
Tracker timeout	**3**	Specify the time in seconds after which the vehicle track is considered lost. The value must be in the range [0, 3600]. **Note** You can use this parameter to avoid double triggerings that can occur, for example, when a license plate is recognized when it appears in the frame, then it is overlapped by a visual obstacle and then recognized by the detection tool again. If you specify the timeout longer than the time of possible overlapping of the license plate in the frame, the detection tool will trigger only once.
Basic settings		
Maximum LP width	**10**	Specify the maximum and minimum width of the license plate as a percentage according to the actual size of the license plate in the frame. The value must be in the range [0, 100]. **Attention!** • Specified values must exclude omissions in license plate recognition, that is the values must not be smaller than the real size of the license plate in the frame. Otherwise, the license plates won't be recognized. • The **Minimum LP width** parameter affects the CPU load: the higher the value, the lower the load. • Reducing the difference between the maximum and minimum width reduces the CPU load.
Minimum LP width	**1**	

In the window, specify the area in which license plate detection and recognition will be performed. You can adjust the area by moving the anchor points .



Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

Configuration of **License plate recognition BRS** is complete.

License Plate Recognition IV

License Plate Recognition IV features and specifications

> **Attention!**
>
> Only a 64-bit version of the detection tool is available.

Description	License Plate Recognition IV is used to implement the following functions: 1. Recognize license plates of vehicles. **List of supported countries**: Australia, Austria, Bangladesh, Belarus, Brazil, Canada, China, Costa Rica, Czech Republic, Dubai, Egypt, Finland, France, Germany, Great Britain, India, Indonesia, Iraq, Israel, Italy, Japan, Kazakhstan, Kuwait, Mexico, Monaco, Mongolia, Netherlands, Pakistan, Poland, Qatar, Republic of South Africa, Russia, Saudi Arabia, Slovenia, South Korea, Spain, Sri Lanka, Switzerland, Taiwan, Thailand, Turkey, Ukraine, United Arab Emirates, United States of America, Uzbekistan, Vietnam. Recognition of license plates of vehicles as part of conglomerates: • European Union (Austria, Germany); • K.U.B.R (Kazakhstan, Ukraine, Belarus, Russia); • Malaysia, Singapore; • Middle East (Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, Syria, United Arab Emirates, Yemen); • North America (Canada, Mexico, United States of America). Motorcycle license plate recognition is only for Brazil. 2. Write a recognized license plate to a database. 3. Check the recognized license plates of vehicles on the lists of license plates
Add-ons	For the **License Plate Recognition IV** operation, you must install the License Plate Recognition IV add-on (see Installing DetectorPack add-ons)

Hardware requirements for License Plate Recognition IV

Hardware requirements

If License Plate Recognition IV runs on GPU, the following hardware requirements must be met:

1. Support for TensorRT 7.2.1 (see documentation).
2. NVIDIA driver version 450.36.06 or higher.
3. CPUs that support the AVX2 instruction set, see the list.
4. Compute Capability 3.5 or higher, recommended 5.0 or higher.

> **Note**
>
> You can check the GPU Compute Capability version on the manufacturer's website.

Camera requirements for License Plate Recognition IV and its sub-tools

To ensure the recognition of state license plates with **License Plate Recognition IV**, it is necessary to install and configure the cameras to meet the following requirements:

Camera	• Minimum video resolution is 640*480, recommended resolution is 720p or 1080p • Minimum frame rate is 15 FPS, recommended frame rate is 25–30 FPS • Autofocus and zoom would be useful for making small adjustments after configuring the detection tool • IR for night mode with good contrast of license plate images • HDR or WDR • In order to recognize state license plates on high-speed roads, the camera must have the Global Shutter mode
Video	• Video image must be clear, contrasting, without distortion, not blurred • Video image must have minimum noise in low light conditions • Size of the license plate must be 15–70% of the total size of the image • License plate must contain no more than two rows of characters
Camera installation	• Video camera must be mounted at 0.6–2.4 meters above the ground • Angle formed by the lower line of the license plate and the horizon line must be from 0 to 20 degrees

Examples of correct and incorrect video images

Video images that meet the video camera mounting and setup requirements for Licence Plate Recognition IV.















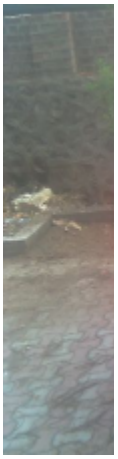




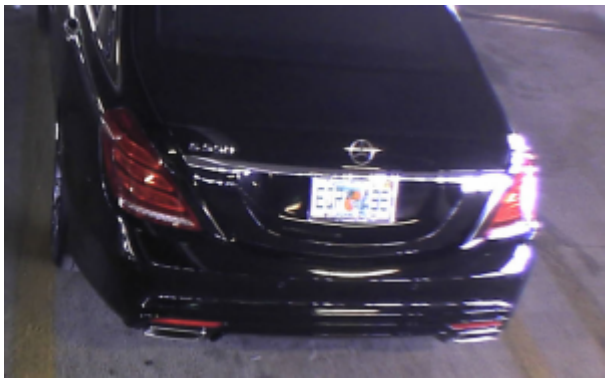
Video images that don't meet the video camera mounting and setup requirements for Licence Plate Recognition IV.


MH 12 GF 800











Configuring License Plate Recognition IV

To configure the **License Plate Recognition IV** detection tool, do the following:

1. Submit to the technical support the MAC address of the Server on which you will use the detection tool.

   > **Attention!**
   >
   > The detection tool won't operate on the Server with a different MAC address.

2. Copy the license received from technical support into the C:\Program Files\Common Files\AxxonSoft\DetectorPack\LicenseFile_LprIV.txt file.
3. Restart the Server (see Shutting down a Server, Starting a Server).

To create the **License Plate Recognition IV** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle License Plate Recognition IV**.

By default, the detection tool is enabled and set to recognize vehicle license plates.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes**	The parameter is disabled by default. If you want to use this detection tool to check in lists of vehicle license plates, select the **Yes** value (see Configuring vehicle license plate recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**License Plate Recognition IV**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Type	**License Plate Recognition IV**	Name of the detection tool type (non-editable field)
Advanced settings		
Event timeout	**1**	Specify the time in seconds after which the alarm must be generated after recognizing a license plate in the frame. The value must be in the range [1, 3600]. If the value is **0**, the alarm will be generated after the track with a license plate is lost

Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (**1920** pixels on the longer side) by default. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
GDPR policy	**-**	By default, on the layout and in the archive, the characters of a license plate are completely hidden "GDPR ON". To display the characters of a license plate, you must enter a value: "**-**"—hide all characters (default value), " (blank field of a parameter value)"—show all characters, "**N-**"—hide the first N characters, "**-N**"—hide the last N characters, where **N** is the number of characters
Maximal number of characters in LP	**10**	Specify the maximum number of characters in the license plate. The value must be in the range [1, 20]
Minimal number of characters in LP	**5**	Specify the minimum number of characters in the license plate. The value must be in the range [1, 20]
Minimum recognition quality, in %	**80**	Specify the minimum quality of license plates recognition as a percentage. The higher the minimum recognition quality, the fewer false alarms. The value must be in the range [0, 100]

Tracker timeout	**3**	Specify the time in seconds after which the vehicle track is considered lost. The value must be in the range [0, 3600]. **Note** You can use this parameter to avoid double triggerings that can occur, for example, when a license plate is recognized when it appears in the frame, then it is overlapped by a visual obstacle and then recognized by the detection tool again. If you specify the timeout longer than the time of possible overlapping of the license plate in the frame, the detection tool will trigger only once.
Basic settings		
Algorithm for detecting vehicle direction	**By LP coordinates** **By LP scale change**	The **By LP coordinates** algorithm is used by default. It works as follows: if the coordinates of the vehicle license plate shift from top to bottom (the vehicle moves towards the camera) and if the coordinates of the vehicle license plate shift from bottom to top (the vehicle moves away from the camera). Select the **By LP scale change** parameter if in the Surveillance window, the scale of the vehicle license plate increases (the vehicle moves towards the camera) and if the scale of the vehicle license plate decreases (the vehicle moves away from the camera)
Maximum LP width	**10**	Specify the maximum and minimum width of the license plate as a percentage according to the actual size of the license plate in the frame. The value must be in the range [0, 100]. **Attention!** • Specified values must exclude omissions in license plate recognition, that is the values must not be smaller than the real size of the license plate in the frame. Otherwise, the license plates won't be recognized. • The **Minimum LP width** parameter affects the CPU load: the higher the value, the lower the load. • Reducing the difference between the maximum and minimum width reduces the CPU load.
Minimum LP width	**1**	
Processing unit	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2**	Select the processor for the detection tool operation—CPU or one of NVIDIA GPUs (see Selecting Nvidia GPU when configuring detection tools). **Attention!** • It may take several minutes to launch the algorithm on NVIDIA GPU. • If you have multiple graphics cards in your system, you can assign a

	Nvidia GPU 3	specific NVIDIA GPU value to each **License Plate Recognition IV** detection tool.
Country selection		
Country name	**Australia**, **Austria**, **Bangladesh**, **Belarus**, **Brazil**, **Canada**, **China**, **Costa Rica**, **Czech Republic**, **Dubai**, **Egypt**, **Finland**, **France**, **Germany**, **Great Britain**, **India**, **Indonesia**, **Iraq**, **Israel**, **Italy**, **Japan**, **Kazakhstan**, **Kuwait**, **Mexico**, **Monaco**, **Mongolia**, **Netherlands**, **Pakistan**, **Poland**, **Qatar**, **Republic of South Africa**, **Russia**, **Saudi Arabia**, **Slovenia**, **South Korea**, **Spain**, **Sri Lanka**, **Switzerland**, **Taiwan**, **Thailand**, **Turkey**, **Ukraine**, **United Arab Emirates**, **United States of America**, **Uzbekistan**, **Vietnam**	Select from the list the country whose license plates you want to recognize and select the recognition accuracy: a. **High load, high recognition**—provides maximum recognition accuracy, but creates a high load on the CPU and/or graphics processing unit (GPU). b. **Medium load, medium recognition**—provides high recognition accuracy, requires less computing resources than at maximum accuracy. c. **Low load, low recognition**—provides the fastest recognition speed, while lowering recognition accuracy

In the window, specify the area in which license plate detection and recognition will be performed. You can adjust the area by moving the anchor points .



Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

Activating the license for the License plate recognition IV in Linux OS

To activate the license of the License plate recognition IV, do the following:

1. Submit to the technical support the MAC address of the Server where the detection tool will be used.

   > ⚠ **Attention!**
   >
   > The detection tool will not work on the Server with a different MAC address.

2. Get the license activation key from the technical support.
3. Create the LicenseFile_LprIV.txt file and put it into the /opt/AxxonSoft/DetectorPack/ folder.

   ```
   sudo touch /opt/AxxonSoft/DetectorPack/LicenseFile_LprIV.txt
   ```

4. Enter the received key into the LicenseFile_LprIV.txt file.

   ```
   echo '<License activation key>' | sudo tee -a /opt/AxxonSoft/DetectorPack/LicenseFile_LprIV.txt
   ```

5. Restart the Server.

   ```
   sudo reboot
   ```

Activating the license of the License plate recognition IV is complete.

License Plate Recognition RR and Vehicle Recognition RR

Functionality of License Plate Recognition RR and Vehicle Recognition RR

Description

The **License Plate Recognition RR** detection tools are used to:

1. Recognize license plates of vehicles. List of supported countries:
   Armenia, Austria, Azerbaijan, Argentina, Belarus, Belgium, Brazil, Brunei, Bulgaria, China, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Indonesia, Italy, Ivory Coast, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Moldova, Myanmar, Netherlands, Panama, Paraguay, Peru, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, Tajikistan, Turkmenistan, Ukraine, Uruguay, USA (starting with *Detector Pack* 3.12), Uzbekistan, Venezuela, Vietnam
2. Write the recognized license plates into a database
3. Check the recognized license plates on the lists of license plates
4. Determine the vehicle driving direction

Depending on the features required, *Axxon One* offers three types of the **License Plate Recognition RR** detection tools:

1. **License Plate Recognition RR** recognizes license plates based on the created lists. Recognition is performed in the Fast mode (video stream processing at a speed of up to 30 FPS).
2. **License Plate Recognition RR—Search In Archive** recognizes license plates in the archive. Recognition is performed in the Fast mode (video stream processing at a speed of up to 30 FPS). This detection tool generates events with a 30-second delay after the license plate recognition.
3. **License Plate Recognition RR—Parking** recognizes license plates based on the created lists. Recognition is performed in the Slow mode (video stream processing at a speed of up to 6–7 FPS). The sampling rate for the detection tool is 150 milliseconds, all other frames are skipped

The **Vehicle Recognition RR** detection tool is used to:

1. Recognize the color of a vehicle: Beige, White, Yellow, Green, Brown, Red, Unknown, Orange, Gray, Blue, Purple, Black
2. Recognize the class of a vehicle: Bus, Car, Truck, Unknown, Mini truck, Motorcycle
3. Recognize the make and model of a vehicle

Make	Model	Vehicle class
Acura	MDX, RDX, TLX, ZDX	Car
Alfa Romeo	147, 159, Brera, Giulietta, MiTo	
Asia	Rocsta	
Aston Martin	DB11, DB9, Rapide, V8 Vantage, Vanquish	
Audi	100, 80, 90, A1, A3, A4, A5, A6, A7, A8, Cabriolet, Q3, Q5, Q7, R8, RS4, RS5, RS6, RS Q3, S3, S5, S6, S8, SQ5, TT	
Autosan	H10 12	Bus
Avia	D Series	Truck
BAW	Fenix	
BAZ	A079 Etalon	Bus
BMW	1 Series, 2 Series, 3 Series, 4 Series, 5 Series, 6 Series, 7 Series, X1, X3, X4, X5, X6, Z3, Z4	Car
BYD	F3	
Beifang Benchi	BFC6123C	Truck
Bentley	Arnage, Bentayga, Continental, Flying Spur, Mulsanne	Car
Berkhof	Axial, Excellence	Bus
Beulas	Eurostar	
Bogdan	2110, 2310, Lada 2310 Pickup, Lada 2312	Car

	A092, A201, A202	Bus
Brilliance	V5	Car
Bronto	Niva	
Buerstner	Ixeo	Mini truck
CNHTC	Howo ZZ Series	Truck
Cadillac	ATS, CTS, Escalade, SRX, STS, XT5	Car
Carrus	Regal, Star	Bus
Changan	CS35	Car
Chery	A13, A15, A21, Amulet A15, Arrizo 7, Fora, Indis, Kimo S12, S12, S18D, T11, T21, Tiggo, Tiggo 5	
Chevrolet	Aveo, Blazer, Camaro, Caprice, Captiva, Cobalt, Cruze, Epica, Express, Lacetti, Lanos, Malibu, Niva, Orlando, Rezzo, Spark, Suburban, Tahoe, TrailBlazer, Viva	
Chrysler	300, 300C, Concorde, Grand Voyager, PT Cruiser, Pacifica, Sebring, Town and Country, Voyager	
Citroen	BX, Berlingo, C1, C2, C3, C3 Picasso, C4, C4 AirCross, C4 Picasso, C5, C Crosser, C Elysee, DS3, DS4, DS5, Grand C4 Picasso, Xantia, Xsara, Xsara Picasso	
	Jumper, Jumpy	Mini truck
DAF	95, 95 XF, CF, FT, FT CF, FT XF, XF	Truck
DS	4	Car
DW Hower	H3	
Dacia	Logan MCV, Sandero	
Daewoo	BS106	Bus
	Espero, Gentra, Lanos, Leganza, Matiz, Nexia, Nubira	Car
Daihatsu	Materia, Mira, Move, Sirion, Tanto, Terios, YRV	
Datsun	mi DO, on DO	
Derways	Plutus	
Dodge	Caliber, Caravan, Challenger, Durango, Grand Caravan, Intrepid, Journey, Magnum, Neon, Nitro, Ram, Stratus	
DongFeng	DFL	Truck
	H30 Cross, S30	Car
Doninvest	Kondor	
Drogmoller	EuroComet	Bus
EOS	200, 233, 90	
Elnagh	Baron, Nobel Art	Mini truck
Emgrand	EC7, X7, Phantom	Car
FAW	Besturn B50, Besturn X80, V5	
FIAT	500, Albea, Brava, Bravo, Doblo, Grande Punto, Linea, Panda, Punto, Stilo Uno	
	Ducato, Scudo	Mini truck
Ferrari	458, 488, 612, California, F12, F141, F149, F430, GTC4 Lusso	Car

Ford	C Max, EcoSport, Edge, Escape, Escort, Expedition, Explorer, F 150, Fiesta, Focus, Focus C Max, Freestar, Fusion, Galaxy, Granada, Grand C Max, Ka, Kuga, Maverick, Mondeo, Mustang, Probe, Ranger, S Max, Scorpio, Sierra, Taunus, Taurus, Tourneo Connect, Transit Connect	
	Cargo	Truck
	Tourneo, Transit, Transit Custom	Mini truck
Foton	1049, Auman, Aumark, BJ	Truck
FoxBus	22501	Bus
Freightliner	Argosy, Business Class, CL Series, CST, Century, Century Class, Columbia, FLC, FLD, FLD SD, FL Series, M2, ST Series	Truck
GAZ	172200 Volga, 24 Volga, 31 Volga, 69, Volga Siber	Car
	1724 Gazel, 22 Gazel, 23 Gazel, 27 Gazel, 3221 Gazel, 32 Gazel, 3302 Gazel, 3310 Valday, 33 Gazel, GAZel Biznes, GAZon Next, Gazel, Gazel Next	Mini truck
	3307, 3308 Sadko, 3309, 52, 53, 66, SAZ 2507, SAZ 3507	Truck
GolAZ	5291 Cruise	Bus
Golden Dragon	XML6126, XML6957	
GMC	Yukon	Car
Geely	CK, Emgrand, GC6, MK	
Genesis	G80	
Great Wall	Hover, Hover H3, Hover H5, Hover H6, Hover M2, Hover M4	
HUMMER	H2, H3	
Hafei	Simbo	
Haima	3, 7	
Haval	H6, H9	
Higer	A80, KLQ	Bus
Hino	300 Series, 500 Series, Profia, Ranger	Truck
Honda	Accord, Accord Crosstour, Airwave, CR V, Civic, Civic Ferio, Crossroad, Crosstour, Element, Freed, Freed Spike, HR V, Integra, Jazz, Legend, Odyssey, Pilot, Prelude, Stepwgn, Stream, Torneo	Car
Hymer	Mobil	Mini truck
Hyundai	Accent, Avante, Coupe, Creta, Elantra, Equus, Galloper, Genesis, Genesis Coupe, Getz, Grand Santa Fe, Grand Starex, Grandeur, H 1, Matrix, NF, Santa Fe, Solaris, Sonata, Starex, Terracan, Tiburon, Trajet, Tucson, Tuscani, Veloster, i20, i30, i40, ix35, ix55	Car
	Aero City, County, Universe, Universe Space	Bus
	HD	Truck
	Porter	Mini truck
Ikarus	250, 256, 260, 280	Bus
Infiniti	EX Series, FX Series, G Series, JX Series, M Series, QX Series, Q Series	Car
International	9000 Series	Truck
Iran Khodro	Samand	Car
Irisbus	Crossway, Magelys	Bus

Isuzu	Axiom	Car
	AF, Elf, F Series, Forward, NPR, N Series	Truck
Iveco	AMT, EuroCargo, EuroStar, EuroTech, Stralis, Trakker	Truck
	Daily, TurboDaily	Mini truck
Izh	2125, 2126, 21261 Fabula, 2715, 2717, 412	Car
JAC	HK6120 KY	Bus
	S5	Car
JMC	Carrying	Truck
Jaguar	F Pace, F Type, S Type, XE, XF, XJ, XK, XKR, X Type	Car
Jeep	Cherokee, Commander, Compass, Grand Cherokee, Liberty, Renegade, Wrangler	
Jonckheere	Deauville	Bus
KAvZ	3976, 4235, 4238	
KIA	Bongo	Mini truck
	Carens, Carnival, Ceed, Cerato, Magentis, Mohave, Opirus, Optima, Picanto, Quoris, Rio, Rio X Line, Sorento, Soul, Spectra, Sportage, Stinger, Venga, Pro ceed	Car
	Granbird	Bus
KamAZ	4308, 4310, 44108, 4539, 5308, 5321, 5410, 5411, 5460, 5490, 551, 5511, 6460, 6511, 6520, 6522, NefAz 4208	Truck
Kenworth	T2000, W900	
King Long	XMQ	Bus
KrAZ	6322	Truck
LDV	Maxus	Mini truck
Lamborghini	Aventador, Gallardo	Car
Lancia	Delta	
Land Rover	Defender, Discovery, Discovery Sport, Freelander, Range Rover, Range Rover Evoque, Range Rover Sport, Range Rover Velar	
Lexus	CT, ES, GS, GX, IS, LC, LS, LX, NX, RX, SC	
LiAZ	4292, 5256, 5292, 5293, 6213, 677	
Liebherr	LTM	Truck
Lifan	Breez, Cebrium, Smily, Solano, Solano II, X60	Car
Lincoln	Aviator, Continental, LS, MKS, MKT, MKX, Navigator, Town Car	
MAN	F2000, F90, L2000, LE2000, M2000, M90, ME2000, TGA, TGL, TGM, TGS, TGX	Truck
	Lions Coach, Lions Regio, Lions Top Star	Bus
MAZ	103, 107, 152, 203, 206	
	43, 53, 54, 55, 63, 64, 65	Truck
MG	ZT T	Car
MINI	Clubman, Cooper, Countryman, Hatch	

Marcopolo	Andare, Bravis	Bus
Maserati	Ghibli, Levante, Quattroporte	Car
Maybach	57, 62	
Mazda	2, 3, 323, 5, 6, 626, BT 50, Bongo, Bongo Friendee, CX 5, CX 7, CX 9, Capella, Demio, Familia, MPV, MX 5, Premacy, RX 8, Titan, Tribute	
Mercedes Benz	A Klasse, B Klasse, CLA Klasse, CLK Klasse, CLS Klasse, CL Klasse, C Klasse, Citan, E Klasse, GLA Klasse, GLC Klasse, GLE Klasse, GLK Klasse, GLS Klasse, GL Klasse, G Klasse, M Klasse, R Klasse, SLK Klasse, SL Klasse, S Klasse, X Klasse	
	Actros, Atego, Axor, LK Series, SK Series	Truck
	MB Series, Sprinter, T1, T2, V Klasse, Vario, Viano, Vito	Mini truck
	Travego, Conecto, O303, O330, O350 Tourismo, O403, O404, O405, O560 Intouro	Bus
Mercury	Grand Marquis, Mariner, Mystique, Villager	Car
Mitsubishi	ASX, Airtrek, Carisma, Colt, Delica, Delica Space Gear, Eclipse, Galant, Grandis, L200, Lancer, Lancer Cargo, Lancer Cedia, Lancer Evolution, Legnum, Outlander, Outlander XL, Pajero, Pajero Mini, Pajero Pinin, Pajero Sport, Pajero iO, RVR, Space Gear, Space Wagon	
	Canter, Fuso Canter, Fuso Fighter	Truck
Moskvich	2137, 2140, 2141, 403, 408, 412	Car
Multicar	M25, M26	Mini truck
Nefaz	5299	Bus
Neoplan	Cityliner, Euroliner, Jetliner, Skyliner, Spaceliner, Starliner, Transliner	
Nissan	AD, Almera, Almera Classic, Atlas, Avenir, Bluebird, Bluebird Sylphy, Cedric, Cefiro, Cube, Expert, GT R, Juke, Laurel, Liberty, March, Maxima, Maxima QX, Micra, Murano, NP300 Pickup, Navara, Note, Pathfinder, Patrol, Presage, Primera, Pulsar, Qashqai, Qashqai 2, Safari, Sentra, Serena, Skyline, Sunny, Teana, Terrano, Terrano II, Tiida, Vanette, Wingroad, X Trail	Car
	Cabstar, Diesel Condor	Mini truck
Noge	Vesubio	Bus
Oldsmobile	Alero	Car
Opel	Antara, Ascona, Astra, Calibra, Combo, Corsa, Frontera, Insignia, Kadett, Meriva, Mokka, Monterey, Omega, Rekord, Tigra, Vectra, Zafira	
	Vivaro	Mini truck
Perodua	Alza, Aruz, Ativa, Axia, Bezza, Kancil, Kelisa, Kembara, Kenari, Myvi, Nippa, Viva	Car
	387	Truck
Peugeot	1007, 106, 107, 2008, 205, 206, 207, 208, 3008, 301, 306, 307, 308, 4007, 4008, 405, 406, 407, 408, 5008, 508, 605, 607, 806, 807, Partner, RCZ	Car
	Boxer, Expert, Expert Tepee, Traveller	Mini truck
Plymouth	Neon, Voyager	Car
Pontiac	Bonneville, Firebird, Grand Am, Grand Prix, Solstice, Sunfire, Trans Sport, Vibe	Car
Porsche	911, 924, 928, Boxster, Cayenne, Cayman, Macan, Panamera, Taycan	Car
RAM	ProMaster City	Mini truck
Ravon	Gentra, Matiz, Nexia, Nexia R3, R2, R4	Car

Renault	19, 21, 25, Arkana, Captur, Clio, Dokker, Duster, Espace, Fluence, Grand Scenic, Kadjar, Kangoo, Koleos, Kwid, Laguna, Latitude, Logan, Logan Stepway, Megane, Modus, Oroch, SR, Safrane, Sandero, Sandero Stepway, Scenic, Symbol, Talisman, Twingo, Vel Satis, Wind, ZOE	Car
	Kerax, Magnum, Midlum, Premium, T Series	Truck
	Mascott, Master, Trafic	Mini truck
Skoda	Citigo, Fabia, Favorit, Felicia, Forman, Kamiq, Karoq, Kodiaq, Octavia, Praktik, Rapid, Roomster, Superb, Yeti	Car
Subaru	Ascent, B9 Tribeca, BRZ, Crosstrek, Domingo, Exiga, Forester, Impreza, Impreza WRX, Impreza WRX, Impreza XV, Justy, Legacy, Legacy Lancaster, Legacy Outback, Leone, Levorg, Outback, Pleo, Pleo Plus, R1, R2, SVX, Sambar, Stella, Traviq, Trezia, Tribeca, Vivio, WRX, XV	Car
Suzuki	Aerio, Alto, Baleno, Cervo, Ciaz, Cultus, Ertiga, Escudo, Esteem, Every, Forenza, Grand Vitara, Hustler, Ignis, Jimny, Kei, Kizashi, Landy, Liana, Palette, SX4, SX4 S Cross, Samurai, Sidekick, Solio, Splash, Swift, Vitara, Wagon R, XL7, Xbee	Car
	Spacia	Mini truck
Toyota	4Runner, Agya, Allex, Allion, Alphard, Altezza, Aqua, Aristo, Auris, Avalon, Avanza, Avensis, Avensis Verso, Aygo, Belta, Blade, Brevis, C HR, Caldina, Cami, Camry, Camry Gracia, Camry Solara, Carina, Carina E, Carina ED, Cavalier, Celica, Celsior, Chaser, Corolla, Corolla Allex, Corolla Axio, Corolla Ceres, Corolla Cross, Corolla Fielder, Corolla II, Corolla Levin, Corolla Rumion, Corolla Runx, Corolla Spacio, Corolla Verso, Corona, Corona Exiv, Corona Premio, Corsa, Cresta, Crown, Crown Majesta, Curren, Cynos, Duet, Echo, Esquire, Estima, Estima Emina, Estima Lucida, Etios, FJ Cruiser, Fortuner, Fun Cargo, GT86, Gaia, Grand Hiace, Hiace Regius, Highlander, Hilux, Hilux Surf, Innova, Ipsum, Isis, Ist, Kijang, Kluger, Land Cruiser, Land Cruiser Prado, Lite Ace, Lite Ace Noah, MR2, MR S, Mark II, Mark II Blit, Mark II Qualis, Mark X, Mark X Zio, Master Ace Surf, Matrix, Nadia, Noah, Opa, Paseo, Passo, Passo Sette, Picnic, Pixis Epoch, Pixis Joy, Pixis Space, Pixis Van, Platz, Porte, Premio, Previa, Prius, Probox, Progres, Pronard, RAV4, Ractis, Raize, Raum, Roomy, Rush, Sai, Scepter, Sequoia, Sera, Sienna, Sienta, Soarer, Spade, Sparky, Sprinter, Sprinter Carib, Sprinter Marino, Sprinter Trueno, Starlet, Succeed, Supra, Tacoma, Tank, Tercel, Town Ace, Town Ace Noah, Tundra, Urban Cruiser, Vanguard, Vellfire, Venza, Verossa, Verso, Vios, Vista, Vista Ardeo, Vitz, Voltz, Voxy, Will, Windom, Wish, Yaris, Yaris Verso	Car
	Dyna, Granvia, Hiace, ProAce, Regius, Regius Ace, Toyo Ace	Mini truck
Volkswagen	Amarok, Arteon, Atlas, Beetle, Bora, Caddy, Corrado, CrossPolo, Eos, EuroVan, Fox, Fusca, Gol, Golf, Golf, ID3, ID4, ID6, Jetta, Lavida, Lupo, Multivan, New Beetle, Nivus, Parati, Passat, Passat Alltrack, Passat CC, Phaeton, Pointer, Polo, Routan, Santana, Saveiro, Scirocco, Sharan, Spacefox, T Cross, T Roc, Talagon, Taos, Tavendor, Tayron, Teramont, Tharu, Tiguan, Touareg, Touran, Type 1, Type 2, Up, Vento, Viloran, Virtus, Voyage	Car
	California, Caravelle, Crafter, LT, Transporter	Mini truck
Volvo	240 Series, 300, 440, 460, 740, 760, 850, 940, 960, C30, C70, S40, S60, S70, S80, S90, V40, V40 Cross Country, V50, V60 Cross Country, V70, V70XC, V90 Cross Country, XC40, XC60, XC70, XC90	Car
	7300, 7350, 8900, 9500, 9700, 9900, B10	Bus
	F12, FE, FH, FL, FM, FMX, VN Series	Truck

Licensing	For the detection tools to operate, contact an AxxonSoft manager and get a license file (see Types of licenses)
Add-ons	For the **License Plate Recognition RR** detection tools and **Vehicle Recognition RR** detection tool to operate, you must install the License Plate Recognition RR add-on (see Installing DetectorPack add-ons)

Hardware requirements for License Plate Recognition RR and Vehicle Recognition RR

Hardware requirements

If License Plate Recognition RR and Vehicle Recognition RR run on GPU, the following hardware requirements must be met:

1. The detection tools can run only on NVIDIA devices with at least 1.4 GB of video memory or more.
2. NVIDIA driver version 450.36.06 or higher.
3. CPU with the support for the AVX2 instruction set that is listed here.
4. Compute Capability from 3.5 to 7.5 inclusive.

> **Note**
>
> You can check the GPU Compute Capability version on the manufacturer's website.

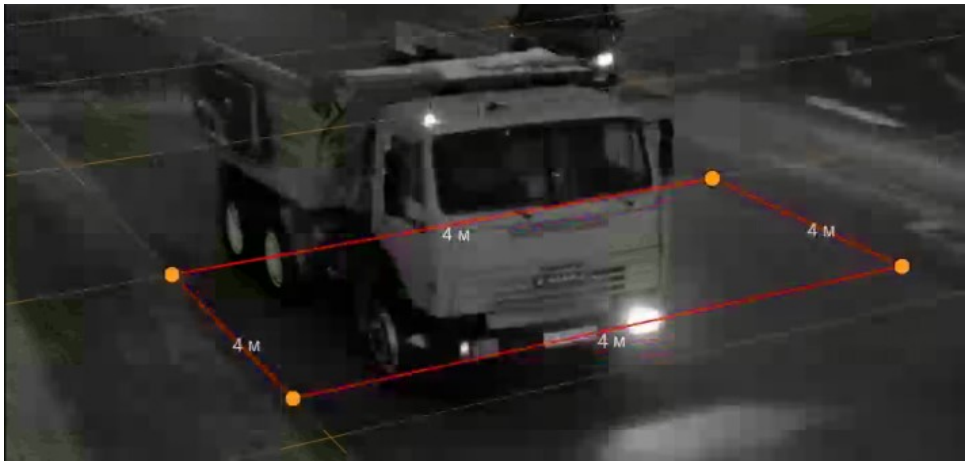
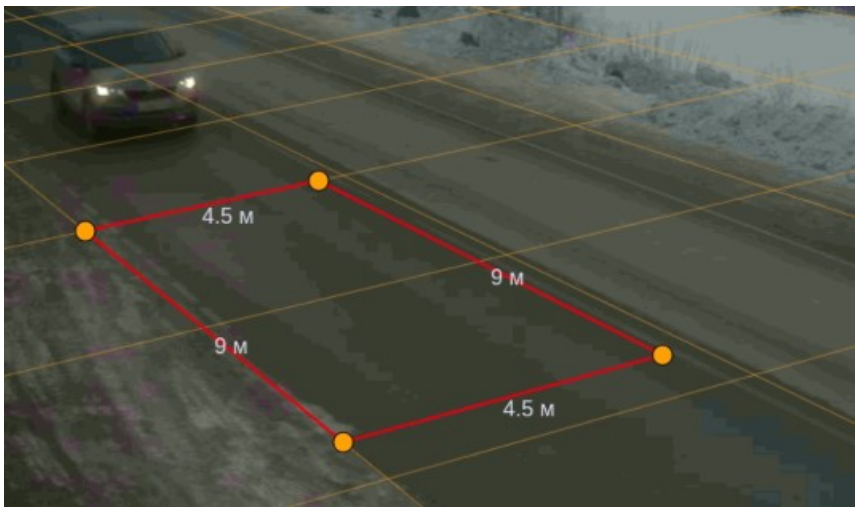
Camera requirements for License Plate Recognition RR, Vehicle Recognition RR and their sub-tools

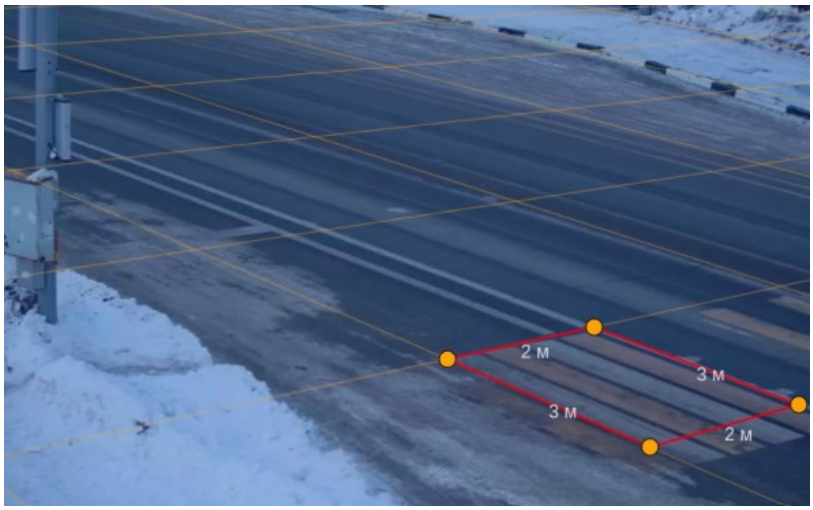
You must install and configure the cameras in such a way that the following requirements are met:

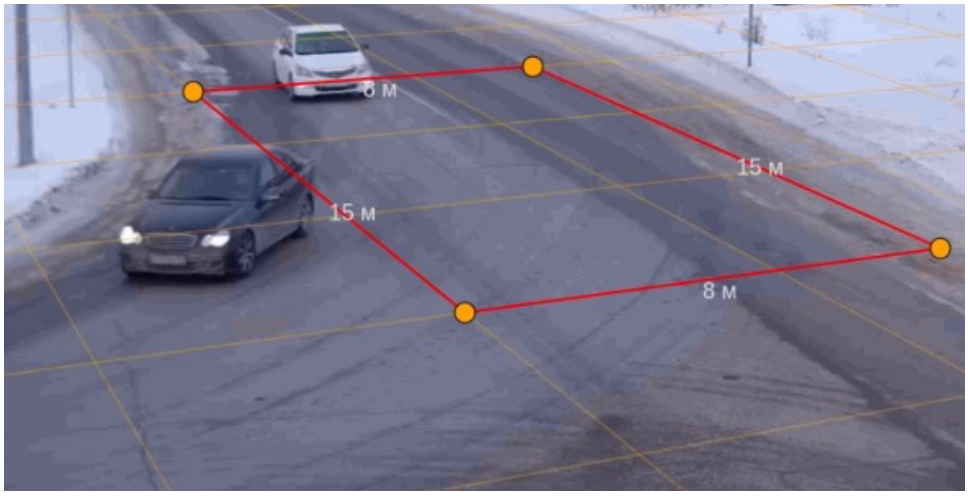
Type of requirements	Purpose	Requirements for the video image from the camera that will be used for detection	
Basic requirements	To ensure the recognition of state license plates and vehicles	Camera	• Minimum resolution is 1280*720, recommended resolution is 1920*1080 and more • Video codec: MJPEG minimum, H.264 or H.265 are recommended, preferably uncompressed • Bitrate: depends on the frame (license plate must be readable) • Minimum frame rate: at least five FPS at speed up to 20 km/h (Slow mode), from 20 FPS at speed over 20 km/h (Fast mode) • Maximum horizontal angle is 30°, recommended angle is 0° • Maximum vertical angle is 45°, recommended angle is 20° • Maximum camera rotation angle is 20°, recommended angle is 0° • In order to recognize state license plates on high-speed roads, the camera must have the Global Shutter mode
		Lighting	• Illuminated control area. We recommend using conventional spotlights and/or cameras with IR illumination for additional illumination • Expected image contrast: the contrast difference between characters of the license plate and the background must be at least 20 units with the image brightness scale from 0 to 255 • During daytime and nighttime, we recommend selecting the values of the light sensitivity (ISO) parameter separately with the minimum exposure time (maximum shutter speed)
		Scene	• We recommend installing camera in such a way that various objects that block the vehicle during its recognition are not in the frame. For example, a barrier or fence • The state license plate must be readable • Height of characters (letters and digits) on the state license plates is at least 10px and not more than 60px. Preferably 20px or more • Width of the dash board: minimum 80 pixels, recommended 100 pixels • Thickness of the character line: minimum 1 pixel, recommended 2 pixels • Vehicles during the passage must be completely within the camera FOV for at least five frames • The size of the vehicle's bounding rectangle: 1. Minimum: height/width is at least 150px and at least 15% of the frame height/width. Recommended: 250px/30%. 2. Maximum: height/width isn't limited, but no more than 80% of the height/width of the frame
		Object images	• To avoid blurring of the image, you must set the camera to a slow shutter speed. We recommend keeping the shutter speed of not more than three ms. The exact value depends on the camera angle and vehicle speed
Additional requirements	To determine the speed of the vehicle	• Camera installation height is at least four meters • The time period when a vehicle is in front of the camera with a fully readable state license plate, or when a vehicle that is fully in the frame and accurately recognized must be at least 500 ms • Time stamps for frames must not differ from the real time by more than two ms • When calibrating values, the measured road section must be at least three meters wide and five meters long. In this case, the key points in the image must be at least 300 pixels apart. The measurement error during calibration (difference between actual and entered measured values) must not exceed 1% • Camera must be rigidly fixed and must not move during gusts of wind and other physical forces • All of the following rules must be followed by default: ◦ The bounding rectangle of the state license plates doesn't touch the bottom part of the frame in both selected frames for speed calculation ◦ The offset of the center of the rectangle between the two selected frames is at least four meters and 100 pixels ◦ The time difference between two selected frames is at least 100 ms  Recommendations for configuring the speed detection area	

	To determine the driving direction of the vehicle	• Camera installation height is at least three meters • Angle between camera and road direction is not more than 30° • Minimum camera tilt
	To recognize the make and model of the vehicle	• Visible width of the vehicle is from 100px • Color or black and white image • Front view of the vehicle
	To recognize the color of the vehicle	• Visible width of the vehicle is from 100px • The scene illumination must be at least 50 lux. Under low or excessive illumination (night or backlight), the stability of the analytics operation is not guaranteed. There are no abrupt changes in illumination • Color image with a normal color grade
	To determine the condition of the headlights	• Visible width of the vehicle is from 100px • Front view of the vehicle • Evening, night or foggy shooting conditions are required

Recommendations for configuring the speed detection area

Recommendations	1. You must install the camera according to the requirements (see Camera requirements for License Plate Recognition RR, Vehicle Recognition RR and their sub-tools). 2. You must select an area in the frame that meets the following conditions: a. The sides of the selected area (**Speed detection area height** and **Speed detection area width**) must be equal in pairs. b. The angles of the selected area must be 90° in the real world. 3. When you specify the area in the Surveillance window, you must focus on: a. Traffic lanes (solid and broken lines on the roadway). b. Road curbs. c. Vehicle bumpers and wheel contact points with the roadway. d. Crosswalks. 4. The quality of vehicle recognition will be higher if the selected area occupies a significant part of the frame and is as close to the camera as possible. 5. You can use the dimensions of a particular vehicle as a reference point. For example, Hyundai Solaris: length (**Speed detection area heigh**)—2.6 meters, width (**Speed detection area width**)—1.73 meters **Attention!** Margin of error in determining the speed of vehicles is about 5% with a good calibration, as this function gives only a general idea of the situation. The consumption of resources doesn't change when the **Speed detection** parameter is enabled.
Examples of the corresponding selected area	Lines are parallel to road marking and vehicle bumpers:  


2 м
3 м
3 м
2 м


8 м
15 м
15 м
8 м

Optimizing the operation of License Plate Recognition RR and Vehicle Recognition RR on GPU

Starting with *DetectorPack* 3.10, a utility was added to the License Plate Recognition RR add-on (see Installing DetectorPack add-ons), which allows you to create GPU neural network caches without using *Axxon One*. The presence of the cache speeds up the initialization and optimizes video memory consumption.

To optimize the operation of **License Plate Recognition RR** and **Vehicle Recognition RR** on GPU, do the following:

1. Stop the Server (see Shutting down a Server).

   > ⚠ **Attention!**
   >
   > If the system has the software running on GPU, it is necessary to stop its operation.

2. Create the **GPU_CACHE_DIR** system variable (see Appendix 9. Creating system variable) by specifying in the **Variable value** field the path to the cache location with an arbitrary folder name. For example, D:\AO_GPU_cache. The specified directory will store the cache for all used detection tools and neural networks.
3. To call the utility, open in the command line: **C:\Program Files\Common Files\AxxonSoft\DetectorPack\RoadarGpuCacheGenerator.exe** and press **Enter**.
4. Select the required cache sets by specifying the **y** value:

   a. **lpr recognition**—recognition of a vehicle license plate;
   b. **vehicle recognition**—recognition of a vehicle.

```
------------------------------
Do you need lpr recognition? y/n
y
------------------------------
Do you need vehicle recognition? y/n
y
```

When you select the **lpr recognition** cache set, you need to specify the required countries in the numeric or alphabetic form. After you select all required countries, enter the **-1** value.

```
Please choose the countries...
0. AM          15. DK         30. LT         45. RS
1. AR          16. EE         31. LU         46. RU
2. AT          17. EG         32. LV         47. SE
3. AZ          18. ES         33. MD         48. SI
4. BE          19. FI         34. MM         49. SK
5. BG          20. FR         35. MT         50. TJ
6. BN          21. GE         36. MX         51. TM
7. BR          22. GR         37. MY         52. UA
8. BY          23. HR         38. NL         53. UZ
9. CY          24. HU         39. PE         54. UY
10. CI         25. IE         40. PL         55. VE
11. CZ         26. IT         41. PT         56. VN
12. CN         27. ID         42. PA         57. US
13. DE         28. KG         43. PY
14. CO         29. KZ         44. RO

   Enter the codes of the countries, separated by enter:
   Enter -1 when you are done
Enter your choice: 46
Enter your choice: AM
Enter your choice: 11
Enter your choice: -1
```

c. When you select the **vehicle recognition** cache set without **lpr recognition**, you must choose the territory where vehicle recognition is going to be performed:

```
Do you need lpr recognition? y/n
n
------------------------------
Do you need vehicle recognition? y/n
y
```

i. **CIS countries**—1;
ii. **Other countries**—2.

```
Choose territory where vehicle recognition is going to be performed:
1. CIS
2. Other countries
1
------------------------------
```

5. Select one of the accuracy and performance values by specifying the corresponding number:
   a. **Medium accuracy, high performance**—**1**, provides medium recognition accuracy and high performance of the GPU (less load on the GPU);
   b. **High accuracy, medium performance**—**2**, provides high recognition accuracy and medium performance of the GPU (high load on the GPU).

```
------------------------------
Choose accuracy and performance for vehicle recognition:
1. Medium accuracy, high performance
2. Hight accuracy, medium performance
1
```

6. Specify the **ID** of the required GPU (see Selecting Nvidia GPU when configuring detection tools) and press **Enter**.

```
Please enter device ordinal mentioned in the list above, to generate cache for...
   NOTE: the device should have MORE than 1.4GB of free GPU memory in order to success
   NOTE: this application will fail if the GPU is being used by other applications
         please quit all such applications before starting the caching process.
   Availble choices: [0-0]
Enter your choice:
```

As a result, the process of creating cache will start, which will take about 30 minutes. The duration of the process depends on the selected types of cache, number of countries and NVIDIA GPU model.

Optimizing the operation of **License Plate Recognition RR** and **Vehicle Recognition RR** on GPU is complete.

Attention!

Cache must be recreated:

- if you update the License Plate Recognition RR add-on (see Installing DetectorPack add-ons),
- if you change the NVIDIA GPU model,
- if you update NVIDIA GPU drivers.

Configuring the License Plate Recognition RR detection tools

Configuring License Plate Recognition RR

To configure the **License Plate Recognition RR** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle License Plate Recognition RR**.

By default, the detection tool is enabled and set to recognize vehicle license plates.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes**	The parameter is disabled by default. If you want to use this detection tool to check in lists of vehicle license plates, select the **Yes** value (see Configuring vehicle license plate recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**License Plate Recognition RR**	Enter the detection tool name or leave the default name
Accuracy and performance	**Medium accuracy and high performance**	Select the accuracy and performance of vehicle recognition: • **Medium accuracy and high performance**— provides medium recognition accuracy and high GPU performance (less load on GPU); • **High accuracy and medium performance**— provides maximum recognition accuracy and medium GPU performance (high load on GPU)
	High accuracy and medium performance	
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Type	**License Plate Recognition RR**	Name of the detection tool type (non-editable field)
Advanced settings		
Event timeout	**0**	Specify the time in seconds after which the alarm must be generated after recognizing a license plate in the frame. If the value is **0**, the alarm will be generated after the track with a license plate is lost. The value must be in the range [1, 3600]

Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The value must be in the range [640, 10000]. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** fiel d, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
Minimum recognition quality, in %	**80**	Specify the minimum quality of license plates recognition as a percentage. The higher the minimum recognition quality, the fewer false alarms. The value must be in the range [0, 100]
GDPR policy	**-**	By default, on the layout and in the archive, the characters of a license plate are completely hidden "GDPR ON". To display the characters of a license plate, you must enter a value: "**-**"—hide all characters (default value), " (blank field of a parameter value)"—show all characters, "**N-**"—hide the first N characters, "**-N**"—hide the last N characters, where **N** is the number of characters
Speed detection	**Off** **Kmph**	Select from the list the mode for determining the speed unit of vehicles. **Attention!** Margin of error in determining the speed of vehicles is about 5% with a good calibration, as this function gives only a general idea of the situation. The consumption of resources doesn't change when the **Speed detection** p arameter is enabled. **Note** For the correct displaying of the speed measurement unit, you must create the MEASUREMENT_UNIT system variable (see A ppendix 9. Creating system variable) and specify the value:

	Mph	• 0—to display kmph; • 1—to display mph.
Speed detection area height	**0**	**Attention!** Before you specify the value of the **Speed detection area height** parameter, you must select the area in the preview window (see Recommendations for configuring the speed detection area). Specify the speed detection area height in meters. The value must be in the range [0, 500]
Speed detection area width	**0**	**Attention!** Before you specify the value of the **Speed detection area width** parameter, you must select the area in the preview window (see Recommendations for configuring the speed detection area). Specify the speed detection area width in meters. The value must be in the range [0, 500]
Basic settings		
Algorithm for detecting vehicle direction	**By LP coordinates** **By LP scale change**	The **By LP coordinates** algorithm is used by default. It works as follows: if the coordinates of the vehicle license plate shift from top to bottom (the vehicle moves towards the camera) and if the coordinates of the vehicle license plate shift from bottom to top (the vehicle moves away from the camera). Select the **By LP scale change** parameter if in the Surveillance window, the scale of the vehicle license plate increases (the vehicle moves towards the camera) and if the scale of the vehicle license plate decreases (the vehicle moves away from the camera)
Info on unrecognized LPs	**Yes** **No**	The parameter is disabled by default. If it is necessary to determine all possible information from unrecognized license plates, select the **Yes** value
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3**	Select the processor for the detection tool operation—CPU or NVIDIA GPU (see Selecting Nvidia GPU when configuring detection tools). **Attention!** It may take several minutes to launch the algorithm on NVIDIA GPU. You can use caching to speed up future launches (see Optimizing the operation of License Plate Recognition RR and Vehicle Recognition RR on GPU)
Vehicle recognition	**Yes** **No**	The parameter is disabled by default. If you want to search for vehicles in the archive by vehicle make, model, vehicle class, or other specified criteria, select the **Yes** value (see Search by LPs)
Country selection		

Country 1 name	**Armenia**, **Argentina**, **Austria**, **Azerbaijan**, **Bulgaria**, **Brunei**, **Belarus**, **Brazil**, **Belgium**, **China**, **Cyprus**, **Ivory Coast**, **Czech Republic**, **Germany**, **Colombia**, **Denmark**, **Estonia**, **Egypt**, **Finland**, **France**, **Georgia**, **Greece**, **Croatia**, **Hungary**, **Indonesia**, **Ireland**, **Italy**, **Kyrgyzstan**, **Kazakhstan**, **Lithuania**, **Luxembourg**, **Latvia**, **Malta**, **Malaysia**, **Mexico**, **Moldova**, **Myanmar**, **Netherlands**, **Peru**, **Poland**, **Portugal**, **Romania**, **Serbia**, **Russia**, **Sweden**, **Slovakia**, **Slovenia**, **Turkmenistan**, **Tajikistan**, **Spain**, **Ukraine**, **USA** (starting with *Detector Pack 3. 12*), **Uzbekistan**, **Vietnam**, **Not used**	In the corresponding fields, select from the list one or more countries whose license plates you want to recognize
Country 2 name		
Country 3 name		
Country 4 name		
Country 5 name		

In the window, specify the area in which license plate detection and recognition will be performed. You can adjust the area by moving the anchor points .



Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the button. To cancel the action, click this button again.
- To delete the selected area, click the button.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

Configuring License Plate Recognition RR—Parking

To configure the **License Plate Recognition RR—Parking** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle License Plate Recognition RR—Parking**.

By default, the detection tool is enabled and set to recognize vehicle license plates in the parking lot.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes** **No**	The parameter is disabled by default. If you want to use this detection tool to check in lists of vehicle license plates, select the **Yes** value (see Configuring vehicle license plate recognition based on the created lists)
Record objects tracking	**Yes** **No**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
Video stream	**Main stream** **Second stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
Other		
Enable	**Yes** **No**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
Name	**License Plate Recognition RR—Parking**	Enter the detection tool name or leave the default name
Accuracy and performance	**Medium accuracy and high performance** **High accuracy and medium performance**	Select the accuracy and performance of vehicle recognition: • **Medium accuracy and high performance**—provides medium recognition accuracy and high GPU performance (less load on GPU); • **High accuracy and medium performance**—provides maximum recognition accuracy and medium GPU performance (high load on GPU)
Decoder mode	**Auto** **CPU** **GPU** **HuaweiNPU**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
Type	**License Plate Recognition RR—Parking**	Name of the detection tool type (non-editable field)
Advanced settings		
Event timeout	**0**	Specify the time in seconds after which the alarm must be generated after recognizing a license plate in the frame. If the value is **0**, the alarm will be generated after the track with a license plate is lost. The value must be in the range [1, 3600]

Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The value must be in the range [640, 10000]. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** fiel d, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
Minimum recognition quality, in %	**80**	Specify the minimum quality of license plates recognition as a percentage. The higher the minimum recognition quality, the fewer false alarms. The value must be in the range [0, 100]
GDPR policy	**-**	By default, on the layout and in the archive, the characters of a license plate are completely hidden "GDPR ON". To display the characters of a license plate, you must enter a value: "**-**"—hide all characters (default value), " (blank field of a parameter value)"—show all characters, "**N-**"—hide the first N characters, "**-N**"—hide the last N characters, where **N** is the number of characters
Speed detection	**Off** **Kmph**	Select from the list the mode for determining the speed unit of vehicles. **Attention!** Margin of error in determining the speed of vehicles is about 5% with a good calibration, as this function gives only a general idea of the situation. The consumption of resources doesn't change when the **Speed detection** p arameter is enabled. **Note** For the correct displaying of the speed measurement unit, you must create the

	Mph	MEASUREMENT_UNIT system variable (see Appendix 9. Creating system variable) and specify the value: • 0—to display kmph; • 1—to display mph.
Speed detection area height	**0**	**Attention!** Before you specify the value of the **Speed detection area height** parameter, you must select the area in the preview window (see Recommendations for configuring the speed detection area). Specify the speed detection area height in meters. The value must be in the range [0, 500]
Speed detection area width	**0**	**Attention!** Before you specify the value of the **Speed detection area width** parameter, you must select the area in the preview window (see Recommendations for configuring the speed detection area). Specify the speed detection area width in meters. The value must be in the range [0, 500]
Basic settings		
Algorithm for detecting vehicle direction	**By LP coordinates** **By LP scale change**	The **By LP coordinates** algorithm is used by default. It works as follows: if the coordinates of the vehicle license plate shift from top to bottom (the vehicle moves towards the camera) and if the coordinates of the vehicle license plate shift from bottom to top (the vehicle moves away from the camera). Select the **By LP scale change** parameter if in the Surveillance window, the scale of the vehicle license plate increases (the vehicle moves towards the camera) and if the scale of the vehicle license plate decreases (the vehicle moves away from the camera)
Info on unrecognized LPs	**Yes** **No**	The parameter is disabled by default. If it is necessary to determine all possible information from unrecognized license plates, select the **Yes** value
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3**	Select the processor for the detection tool operation—CPU or NVIDIA GPU (see Selecting Nvidia GPU when configuring detection tools). **Attention!** It may take several minutes to launch the algorithm on NVIDIA GPU. You can use caching to speed up future launches (see Optimizing the operation of License Plate Recognition RR and Vehicle Recognition RR on GPU)
Vehicle recognition	**Yes**	

	No	The parameter is disabled by default. If you want to search for vehicles in the archive by vehicle make, model, vehicle class, or other specified criteria, select the **Yes** value (see Search by LPs)
Country selection		
Country 1 name **Country 2 name** **Country 3 name** **Country 4 name** **Country 5 name**	**Armenia**, **Argentina**, **Austria**, **Azerbaijan**, **Bulgaria**, **Brunei**, **Belarus**, **Brazil**, **Belgium**, **China**, **Cyprus**, **Ivory Coast**, **Czech Republic**, **Germany**, **Colombia**, **Denmark**, **Estonia**, **Egypt**, **Finland**, **France**, **Georgia**, **Greece**, **Croatia**, **Hungary**, **Indonesia**, **Ireland**, **Italy**, **Kyrgyzstan**, **Kazakhstan**, **Lithuania**, **Luxembourg**, **Latvia**, **Malta**, **Malaysia**, **Mexico**, **Moldova**, **Myanmar**, **Netherlands**, **Peru**, **Poland**, **Portugal**, **Romania**, **Serbia**, **Russia**, **Sweden**, **Slovakia**, **Slovenia**, **Turkmenistan**, **Tajikistan**, **Spain**, **Ukraine**, **USA** (starting with *Detector Pack 3. 12*), **Uzbekistan**, **Vietnam**, **Not used**	In the corresponding fields, select from the list one or more countries whose license plates you want to recognize

In the window, specify the area in which license plate detection and recognition will be performed. You can adjust the area by moving the anchor points .



Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the button. To cancel the action, click this button again.
- To delete the selected area, click the button.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

Configuring License Plate Recognition RR—Search In Archive

To configure the **License Plate Recognition RR—Search In Archive** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle License Plate Recognition RR—Search In Archive**.

By default, the detection tool is enabled and set to recognize vehicle license plates in the archive.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes**	The **Check in lists** parameter is disabled by default. If you want to use this detection tool to check in lists of vehicle license plates, select the **Yes** value (see Configuring vehicle license plate recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**License Plate Recognition RR—Search In Archive**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Type	**License Plate Recognition RR—Search In Archive**	Name of the detection tool type (non-editable field)
Advanced settings		

Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The value must be in the range [640, 10000]. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** fiel d, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
GDPR policy	**-**	By default, on the layout and in the archive, the characters of a license plate are completely hidden "GDPR ON". To display the characters of a license plate, you must enter a value: "**-**"—hide all characters (default value), " (blank field of a parameter value)"—show all characters, "**N-**"—hide the first N characters, "**-N**"—hide the last N characters, where **N** is the number of characters
Minimum recognition quality, in %	**80**	Specify the minimum quality of license plates recognition as a percentage. The higher the minimum recognition quality, the fewer false alarms. The value must be in the range [0, 100]
Basic settings		
Algorithm for detecting vehicle direction	**By LP coordinates** **By LP scale change**	The **By LP coordinates** algorithm is used by default. It works as follows: if the coordinates of the vehicle license plate shift from top to bottom (the vehicle moves towards the camera) and if the coordinates of the vehicle license plate shift from bottom to top (the vehicle moves away from the camera). Select the **By LP scale change** parameter if in the Surveillance window, the scale of the vehicle license plate increases (the vehicle moves towards the camera) and if the scale of the vehicle license plate decreases (the vehicle moves away from the camera)
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1**	Select the processor for the detection tool operation—CPU or NVIDIA GPU (see Selecting Nvidia GPU when configuring detection tools). **Attention!**

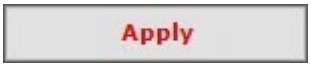
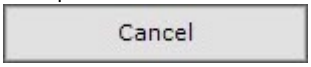
	Nvidia GPU 2	It may take several minutes to launch the algorithm on NVIDIA GPU. You can use caching to speed up future launches (see Optimizing the operation of License Plate Recognition RR and Vehicle Recognition RR on GPU)
	Nvidia GPU 3	
Country selection		
Country 1 name **Country 2 name** **Country 3 name** **Country 4 name** **Country 5 name**	**Armenia**, **Argentina**, **Austria**, **Azerbaijan**, **Bulgaria**, **Brunei**, **Belarus**, **Brazil**, **Belgium**, **China**, **Cyprus**, **Ivory Coast**, **Czech Republic**, **Germany**, **Colombia**, **Denmark**, **Estonia**, **Egypt**, **Finland**, **France**, **Georgia**, **Greece**, **Croatia**, **Hungary**, **Indonesia**, **Ireland**, **Italy**, **Kyrgyzstan**, **Kazakhstan**, **Lithuania**, **Luxembourg**, **Latvia**, **Malta**, **Malaysia**, **Mexico**, **Moldova**, **Myanmar**, **Netherlands**, **Peru**, **Poland**, **Portugal**, **Romania**, **Serbia**, **Russia**, **Sweden**, **Slovakia**, **Slovenia**, **Turkmenistan**, **Tajikistan**, **Spain**, **Ukraine**, **USA** (starting with *Detector Pack 3. 12*), **Uzbekistan**, **Vietnam**, **Not used**	In the corresponding fields, select from the list one or more countries whose license plates you want to recognize

In the window, specify the area in which license plate detection and recognition will be performed. You can adjust the area by moving the anchor points  .



Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.
- To delete the selected area, click the  button.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Configuring Vehicle Recognition RR

Hardware requirements for License Plate Recognition RR and Vehicle Recognition RR

Camera requirements for License Plate Recognition RR, Vehicle Recognition RR and their sub-tools

Optimizing the operation of License Plate Recognition RR and Vehicle Recognition RR on GPU

Parameters that specify the conditions for triggering macros when recognizing a vehicle

To configure the **Vehicle Recognition RR** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle Vehicle Recognition RR**.

By default, the detection tool is enabled and set to recognize vehicles. See the full list of possible classes of a vehicle, makes and models here.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Vehicle Recognition RR**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Type	**Vehicle Recognition RR**	Name of the detection tool type (non-editable field)
Advanced settings		
Event timeout	**0**	Specify the time in seconds after which the alarm must be generated after recognizing a vehicle in the frame. If the value is **0**, the alarm will be generated after the track with a vehicle is lost. The value must be in the range [1, 3600]
Frame processing period (msec)	**750**	Specify the time in milliseconds between the operations of vehicle search in the frame. The larger this value, the less load on the Server, but some vehicles may not be recognized. The value must be in the range [1, 10 000]

<table>
<tr><td>Frame size change</td><td>1920</td><td>The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The value must be in the range [640, 10 000]. The following algorithm is used:
If the longer side of the source image exceeds the value specified in the Frame size change field, it is divided by two.
If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further.
If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution.
Note
For example, the source image resolution is 2048*1536, and the specified value is set to 1000. I n this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.</td></tr>
<tr><td>Speed detection</td><td>Off
Kmph
Mph</td><td>Select from the list the mode for determining the speed unit of vehicles.
Attention!
Margin of error in determining the speed of vehicles is about 5% with a good calibration, as this function gives only a general idea of the situation. The consumption of resources doesn't change when the Speed detection parameter is enabled.
Note
For the correct displaying of the speed measurement unit, you must create the MEASUREMENT_UNIT system variable (see Appendix 9. Creating system variable) and specify the value:
0—to display kmph;
1—to display mph.</td></tr>
<tr><td>Speed detection area height</td><td>0</td><td>Attention!
Before you specify the value of the Speed detection area height parameter, you must select the area in the preview window (see Recommendations for configuring the speed detection area).
Specify the speed detection area height in meters. The value must be in the range [0, 500]</td></tr>
<tr><td>Speed detection area width</td><td>0</td><td>Attention!
Before you specify the value of the Speed detection area height parameter, you must select the area in the preview window (see Recommendations for configuring the speed detection area).
Specify the speed detection area width in meters. The value must be in the range [0, 500]</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td>Accuracy and performance</td><td>Medium accuracy and high performance</td><td>Select the accuracy and performance of vehicle recognition:
Medium accuracy and high performance—provides medium recognition accuracy and high GPU performance (less load on GPU);
High accuracy and medium performance—provides maximum recognition accuracy and medium GPU performance (high load on GPU)</td></tr>
</table>

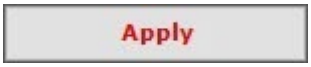
	High accuracy and medium performance	
Algorithm for detecting vehicle direction	**By LP coordinates**	The **By LP coordinates** algorithm is used by default. It works as follows: if the coordinates of the vehicle shift from top to bottom (the vehicle moves towards the camera) and if the coordinates of the vehicle shift from bottom to top (the vehicle moves away from the camera). Select the **By LP scale change** parameter if in the Surveillance window, the scale of the vehicle increases (the vehicle moves towards the camera) and if the scale of the vehicle decreases (the vehicle moves away from the camera)
	By LP scale change	
Detection mode	**CPU**	Select the processor for the detection tool operation—CPU or NVIDIA GPU (see Selecting Nvidia GPU when configuring detection tools). **Attention!** It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings.
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	
	Nvidia GPU 3	
Territory	**Countries of CIS**	Select the territory of vehicle recognition
	Other countries	

The entire frame is analyzed by default. If you want to analyze only a part of the frame, in the window specify the area in which the detection and recognition of vehicles will be performed. You can adjust the area by moving the anchor points .



Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.
- To delete the selected area, click the  button.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

The **Vehicle Recognition RR** detection tool is configured.

Parameters that specify the conditions for triggering macros when recognizing a vehicle

On this page:

- General information
- Algorithm for setting the clarifying parameters
- Example for a license plate number recognition when the vehicle is approaching the camera or moving away from it
- Example for speed determination

General information

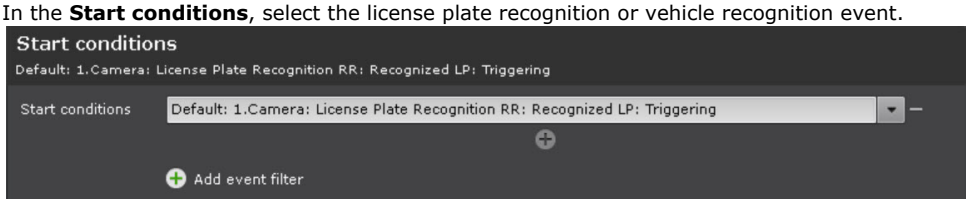
You can filter the launch of macro commands triggered by vehicle recognition by specifying the following clarifying parameters:

Parameter	Value	Max value	Description
Direction	**0**		The macro will run if the license plate was recognized when the vehicle was moving in an unspecified direction towards the video camera
	1		The macro will run if the license plate was recognized when the vehicle was approaching the video camera
	2		The macro will run if the license plate was recognized when the vehicle was moving away from the video camera
SpeedKmph	Minimum speed value in km/h	Maximum speed value in km/h	The macro will run if the license plate was recognized when the vehicle was moving within the specified speed limits
VehicleBrand	Vehicle manufacturer name (for example, **Audi**). See the full list of possible manufacturers here		The macro will run if a vehicle of a certain manufacturer was recognized
VehicleColor	Vehicle color (for example, **Black**)		The macro will run if a vehicle of a certain color was recognized
VehicleModel	Vehicle model name (for example, **A6**). See the full list of possible models here		The macro will run if a vehicle of a certain model was recognized
VehicleClass	[0, 16], where: • **0**—Unknown (vehicles whose class could not be recognized); • **1**—Car; • **2**—Truck; • **3**—Bus; • **4**—Motorcycle; • **5**—Light commercial vehicle; • **6**—Trolleybus; • **7**—Tram; • **8**—Van; • **9**—Minivan; • **10**—SUV; • **11**—Pickup truck; • **12**—Average size vehicle; • **13**—Large vehicle; • **14**—Heavy-duty vehicle; • **15**—Special vehicle; • **16**—Dump truck		The macro will run if a vehicle of a certain class was recognized

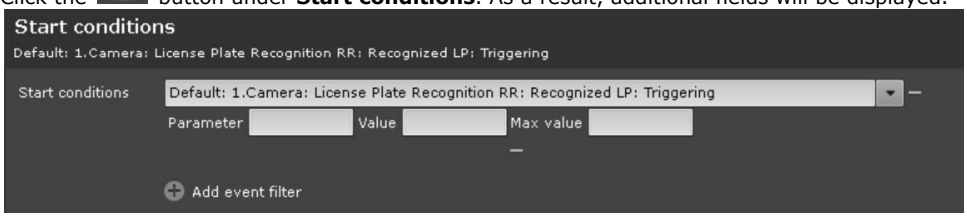
Algorithm for setting the clarifying parameters

To set the parameters that specify the conditions for triggering macros, do the following:

1. In the **Start conditions**, select the license plate recognition or vehicle recognition event.

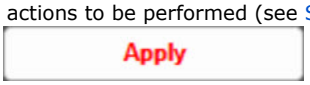


2. Click the  button under **Start conditions**. As a result, additional fields will be displayed.



3. In the **Parameter** field, specify the required parameter.

> **Attention!**
>
> The parameter value is case sensitive.

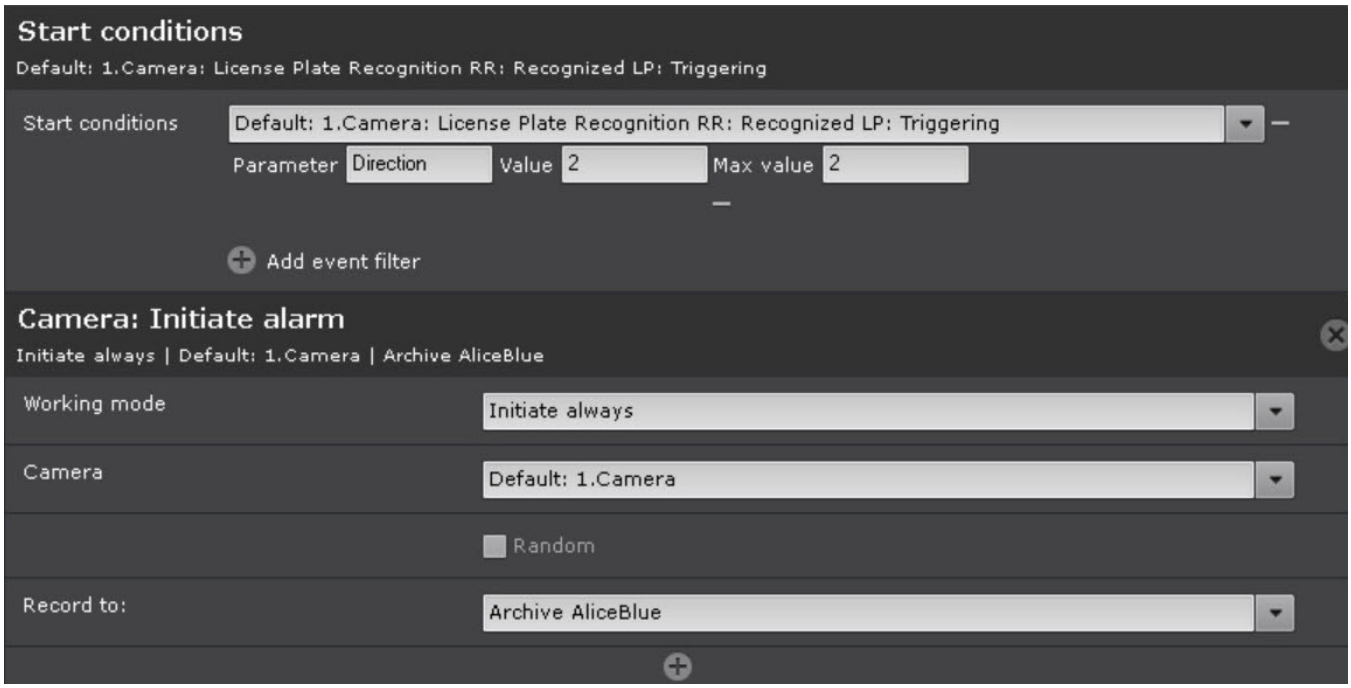
4. Depending on the parameter used, in the **Value** and **Max value** fields, set the range of values within which the macro will be triggered.
5. Set one or more actions to be performed (see Settings specific to actions).
6. Click the **Apply** 

button.

The clarifying parameters are set.

Example for a license plate number recognition when the vehicle is approaching the camera or moving away from it

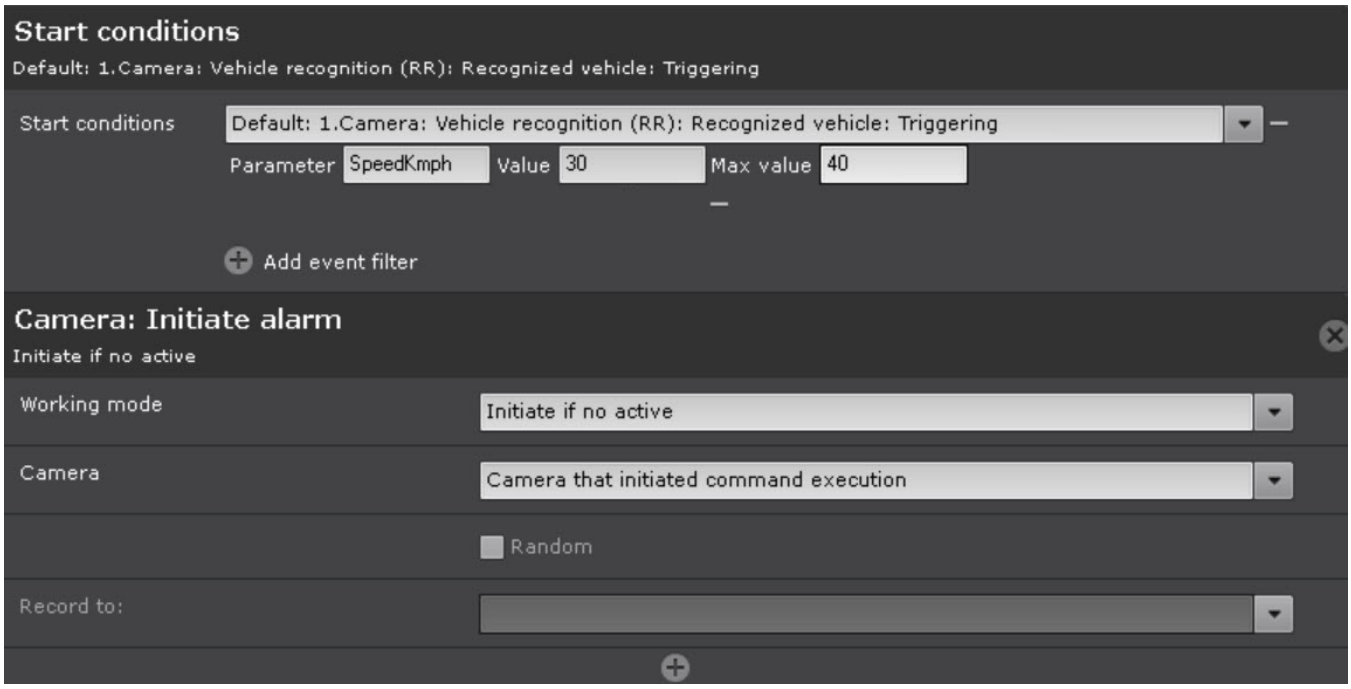
You can configure a macro to trigger an alarm if a license plate number is recognized when the vehicle is approaching or moving away from the video camera. To configure this macro, you should first create and configure the **License Plate Recognition RR** detection tool (see Configuring License Plate Recognition RR).



In this case, the alarm will be triggered when the license plate number is recognized while the vehicle is moving away from the video camera.

Example for speed determination

You can configure a macro to trigger an alarm if a vehicle is recognized at a certain vehicle speed. To configure this macro, you should first create and configure the **Vehicle Recognition RR** detection tool (see Configuring Vehicle Recognition RR). You should also select the **Speed detection** value as **Kmph** in the detection tool settings.



In this case, the alarm will be triggered when a vehicle is recognized within a speed range of 30-40 km/h.

License plate recognition VT

License plate recognition (VT) features and specifications

License plate recognition (VT) (Automatic Number Plate Recognition Tool) is designed to implement the following functions:

1. Recognize vehicle license plates. The full list of supported countries:

Proven installations	Tested
LPR VT is already used in multiple deployments to recognize the license numbers of the countries, listed below	LPR VT is comprehensively tested in recognition of license plates of countries listed below. The results quality obtained in test environment is satisfactory. However, LPR VT is not yet used in actual installations in these countries

• Albania • Argentina • Austria • Azerbaijan • Belarus • Belgium • Brazil • Bulgaria • Chile • Colombia • Czech Republic • France • Georgia • Guatemala • Hungary • Iran • Israel • Jordan • Kazakhstan • Latvia • Lithuania • Mexico • Moldova • Mongolia • Netherlands • Paraguay • Poland • Russia • Spain • Taiwan • Ukraine • United Kingdom • Uruguay • Uzbekistan	• Algeria • Andorra • Armenia • Australia • Bahrain • Bolivia • Bosnia and Herzegovina • Botswana • Brunei • Canada • Croatia • Denmark • Ecuador • El Salvador • Estonia • Finland • Germany • Greece • Honduras • Hong Kong • India • Indonesia • Italy • Kenya • Korea Republic • Kyrgyzstan • Liechtenstein • Luxembourg • Malaysia • Malta • Monaco • Montenegro • New Zealand • Nicaragua • Nigeria • Norway • Panama • Peru • Philippines • Portugal • Romania • Serbia • Singapore • Slovakia • Slovenia • South Africa • Sri Lanka • Sweden • Switzerland • Tajikistan • Tunisia • Turkey • Turkmenistan • USA • Vietnam • Zambia

2. Write a recognized number to a database.
3. Check the recognized license plates of vehicles on the lists of license plates (see Configuring macros when working with vehicles lists).
4. Determine the direction of the vehicle.

License plate recognition (VT) works in one of the following modes (see Configuring License Plate Recognition VT):

1. Fast—it processes video feeds up to 25 fps with a maximum vehicle speed of 180 km/h.
2. Slow—it processes video feeds up to 6 fps with a maximum vehicle speed of 20 km/h.

> **Note**
>
> Install the additional Addon VT LPR to work with License plate recognition (VT) (see Installing DetectorPack add-ons).

Hardware requirements for License Plate Recognition VT

Hardware requirements

License Plate Recognition VT can run on the following devices: CPU, Intel GPU, VPU (IntelNCS).

For NVIDIA GPUs:

Attention!

GPUs with NVIDIA Ampere architecture aren't supported.

1. Compute Capability 3.5 and higher.

   Note

   You can check the GPU Compute Capability version on the manufacturer's website.

2. Support for CUDA 10.2 or higher.
3. Processor with support for SSE4.1 / SSE4.2 instructions.

You can find the list of supported devices at OpenVINO™ toolkit.

Camera requirements for License plate recognition (VT)

On this page:

- General requirements
- Video camera requirements
- Camera installation requirements
- License plate image requirements
- Recommendations for highways

To ensure the recognition of state license plates using the License plate recognition (VT), it is necessary to install and configure video cameras in such a way that the requirements described below are met.

General requirements

1. The video camera must be permanently installed.
2. In order to recognize state license plates on highways, the camera should have the Global Shutter mode.
3. The frame size is at least 704*288 px.
4. The character height for IP cameras is at least 20-30 px, for analog cameras—at least 14-20 px, the stroke width is at least 2 px. If it is necessary to recognize two-line license plates, then these requirements are relevant for each line.
5. The minimum allowable contrast in case of even staining of the license plate must be at least 20% (contrast visibility of characters relative to the background is 25 units with a 256-point scale).
6. The maximum allowable uneven staining is not more than 12% (the ratio of the stained area to the total area of the license plate).
7. The geometric proportions of the image must not differ by more than 10% from the geometric proportions of the state license plate itself.

Note

For MPEG-4 and H.264 formats, the recommended distance between key frames is no more than 4-8 frames in case of a stable connection.

Attention!

The maximum vehicle speed for correct license plate recognition is limited to 180 km/h.

Video camera requirements

1. The focal length settings of the camera must be correctly set. The table below provides an example of the correlation between the viewing angle, sensor size, and lens focal length. For calculations, a standard video surveillance calculator was used.

Distance to the object, m	Object width, m	Focal length, mm	Viewing angle, degrees	Sensor size, inches
3	4	4	85	1/3
3	4	5	65	1/2
3	3	5	65	1/3
3	3	6	55	1/2
7	4	8	40	1/3
7	4	10	35	1/2
7	3	10	35	1/3
7	3	12	25	1/2
11	4	13	28	1/3

11	4	18	22	1/2
11	3	18	22	1/2
11	3	23	16	1/2
15	4	18	22	1/3
15	4	23	16	1/2
15	3	23	16	1/3
15	3	30	12	1/2

2. The camera must have a lens with an aperture of f/1.0, f/1.2, f/1.3, f/1.4, or f/1.8.
3. Color space model: Y800, RGB32, RGB24, YUY2, or UYUY.
4. The camera must have infrared illumination (built-in or stand-alone IR projector) to ensure round-the-clock recognition in an area with changing lighting conditions.
5. The shutter speed settings of the camera must be correctly set depending on the level of the camera's tilt to the license plate, as well as on the vehicle speed. The table below provides approximate shutter speeds for different vehicle speeds.

Shutter speed, s	Maximum vehicle speed in the surveillance area, km/h
1/200	18
1/250	22
1/500	45
1/750	68
1/1000	90
1/1500	136
1/2000	181

6. The camera must have a photo sensor suitable for license plate recognition:

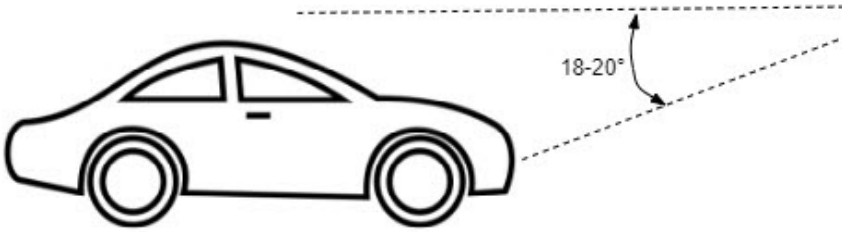
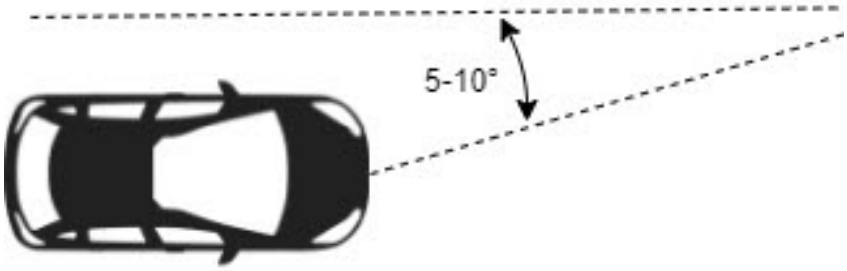
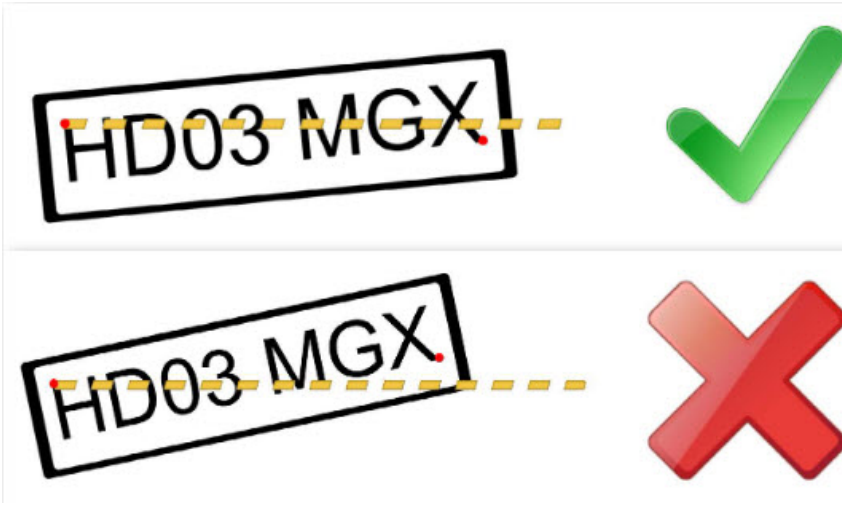
Sensor type	Both CCD and CMOS sensors are suitable for license plate recognition. CMOS is preferred because it does not have the blur effect that is common with CCD sensors
Sensor size	1/3 inch or more. During recognition, the physical size (area) of an individual pixel in a sensor is more important than the physical size (area) of the sensor itself. Larger pixel size provides better recognition in low light conditions
Pixel size	3.75 micrometers (μm) or more. The larger the sensor pixel size (area), the higher its sensitivity
Sensitivity	Dynamic range of 60 decibels or more (approximate contrast ratio of 1:1000). It is recommended to use the wide dynamic range (WDR) function. It improves the quality of recognition in high-contrast lighting conditions—it is possible to capture image details in both dark and bright areas of the field of view
Color depth	10 bits per pixel (bpp) or more

> **Note**
>
> When choosing a video camera, we recommend you to rely on a comparison of the photo sensor characteristics obtained as a result of measurements in accordance with the EMVA 1288 standard. This standard was developed by the EMVA (European Machine Vision Association) and it is offered to video camera manufacturers as a way to unify product evaluation methods.

Camera installation requirements

1. There are no high-contrast objects in the frame (for example, billboards, trees, wire fences)—they cause an increase in the number of false positives during recognition.
2. The camera is not aimed directly at a light source (sun, street lights) or reflective surfaces.
3. The camera for surveillance in gateway conditions is usually installed at the edge of the traffic lane. In this case:
    a. The installation height must be above the headlights level.
    b. The distance between the installation site and the focal point must be at least three meters.

4. The camera tilt angles do not exceed the maximum values:

Angle	Recommended value	Maximum value	Scheme
Vertical angle (camera tilted down to license plate)	18-20°	30°	
Horizontal angle (camera tilted left /right towards license plate)	5-10°	20°	
Tilt of the license plate in relation to the road surface	0	5°	During the recognition of a single-line license plate (with a minimum of six characters), the c is checked by the "one-line rule": an imaginary horizontal line must cross both the first and l characters on the license plate. 

License plate image requirements

For correct license plate recognition, make sure that the image of the license plate is not:

- unevenly lit;



- overexposed;



- blurry (due to incorrect shutter speed setting that does not match the vehicle speed);



- distorted (due to incorrect camera position);



- interlaced;

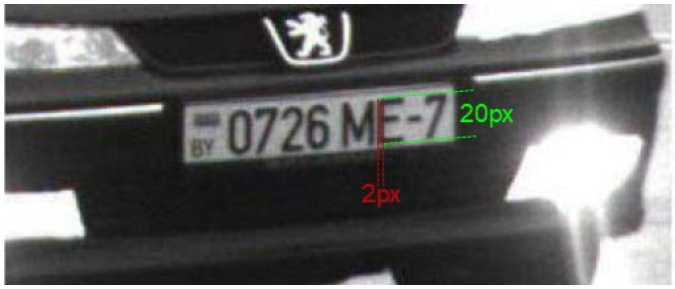


- dirty.



> **Attention!**
>
> Any deviation from the above requirements reduces the probability of correct license plate recognition.

An example of license plate images that will be recognized correctly and completely:





Recommendations for highways

1. The cameras should be mounted on L-shaped posts at the edge of the lane or on arches above the middle of the lane.
2. The recommended installation height is 4-6 meters, the maximum height is 20 meters.
3. Analog cameras have a relatively low resolution, so their surveillance area should not cover more than one traffic lane. IP cameras have a much higher resolution: their surveillance area can cover up to 4 traffic lanes.
4. The higher the camera is mounted, the higher the probability of capturing (and therefore detecting and recognizing) the license plates of vehicles moving at a short distance from each other (for example, during traffic jams). However, it is important to keep in mind that increasing the installation height leads to distortion of the license plate image, while the character size is almost at the minimum allowable level. In such cases, by reducing the vertical angle and changing the focal length (zoom), you can move the surveillance area to a greater distance so that the license plates can be recognized at the required installation height.

Configuring License Plate Recognition VT

> **Attention!**
>
> The operation of **License Plate Recognition VT** in *Axxon One* isn't compatible with *Auto PSIM*. Uninstall *Axxon One* and *Auto PSIM*, then reinstall *Axxon One*.

To configure the **License Plate Recognition VT** detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Vehicle License Plate Recognition VT**.

By default, the detection tool is enabled and set to recognize vehicle license plates.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Check in lists	**Yes**	The parameter is disabled by default. If you want to use this detection tool to check in lists of vehicle license plates, select the **Yes** value (see Configuring vehicle license plate recognition based on the created lists)
	No	
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**License Plate Recognition VT**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Type	**License Plate Recognition VT**	Name of the detection tool type (non-editable field)
Advanced SDK settings		
VodiCTL_VPW_DYNAMIC_ENABLE	**Yes**	By default, the license plate recognition dynamics is enabled, that is, tracking is enabled, and license plate recognition is based on a set of frames. To disable tracking and license plate recognition for each frame separately without reference to the previous frames, and the quality can vary from 0% to 100%, select the **No** value
	No	

VodiCTL_VPW_DYNAMIC_OUTPUT_PERIOD	**0.5**	Specify the time period in seconds for which the recognition result must be output. You can use this parameter only if the **VodiCTL_VPW_DYNAMIC_WITH_DUPLICATE** parameter is enabled. The value must be in the range [0, 3600]
VodiCTL_VPW_DYNAMIC_OUTPUT_TIMEOUT	**1**	Specify the minimum required time of license plate monitoring in seconds before the recognition result is output to the user. You can use this parameter only if the **VodiCTL_VPW_DYNAMIC_ENABLE** parameter is enabled. In this mode, the vehicle track is monitored, and the user doesn't receive the license plate recognition result immediately, rather after the time specified in this parameter. In this case, the first recognition result will be replaced by a better one and subsequently output to the user. If you specify the **0** value for this parameter, you will receive the first recognition result. Note that after the time specified in this parameter has elapsed, the monitoring of the license plate track continues until it disappears from the frame. The value must be in the range [0, 3600]
VodiCTL_VPW_DYNAMIC_WITH_DUPLICATE	**Yes** **No**	By default, periodic output of license plate recognition results is enabled. To disable the periodic output of results, select the **No** value
VodiCTL_VPW_IMAGE_BLUR	**13**	Parameter used for internal requirements. We recommend specifying the **13** value. The value must be in the range [0, 100000]
VodiCTL_VPW_LOG_SETTINGS	**Yes** **No**	By default, the parameter is disabled. To enable logging of all recognition parameters to the log file, select the **Yes** value
VodiCTL_VPW_PLATE_FILTER_RODROPFACTOR	**0**	Specify the coefficient of license plates filtering by image density (second strategy). Type is unsigned. This coefficient is used during image binarization and has optimal values, which are determined by developers using their own test samples. The parameter is considered a service parameter, and its value must be set according to the recommendations of technical support specialists. The value must be in the range [0, 100000]
VodiCTL_VPW_PLATE_FILTER_ROFACTOR	**95**	Specify the coefficient of license plates filtering by the so-called image density—the ratio of white pixels to the total number of pixels (first strategy). Type is unsigned. This coefficient is used during image binarization and has optimal values, which are determined by developers using their own test samples. The parameter is considered a service parameter, and its value must be set according to the recommendations of technical support specialists. The value must be in the range [0, 100000]

VodiCTL_VPW_PLATE_FILTER_SYMCOUNT	**0**	Enable/disable the algorithm of simple license plate filtering by the minimum number of recognized characters on the plates. If the algorithm is enabled (the parameter value is greater than **0**), a basic search for characters on the license plate candidate (geometry, proportions) is performed. If fewer characters are detected on the candidate than the value of this parameter, this candidate isn't considered a license plate. That is, the value of this parameter is the minimum number of characters that must be present on a license plate candidate when the basic algorithm is running. The value must be in the range [0, 100000]
VodiCTL_VPW_PLATE_STAR_MAX	**0**	Specify the maximum number of unrecognized characters on the license plate, at which the result is still considered the result of license plate recognition. The value must be in the range [0, 100000]
VodiCTL_VPW_TEXT_WITH_PUNCTUATION (Advanced) (starting with Detector Pack 3.12)	**Yes** **No**	Only for **Germany** and **Taiwan**. The parameter divides the characters on the license plate by hyphens into groups that determine the city/area and a group of the unique part of the license plate. By default, recognized license plate characters are displayed without hyphen. If you want to display recognized license plate characters with a hyphen, select the **Yes** value

Advanced settings

> ⚠ **Attention!**
>
> Advanced configuration of the detection tool must be performed with the assistance of AxxonSoft technical specialists.

Advanced image analysis	**Yes** **No**	By default, the parameter is disabled. Under normal conditions, this parameter doesn't affect the detection quality. Under poor conditions (for example, if the camera characteristics/settings don't fully meet the requirements, or detection occurs in bad weather), to improve the recognition quality, select the **Yes** value. This will increase the frame processing time by 20-30% depending on the frame size
Algorithm of recognition of distorted LP image	**Yes** **No**	By default, the algorithm of recognition of distorted license plate image is disabled. If you want to recognize license plates that are at a sharp angle to the camera, select the **Yes** value
Contrast threshold	**40**	Specify the image contrast threshold. We recommend increasing the value up to **50-60** on a good quality image, on an image with poor contrast, the value must be reduced. The value must be in the range [0, 100]

Event timeout	**0**	By default, the license plate recognition event is generated after the license plate track disappears from the frame. It is possible to generate a recognition event either after expiration of the time specified in seconds in the **Event timeout** field, or after reaching the similarity percentage specified in the **LP display quality** field. If the value of both parameters is different from **0**, the recognition event will be generated when the first of the two conditions is met. The value must be in the range [0, 3600]
Frame size change	**1920**	The analyzed frames are scaled down to a specified resolution (**1920** pixels on the longer side) by default. The following algorithm is used: • If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. • If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. • If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
GDPR policy	**-**	By default, on the layout and in the archive, the characters of a license plate are completely hidden "GDPR ON". To display the characters of a license plate, you must enter a value: "**-**"—hide all characters (default value), " (blank field of a parameter value)"—show all characters, "**N-**"—hide the first N characters, "**-N**"—hide the last N characters, where **N** is the number of characters
LP advanced search algorithm	**Yes** **No**	By default, the parameter is disabled. If license plates of different sizes will be present in the frame, select the **Yes** value. This parameter takes into account the specified maximum and minimum width of a license plate and, in some cases, can help to improve the recognition quality and optimize the processor load

LP display quality	**0**	**Attention!** The value of the **LP display quality** parameter must not be less than the value of the **Minimum similarity** para meter. By default, the license plate recognition event is generated after the license plate track disappears from the frame. It is possible to generate a recognition event either after expiration of the time specified in seconds in the **Event timeout** field, or after reaching the similarity percentage specified in the **LP display quality** field. If the value of both parameters is different from **0**, the recognition event will be generated when the first of the two conditions is met. The value must be in the range [0, 100]

Maximum number of threads	**1**	Specify the maximum number of recognition threads. If the value is **0**, the recognition process takes place in the same thread that starts it. The value must be in the range [0, 10].
		
		Attention!
		• If you specify several countries, we recommend setting the value of the parameter to at least **4**.
		• Increasing the number of recognition threads reduces possible drops in the frame rate, but at the same time increases the load on the device.
		• The total value of this parameter for all license plate recognition detection tools must not exceed:
		  ○ the number of recognition threads in the license (you can check it with the lsvpwc utility, see the manufacturer's documentation);
		  ○ number of logical processors;
		  ○ **100**.

Minimum similarity	**40**	Specify the minimum percentage of similarity between the recognition result and the corresponding license plate template, at which this result can be considered a license plate recognition result. This parameter is used to filter the obtained results by validity. The value must be in the range [0, 100]

Tracker timeout	**3**	Specify the time in seconds after which the vehicle track is considered lost. The value must be in the range [0, 3600]. **Note** • You can use this parameter to avoid double triggerings that can occur, for example, when a license plate is recognized when it appears in the frame, then it is overlapped by a visual obstacle and then recognized by the detection tool again. • If you specify the timeout longer than the time of possible overlapping of the license plate in the frame, the detection tool triggers only once.
Basic settings		
Algorithm for detecting vehicle direction	**By LP coordinates** **By LP scale change**	The **By LP coordinates** algorithm is used by default. It works as follows: if the coordinates of the vehicle license plate shift from top to bottom (the vehicle moves towards the camera) and if the coordinates of the vehicle license plate shift from bottom to top (the vehicle moves away from the camera). Select the **By LP scale change** parameter if in the Surveillance window, the scale of the vehicle license plate increases (the vehicle moves towards the camera) and if the scale of the vehicle license plate decreases (the vehicle moves away from the camera)
Analysis mode	**Standard (Morph)** **Advanced (DNN)**	Select the analysis mode of the detection tool: standard or neural network mode
License type	**Search in archive**	Standard license for searching recognized license plates in the archive. **Attention!** This type of license provides a 30-second delay between the license plate recognition and the corresponding event (see Vehicle number plate recognition and search).
	Normal (25 FPS or 6 FPS)	The 25 FPS license has a priority. If you don't have the 25 FPS license, the 6 FPS license is used. You cannot use the license plate recognition function if you haven't purchased both licenses
	Fast (25 FPS)	The Fast license allows you to process video streams at up to 25 FPS. License plate recognition for vehicles moving at speeds up to 150 km/h. You cannot use the license plate recognition function if you haven't purchased the license

	Slow (6 FPS)	The Slow license allows you to process video streams at up to 6 FPS. License plate recognition for vehicles moving at speeds up to 20 km /h. You cannot use the license plate recognition function if you haven't purchased the license
	Attention! All license types except the standard one (**Search in archive**) require the hardware key or the software key activation (see Licensing of the software module for License plate recognition (VT)). You can use a 60-day trial key (see Licensing of the software module for License plate recognition (VT)). You can use only a hardware key on virtual machines. To use a hardware key, select the **Normal** (25 FPS or 6 FPS) license type.	
Maximum LP width	**20**	Specify the maximum and minimum width of the license plate as a percentage according to the actual size of the license plate in the frame. The value must be in the range [0, 100]. **Attention!** • Specified values must exclude omissions in license plate recognition, that is, the values must not be smaller than the real size of the license plate in the frame. Otherwise, the license plates won't be recognized. • The **Minimum LP width** parameter affects the CPU load: the higher the value, the lower the load. • Reducing the difference between the maximum and minimum width reduces the CPU load.
Minimum LP width	**5**	
Minimum number of detection triggers	**6**	Specify the minimum number of triggers to display the object track. The higher the value of this parameter, the longer the time from object detection to displaying its track. A low value of this parameter can result in false alarms. The value must be in the range [1, 20]
Mode	**CPU**	Select the processor for the operation of the detection tool algorithm (see Hardware requirements for License Plate Recognition VT, Selecting Nvidia GPU when configuring detection tools). In the standard mode, the algorithm can only run on CPU. In the neural network analysis mode, the algorithm can run on any of the supported processors
	Intel GPU	
	Intel NCS (not supported)	
	Intel HDDL (not supported)	
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	
	Nvidia GPU 3	
	NvidiaDLA	
Country selection		
Country 1 name **Country 2 name**	**Albania**, **Algeria**, **Andorra**, **Argentina**, **Armenia**, **Australia**, **Austria**, **Azerbaijan**, **Bahrain**, **Brunei**, **Belarus**, **Belgium**, **Bolivia**, **Bosnia and Herzegovina**, **Botswana**, **Brazil**, **Bulgaria**, **Canada**, **Chile**, **Colombia**, **Croatia**, **Czech Republic**, **Denmark**, **Ecuador**, **El Salvador**, **Estonia**, **Finland**, **France**,	In the corresponding fields, select from the list one or more countries whose license plates you want to recognize. **Attention!**

Country 3 name **Country 4 name** **Country 5 name**	**Georgia**, **Germany**, **Greece**, **Guatemala**, **Honduras**, **Hong Kong**, **Hungary**, **India**, **Indonesia**, **Iran**, **Israel**, **Italy**, **Jordan**, **Korea**, **Kazakhstan**, **Kenya**, **Kyrgyzstan**, **Latvia**, **Liechtenstein**, **Sri Lanka**, **Lithuania**, **Luxembourg**, **Malaysia**, **Malta**, **Mexico**, **Moldova**, **Monaco**, **Mongolia**, **Montenegro**, **Nicaragua**, **Nigeria**, **Norway**, **Panama**, **Paraguay**, **Peru**, **Philippines**, **Poland**, **Portugal**, **Romania**, **Russian Federation**, **Serbia**, **Singapore**, **Slovakia**, **Slovenia**, **South Africa**, **Spain**, **Sweden**, **Switzerland**, **Taiwan**, **Tajikistan**, **Tunisia**, **Turkey**, **Turkmenistan**, **USSR**, **Ukraine**, **United Kingdom of Great Britain and Northern Ireland**, **Uruguay**, **USA**, **Uzbekistan**, **Vietnam**, **Zambia**, **Not used**	• The more countries you select, the slower the recognition works and the higher the probability of license plate recognition error. • To recognize old USSR license plates, you must additionally select the USSR country in the list.

In the window, specify the area in which license plate detection and recognition will be performed. You can adjust the area by moving the anchor points .



Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** Apply button. To cancel the changes, click the **Cancel** Cancel button.

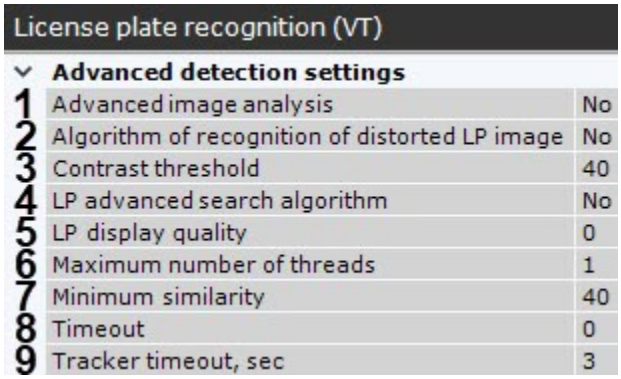
Fine-tuning the VT number plate detection tool

Attention!

To fine tune this detection tool, you will require assistance from AxxonSoft tech support.

To fine-tune the detection tool, do as follows:

1. If necessary, enable **Advanced image analysis** (**1**). If enabled, it improves the quality of recognition under adverse conditions (for example, if the characteristics/settings of the camera do not fully meet the requirements, or in bad weather). The processing time of the frame increases by 20-30%, depending on its size. Under normal conditions, this setting does not affect the quality of recognition.



2. To recognize the numbers at sharp angles with respect to the camera, select **Yes** in the **Algorithm of recognition of distorted LP image** field (**2**).
3. Set the image contrast threshold (**3**). The default value is **40**. On a high-quality image, increase this value to 50-60. If the image has poor contrast, lower this value.
4. If you expect different sizes of number plates within FOV, activate the **LP advanced search algorithm** (**4**). This parameter accounts for max and min width of number plates, and, in some cases, may help increasing recognition quality and optimizing CPU load.
5. To set up a number plate recognition event:

    a. Specify the minimum percentage of similarity between the recognition result and the corresponding number plate template, for positive LPR result (**7**). Use this parameter to filter the results by reliability.
    b. By default, a number plate recognition event is registered after a track containing a number plate disappears from FOV. You can set the moment of registration to a **Timeout** in seconds (**8**), or to reaching a similarity percentage specified in the **LP display quality** field (**5**). If both parameters are set to non-zero, the recognition event will be registered upon matching the first condition.

    Note

    The **LP display quality** parameter value must be no lower than the **Minimum similarity** value.

6. Specify the maximum number of recognition threads (**6**). If the value is **0**, the recognition process will occur in the same thread that starts it.

    Important

    The cumulative value of this parameter across all NPR detection tools must not exceed:

    - the licensed number of recognition threads (check your license with the lsvpwcutility);
    - the number of CPU cores;
    - 100.

7. In the **Tracker timeout, sec** field, set a time interval in seconds after which the tracking of a vehicle is reset (**9**).

> **Note**
>
> Use this setting to eliminate double-triggering in such cases as, for example, another recognition of the same number after it has been obstructed for some time, and then reappears in scene.
>
> If you set Tracker timeout to a value greater than a probable time of obstruction, the detection tool will not double-trigger.

8. If necessary, set additional parameters. For more details, refer to the table.

License plate recognition (VT)	
VodiCTL_VPW_DYNAMIC_ENABLE	Yes
VodiCTL_VPW_DYNAMIC_OUTPUT_PERIOD	0.5
VodiCTL_VPW_DYNAMIC_OUTPUT_TIMEOUT	1
VodiCTL_VPW_DYNAMIC_WITH_DUPLICATE	Yes
VodiCTL_VPW_IMAGE_BLUR	13
VodiCTL_VPW_LOG_SETTINGS	No
VodiCTL_VPW_PLATE_FILTER_RODROPFACTOR	0
VodiCTL_VPW_PLATE_FILTER_ROFACTOR	95
VodiCTL_VPW_PLATE_FILTER_SYMCOUNT	0
VodiCTL_VPW_PLATE_STAR_MAX	0

Parameter	Description
VodiCTL_VPW_DYNAMIC_ENABLE	Enable/disable the number recognition dynamics (by default, the dynamics is enabled). If the value is **Yes**, then tracking is enabled, and the number is recognized by the set of frames. If the value is **No**, then tracking is disabled, and the number is recognized by each frame separately without taking to account the previous ones, and the quality can vary from 0 to 100%
VodiCTL_VPW_DYNAMIC_OUTPUT_PERIOD	Time period (in seconds) over which the recognition result is to be displayed to the user. This parameter can be used only if the VodiCTL_VPW_DYNAMIC_WITH_DUPLICATE parameter is set
VodiCTL_VPW_DYNAMIC_OUTPUT_TIMEOUT	The minimum time required to monitor the license plate (in seconds) before displaying the recognition result to the user. This parameter can only be used when the “Dynamic” mode is on. In this mode, the trajectory of the vehicle is monitored, and the user does not immediately receive the recognition result of the license plate, but after the time specified for this setting. In this case, the first recognition result will be replaced by the result of higher quality and subsequently displayed to the user. If parameter 0 is set for this value, the user gets the first result of recognizing the detected license plate. After the time specified in this parameter expires, the monitoring of the trajectory of the license plate continues until it disappears from the frame
VodiCTL_VPW_DYNAMIC_WITH_DUPLICATE	Enable/disable the periodic output of license plate recognition results

VodiCTL_VPW_IMAGE_BLUR	The parameter for internal use. The recommended value to set is 13
VodiCTL_VPW_LOG_SETTINGS	Enable/disable logging of all recognition parameters
VodiCTL_VPW_PLATE_FILTER_RODROPFACTOR	The license plate filter coefficient by the so-called image density—ratio of white pixels to total pixels (second strategy). The type is unsigned. This coefficient is used for image threshold and has the optimal values, which are determined by developers using their own test samples. The parameter is considered as a service one, and its value should be set according to the recommendations of technical support specialists
VodiCTL_VPW_PLATE_FILTER_ROFACTOR	The license plate filter coefficient by the so-called image density – ratio of white pixels to total pixels (first strategy). The type is unsigned. This coefficient is used for image threshold and has the optimal values, which are determined by developers using their own test samples. The parameter is considered as a service one, and its value should be set according to the recommendations of technical support specialists
VodiCTL_VPW_PLATE_FILTER_SYMCOUNT	Enable/disable the simple license plates filter algorithm by the minimum number of recognized symbols on them. If the algorithm is enabled (the value of the parameter is greater than 0), the base search for symbols on the prospective license plate (geometry, proportions) is performed. If less symbols are recognized on the prospective license plate than specified in this parameter, this prospective license plate is not considered a license plate. That is, the value of this parameter is the minimum characters that must be present on the prospective license plate when the basic algorithm is in use
VodiCTL_VPW_PLATE_STAR_MAX	Maximum unrecognized symbols on the license plate, at which the result will still be considered the result of the recognition of the license plate

9. Click the **Apply** button.

Licensing of the software module for License plate recognition (VT)

On this page:

- Installing the license key environment
- Installing a demo license
- Installing a hardware key
- Installing a software key
- Activating and updating the license
- Removing a license
- Checking a license

Installing the license key environment

The license keys for License plate recognition (VT) require the Sentinel LDK Run-time environment. It is installed automatically with the Addon VT LPR (see Installing DetectorPack add-ons).

To manually install the Sentinel LDK Run-time environment, do the following:

1. Download the haspdinst_EOAWT.exe installer.
2. Run the command line as system administrator.
3. Execute the **haspdinst_EOAWT.exe -i -fi -fss** command.
4. Restart the Sentinel LDK License Manage service or restart the OS.

Note

If the environment is successfully installed, the Sentinel Admin Control Center web application will open in the Web browser at http://127.0.0.1:1947/.

Installation of the Sentinel LDK Run-time environment is complete.

Installing a demo license

Attention!

Before you install a demo license, it is necessary to install the Sentinel LDK Run-time environment.

The Sentinel LDK Run-time environment and a standard demo license for searching the recognized license plates in the archive are installed automatically with the Addon VT LPR (see Installing DetectorPack add-ons).

Attention!

If you use this license, note that there is a 30 seconds delay between the recognition of a license plate and the appearance of a corresponding event (see Vehicle number plate recognition and search).

With demo license, the License plate recognition (VT) works for all available countries on 4 channels at 25 FPS or on 4 channels at 6 FPS. The demo mode is valid for 60 days from the moment the demo key is activated.

Attention!

Demo mode of the License plate recognition (VT) is not allowed on virtual machines.

To install a demo license, do the following:

1. Download the distribution package: 25 FPS or 6 FPS.
2. Run the command line as system administrator.
3. Execute the **SDK_4hi_60d_WORLD.exe -i -fi -fss** command (for a 25 FPS demo license) or **SDK_4lo_60d_WORLD.exe -i -fi -fss** command (for a 6 FPS demo license).

4. Restart the Sentinel LDK License Manage service or restart the OS.

> **Note**
>
> Information about the installed demo license is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The installation of the demo license is now complete.

Installing a hardware key

> **Attention!**
>
> Before you install a hardware key, it is necessary to install the Sentinel LDK Run-time environment.

To install a hardware key, do the following:

1. Download and install the HASPUserSetup.exe driver distribution package.
2. Connect the hardware key to the Server where you plan to use the License plate recognition (VT). If the Sentinel LDK Run-time environment is successfully installed, the license is automatically recognized by *Axxon One* and it is ready to use.

> **Note**
>
> Information about the installed hardware key is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The installation of the hardware key is now complete.

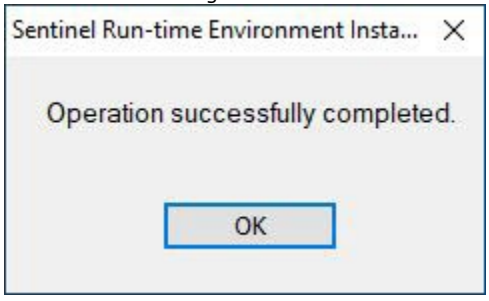
Installing a software key

> **Attention!**
>
> Before you install a software key, it is necessary to install the Sentinel LDK Run-time environment.

> **Attention!**
>
> The License plate recognition (VT) license is not automatically transferred to a new node in a failover system (see Configuring Failover VMS).
>
> To ensure the License plate recognition (VT) operation, it is necessary to manually activate the license on the computer where the node is running.

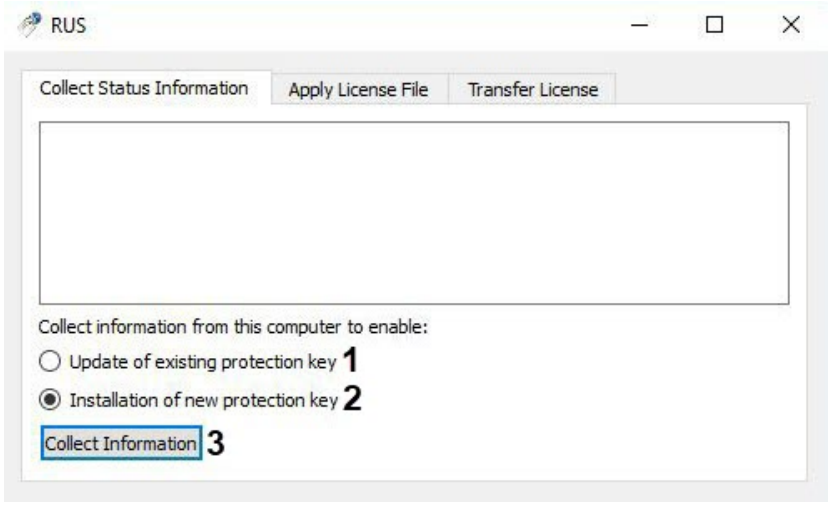
To install a software key, do the following:

1. Download the RUS_EOAWT.exe.
2. Run the command line as system administrator.
3. Execute the **haspdinst_EOAWT.exe -fr -purge** command.
4. Click **OK** in the dialog box to confirm the installation is completed.

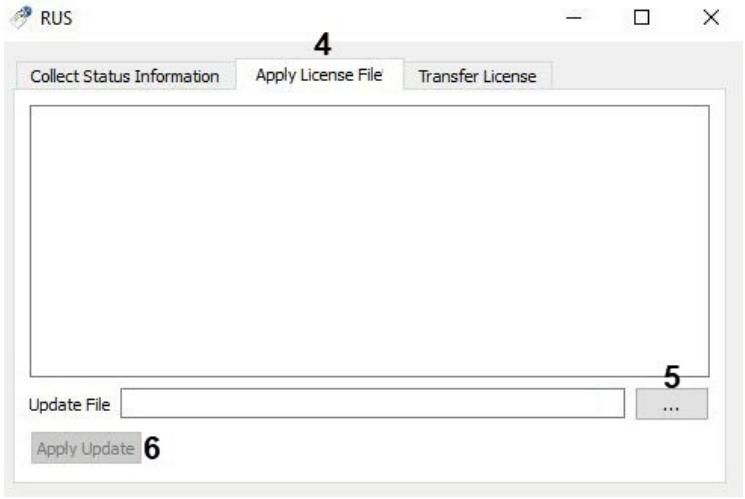


5. Run the RUS_EOAWT.exe file to start the Remote Update System. The **RUS** dialog box opens.

> **Note**
>
> The abbreviation RUS stands for "Remote Update System".



6. Set the **Collect information from this computer to enable** switch into one of the following positions:
   a. **Update of existing protection key** (**1**) if a demo license is already in use.
   b. **Installation of new protection key** (**2**) if license for a "clean computer" is required, i.e. if there is no demo license on the Server.
7. Click **Collect Information** (**3**).
8. Save the file with the c2v extension to the required directory.
9. Close the RUS_EOAWT.exe utility.
10. Give the created file with the c2v extension to the AxxonSoft manager.
11. Get a v2c file from the AxxonSoft manager.
12. Run the RUS_EOAWT.exe utility and go to the **Apply License File** tab (**4**).



13. Specify location of the license file in the **Update File** field using the **...** button (**5**).
14. Click **Apply Update** (**6**).
15. Restart the Sentinel LDK License Manage service or restart the OS.

> **Note**
>
> Information about the installed software key is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The installation of the software key is now complete.

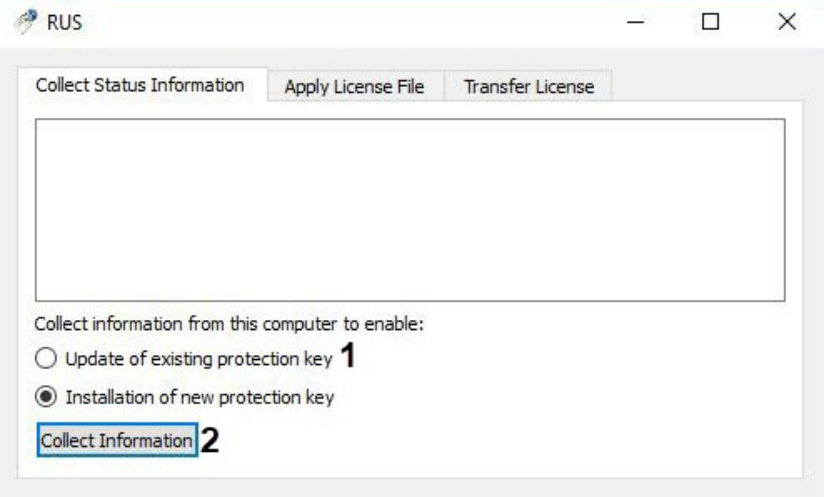
Activating and updating the license

Attention!

Before you install a software key, it is necessary to install the Sentinel LDK Run-time environment and the RUS_EOAWT.exe utility.

To activate/update the license, do the following:

1. Run the RUS_EOAWT.exe utility.
2. Set the **Collect information from this computer to enable** switch to the **Update of existing protection key** position (**1**).



3. Click **Collect Information** (**2**).
4. Save the file with the c2v extension to the required directory.
5. Close the RUS_EOAWT.exe utility.
6. Give the created file with the c2v extension to the AxxonSoft manager.
7. Get a v2c file from the AxxonSoft manager.
8. Run the RUS_EOAWT.exe utility and go to the **Apply License File** tab (**3**).



9. Specify location of the license file in the **Update File** field using the **...** button (**4**).
10. Click **Apply Update** (**5**).
11. Restart the Sentinel LDK License Manage service or restart the OS.

Note

Information about the activated/updated license is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The activation/update of the license is now complete.

Removing a license

To delete a license, do the following:

1. Delete the v2c license file from the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK\installed\ folder.
2. Restart the Sentinel LDK License Manage service or restart the OS.

The removal of the license is now complete.

Checking a license

You can check the current license status on the Server. To do this, open the Sentinel Admin Control Center web application. The license information is displayed on the **Features** tab.

Licensing of the software module for the License plate recognition (VT) in Linux OS

On this page:

- General information
- Installing the Sentinel LDK Run-time environment
- Installing a hardware key
- Installing a software key
- Updating the license
- Removing a license
- Checking a license

General information

The software module for the License plate recognition (VT) in *Axxon One* is licensed by the processed video channels and by countries (see License plate recognition VT).

Attention!

It is necessary to run the commands as the root user.

Installing the Sentinel LDK Run-time environment

To install the Sentinel LDK Run-time environment, do the following:

1. Upload the aksusbd-8.52.1.tar environment to the Server on which the license will be used.
2. Unpack the archive.

```
sudo tar xvf ~/aksusbd-8.52.1.tar -C ~
```

3. Run the installation.

```
sudo ./aksusbd-8.52.1/dinst /home/<Username>/aksusbd-8.52.1
```

Installation of the Sentinel LDK Run-time environment is complete. Together with the Sentinel LDK Run-time environment, a standard demo license for searching the recognized license plates in the archive will be installed. When you use this license, note that there is a 30-second delay between the recognition of a license plate and the appearance of a corresponding event (see Vehicle number plate recognition and search).

Attention!

Demo mode of the License plate recognition (VT) is not allowed on virtual machines.

Note

If the environment is successfully installed, the Sentinel Admin Control Center web application will open in the Web browser at http://127.0.0.1:1947/. Information about the installed demo license will be displayed on the **Sentinel Keys** tab.

Installing a hardware key

Attention!

Before you install a hardware key, it is necessary to install the Sentinel LDK Run-time environment.

To ensure the hardware key operation, it is necessary to connect the hardware key to the Server where you plan to use the License plate recognition (VT). If the Sentinel LDK Run-time environment is successfully installed, the license is automatically recognized by *Axx on One* and it is ready to use.

> **Note**
>
> Information about the installed hardware key is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The installation of the hardware key is now complete.

Installing a software key

> **Attention!**
>
> Before you install a software key, it is necessary to install the Sentinel LDK Run-time environment.

To install a software key, do the following:

1. Upload the hasp_SDK_2.14.tar.gz environment to the Server on which the license will be used.
2. Unpack the archive.

   ```
   sudo tar zxvf ~/hasp_SDK_2.14.tar.gz -C ~
   ```

3. Create a snapshot of the Server hardware. A snapshot is a file with the c2v extension. The created file fingerprint.c2v will be located in the current directory.

   ```
   cd ~/hasp/bin
   ```

   a. for 64-bit system:

   ```
   sudo ./hasp_update_x86_64 f > fingerprint.c2v
   ```

   b. for 32-bit system:

   ```
   sudo ./hasp_update f > fingerprint.c2v
   ```

4. Give the created file with the c2v extension to the AxxonSoft manager.
5. Get a v2c file from the AxxonSoft manager. The received file will contain license information that will be available for use only on your Server.
6. Activate the license to install a software key.

   a. for 64-bit system:

   ```
   cd ./hasp/bin
   ```

   ```
   sudo ./hasp_update_x86_64 u <Received file with the v2c extension>
   ```

   b. for 32-bit system:

   ```
   cd ./hasp/bin
   ```

   ```
   sudo ./hasp_update u <Received file with the v2c extension>
   ```

7. After you activate the license, restart the hasplmd service:

```
sudo systemctl stop hasplmd.service
```

```
sudo systemctl start hasplmd.service
```

or restart the Server:

```
sudo reboot
```

> **Note**
>
> Information about the installed software key is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The installation of the software key is now complete.

Updating the license

To update the license, do the following:

1. Create a snapshot of the Server hardware. A snapshot is a file with the c2v extension. The created file haspinfo.c2v will be located in the current directory.

   ```
   cd ~/hasp/bin
   ```

   a. for 64-bit system:

   ```
   sudo ./hasp_update_x86_64 i <HASP ID> > haspinfo.c2v
   ```

   where <HASP ID>

   ```
   hasp_update_x86_64 lf
   ```

   b. for 32-bit system:

   ```
   sudo ./hasp_update i <HASP ID> > haspinfo.c2v
   ```

   where <HASP ID>

   ```
   hasp_update lf
   ```

2. Give the created file with the c2v extension to the AxxonSoft manager.
3. Get a v2c file from the AxxonSoft manager. The received file will contain license information that will be available for use only on your Server.
4. Update the license.

   ```
   cd ./hasp/bin
   ```

   a. for 64-bit system:

   ```
   sudo ./hasp_update_x86_64 u <Received file with the v2c extension>
   ```

   b. for 32-bit system:

```
sudo ./hasp_update u <Received file with the v2c extension>
```

5. After you update the license, restart the hasplmd service:

```
sudo systemctl stop hasplmd.service
```

```
sudo systemctl start hasplmd.service
```

or restart the Server:

```
sudo reboot
```

> **Note**
>
> Information about the updated license is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

The update of the license is now complete.

Removing a license

To remove a license, do the following:

1. Open the contents of the c2v file that was created for the installation, activation or update of the current license. The license ID in the body of the key is indicated as <hasp id="Identifier of the current license">.
2. Delete the v2c file that has the same ID as the c2v file located in /var/hasplm/installed/107392/.
3. Stop the processes.

```
killall aksusbd
killall haspmld
```

4. Start the services.

```
haspmld -s
aksusbd
```

5. After you remove the license, restart hasplmd service:

```
sudo systemctl stop hasplmd.service
```

```
sudo systemctl start hasplmd.service
```

or restart the Server:

```
sudo reboot
```

The removal of the license is now complete.

Checking a license

You can check the current license status on the Server. To do this, open the Sentinel Admin Control Center web application. The license information is displayed on the **Features** tab.

If there is no Web browser on the Server, execute the following two commands in the console one by one:

```
curl -X POST -d 'accremote=1' http://localhost:1947/_int_/config.html
wget --post-data 'accremote=1' http://localhost:1947/_int_/config.html
```

Vehicle Recognition XR

Functions of the Vehicle Recognition XR

Description

The **Vehicle Recognition XR** is used to:

1. Recognize license plates of vehicles. List of countries:

Supported	Albania, Algeria, American Samoa, Andorra, Angola, Anguilla, Antigua and Barbuda, Argentina, Armenia, Aruba, Australia, Austria, Azerbaijan, Bahamas, Bahrain, Barbados, Belarus, Belgium, Benin, Bermuda, Bhutan, Bolivia, Bosnia, Botswana, Brazil, Brunei, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Canada, Cape Verde, Cayman Islands, Central African Republic, Chad, Chile, Christmas Island, Colombia, Comoros, Congo, Cook Islands, Croatia, Cyprus, Czech Republic, Denmark, Dominica, Dominican Republic, East Timor, Ecuador, Egypt, El Salvador, Equatorial Guinea, Estonia, Faroe Islands, Fiji, Finland, France, French Guiana, French Polynesia, French Southern Territories, Gabon, Gambia, Georgia, Germany, Ghana, Gibraltar, Great Britain, Greece, Greenland, Grenada, Guadeloupe, Guatemala, Guinea, Guyana, Haiti, Honduras, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Ivory Coast, Jamaica, Jordan, Kazakhstan, Kenya, Kiribati, Kosovo, Kuwait, Kyrgyzstan, Laos, Latvia, Liberia, Liechtenstein, Lithuania, Luxembourg, Macau, Macedonia, Madagascar, Malawi, Malaysia, Mali, Malta, Marshall Islands, Martinique, Mauritania, Mauritius, Mayotte, Mexico, Micronesia, Moldova, Monaco, Mongolia, Montenegro, Morocco, Mozambique, Namibia, Nauru, Netherlands, Netherlands Antilles, New Caledonia, New Zealand, Nicaragua, Niger, Nigeria, Northern Mariana Islands, Norway, Oman, Pakistan, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Poland, Portugal, Qatar, Reunion Island, Romania, Russia, Rwanda, Saint Kitts and Nevis, Saint Lucia, Samoa, San Marino, Sao Tome and Principe, Saudi Arabia, Senegal, Serbia, Seychelles, Singapore, Slovakia, Slovenia, Solomon Islands, South Africa, South Sudan, Spain, Sri Lanka, Swaziland, Sweden, Switzerland, Taiwan, Tajikistan, Tanzania, Thailand, Togo, Tonga, Trinidad and Tobago, Turkey, Turkmenistan, Turks and Caicos Islands, Uganda, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay, Uzbekistan, Vatican, Venezuela, Vietnam, Virgin Islands British, Virgin Islands USA, Wallis and Futuna Islands, Zambia, Zimbabwe
Unsupported	Afghanistan, and, Antarctica, Bangladesh, Belize, Bissau, China, Cocos, Costa, Cuba, Djibouti, Eritrea, Ethiopia, Falkland, Grenadines, Guam, Guinea, Iran, Iraq, Island, Islands, Islands, Japan, Korea, Korea, Lebanon, Leone, Lesotho, Lesotho, Leste, Libya, Maldives, Montserrat, Myanmar, Nepal, Niue, North, Palau, Palestina, Pitcairn, Rica, Sahara, Saint, Sierra, Somalia, South, Sudan, Suriname, Syria, Tibet, Timor, Tokelau, Tunisia, Tuvalu, Vanuatu, Vincent, Western, Yemen

2. Write the recognized license plates into a database
3. Check the recognized license plates on the lists of license plates

Licensing

For the detection tool to operate, contact a manager of AxxonSoft and get a license file (see Types of licenses, Licensing of the software module for the Vehicle Recognition XR)

Add-ons

For the detection tool to operate, install the XR Vehicle Recognition Pack (see Installing DetectorPack add-ons)

Hardware requirements for the Vehicle Recognition XR

Operating system and software	• Microsoft Windows 8 or higher (64-bit version) • Microsoft Visual C++ 2015 Redistributable Package (x64) • .NET Framework 4.5.2 • Installed license (see Licensing of the software module for the Vehicle Recognition XR)
RAM usage	• Each camera requires at least 500 MB of RAM. This must be considered if you use many cameras on one computer **Note** For example, a configuration with 16 cameras requires at least 8 GB of RAM.
CPU	• Intel i7 or i9 of the latest-generation with a clock speed of at least 3.0 GHz • System must allocate one core per camera at 2MP resolution (since the detection tool operates at 1MP resolution, 20 cores aren't required for a 20-camera setup), plus two additional cores for operating system tasks. CPU must support AVX2 **Note** For example, a configuration with 20 cameras requires 16 GB of RAM and a CPU with the specified characteristics with at least 16 cores.

Video stream and scene requirements for the Vehicle Recognition XR

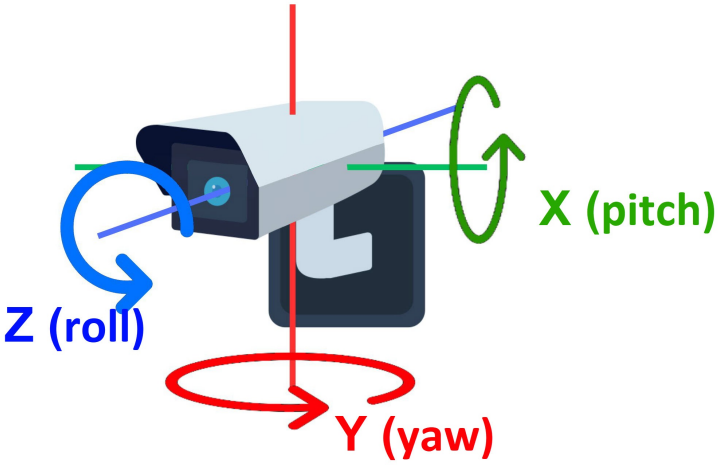
Requirements for the operation of the **Vehicle Recognition XR** are given in the table:

Camera	• Minimum resolution is 640*480, recommended resolution is 1280x720px • Minimum frame rate is 15 FPS, recommended frame rate is 25–30 FPS • Autofocus and zoom functions are desirable (for making small adjustments after the detection tool is configured)
Lighting	• Lighting in the scene is at least 50 lux. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting

Scene and camera angle	• To achieve the highest accuracy, set up the camera to capture only one lane of traffic, preferably the one closest to the camera (dual lanes are possible if the camera is positioned between two lanes)
	• Maximum horizontal tilt angle of the camera must be no more than 15º. This is the angle from the road to the capture point
	• Working distance from the camera to the capture point must be:
	  ◦ 15–20 meters for urban conditions and low speed;
	  ◦ 20–30 meters for higher speed measurements
	• Camera installation height is 4–6 meters above the ground
	• Angle formed by the bottom line of a license plate and the horizon line must be between 0º and 20º
	• Camera must not be installed near road bends, speed bumps, road junctions, traffic lights or roundabouts, as vehicles are likely to accelerate or decelerate at these locations. Detection area must not be on a curve in the road

Image requirements for the Vehicle Recognition XR

Requirements for the operation of the **Vehicle Recognition XR** are given in the table:

Image tilt	The following limits are recommended: • X-axis rotation (pitch): ± 35° • Y-axis rotation (yaw): ± 40° • Z-axis rotation (roll): ± 35° 
Correct tilt	 
Incorrect tilt	 
	If you exceed these values, the recognition accuracy can significantly reduce

Object images	• Clear, sharp, no distortion, no blurring • Image must have minimum noise in low light conditions • Size of license plate must be 15–70% of the total image size • License plate must have no more than two rows of characters on it • Optimal height of characters is 20–30 pixels

Licensing of the software module for the Vehicle Recognition XR

On the page:

- Installing the environment for license keys
- Installing a demo license
- License activation and update
- Deleting the license

Installing the environment for license keys

The Sentinel LDK Run-time environment is required for the operation of the license keys of the **Vehicle Recognition XR**. The environment is installed automatically with the XR Vehicle Recognition Pack (see Installing DetectorPack add-ons).

To install the Sentinel LDK Run-time environment manually, do the following:

1. Download the haspdinst_EOAWT.exe installer.
2. Run the command line as the system administrator.
3. Run the **haspdinst_EOAWT.exe -i -fi -fss** command.
4. Restart the Sentinel LDK License Manage service or restart the OS.

Note

When the environment is successfully installed, the Sentinel Admin Control Center web application opens in a web browser at http://127.0.0.1:1947/.

Installation of the Sentinel LDK Run-time environment is complete.

Installing a demo license

Attention!

Before you install a demo license, you must install the Sentinel LDK Run-time environment.

The Sentinel LDK Run-time environment for the operation of the license keys and a standard license for searching the recognized license plates in the archive are installed automatically with the XR Vehicle Recognition Pack (see Installing DetectorPack add-ons).

If you install a demo license, XR license plates of all available countries can be recognized. Demo license is valid for 30 days after activation of the software key.

Attention!

Operation of the **License plate recognition VT** in demo mode isn't allowed on virtual machines.

To install a demo license, do the following:

1. Download the archive with files to activate demo license.
2. Unzip the downloaded file.
3. In the unzipped folder, run the .bat file as administrator.
4. Run the command prompt as system administrator.
5. Write the full path to the unzipped folder with files. For example, C:\Users\user\Licenses\XR.
6. Run the command:

```
.\vaxtordemo.exe -i
```

7. Restart the Sentinel LDK License Manage service or restart the OS.

> **Note**
>
> Information about the installed demo license is displayed in the Sentinel Admin Control Center web application, on the **Sentinel Keys** tab.

Installation of a demo license is complete.

License activation and update

> **Attention!**
>
> Before you install the software key, you must install the Sentinel LDK Run-time environment.

To activate/update the license, do the following:

1. Open a browser and go to http://127.0.0.1:1947/checkin.html.
2. On the page that opens, in the **Select File** line, select the key with v2c extension.

   > **Attention!**
   >
   > To get the key with v2c extension, you need to contact a manager of AxxonSoft.

3. Click **Apply File**.
4. If activation is successful, the key is displayed at http://127.0.0.1:1947/devices.html.

After activation, in the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK directory, the **installed** folder appears.

The license activation/update is complete.

Deleting the license

To delete the license, do the following:

1. Delete the license file with v2c extension from the C:\Program Files (x86)\Common Files\SafeNet Sentinel\Sentinel LDK\installed\ directory.
2. Restart the OS.

> **Note**
>
> - When you delete the license, only the key is deleted. All counters of license restriction remain in the secure storage.
> - If you return the key to the root directory, it will be fully restored. Its counters will continue counting license restrictions from the moment when they stopped when the license file with v2c extension was deleted. The validity time of the license continues to count down even when the key is missing.

The license deletion is complete.

When you delete the **installed** folder with licenses, you must restart the Sentinel LDK Run-time environment:

1. Press the **Win + R** keyboard shortcut.
2. In the window that opens, enter **services.msc** and press **Enter**.
3. In the **Services** window, find **Sentinel LDK License Manager**.
4. Right-click **Sentinel LDK License Manager** and select **Restart**.

The **Sentinel LDK License Manager** service will stop and then automatically start again.

Category: Poses

Person-Based Privacy Masking

Functions of the Person-Based Privacy Masking

Description	**Person-Based Privacy Masking** allows you to hide specified parts of a person's body in a video
Neural networks	Detection tool uses a segmenting network that breaks the human body into zones (head, shoulders, forearms, hands, body, hips, shins, feet)
Add-ons	For the detection tool to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Person-Based Privacy Masking

Hardware requirements for neural analytics operation

For the correct operation of the **Person-Based Privacy Masking** the following requirements must be met:

Attention!

We cannot guarantee correct operation of the detection tool when you use a fisheye lens.

Camera	• FSP is at least 12 • Minimum value of pixel density per meter is 170
Lighting	• Average lighting of scenes with a person is at least 200 lux

Configuring the Person-Based Privacy Masking

Video stream and scene requirements for the Person-Based Privacy Masking

Hardware requirements for neural analytics operation

To configure the **Person-Based Privacy Masking**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Poses Person-Based Privacy Masking**.

By default, the detection tool is enabled and set to mask a person's head.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, the recording of the mask to the archive is disabled. To record mask to the archive (see Displaying information from a detection tool (mask)), select the **Yes** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream allows reducing the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Person-Based Privacy Masking**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei NPU	
Number of frames processed per second	**1**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100]
Type	**Person-Based Privacy Masking**	Name of the detection tool type (non-editable field)
Advanced settings		
Number of measurements in a row to trigger detection	**3**	Specify the minimum number of frames on which the detection tool must detect objects to generate an event. The value must be in the range [1, 20]

<table>
<tr><td>Segmenting network file</td><td></td><td>Select a neural network file.

The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, specify the path to the file.

Note

To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

Attention!

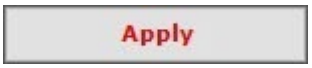
If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td rowspan="8">Neural network mode</td><td>CPU</td><td rowspan="8">Select the neural network mode (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

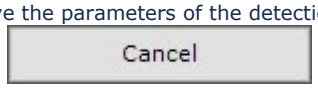
Attention!

• It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS).
• If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
• Starting with Detector Pack 3.11, Intel HDDL and Intel NCS aren’t supported.</td></tr>
<tr><td>Nvidia GPU 0</td></tr>
<tr><td>Nvidia GPU 1</td></tr>
<tr><td>Nvidia GPU 2</td></tr>
<tr><td>Nvidia GPU 3</td></tr>
<tr><td>Intel HDDL (not supported)</td></tr>
<tr><td>Intel GPU</td></tr>
<tr><td>Intel NCS (not supported)</td></tr>
<tr><td colspan="3">Mask</td></tr>
<tr><td rowspan="2">Body</td><td>Yes</td><td rowspan="8">By default, the detection tool masks only a person's head. To mask other parts of the body, select the Yes value for the corresponding parameters</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Feet</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Forearms</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Hands</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Head</td><td>Yes</td></tr>
<tr><td>No</td></tr>
</table>

Hips	**Yes**
	No
Shins	**Yes**
	No
Shoulders	**Yes**
	No

By default, the entire frame is a detection area.

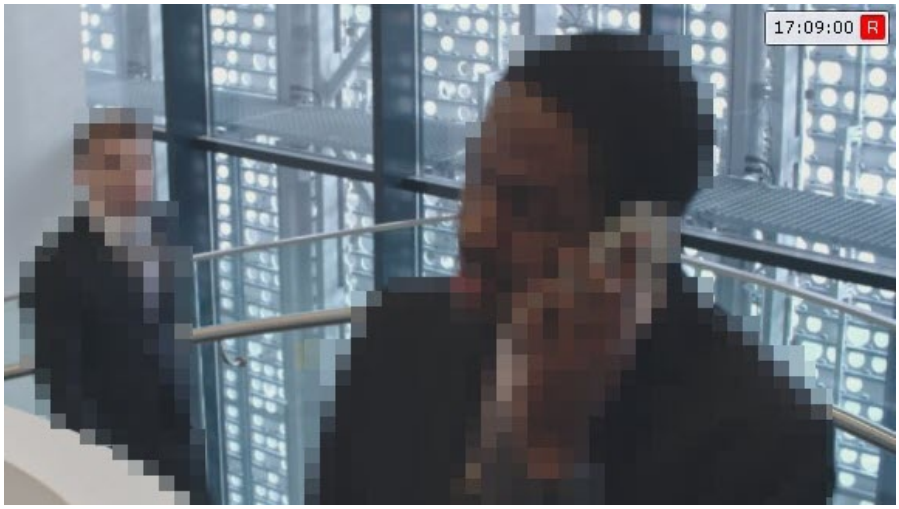
To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring the **Person-Based Privacy Masking** is complete.

Selected body parts of all persons will be hidden in the frame. For a user group with limited permissions to view masked video (see Creating and configuring roles), the mask is displayed on the video image of the selected camera in the **Detection Tools** and **Hardware** sections, on the layouts, in the archive and when exporting. For the **admin** user group, the mask is displayed only on the video image of the selected camera in the **Detection Tools** and **Hardware** sections, and when exporting, if the **View masked video** checkbox is clear (see Standard video recordings export).



Pose Detection

Functions of the Pose Detection and its sub-tools

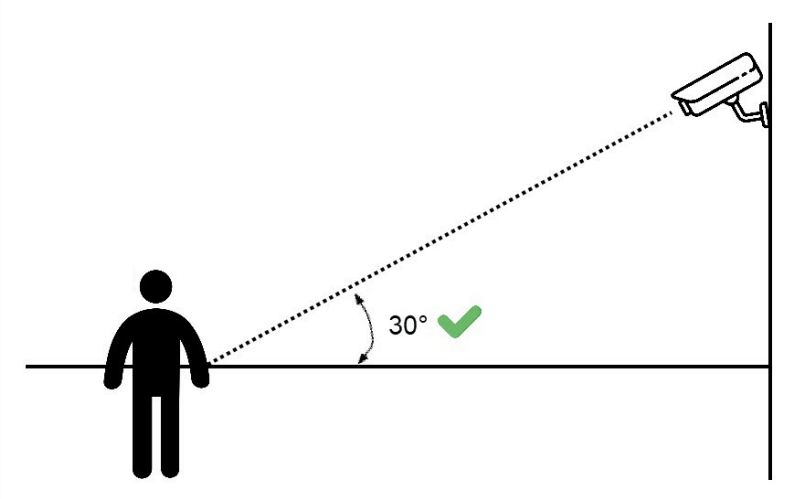
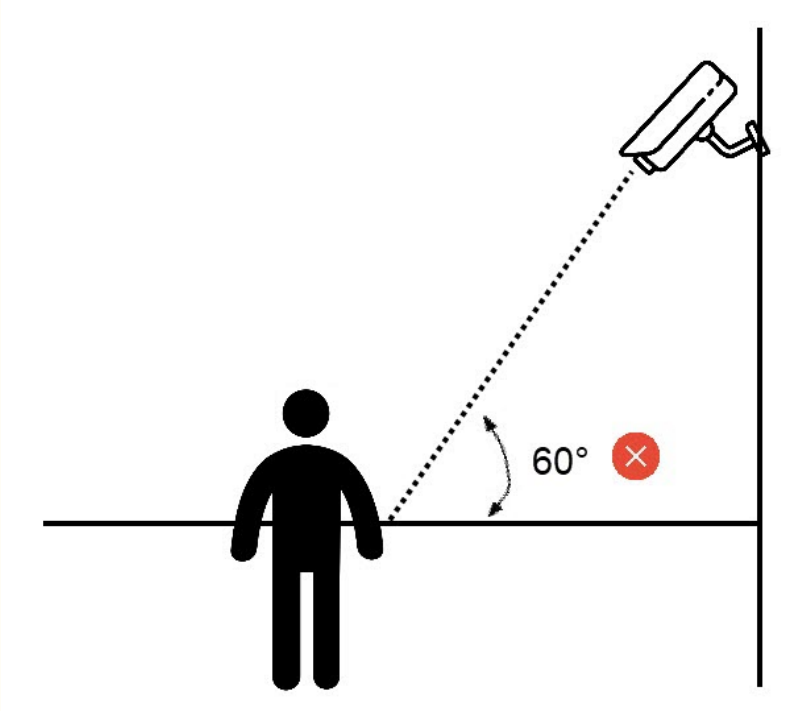
Description	**Pose Detection** uses a neural network and detection sub-tools to determine each person's skeleton and detect poses that could indicate a potentially dangerous situation
Detection sub-tools	You can create the following sub-tools on the basis of the Pose Detection: 1. Sitting person detection—detection tool generates an event when there is a sitting person in the frame. 2. Man down detection—detection tool generates an event when there is a prostrate person in the frame. 3. Hands up detection—detection tool generates an event when there is a person with one or two hands raised in the frame. A hand is considered raised if the forearm is parallel to the back. 4. Handrail holding detection—detection tool generates an event when there is a person in the specified part of the frame who doesn't hold any of the specified handrails. 5. People counter detection—detection tool counts objects in the specified area. Detection tool generates an event when the number of objects reaches or exceeds the specified limit. 6. Close-standing people detection—detection tool generates an event when the distance between people in the frame exceeds the specified minimum value. 7. People masking detection—detection tool masks people in the video image, doesn't generate an event 8. Standard detection sub-tools
Add-ons	For the Pose Detection and its sub-tools to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Pose Detection and its sub-tools

Image requirements for the Pose Detection and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the **Pose Detection** and its sub-tools are given in the table:

Camera	• Resolution must be at least 640x360 pixels. We also don't recommend using a resolution higher than 1920×1080, since higher resolution doesn't increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 • The frame rate per second in the video stream from the camera is at least 8 • Color image only **Attention!** • Correct operation of the **Pose Detection** tools isn't guaranteed when using fisheye cameras and other cameras with strong image distortion. • The camera tilt angle from top to bottom on a person must not exceed 30°. Otherwise, the detection tool won't operate correctly. The following diagrams show the examples of: ○ The acceptable tilt angle:  ○ The unacceptable tilt angle: 

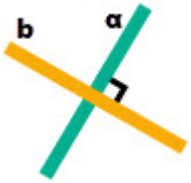
Lighting	• Lighting in the scene is at least 50 lux per square meter. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on) • The analyzed scene doesn't have reflective surfaces and sharp shadows from moving objects. If present, they must be masked • Camera shake doesn't result in image offsets greater than 1% of the frame size • For the correct operation of the **Sitting Person Detection** and **Person Down Detection** sub-tools, the area of interest must be covered from at least two perpendicular angles (a and b are the directional beams from the cameras and the point of their intersection is the area of interest):  The algorithms have a limitation and won't work correctly if: ○ a person falls down or sits down with their head or face towards the camera, ○ a person falls down with their feet towards the camera (for the Person Down Detection sub-tool)

Image requirements for the Pose Detection and its sub-tools

Video stream and scene requirements for the Pose Detection and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the Pose Detection and its sub-tools are given in the table:

Object images

- The detected object must be clearly distinguishable by the human eye
- The detected object must be completely within the frame
- The image isn't noisy and not distorted by the artifacts of compression algorithm
- The duration of the object visibility is at least two frames
- The minimum value of pixel density per meter is observed:

Image resolution	Object type	Minimum pixel density per meter (ratio of the object width in pixels to the object width in meters)	Minimum object size in pixels, width x height
For Pose Detection sub-tools (see Configuring the Pose Detection sub-tools)			
1920x1080	Human	170	~102x309
1280x720	Human	128	~77x233
640x360	Human	80	~48x145
For standard sub-tools (see Standard detection sub-tools)			
1920x1080	Human	100	~45x187
1280x720	Human	68	~31x134
640x360	Human	35	~15x65

Configuring the Pose Detection

Video stream and scene requirements for the Pose Detection and its sub-tools

Image requirements for the Pose Detection and its sub-tools

Hardware requirements for neural analytics operation

To configure the **Pose Detection**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Poses Pose Detection**.

By default, the detection tool is enabled and set to detect poses.

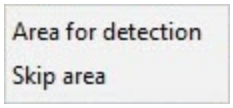
If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream allows reducing the load on the Server
	Second stream	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Pose Detection**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**3**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100] **Attention!** With static persons in scene, set the FPS to no less than **2**. With moving persons in scene, the FPS must be at least **4**. The higher the FPS value, the higher the accuracy of pose detection, but the load on the selected processor is higher as well. For FPS=1, the accuracy will be no less than 70%. This parameter varies depending on the object speed of movement. To solve typical tasks, FPS value from 3 to 20 is sufficient. Examples: • pose detection for moderately moving objects (without sudden movements)—FPS **3**; • pose detection for moving objects—FPS **12**.

Type	**Pose Detection**	Name of the detection tool type (non-editable field)
Advanced settings If detection of small objects or objects in areas far away from the camera is ineffective, you can use the scanning mode (see Configuring the scanning mode). This mode doesn't provide absolute detection accuracy, but can improve detection performance		
Neural network file		Select a neural network file. The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, enter a path to the file. **Note** For the correct neural network operation on Linux OS, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. **Attention!** If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.
Scanning window	**Yes** **No**	The scanning mode is disabled by default. To enable the scanning mode, select the **Yes** value
Scanning window height	**540**	The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels
Scanning window step height	**540**	The scanning step determines the relative offset of the windows. If the step is equal to the height and width of the scanning window respectively, the segments will line up one after another. Reducing the height or width of the scanning step will increase the number of windows due to their overlapping each other with an offset. This will increase the detection accuracy, but will also increase the CPU load **Attention!** The height and width of the scanning step must not be greater than the height and width of the scanning window. The detection tool won't operate with such settings.
Scanning window step width	**480**	The scanning step determines the relative offset of the windows. If the step is equal to the height and width of the scanning window respectively, the segments will line up one after another. Reducing the height or width of the scanning step will increase the number of windows due to their overlapping each other with an offset. This will increase the detection accuracy, but will also increase the CPU load **Attention!** The height and width of the scanning step must not be greater than the height and width of the scanning window. The detection tool won't operate with such settings.
Scanning window width	**480**	The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels
Basic settings		
Mode	**CPU** **Nvidia GPU 0**	Select the operation mode of the detection tool and neurofilter (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). Neurofilter operation mode is used only if you select the **Yes** value in the **Neurofilter** parameter.

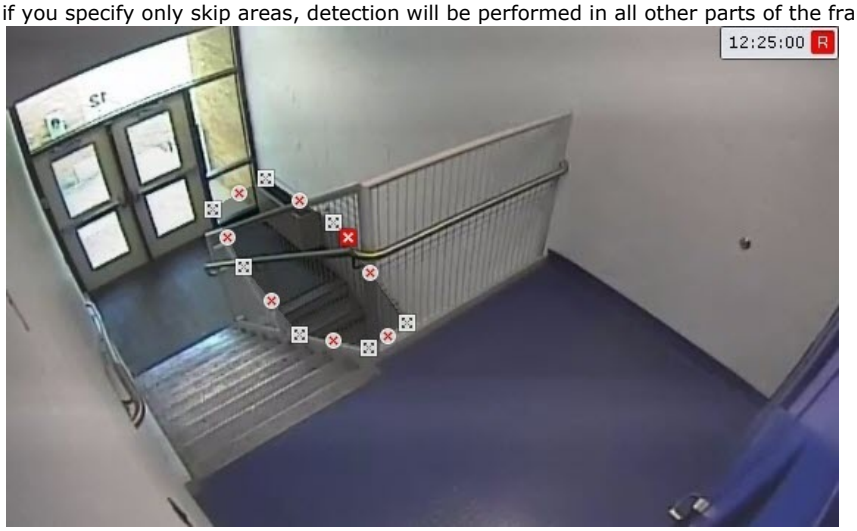
	Nvidia GPU 1 **Nvidia GPU 2** **Nvidia GPU 3** **Intel GPU** **Huawei NPU**	**Attention!** • It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS). • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool. • For the Person Down Detection and Sitting Person Detection, the accuracy can depend on the selected processor. If the recognition quality deteriorates when you change the processor, we recommend selecting the best values of the parameters of detection tools and configuring perspective empirically (see Configuring the Sitting Person Detection, Configuring the Person Down Detection).
Neural network filter		
Neurofilter	**Yes** **No**	Neurofilter is disabled by default. To use the neurofilter to filter out parts of tracks, select the **Yes** value
Neurofilter file		Select a neural network file

By default, the entire frame is area for detection. In the preview window, you can specify the custom areas for detection and skip areas. To specify areas, right-click the frame, and select the required area (see Configuring a skip area, Configuring a detection area).



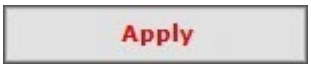
The following logic is used for this:

a. if you specify only areas for detection, no detection will be performed in all other parts of the frame;
b. if you specify only skip areas, detection will be performed in all other parts of the frame.



Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The area for detection is displayed by default. To hide it, click the  button. To cancel the action, click this button again.
- To delete the selected area, click the  button.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring the Pose Detection sub-tools

Configuring the Sitting Person Detection

On the page:

- Configuring the parameters of the detection tool
- Configuring the frame perspective

Configuring the parameters of the detection tool

To configure the **Sitting Person Detection**, do the following:

1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... Sitting Person Detection**.

By default, the **Sitting Person Detection** generates an event if a sitting person is detected in the specified area.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Sitting Person Detection**	Enter the detection tool name or leave the default name
Type	**Sitting Person Detection**	Name of the detection tool type (non-editable field)
Basic settings		
Number of measurements in a row to trigger detection	**2**	Specify the minimum number of frames with the corresponding pose or behavior for the detection tool to generate an event. The value must be in the range [1, 20]. The recommended (default) value is **2**. Increasing the value can help eliminate false events, but increases the risk of skips. Decreasing the value can help reduce skips, but increases the probability of false events

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

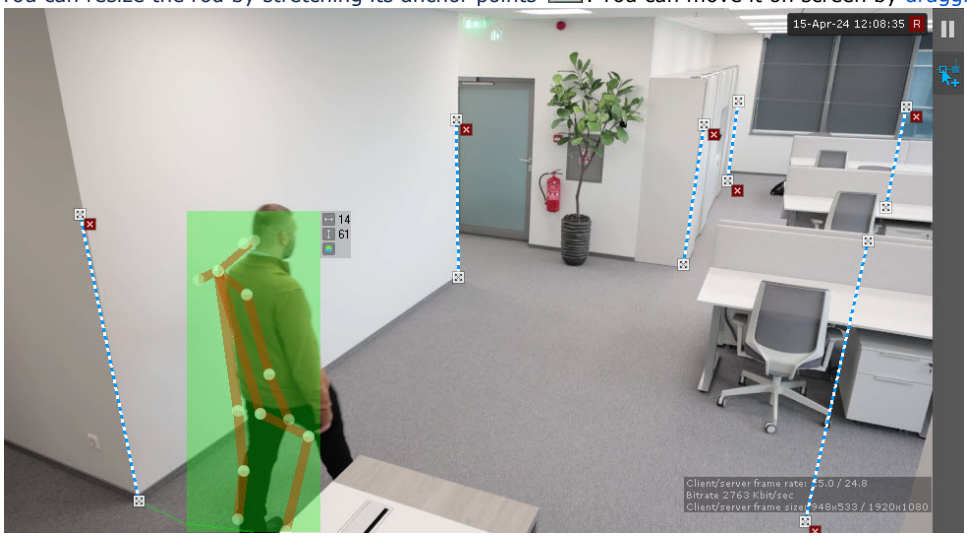
Configuring the frame perspective

If camera angle doesn't meet the requirements (see Video stream and scene requirements for the Pose Detection and its sub-tools), this can result in false events. In this case, we recommend configuring the frame perspective using the leveling rods.

For this, do the following:

1. In the preview window, click the  button.
2. Specify the size of the same person in different parts of the frame by eye:
   - To create a leveling rod, left-click the video image to add two anchor points.
   - Set at least three calibration rods. The lower anchor points of any three rods must not be located on the same line (horizontal, vertical, slanting, etc.).
   - The size of the leveling rod must be about the average height of a person at this part of the frame.

- You can resize the rod by stretching its anchor points . You can move it on screen by dragging and dropping.



> **Attention!**
>
> When you set up leveling rods, the following conditions must be met:
>
> a. the rods that are located at the same distance from the camera lens, must be of the same size;
> b. the feet of the rods must be located on the same surface (for example, floor);
> c. in complex scenes, we recommend adding more than three rods to increase the accuracy of the detection;
> d. in the parts of the frame where the lens vertical distortion is observed, the rods must be parallel to the nearest vertical objects (for example, door, wardrobe);
> e. for portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, and so on), the arrangement of the rods must form triangles.

> **Note**
>
> - For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
> - The area for detection is displayed by default. To hide it, click the button. To cancel the action, click this button again.
> - To delete a rod, click the button.

3. Click the **Apply** button.

Configuring the Person Down Detection

On the page:

- Configuring the parameters of the detection tool
- Configuring the frame perspective

Configuring the parameters of the detection tool

> **Attention!**
>
> When a recumbent person is facing a camera or away from a camera, the correct operation of the detection tool isn't guaranteed.

To configure the **Person Down Detection**, do the following:

1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... Person Down Detection**.

By default, the **Person Down Detection** generates an event if a recumbent person is detected in the specified area.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Person Down Detection**	Enter the detection tool name or leave the default name
Type	**Person Down Detection**	Name of the detection tool type (non-editable field)
Basic settings		
Number of measurements in a row to trigger detection	**2**	Specify the minimum number of frames with the corresponding pose or behavior for the detection tool to generate an event. The value must be in the range [1, 20]. The recommended (default) value is **2**. Increasing the value can help eliminate false events, but increases the risk of skips. Decreasing the value can help reduce skips, but increases the probability of false events

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

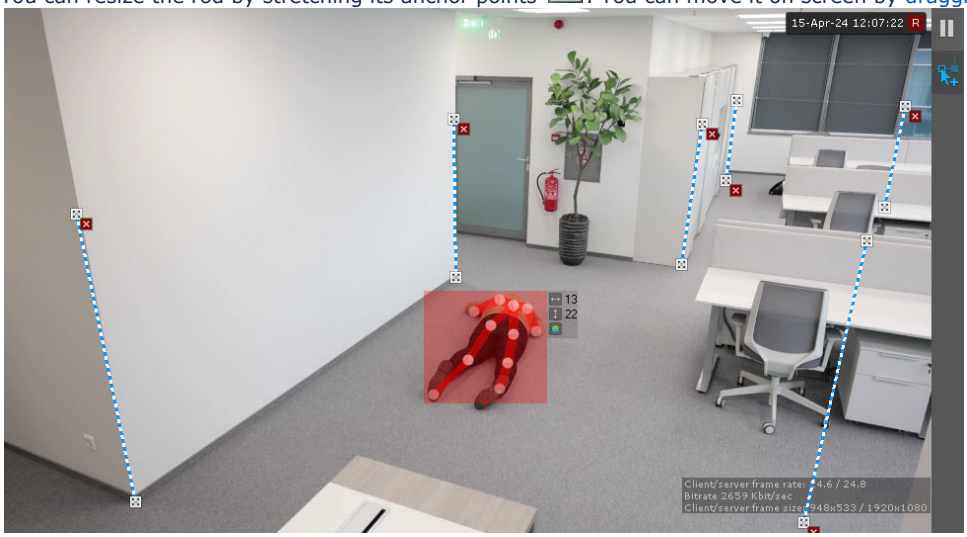
button.

Configuring the frame perspective

For the **Person Down Detection** operation, you must configure the frame perspective first.

For this, do the following:

1. In the preview window, click the  button.
2. Specify the size of the same person in different parts of the frame by eye:
   - To create a leveling rod, left-click the video image to add two anchor points.
   - Set at least three calibration rods. The lower anchor points of any three rods must not be located on the same line (horizontal, vertical, slanting, etc.).
   - The size of the leveling rod must be about the average height of a person at this part of the frame.
   - You can resize the rod by stretching its anchor points  . You can move it on screen by dragging and dropping.



> **Attention!**
>
> When you set up leveling rods, the following conditions must be met:
>
> a. the rods that are located at the same distance from the camera lens, must be of the same size;
> b. the feet of the rods must be located on the same surface (for example, floor);
> c. in complex scenes, we recommend adding more than three rods to increase the accuracy of the detection;
> d. in the parts of the frame where the lens vertical distortion is observed, the rods must be parallel to the nearest vertical objects (for example, door, wardrobe);
> e. if you add only three leveling rods to a scene, you cannot remove them from the scene, you can resize them and change their location;
> f. if you add more than three leveling rods to a scene, you can resize them and change their location, and remove them from the scene;
> g. for portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, and so on), the arrangement of the rods must form triangles.

> **Note**
>
> - For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
> - The area for detection is displayed by default. To hide it, click the  button. To cancel the action, click this button again.
> - To delete a rod, click the  button.

3. Click the **Apply** button.

Configuring the Hands up detection

To configure the **Hands up detection**, do the following:

1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... Hands up detection**.

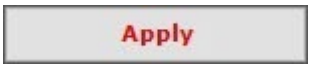
By default, the **Hands up detection** generates an event if there is a person with both hands raised in a specified area.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** va lue
	No	
Name	**Hands up detection**	Enter the detection tool name or leave the default name
Type	**Hands up detection**	Name of the detection tool type (non-editable field)
Basic settings		
Mode	**Both hands**	Select this value if you want the detection tool to generate an event only when a person has both hands raised
	One hand	Select this value if you want the detection tool to generate an event only when a person has either left or right hand raised
	Only left	Select this value if you want the detection tool to generate an event only when a person has one selected hand raised
	Only right	
	Left hand	Select this value if you want the detection tool to generate an event only when a selected hand is raised
	Right hand	
Number of measurements in a row to trigger detection	**2**	Specify the minimum number of frames with a person with a hand/hands raised for the detection tool to generate an event. The value must be in the range [1, 20]. The recommended (default) value is **2**. Increasing the value can help eliminate false events, but increases the risk of skips. Decreasing the value can help reduce skips, but increases the probability of false events

Note

- The Hands up detection works in the areas for detection and skip areas specified in the Pose Detection (see Configurin g the Pose Detection).
- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The area for detection is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring the Handrail holding detection

On the page:

- Configuring the parameters of the detection tool
- Configuring the area for detection

Configuring the parameters of the detection tool

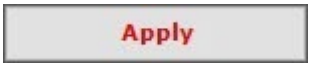
To configure the Handrail holding detection, do the following:

1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... Handrail holding detection**.

The **Handrail holding detection** generates an event if there is a person in the specified area of the frame who doesn't hold on to any of the specified handrails.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Handrail holding detection**	Enter the detection tool name or leave the default name
Type	**Handrail holding detection**	Name of the detection tool type (non-editable field)
Basic settings		
Number of measurements in a row to trigger detection	**2**	Specify the minimum number of frames with the corresponding pose or behavior for the detection tool to generate an event. The value must be in the range [1, 20]. The recommended (default) value is **2**. Increasing the value can help eliminate false events, but increases the risk of skips. Decreasing the value can help reduce skips, but increases the probability of false events

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring the area for detection

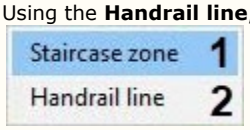
To configure the area for detection of the **Handrail holding detection**, do the following:

1. Click in the preview window.

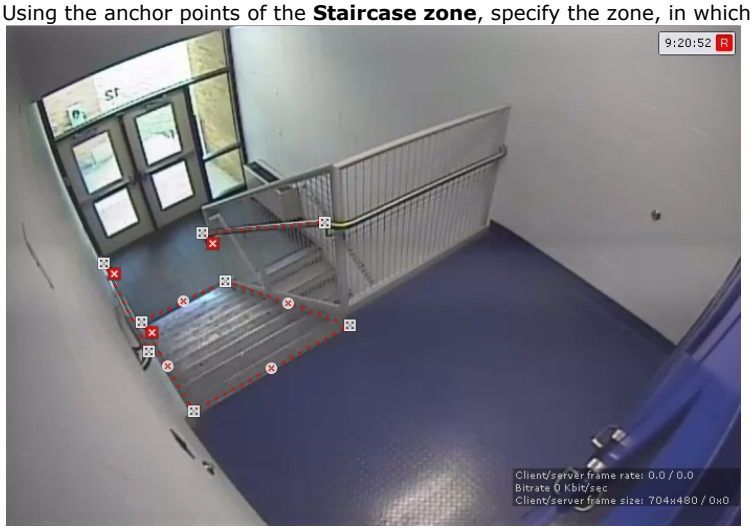
Attention!

- If lens distortion makes the handrail non-linear, use several lines to specify the handrail.
- The presence of a person in the staircase zone is determined by their lower limbs.

Using the **Handrail line**, specify one or several handrails in the frame.



2. Using the anchor points of the **Staircase zone**, specify the zone, in which a person must hold on to the handrail.



Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The area for detection is displayed by default. To hide it, click the  button. To cancel the action, click this button again.
- To delete a line, click the  button.

Configuring the People counter

To configure the People counter, do the following:

1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... People counter**.

People counter counts the number of people in the specified area using the metadata of the Pose Detection.

An event, on the basis of which a macro can be started (see Configuring start conditions for event-driven macros), can be generated if the number of people in the frame meets the specified conditions.

Note

- Unlike the Multiple Objects detection tool (see Configuring Multiple Objects), the counter generates events of just one type—triggering.
- Unlike the Neurocounter (see Configuring the Neurocounter), People counter counts only people.

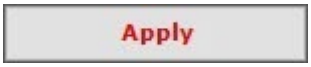
If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

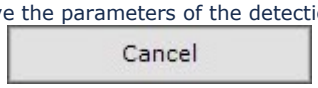
Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	Mask is recorded to the archive by default. To disable the parameter, select the **No** value
	No	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**People counter**	Enter the detection tool name or leave the default name
Type	**People counter**	Name of the detection tool type (non-editable field)
Basic settings		
Alarm when value	**In range**	Specify when the detection tool must generate an event: when the number of people in the specified area is within the set range, or out of the range
	Out of range	
End value of alarm range settings	**100**	Specify the range of the number of people in the frame. The value must be in the range [0, 100]
Event interval	**1**	Specify the interval in seconds between two consecutive events of the detection tool when the number of people in the frame continuously meets the specified conditions. The value must be in the range [1, 10000]
Number of measurements in a row to trigger detection		Specify the minimum number of frames with the set number of people for the detection tool to generate an event. The value must be in the range [1, 20]. The recommended (default) value is **2**. Increasing the value can help eliminate false events, but increases the risk of skips. Decreasing the value can help reduce skips, but increases the probability of false events
Start value of alarm range settings	**5**	Specify the range of the number of people in the frame. The value must be in the range [0, 100]

By default, the entire frame is the area for detection. In the preview window, you can specify the areas for detection using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The area for detection is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

In the **Surveillance window** on the layout next to the counter icon, you can add text and the number of people counted by the detection tool (see Displaying the number of detected objects).

Configuring the Close-standing people detection

On the page:

- Configuring the parameters of the detection tool
- Configuring the frame perspective

Configuring the parameters of the detection tool

To configure the **Close-standing people detection**, do the following:

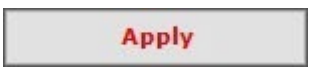
1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... Close-standing people detection**.

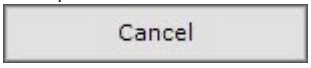
By default, the Close-standing people detection generates an event when "skeleton" bounding boxes around people collide.

> **Note**
>
> Bounding boxes are not displayed in the interface. They are usually a bit larger than the "skeletons" dimensions.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Close-standing people detection**	Enter the detection tool name or leave the default name
Type	**Close-standing people detection**	Name of the detection tool type (non-editable field)
Basic settings		
Distance sensitivity	**2**	Specify the distance between people in meters at which the detection tool must generate an event. Event is generated if the distance between people in the frame is equal to or less than the specified distance. The value must be in the range [0, 20]
Leveling rod length	**1.7**	Specify the average height of a person in meters, according to which the leveling rods are set. The value must be in the range [0 3]
Number of measurements in a row to trigger detection	**4**	Specify the minimum number of frames with close-standing people for the detection tool to generate an eevent. The value must be in the range [1, 100]. Increasing the value can help eliminate false event, but increases the risk of skips. Decreasing the value can help reduce skips, but increases the probability of false events

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

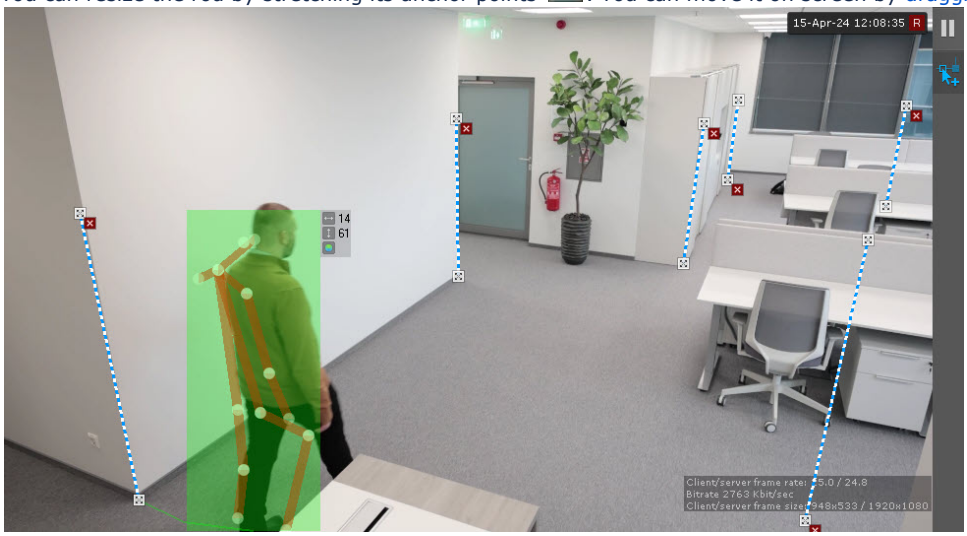
Configuring the frame perspective

if you want to change the distance that must generate an event, you must configure the frame perspective:

Attention!

For portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, and so on), we recommend configuring the perspective in any case.

1. In the preview window, click the  button.
2. Specify the size of the same object in different parts of the frame by eye:
   - To create a leveling rod, left-click the video image to add two anchor points.
   - Set at least three calibration rods. The lower anchor points of any three rods must not be located on the same line (horizontal, vertical, slanting, etc.).
   - The size of the leveling rod must be about the average height of a person at this part of the frame.
   - You can resize the rod by stretching its anchor points  . You can move it on screen by dragging and dropping.



Attention!

When you set up leveling rods, the following conditions must be met:

a. the rods that are located at the same distance from the camera lens, must be of the same size;
b. the feet of the rods must be located on the same surface (for example, floor);
c. in complex scenes, we recommend adding more than three rods to increase the accuracy of the detection;
d. in the parts of the frame where the lens vertical distortion is observed, the rods must be parallel to the nearest vertical objects (for example, door, wardrobe);
e. for portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, and so on), the arrangement of the rods must form triangles.

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The area for detection is displayed by default. To hide it, click the  button. To cancel the action, click this button again.
- To delete a rod, click the  button.

3. Click the **Apply** button.

Configuring the People masking

To configure the **People masking**, do the following:

1. Create **Pose Detection** (see Configuring the Pose Detection).
2. Below the **Pose Detection**, click **Create... People masking**.

People masking doesn't generate events. It uses the metadata from the **Pose Detection** to mask people on the video image:

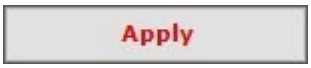
- on live video;
- in the archive;
- when exporting from the archive.

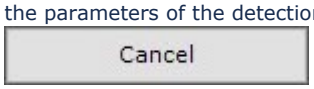
> **Attention!**
>
> People masking works only for those users who have the **View masked video** parameter **disabled** in the role settings (see Creating and configuring roles).



If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	Mask is recorded to the archive by default. To disable the parameter, select the **No** value
	No	
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**People masking**	Enter the detection tool name or leave the default name
Type	**People masking**	Name of the detection tool type (non-editable field)

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring the standard detection sub-tools of the Pose Detection

For the information on configuring the standard detection sub-tools of the Pose Detection, see Standard detection sub-tools.

Category: Production Safety

Audio Analytics Detection IV

Functions of the Audio Analytics Detection IV

Description	The **Audio Analytics Detection IV** is used to recognize and detect various sounds at protected facilities (for example, the sound of broken glass, smoke alarm sound, and so on). An event on the basis of which a macro can be started (see Configuring start conditions for event-driven macros) can be generated if the sound meets the conditions specified in the detection tool settings
Add-ons	For the detection tool to work, you must install Audio Analytics Detection IV add-on (see Installing DetectorPack add-ons)

Attention!

The **Microphone** object must be enabled (see The Microphone Object).

Audio data requirements for the operation of the Audio Analytics Detection IV

> ⚠ **Attention!**
>
> The **Microphone** object must be enabled (see The Microphone Object).

Audio data requirements for the operation of the Audio Analytics Detection IV are given in the table:

Stream	Single channel
Audio data format	16-bit sign integer audio PCM format
Sample rate	8000, 16000, 32000, 48000 Hz

Configuring the Audio Analytics Detection IV

Audio data requirements for the operation of the Audio Analytics Detection IV

Attention!

The **Microphone** object must be enabled (see The Microphone Object).

To configure the Audio Analytics Detection IV, do the following:

1. Submit to the technical support the MAC address of the Server where the detection tool will be used.

   Attention!

   The detection tool will not work on the Server with a different MAC address.

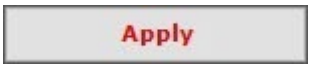
2. Copy the license received from the technical support into the C:\Program Files\Common Files\AxxonSoft\DetectorPack\LicenseFile_AudioIV.txt file.
3. Restart the Server (see Shutting down a Server, Starting a Server).
4. On the **Detection Tools** tab, below the required camera, click **Create...** **Category: Production Safety** **Audio Analytics Detection IV**.

By default, the detection tool is enabled and set to recognize and detect all sounds specified in the settings.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Audio Analytics Detection IV**	Enter the detection tool name or leave the default name
Aggression detection	**Yes**	By default, the aggression detection is enabled. To disable, select the **No** value
	No	
Aggression detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as aggression. The value must be in the range [0.01, 1]
Baby cry detection	**Yes**	By default, the baby cry detection is enabled. To disable, select the **No** value
	No	
Baby cry detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as baby cry. The value must be in the range [0.01, 1]
Dog bark detection	**Yes**	By default, the dog bark detection is enabled. To disable, select the **No** value
	No	
Dog bark detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as dog bark. The value must be in the range [0.01, 1]
Glass break detection	**Yes**	By default, the glass break detection is enabled. To disable, select the **No** value
	No	
Glass break detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as glass break. The value must be in the range [0.01, 1]
Gunshot detection	**Yes**	By default, the gunshot detection is enabled. To disable, select the **No** value
	No	

Gunshot detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as gunshot. The value must be in the range [0.01, 1]
Siren detection	**Yes**	By default, the siren detection is enabled. To disable, select the **No** value
	No	
Siren detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as siren. The value must be in the range [0.01, 1]
Smoke alarm detection	**Yes**	By default, the smoke alarm detection is enabled. To disable, select the **No** value
	No	
Smoke alarm detection threshold	**0.99**	Specify the threshold value at which the sound is recognized as smoke alarm. The value must be in the range [0.01, 1]
Type	**Audio Analytics Detection IV**	Name of the detection tool type

To save the changes to the detection tool parameters, click the **Apply** 

button. To cancel the changes to the parameters, click the **Cancel** 

button.

Configuration of the Audio Analytics Detection IV is complete.

If necessary, you can search the archive for events that were generated by the detection tool. You can search for all types of sounds or for a specific type of sound (see Events search).

Object Presence Detection

Functions of the Object Presence Detection

Description	**Object Presence Detection** generates events when the required type of object appears in the camera field of view. ⚠ **Attention!** The **Object Presence Detection** is based on a neural network, the basic principle of which is learnability. In order for the **Object Presence Detection** to respond to the required type of object in the camera field of view, you must record a video and send it to AxxonSoft. In *Axxon One*, the detection tool will be refined (neural network training) based on the video data for the optimal operation in the specified conditions.
Add-ons	For the **Object Presence Detection** to work, you install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Object Presence Detection

Hardware requirements for neural analytics operation

Requirements for the operation of the **Object Presence Detection** are given in the table:

Camera	• We recommend using color cameras. With black and white cameras, the detection quality can be noticeably worse • Resolution must be at least 640x360 • FPS directly affects detection efficiency. In most cases, the default value (1 detection per 10 seconds) is sufficient to detect the appearance of an object that last more than one minute
Scene and angle	• The minimum area of the object in the frame depends on the neural network that you use • The object must be visually separated from the background

Attention!

If you set a rectangular recognition area for the detection tool, the requirements apply to this area rather than to the entire frame (see Configuring the Object Presence Detection).

Configuring the Object Presence Detection

Video stream and scene requirements for the Object Presence Detection

Hardware requirements for neural analytics operation

To configure the **Object Presence Detection**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Production Safety Object Presence Detection**.

By default, the detection tool is enabled and set to detect objects in the frame.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

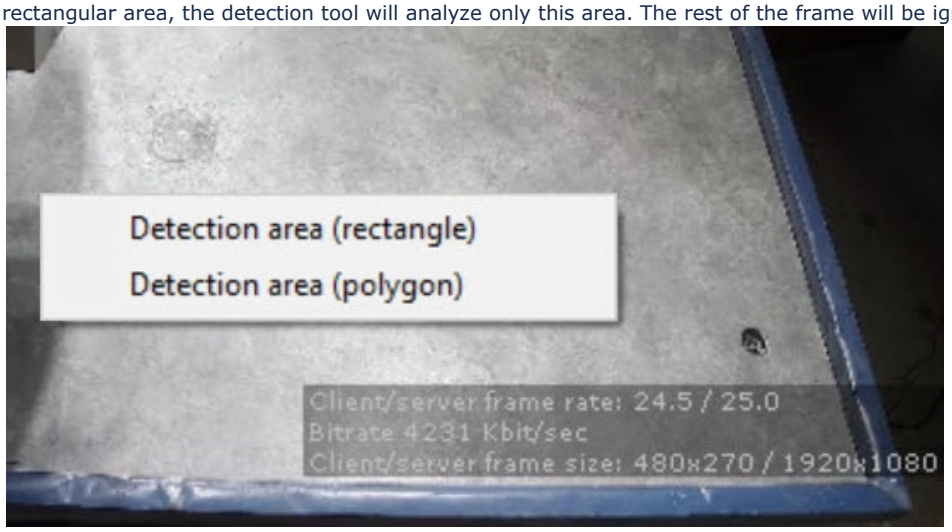
Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, the sensitivity scale of the detection tool is recorded to the archive (see Displaying information from a detection tool (mask)). To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Object Presence Detection**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**0.1**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100]
Type	**Object Presence Detection**	Name of the detection tool type (non-editable field)
Advanced settings		

Neural network file		Select a neural network file. The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, enter a path to the file. **Note** For the correct neural network operation on Linux OS, place the corresponding file in the /opt /AxxonSoft/DetectorPack/NeuroSDK directory.
Number of measurements in a row to trigger detection	**5**	Specify the minimum number of frames on which the detection tool must detect an object to generate an event. The value must be in the range [5; 20]
Scanning mode	**Yes** **No**	The parameter is disabled by default. To detect objects without changing the frame size, select the **Yes** value. To work in the scanning mode, the neural network must support the scanning mode
Basic settings		
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Intel GPU** **Huawei NPU**	Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). **Attention!** • It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS). • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
Sensitivity	**33**	Specify the sensitivity of the detection tool empirically. The value must be in the range [1; 99]. The preview window displays the sensitivity scale of the detection tool that relates to the sensitivity parameter. If the scale is green, object isn't detected. If the scale is yellow, object is detected, but not enough to generate an event. If the scale is red, object is detected and the detection tool will generate an eevent, if the scale is red through the sampling period (50 seconds by default). Example. The sensitivity parameter value of **40** means that the detection tool will generate an event when the scale has at least four divisions full over the entire detection period. An event will stop when the scale has less than two divisions full over the detection period. The detection tool will generate an event again if the scale has at least four divisions full over the entire detection period

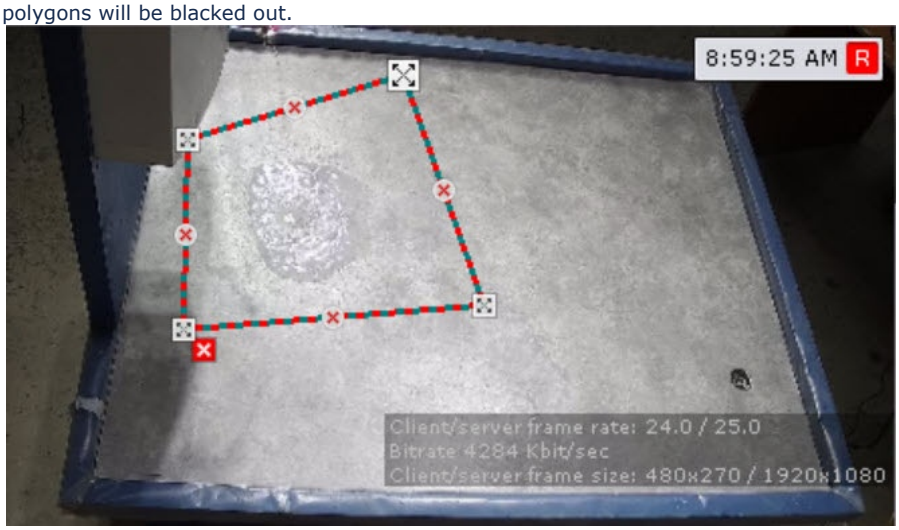
By default, the entire frame is a detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area):

1. Right-click in the preview window.

2. If you want to specify the detection area by one or more rectangles, select **Detection area (rectangle)**. If you specify a rectangular area, the detection tool will analyze only this area. The rest of the frame will be ignored.



3. If you want to specify the detection area by one or more polygons, select **Detection area (polygon)**. If you specify one or several polygonal areas, the detection tool will analyze the entire frame. The part of the frame not included in the specified polygons will be blacked out.

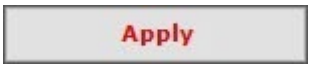
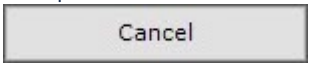


Attention!

You must select the detection area (polygon or rectangle) experimentally. For some neural networks the quality of detection will be better with rectangle, for others—with polygon.

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- To hide detection area, click the  button. To cancel the action, click this button again.
- To delete the selected area, click the  button.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Fire Detection

Functions of the Fire Detection

Description	Unlike standard fire detection systems, the **Fire Detection** faces many issues with the scene and the background in the video image. We cannot guarantee that fire will be detected in all cases. The **Fire Detection** is meant to increase the likelihood of detecting fire. However, there can be both false alarms and failures to detect actual fire in the camera FOV. The **Fire Detection** is based on neural network, the basic principle of which is learnability. ⚠ **Attention!** If the **Fire Detection** doesn't respond to actual fire in the camera FOV, please record a video and send it to AxxonSoft. We will update *Axxon One* to refine the detection tool (neural network training) based on the video data, and in the next versions of the product the detection operation in similar conditions will be optimal.
Add-ons	For the **Fire Detection** to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Fire Detection

Hardware requirements for neural analytics operation

Requirements for the operation of the Fire Detection are given in the table:

Camera	• We recommend using color cameras. With black and white cameras, the detection quality can be noticeably worse • Resolution must be at least 640x360 • FPS directly affects detection efficiency. In most cases, the default value (1 detection per 10 seconds) is sufficient to detect fires that last more than one minute
Scene and angle	• The minimum fire area in the frame depends on the neural network that you use. For a standard neural network (see Configuring the Fire Detection), the fire area must occupy at least 10% of the frame **Note** In some cases, when fire is clearly visible, the width/height of the fire area can be sufficient at 1-3% of the frame width/height. • Fire must be visually separated from the background

Attention!

If you set a rectangular recognition area for the detection tool, the requirements apply to this area rather than to the entire frame (see Configuring the Fire Detection).

Configuring the Fire Detection

Video stream and scene requirements for the Fire Detection

Hardware requirements for neural analytics operation

To configure the **Fire Detection**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Production Safety Fire Detection**.

By default, the detection tool is enabled and set to detect fire.

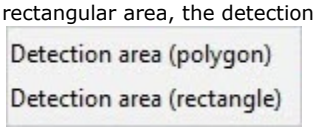
If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, the sensitivity scale of the detection tool is recorded to the archive (see Displaying information from a detection tool (mask)). To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Fire Detection**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**0.1**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100]
Type	**Fire Detection**	Name of the detection tool type (non-editable field)
Advanced settings		

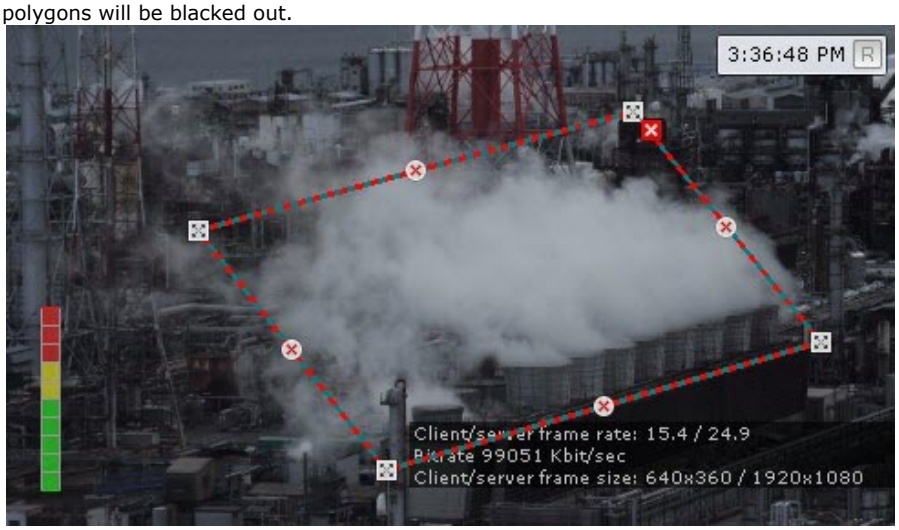
Neural network file		Select a neural network file. The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, enter a path to the file. **Note** For the correct neural network operation on Linux OS, place the corresponding file in the /opt /AxxonSoft/DetectorPack/NeuroSDK directory. **Attention!** If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.
Ignore black and white image	**Yes** **No**	The parameter is disabled by default. If you don't want the detection tool to generate an event when the image is black and white, select the **Yes** value
Number of measurements in a row to trigger detection	**5**	Specify the minimum number of frames with fire for the detection tool to generate an event. The value must be in the range [5; 20]
Scanning mode	**Yes** **No**	The parameter is disabled by default. You can use the scanning mode (see Configuring the scanning mode) to detect small objects or objects in areas far away from the camera. For this, select the **Yes** value. This mode doesn't provide absolute detection accuracy, but can improve detection performance
Basic settings		
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Intel GPU** **Huawei NPU**	Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). **Attention!** • It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS). • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
Sensitivity	**33**	Specify the sensitivity of the detection tool empirically. The value must be in the range [1; 99]. The default value is **33**. The preview window displays the sensitivity scale of the detection tool that relates to the sensitivity parameter. If the scale is green, fire isn't detected. If the scale is yellow, fire is detected, but not enough to generate an event. If the scale is red, fire is detected, and the detection tool generates an event, if the scale is red through the sampling period (50 seconds by default). Example. The sensitivity parameter value of 40 means that the detection tool will generate an event when the scale has at least four divisions full over the entire detection period. An event will end when the scale has less than two divisions full over the detection period. The detection tool will generate an event again if the scale has at least four divisions full over the entire detection period

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area):

1. Right-click in the preview window.
2. If you want to specify the detection area by one or more rectangles, select **Detection area (rectangle)**. If you specify a rectangular area, the detection tool will analyze only this area. The rest of the frame will be ignored.



3. If you want to specify the detection area by one or more polygons, select **Detection area (polygon)**. If you specify one or several polygonal areas, the detection tool will analyze the entire frame. The part of the frame not included in the specified polygons will be blacked out.

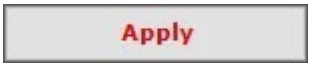
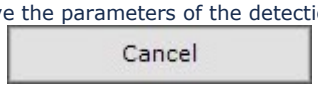


Attention!

You must select the detection area (polygon or rectangle) experimentally. For some neural networks the quality of detection will be better with rectangle, for others—with polygon.

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- To hide detection area, click the  button. To cancel the action, click this button again.
- To delete the selected area, click the  button.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Equipment detection (PPE)

Functions of the Equipment detection (PPE)

Description	**Equipment detection (PPE)** allows you to detect people who enter or stay in the protected area without the necessary equipment and personal protective equipment (PPE), and also people who wear improperly applied PPE. ⚠ **Attention!** We recommend using the detection tool in "gateway" conditions: at the entrance to the area where the equipment or PPE is required, an employee stops for 5–10 seconds, during which the detection tool determines the presence of the necessary equipment (see Configuring the Equipment detection (PPE)).
Neural networks	For detection tool operation, at least two separate neural networks are used: 1. Segmenting network divides the human body into zones (head, shoulders, arms, hands, body, thighs, legs, and feet). 2. Classification network detects equipment (PPE) on a specified body part, and checks if it's properly applied. ⚠ **Attention!** To train a classification neural network, you must provide a list of equipment (see Example of providing a list of valid equipment at the facility for the Equipment detection (PPE)).
Add-ons	For the Equipment detection (PPE) to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Equipment detection (PPE) and its sub-tools

Image requirements for the Equipment detection (PPE) and its sub-tools

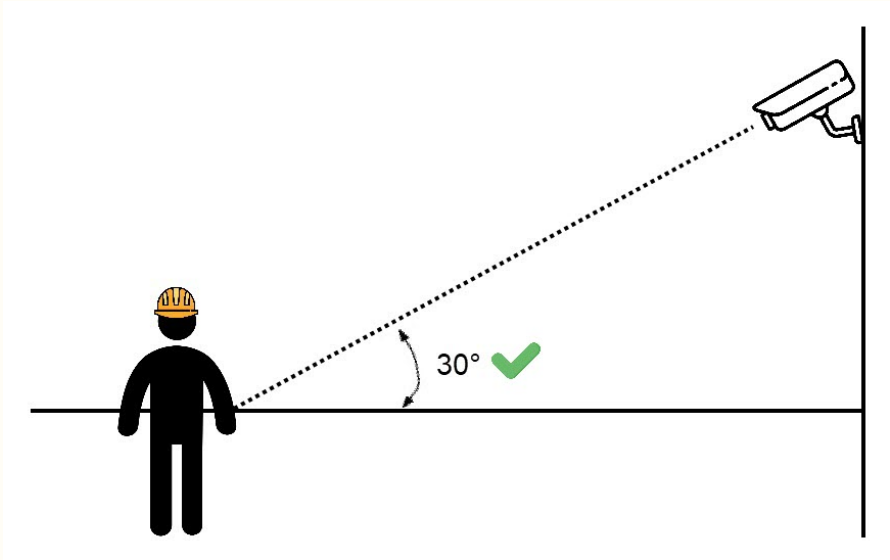
Hardware requirements for neural analytics operation

Requirements for the operation of the Equipment detection (PPE) are given in the table:

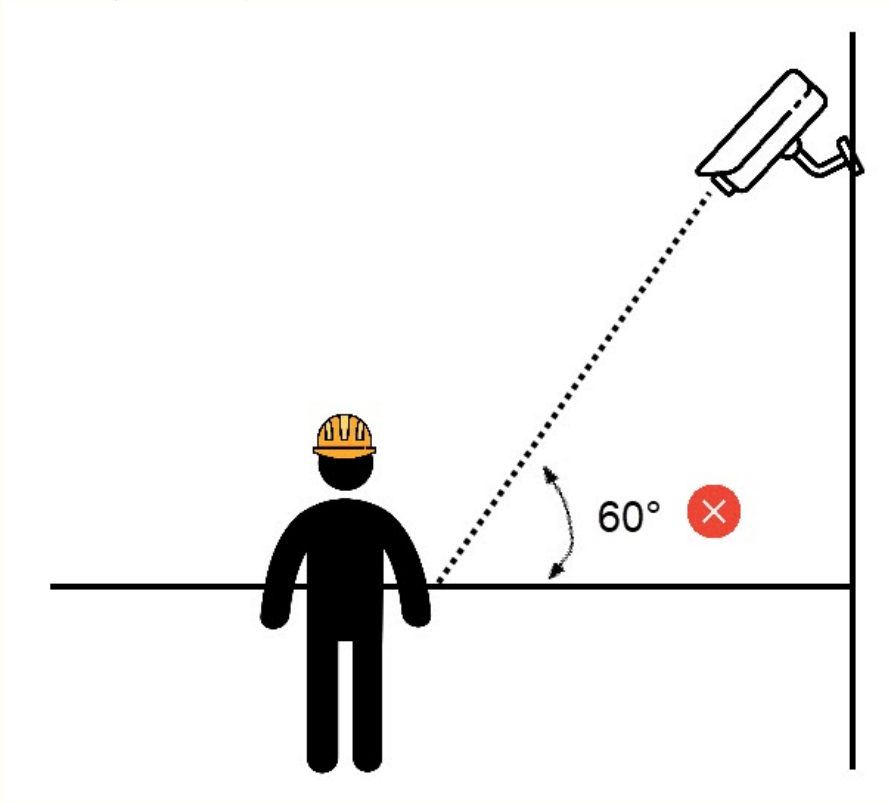
Camera	• Resolution must be at least 640x360. We also don't recommend using a resolution higher than 1920×1080, since higher resolution doesn't increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 • The frame rate per second in the video stream from the camera is at least 3 for solving typical tasks • Detection-based analytics works with color images only

Attention!

- Correct operation of the detection tool isn't guaranteed when using a fisheye lens.
- The camera tilt angle from top to bottom on a person wearing equipment must not exceed 30°. Otherwise, the detection tool won't operate correctly.
  The following diagrams show the examples of:
  - The acceptable tilt angle:



  - The unacceptable tilt angle:



Lighting	• Lighting in the scene is at least 200 lux. The detection tool is applicable in conditions of artificial light. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • There are no products made of rods in the detection area • Moving objects are minimally obscured by static objects in the scene (columns, industrial products, and so on) • The analyzed scene doesn't have reflective surfaces. If present, they must be masked • Camera shake doesn't result in image offsets greater than 1% of the frame size

Image requirements for the Equipment detection (PPE) and its sub-tools

Video stream and scene requirements for the Equipment detection (PPE) and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the Equipment detection (PPE) are given in the table:

Object images	• The detected object (equipment or PPE) must be clearly distinguishable by the human eye
	• The image isn't noisy and not distorted by the artifacts of compression algorithm
	• The width or height of the equipment doesn't exceed 75% of the frame size
	• The duration of the object's visibility is at least 3–8 frames. The minimum number of frames depends on the task
	• There are no visible physical barriers between the camera lens and the analyzed object
	• The minimum sizes of equipment on body parts in pixels are observed. Example of equipment dimensions for a resolution of 1920x1080:
	  ◦ Upper body (torso) 75*100
	  ◦ Legs 75*105
	  ◦ Head 60*65
	  ◦ Hands 65*60
	  ◦ Feet 45*40
	  ◦ Set of equipment 165*295
	• The minimum value of pixel density per meter is observed:

Image resolution	Object type	Minimum pixel density per meter (ratio of the object width in pixels to the object width in meters)	Minimum object size in pixels, width x height
1920x1080	Human	170	~102x309
1280x720	Human	128	~77x233
640x360	Human	80	~48x145

Example of providing a list of valid equipment at the facility for the Equipment detection (PPE)

Data collection requirements for neural network training

For the correct detection, it is important to understand exactly what elements of equipment are used at the facility.

You must provide a complete list of equipment regardless of the current season of the year. This will help to reduce the number of false events from the Equipment detection and get the most positive experience from using this analytics.

Below are examples of lists:

Gloves #1





Gloves #2



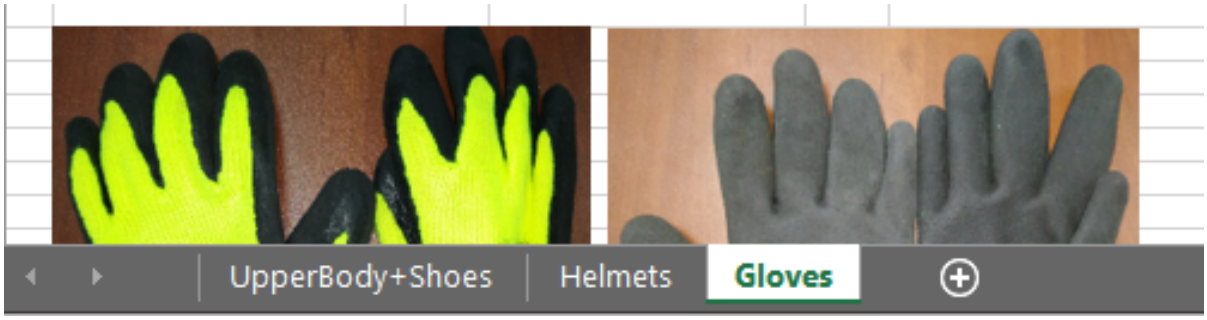


Gloves #3





Gloves #4


UpperBody+Shoes
Helmets
Gloves

Helmet #1:



Helmet #2:



Helmet #3:



Helmet #4:



Helmet #5 (#4 screen:)



Helmet #6 (#4 earmuffs):



UpperBody+Shoes | **Helmets** | Gloves


Weldor:
Cleaning:
Standard:
UpperBody+Shoes
Helmets
Gloves

Configuring the Equipment detection (PPE)

On the page:

- Configuring the detection tool
- Examples of configuring the Equipment detection (PPE) for solving typical tasks

Video stream and scene requirements for the Equipment detection (PPE) and its sub-tools

Image requirements for the Equipment detection (PPE) and its sub-tools

Hardware requirements for neural analytics operation

Configuring the detection tool

To configure the **Equipment detection (PPE)**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create...** **Category: Production Safety** **Equipment detection (PPE)**.

By default, the detection tool is enabled and set to detect people who enter or stay in the protected area without the necessary equipment and personal protective equipment (PPE).

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, mask is recorded to the archive (human body segmentation) (see Displaying information from a detection tool (mask)). To disable the parameter, select the **No** value
	No	
Record objects tracking	**Yes**	The metadata is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Equipment detection (PPE)**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	

Number of frames processed per second	**1**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100]. **Attention!** To operate the detection in a "gateway" (see Examples of configuring the Equipment detection (PPE) for solving typical tasks), we recommend using the standard settings of the detection tool: **1** FPS and **3** FPS for output. In conditions of dynamically moving people, we recommend setting the delay to at least **4** FPS, and the number of frames for output to at least **6** FPS.
Type	**Equipment detection (PPE)**	Name of the detection tool type (non-editable field)
Advanced settings		
Classification network 1 file		By default, the following neural networks are initialized: Classification neural network (equipment and PPE on the head) and Classification neural network (equipment and PPE on the body) according to the selected processing device in the **Neural network mode** parameter. To initialize only one item of equipment, select the required classification neural network file. There must be a separate classification neural network to recognize equipment on each body segment. The standard classification neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, specify the path to the file. **Note** To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. **Attention!** If you use standard classification neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.
Classification network 2 file		
Classification network 3 file		
Classification network 4 file		
Classification network 5 file		
Mask	**Yes** **No**	The parameter is disabled by default. If you want to display the human body segmentation in the preview window, select the **Yes** value
Number of measurements in a row to trigger detection	**3**	Specify the minimum number of frames with a violation for the detection tool to generate an event. The value must be in the range [1, 20]. **Attention!** To operate the detection in a "gateway" (see Examples of configuring the Equipment detection (PPE) for solving typical tasks), we recommend using the standard settings of the detection tool: **1** FPS and **3** FPS for output. In conditions of dynamically moving people, we recommend setting the delay to at least **4** FPS, and the number of frames for output to at least **6** FPS.
One event per PPE element	**Yes**	By default, the detection tool event is generated once for each element of equipment within a track of a person. If you want the detection tool to generate an event for each equipment violation, select the **No** value. **Example**

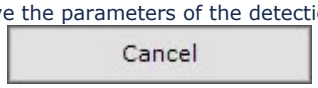
	No	An individual not wearing a helmet appears in the frame, puts on a helmet, then puts it off. If the **One event per PPE element** parameter is enabled, you will have one alarm event, otherwise—two.
Segmenting network file		By default, the Segmenting neural network is initialized according to the selected processing device in the **Neural network mode** parameter. The standard segmenting neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, specify the path to the file. **Note** To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. **Attention!** If you use standard segmenting neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.
Basic settings		
Min person height	**0.01**	Specify the minimum height and width of a person in the frame as a percentage of the frame height/width (0.15 = 15%). Objects that are smaller than the specified size won't be detected. The value must be in the range [0, 1]
Min person width	**0.01**	
Neural network mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Intel GPU**	Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). **Attention!** • It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS). • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool. • If you select Intel HDDL, due to the features of the device, only the segmenting neural network will be processed on it, the CPU will be used to run the classification neural networks.
Invert Results		
Invert results of default network	**No** **OnlyHelmet** **OnlySafetyVest** **AllNet**	The parameter is disabled by default. To receive events about the detection of equipment that are initialized in the **Classification network file** parameter by default (Classification neural network (equipment and PPE on the head) and Classification neural network (equipment and PPE on the body)), select the required value from the list
Invert results of network 0	**Yes** **No**	The parameter is disabled by default. To receive events about the detection of equipment specified in the **Classification network file** parameters, set the **Yes** value in the corresponding parameters **Invert results of network**

Invert results of network 1	**Yes**
	No
Invert results of network 2	**Yes**
	No
Invert results of network 3	**Yes**
	No
Invert results of network 4	**Yes**
	No

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- To hide detection area, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To discard the changes, click the **Cancel**  button.

The Equipment detection (PPE) is now configured.

The **Equipment detection (PPE)** generates an event when a person is in the frame without the necessary equipment and personal protective equipment on the specified parts of the body or when equipment and personal protective equipment is improperly applied.



The **Equipment detection (PPE)** recognizes equipment of the following colors:

1. Helmets:
    a. Yellow.
    b. White.
    c. Blue.
    d. Green.
    e. Orange.
    f. Black.
    g. Red.



2. Vests:
    a. Yellow.

b. Orange.



Attention!

To ensure the correct reception of the E-mail notifications (see E-mail notification) after the detection tool event is generated, you must configure a separate macro with an E-mail message for each item of equipment.

Examples of configuring the Equipment detection (PPE) for solving typical tasks

Typical tasks for detecting equipment and personal protective equipment:

1. Detection in gateway conditions. A gateway is a border, which can either be a virtual line or a door, a barrier, a turnstile. The algorithm for working in gateway conditions is as follows:
    a. A person stops in front of an area where equipment or PPE is required.
    b. A person poses in a way that it is possible to check the presence of all elements of equipment (the element must not be overlapped by the person, other elements of equipment, or items of clothing).
    c. Screening of a person. There must be no obstacles between the person and the camera, blocking the person for screening.
2. Detection in a production conditions: persons move freely in the detection area.

Note

By default, the **Equipment detection (PPE)** is configured for detection in gateway conditions.

The recommended settings for solving typical tasks are as follows:

Parameters	Equipment detection in gateway conditions	Equipment detection in production conditions
Basic		
Number of frames processed per second	**1**	**7**
Min person height	**0.01**	**0.09**
Min person width	**0.01**	**0.03**
Advanced		
Number of measurements in a row to trigger detection	**3**	**7**
Mask	**No**	**No**
One event per PPE element	**Yes**	**Yes**

Smoke Detection

Functions of the Smoke Detection

Description	Unlike standard smoke detection systems, the **Smoke Detection** faces many issues with the scene and the background in the video image. We cannot guarantee that smoke will be detected in all cases. The **Smoke Detection** is meant to increase the likelihood of detecting smoke. However, there can be both false alarms and failures to detect actual smoke in the camera FOV. The **Smoke Detection** is based on neural network, the basic principle of which is learnability. ⚠ **Attention!** If the **Smoke Detection** doesn't respond to actual fire in the camera FOV, please record a video and send it to AxxonSoft. We will update *Axxon One* to refine the detection tool (neural network training) based on the video data, and in the next versions of the product the detection operation in similar conditions will be optimal.
Add-ons	For the Smoke Detection to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Smoke Detection

Hardware requirements for neural analytics operation

Requirements for the operation of the **Smoke Detection** are given in the table:

Camera	• We recommend using color cameras. With black and white cameras, the detection quality can be noticeably worse • Resolution must be at least 640x360 • FPS directly affects detection efficiency. In most cases, the default value (1 detection per 10 seconds) is sufficient to detect smoke that lasts more than one minute
Scene and camera angle	• The minimum smoke area in the frame depends on the neural network that you use. For a standard neural network (see Configuring the Smoke Detection), the smoke area must occupy at least 10% of the frame **Note** In some cases, when smoke is clearly visible, the width/height of the smoke area can be sufficient at 1-3% of the frame width/height. • Smoke must be visually separated from the background

Attention!

If you set a rectangular recognition area for the detection tool, the requirements apply to this area rather than to the entire frame (see Configuring the Smoke Detection).

Configuring the Smoke Detection

Video stream and scene requirements for the Smoke Detection

Hardware requirements for neural analytics operation

To configure the **Smoke Detection**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Production Safety Smoke Detection**.

By default, the detection tool is enabled and set to detect smoke.

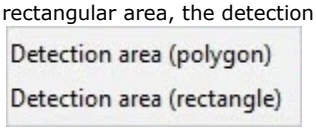
If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes** **No**	By default, the sensitivity scale of the detection tool is recorded to the archive (see Displaying information from a detection tool (mask)). To disable the parameter, select the **No** value
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server
Other		
Enable	**Yes** **No**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
Name	**Smoke Detection**	Enter the detection tool name or leave the default name
Decoder mode	**Auto** **CPU** **GPU** **HuaweiNPU**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
Number of frames processed per second	**0.1**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100]
Type	**Smoke Detection**	Name of the detection tool type (non-editable field)
Advanced settings		

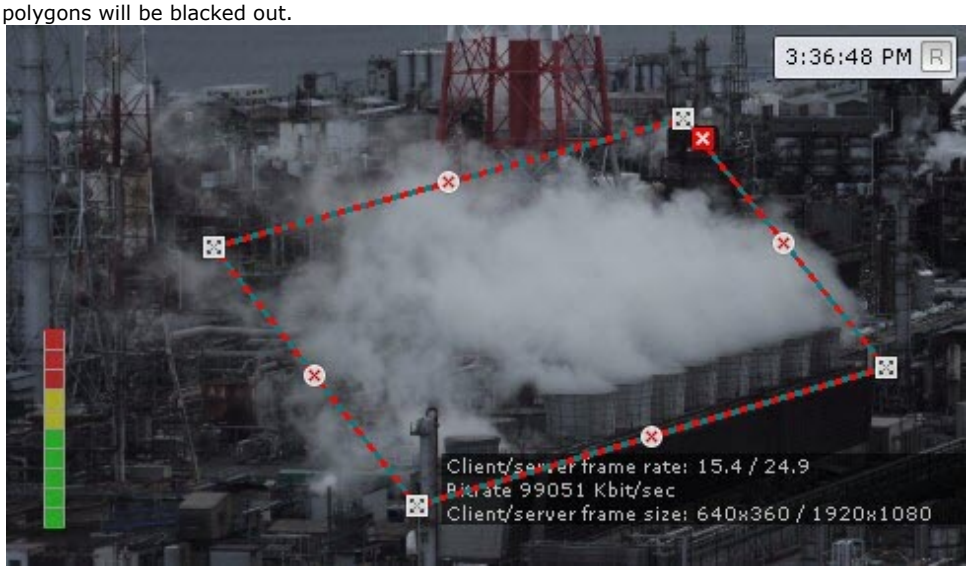
Neural network file		Select a neural network file. The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, enter a path to the file **Note** For correct neural network operation on Linux OS, place the corresponding file in the /opt /AxxonSoft/DetectorPack/NeuroSDK directory. **Attention!** If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.
Ignore black and white image	**Yes** **No**	The parameter is disabled by default. If you don't want the detection tool to generate an event when the image is black and white, select the **Yes** value
Number of measurements in a row to trigger detection	**5**	Specify the minimum number of frames with smoke for the detection tool to trigger. The value must be in the range [5; 20]
Scanning mode	**Yes** **No**	The parameter is enabled by default. You can use the scanning mode (see Configuring the scanning mode) to detect small objects or objects in areas far away from the camera. For this, select the **Yes** value. This mode doesn't provide absolute detection accuracy, but can improve detection performance
Basic settings		
Mode	**CPU** **Nvidia GPU 0** **Nvidia GPU 1** **Nvidia GPU 2** **Nvidia GPU 3** **Intel GPU** **Huawei NPU**	Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). **Attention!** • It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS). • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
Sensitivity	**33**	Specify the sensitivity of the detection tool empirically. The value must be in the range [1; 99]. The default value is **33**. The preview window displays the sensitivity scale of the detection tool that relates to the sensitivity parameter. If the scale is green, smoke isn't detected. If the scale is yellow, smoke is detected, but not enough to generate an event. If the scale is red, smoke is detected and the detection tool will generate an event, if the scale is red through the sampling period (50 seconds by default). Example. The sensitivity parameter value of **40** means that the detection tool will generate an event when the scale has at least four divisions full over the entire detection period. An event will stop when the scale has less than two divisions full over the detection period. The detection tool will generate an event again if the scale has at least four divisions full over the entire detection period

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area):

1. Right-click in the preview window.
2. If you want to specify the detection area by one or more rectangles, select **Detection area (rectangle)**. If you specify a rectangular area, the detection tool will analyze only this area. The rest of the frame will be ignored.



3. If you want to specify the detection area by one or more polygons, select **Detection area (polygon)**. If you specify one or several polygonal areas, the detection tool will analyze the entire frame. The part of the frame not included in the specified polygons will be blacked out.

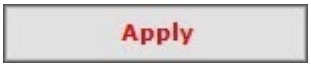
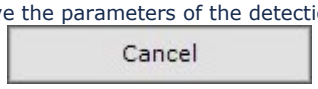


Attention!

You must select the detection area (polygon or rectangle) experimentally. For some neural networks the quality of detection will be better with rectangle, for others—with polygon.

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- To hide detection area, click the  button. To cancel the action, click this button again.
- To delete the selected area, click the  button.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

Water Level Detection

Functions of the Water Level Detection

Description	**Water Level Detection** generates events when the water level exceeds the set level in a specified area
Add-ons	For the **Water Level Detection** to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream requirements for the Water Level Detection

Image requirements for the Water Level Detection

Hardware requirements for neural analytics operation

Requirements for the operation of the **Water Level Detection** are given in the table:

Camera	• You must use only color cameras • Resolution must be at least 640x360

Image requirements for the Water Level Detection

Video stream requirements for the Water Level Detection

Hardware requirements for neural analytics operation

Requirements for the operation of the **Water Level Detection** are given in the table:

Video image	• No glare or shadows on the measuring scale

Configuring the Water Level Detection

Video stream requirements for the Water Level Detection

Image requirements for the Water Level Detection

Hardware requirements for neural analytics operation

To configure the **Water Level Detection**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Production Safety Water Level Detection**.

By default, the detection tool is enabled and set to detect the water level in the frame.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, recording of the water level indicator to the archive is enabled. To disable it, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low quality video stream reduces the load on the Server
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Water Level Detection**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**10**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016; 100]
Type	**Water Level Detection**	Name of the detection tool type (non-editable field)
Advanced settings		

<table>
<tr><td>Frame size change</td><td>1920</td><td>The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The following algorithm is used:

1. If the longer side of the source image exceeds the value specified in the Frame size change field, it is divided by two.
2. If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further.
3. If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution.

Note

For example, the source image resolution is 2048*1536, and the specified value is set to 1000. I n this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.</td></tr>
<tr><td>Neural network file</td><td></td><td>Select a neural network file. The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, enter a path to the file.

Note

For correct neural network operation on Linux OS, place the corresponding file in the /opt /AxxonSoft/DetectorPack/NeuroSDK directory.

Attention!

If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%.</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td>Neural network</td><td>Yes
No</td><td>If the water in the frame is transparent and the detection tool cannot correctly identify its level, use Neur al network:

1. If the No value is selected, the detection tool will work based on the algorithm without using the neural network on the CPU, ignoring the value specified in the Neural network file field.
2. If the Yes value is selected:

a. If no value is selected in the Neural network file field, the system will automatically select the required standard neural network for the device specified in the Neural network mode field.
b. If a custom neural network is selected in the Neural network file field that corresponds to the device specified in the Neural network mode field and is a water level neural network, a detection tool with a neural network algorithm based on this neural network will be created.

Attention!

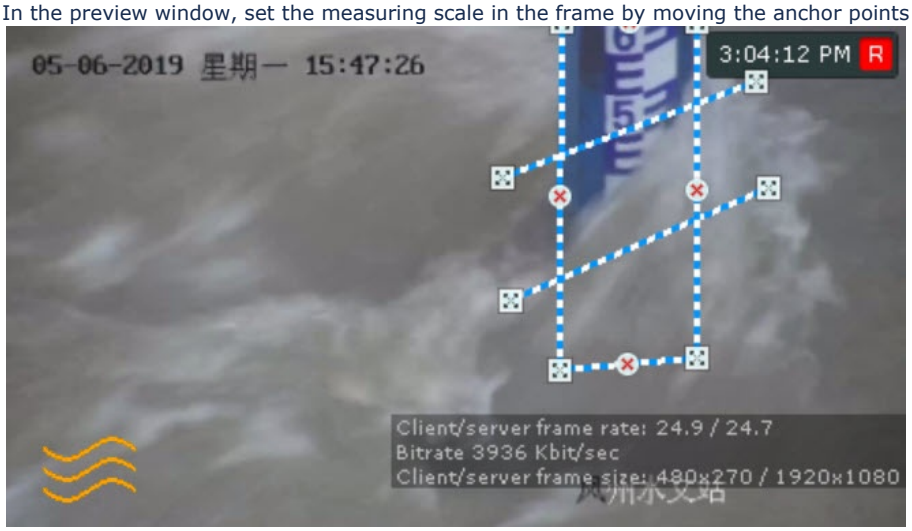
If the neural network file is not specified correctly, the detection tool will not work. The neural network algorithm will recreate itself every 20 seconds.</td></tr>
<tr><td>Neural network mode</td><td>CPU
Nvidia GPU 0
Nvidia GPU 1
Nvidia GPU 2</td><td>Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

Attention!

• It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS).
• If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.</td></tr>
</table>

	Nvidia GPU 3	
	Intel GPU	
Visible bottom value	**0**	Specify the visible bottom value under normal conditions on the measuring scale. The value must be in the range [0, 19]
Visible top value	**1**	Specify the visible top value under normal conditions on the measuring scale. The value must be in the range [0, 19]

In the preview window, set the measuring scale in the frame by moving the anchor points :



Attention!

When ypu specify the measuring scale, its top and bottom borders must match the values specified in the **Visible bottom value** and **Visible top value** parameters.

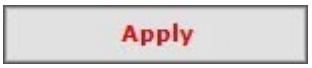
Note

The water level indicator is displayed in the lower left corner. If the indicator is green, the water level is below high and critical marks. If the indicator is orange, the water level is at high mark, but below critical mark. A red indicator means that water level is above critical mark.

a. Specify a line as a limit, exceeding which the detection tool will generate an alarm.
b. Specify a line as a limit, exceeding which the detection tool will give a warning in the form of orange color of the sensor in the **Surveillance window**.

Note

- For convenience of configuration, you can "freeze" the frame. Click the button. To cancel the action, click this button again.
- To hide detection area, click the button. To cancel the action, click this button again.
- To delete the selected area, click the button.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuring the **Water Level Detection** is complete.

When you have created the detection tool, you can see a sensor on the layout in the **Surveillance window**.

If the sensor icon is green  , the water level is lower than both critical and high marks. If the icon is orange  , the water level is above the high mark, but below the critical mark. A red icon  means that the water level is above the critical mark.

You can also add a numerical value of the water level to the **Surveillance window** (see Configuring display of water level detection).

Glow detector

Functions of the Glow detector

Description	**Glow detector** is used to track light sources (lamps) in the surveillance area

Video stream and scene requirements for the Glow detector

Image requirements for the Glow detector

Hardware requirements for neural analytics operation

Video stream and scene requirements for the **Glow detector** are given in the table:

Camera	• Resolution is at least 320x240 pixels • FPS is at least 6 • No camera shake
Scene and angle	• Camera is directed toward the plane in which the light sources are located (ideally, the optical axis of the camera is strictly perpendicular to this plane)

Image requirements for the Glow detector

Video stream and scene requirements for the Glow detector

Hardware requirements for neural analytics operation

Image requirements for the **Glow detector** are given in the table:

Object images	• Light sources in the video are visually distinguishable

Configuring the Glow detector

Video stream and scene requirements for the Glow detector

Image requirements for the Glow detector

Hardware requirements for neural analytics operation

To configure the **Glow detector**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Production Safety Glow detector**.

By default, the detection tool is enabled and set to track light sources (lamps).

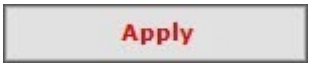
If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

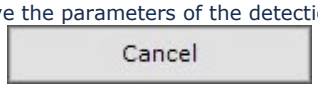
Parameter	Value	Description
Object features		
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Glow detector**	Enter the detection tool name or leave the default name
Brightness threshold	**240**	Specify the sensitivity of the detection tool to changes in the state of the light source. You must select the required value empirically. For a dim light source, we recommend increasing the value of the parameter. The value must be in the range [0, 255]
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**20**	Specify the number of frames that the detection tool will process per second. The value must be in the range [0.016, 100]
Sensitivity	**99**	Specify the sensitivity of the detection tool as a percentage. You must select the required value empirically. The higher the sensitivity, the greater the probability of a false alarm. The lower the sensitivity, the greater the probability of missing an event. The value must be in the range [0, 100]
Time delta between frames	**100**	Specify the time interval between two measurements of light indication in seconds. The value must be in the range [0, 10000]
Type	**Glow detector**	Name of the detection tool type (non-editable field)

To ensure receiving accurate events from the detection tool, in the preview window you can specify one or more detection areas using the anchor points  (see Configuring a detection area). Detection areas must be located on each light source (lamp) and their dimensions must match the dimensions of the light sources.

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

PPE detection VL

Functions of the PPE detection VL

Description	The **PPE detection VL** allows you to detect in the frame people who enter or stay in the protected area without the necessary equipment and personal protective equipment (PPE), and also people who wear improperly applied PPE. **Attention!** We recommend using the detection tool in "gateway" conditions: at the entrance to the area where the equipment or PPE is required, an employee stops for 5–10 seconds, during which the detection tool determines the presence of the necessary equipment The **PPE detection VL** uses an embedded neural network that detects the following types of equipment and PPE: • Helmet, • Hood, • Vest
Licensing	To operate the detection tool, contact an AxxonSoft manager and get a license file (see Types of licenses)
Add-ons	For the **PPE detection VL** to work, you must install VL PPE add-on and SDK Pack (see Installing DetectorPack add-ons)

Video stream and scene requirements for the PPE detection VL and its sub-tools

Image requirements for the PPE detection VL and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the PPE detection VL and its sub-tools are given in the table:

Camera	• Resolution must be at least 640x360. We also don't recommend using a resolution higher than 1920×1080, since higher resolution doesn't increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1920x1080 • The frame rate per second in the video stream from the camera is at least 13 for solving typical tasks • Detection-based analytics works with color images only **Attention!** Correct operation of the detection tool isn't guaranteed when you use a fisheye lens.
Lighting	• Lighting in the scene is at least 200 lux. The detection tool is applicable in conditions of artificial light. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • There are no products made of rods in the detection area • Moving objects are minimally obscured by static objects in the scene (columns, industrial products, and so on) • Avoid large obstructions in the camera FOV (columns, tower cranes, stacked materials, and so on). They will obscure the detected objects and cause track breaks. If obstructions cannot be avoided, we recommend not placing them in the center of the frame • The analyzed scene doesn't have reflective surfaces. If present, they must be masked • The analyzed scene doesn't have strong light flashes (spotlights, active welding zones) • Camera shake doesn't result in image offsets greater than 1% of the frame size • Shooting angle without a strong camera tilt • To improve the quality of the video stream, the camera lens must be cleaned of heavy dirt. We don't recommend locating cameras above the material unloading area or near ventilation shafts

Image requirements for the PPE detection VL and its sub-tools

Video stream and scene requirements for the PPE detection VL and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the PPE detection VL and its sub-tools are given in the table:

Attention!

Correct operation of the detection tool isn't guaranteed when you use a fisheye lens.

Object images	• The detected object (equipment or PPE) must be clearly distinguishable by the human eye
	• Color image, isn't noisy and isn't distorted by the artifacts of compression algorithm
	• Linear dimensions of equipment or PPE must not exceed 65% of the corresponding frame size
	• The duration of the object's visibility is at least 10–13 frames. The minimum number of frames depends on the task
	• There are no visible physical barriers between the camera lens and the analyzed object
	• Obscuring of a person and/or PPE by an obstruction and/or by another person, and/or cropping by frame boundaries must not exceed 25%
	• The minimum sizes of equipment on body parts in pixels are observed:
	  ○ Vest—at least 50 pixels
	  ○ Helmet/Hood—at least 20 pixels
	• PPE must have a standard look and shape, and have the following colors:
	  ○ Vest: green, yellow, orange
	  ○ Helmet/Hood: white, yellow, orange, red, blue, green
	• The minimum value of pixel density per meter is observed:

Image resolution	Minimum pixel density per meter (ratio of the object height in pixels to the object height in meters)	Minimum object height in pixels
1920x1080	60	100
1280x720	60	100
640x360	60	100

Example of providing a list of valid equipment at the facility for the PPE detection VL

Data collection requirements for neural network training

For the correct detection, it is important to understand exactly what elements of equipment are used at the facility.

You must provide a complete list of equipment regardless of the current season of the year. This will help to reduce the number of false events from the PPE detection VL and get the most positive experience from using this analytics.

Below are examples of lists:

Gloves #1





Gloves #2



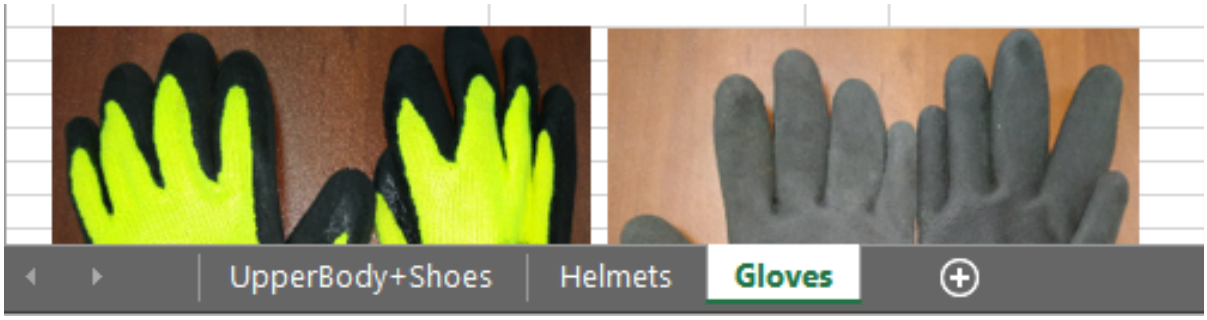


Gloves #3





Gloves #4


UpperBody+Shoes
Helmets
Gloves

Helmet #1:



Helmet #2:



Helmet #3:



Helmet #4:



Helmet #5 (#4 screen:)



Helmet #6 (#4 earmuffs):



UpperBody+Shoes | **Helmets** | Gloves


Weldor:
Cleaning:
Standard:
UpperBody+Shoes
Helmets
Gloves

Activating the license for the PPE detection VL in Windows OS

> **Attention!**
>
> Starting with *Detector Pack* 3.11, a demo license has been added to the VL PPE add-on (see Installing DetectorPack add-ons). Demo license is valid for 30 days after installation on one Server or a virtual machine.

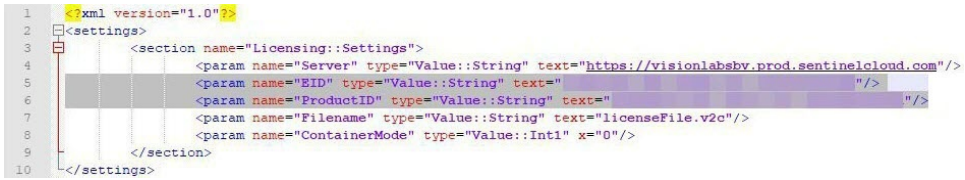
To activate a license for the **PPE detection VL** (see Configuring the PPE detection VL), do the following:

1. Request **EID** and **ProductID** from the technical support.

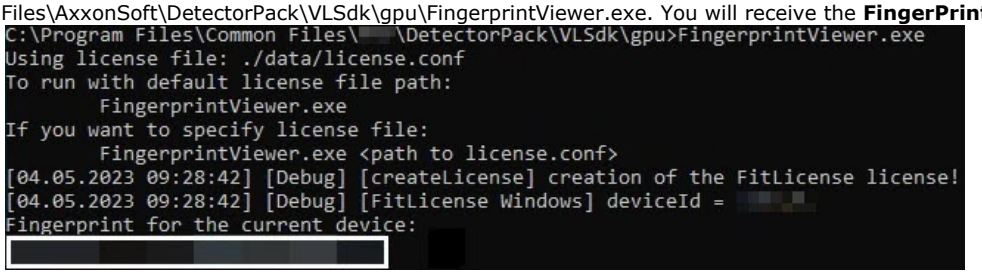
   > **Attention!**
   >
   > **EID** and **ProductID** are linked with the MAC address of the Server. If the MAC address changes, you need to request **EID** and **ProductID** again.

2. Open the following file in a text editor: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
3. Enter the received **EID** and **ProductID**.

```
<param name="EID" type="Value::String" text="received EID"/>
<param name="ProductID" type="Value::String" text="received ProductID"/>
```



4. Save the file: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
5. In the command line, run the following file as administrator: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\FingerprintViewer.exe. You will receive the **FingerPrint** data.

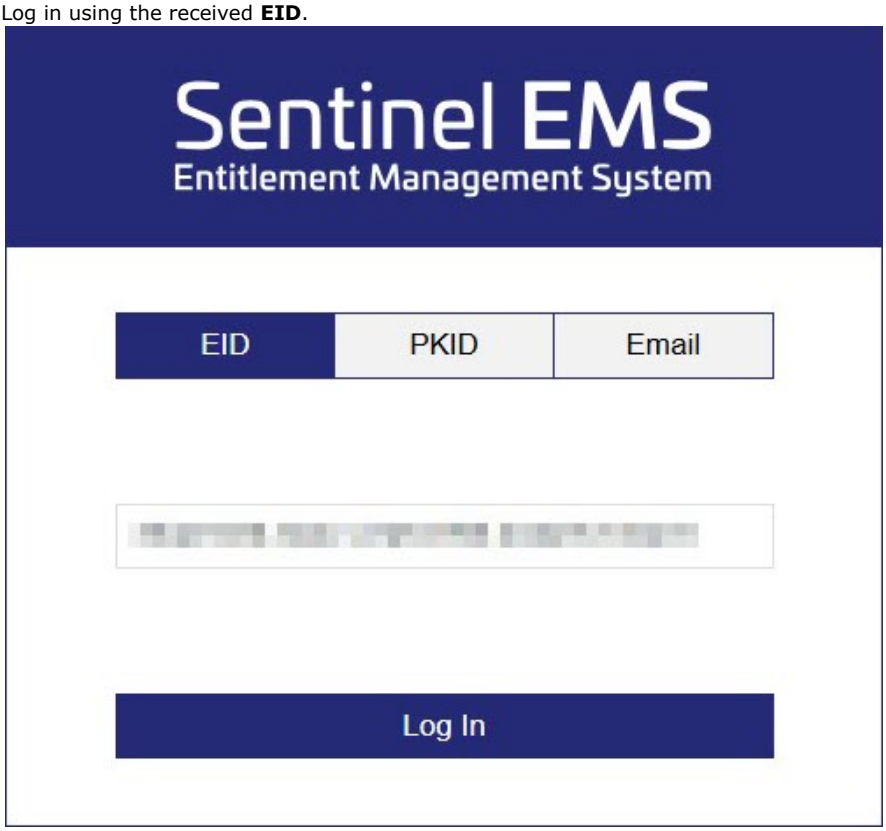


6. Go to the website.

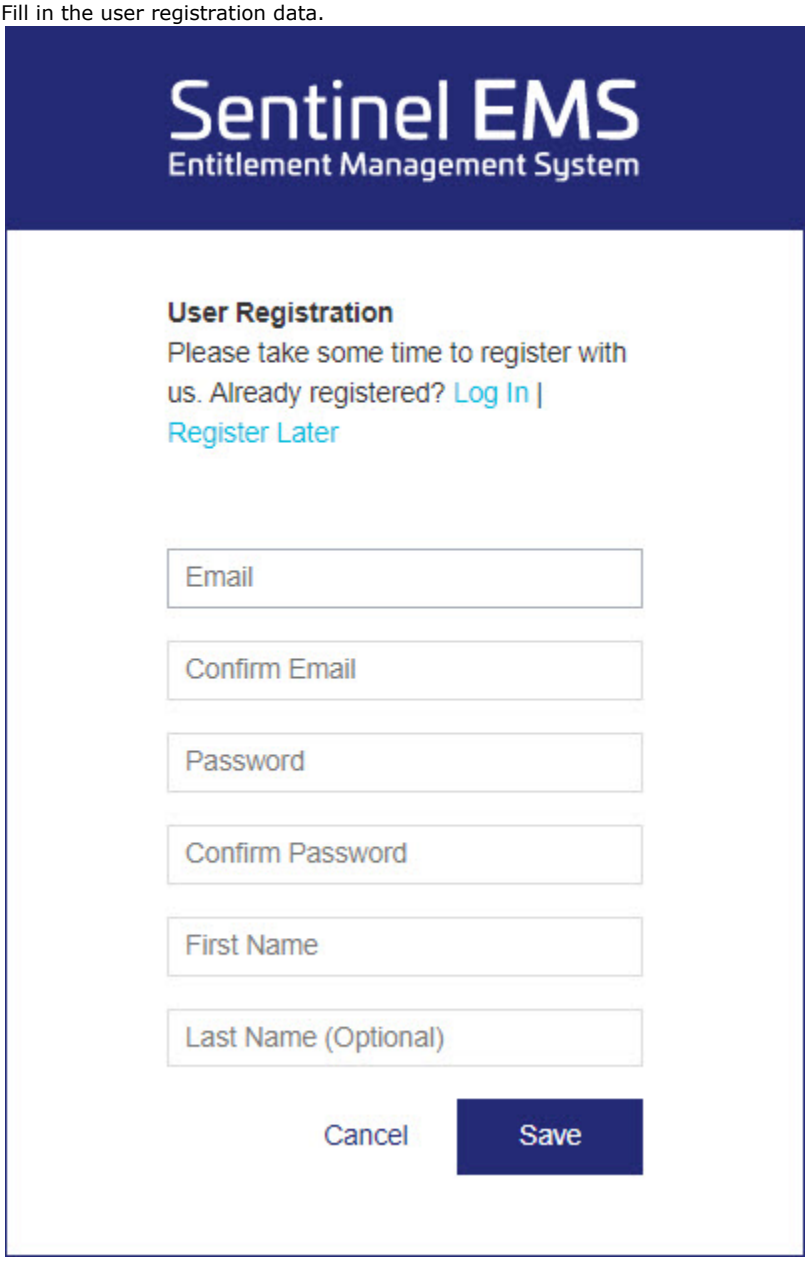
   > **Attention!**
   >
   > If you fail to log in to the website, contact the technical support.

> Guide to the Sentinel EMS Customer Portal

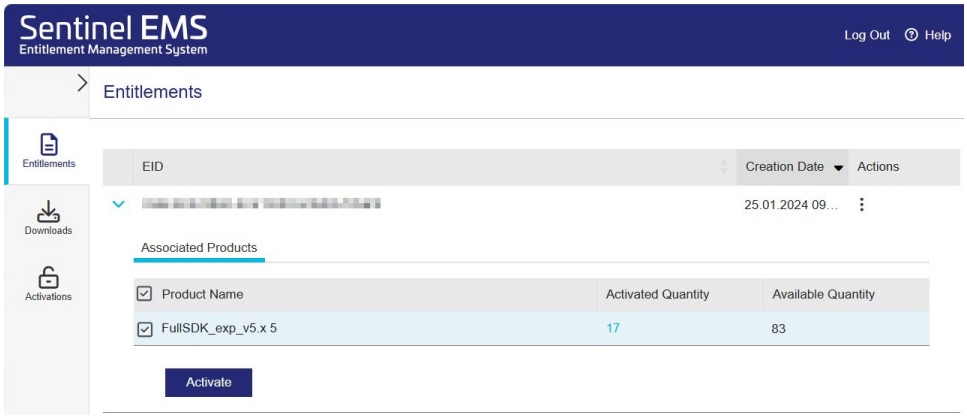
7. Log in using the received **EID**.



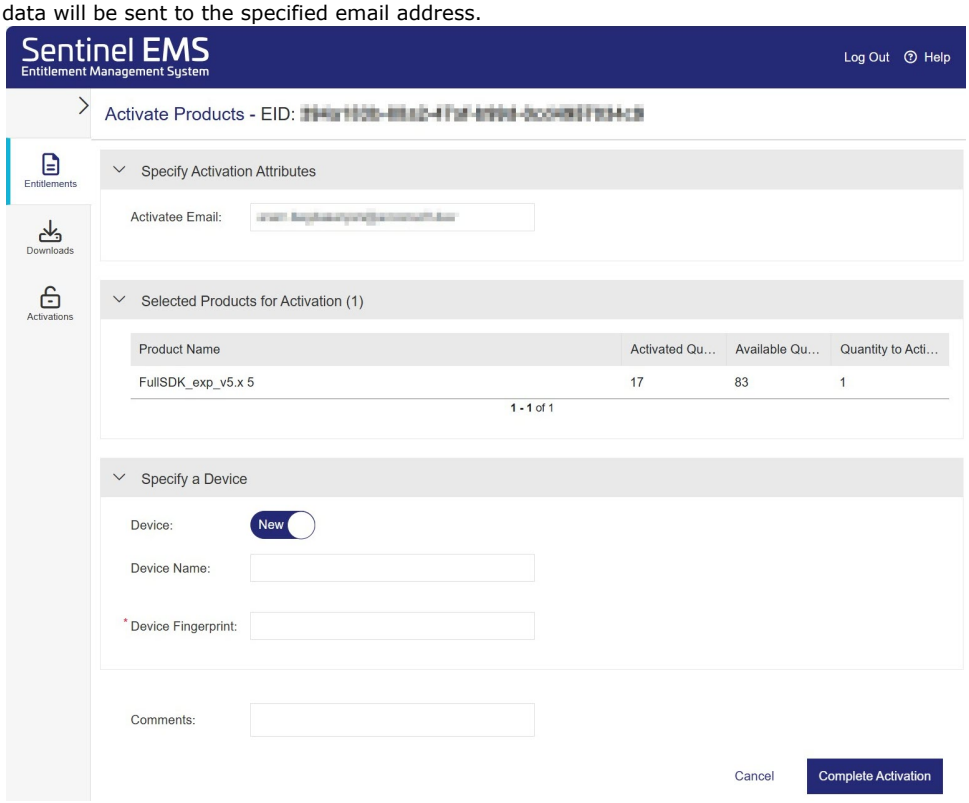
8. Fill in the user registration data.



9. Click the **Save** button.
10. Click the **Activate** button to activate the license.



11. In the **Activatee Email** field, specify the email address to confirm the license activation. The **licenseFile.v2c** file with license data will be sent to the specified email address.



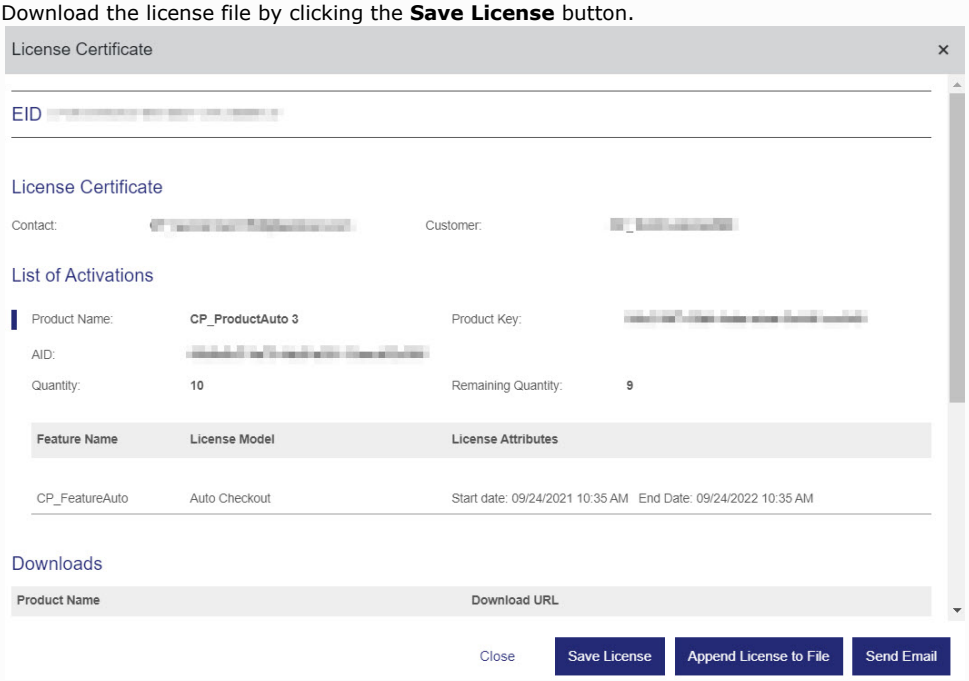
12. In the **Device FingerPrint** field, specify the **FingerPrint** data.
13. Click the **Complete Activation** button.
14. Place the downloaded **licenseFile.v2c** file on the Server in the folder: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\.
15. Make sure the license is successfully activated. If the Server is connected to the internet, the license will be checked automatically.

Note

If the Server doesn't have internet connection, do the following:

1. Do steps 2–5, 14 on the Server where the license will be used.
2. Do steps 1, 6–13, 15 on any computer connected to the internet.
3. Click the **View License Certificate** button.

4. Download the license file by clicking the **Save License** button.



The license is activated on the Server with no internet connection.

The **PPE detection VL** license is activated.

Activating the license for the PPE detection VL in Linux OS

> **Attention!**
>
> Starting with *Detector Pack* 3.11, a demo license has been added to the VL PPE add-on (see Installing DetectorPack add-ons). Demo license is valid for 30 days after installation on one Server or a virtual machine.

To activate a license for the **PPE detection VL** (see Configuring the PPE detection VL), do the following:

1. Request **EID** and **ProductID** from the technical support.

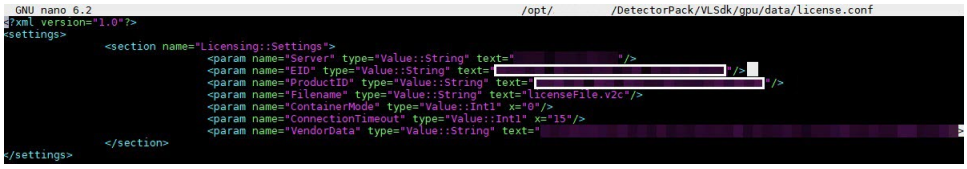
   > **Attention!**
   >
   > **EID** and **ProductID** are linked with the MAC address of the Server. If the MAC address changes, you need to request **EID** and **ProductID** again.

2. Open the **license.conf** file.

   ```
   sudo nano /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data/license.conf
   ```

3. Enter the received **EID** and **ProductID**.

   ```
   <param name="EID" type="Value::String" text="received EID"/>
   <param name="ProductID" type="Value::String" text="received ProductID"/>
   ```

4. Save the file.
5. Run the **FingerprintViewer** file. You will receive the **FingerPrint** data.

   ```
   sudo /opt/AxxonSoft/DetectorPack/VLSdk/gpu/FingerprintViewer
   ```

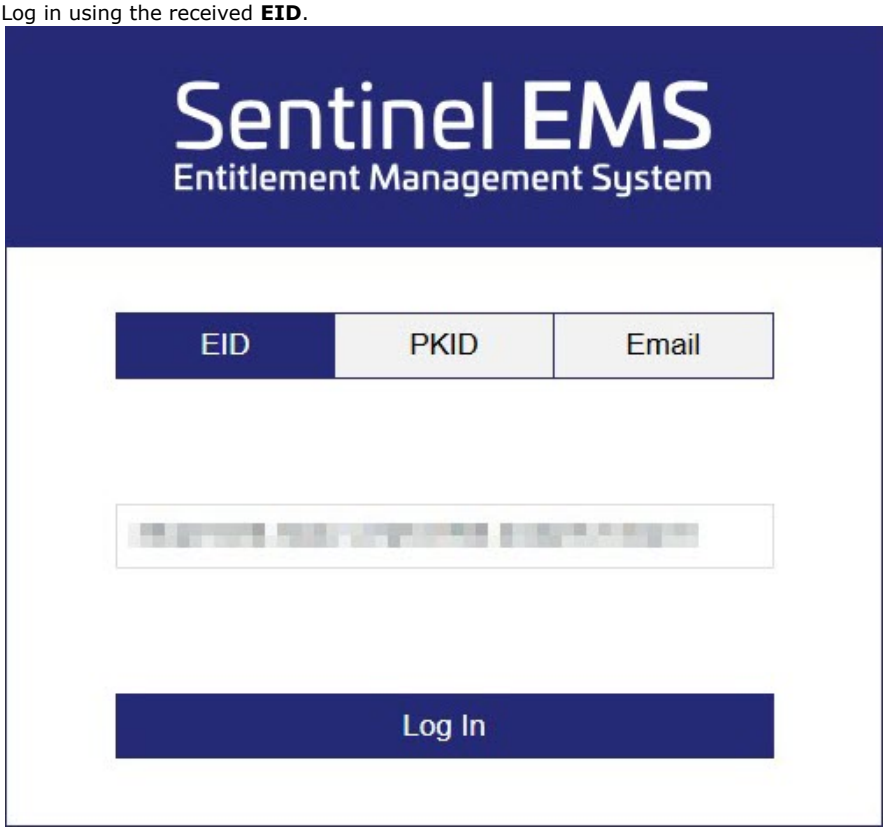
   

6. Go to the website.

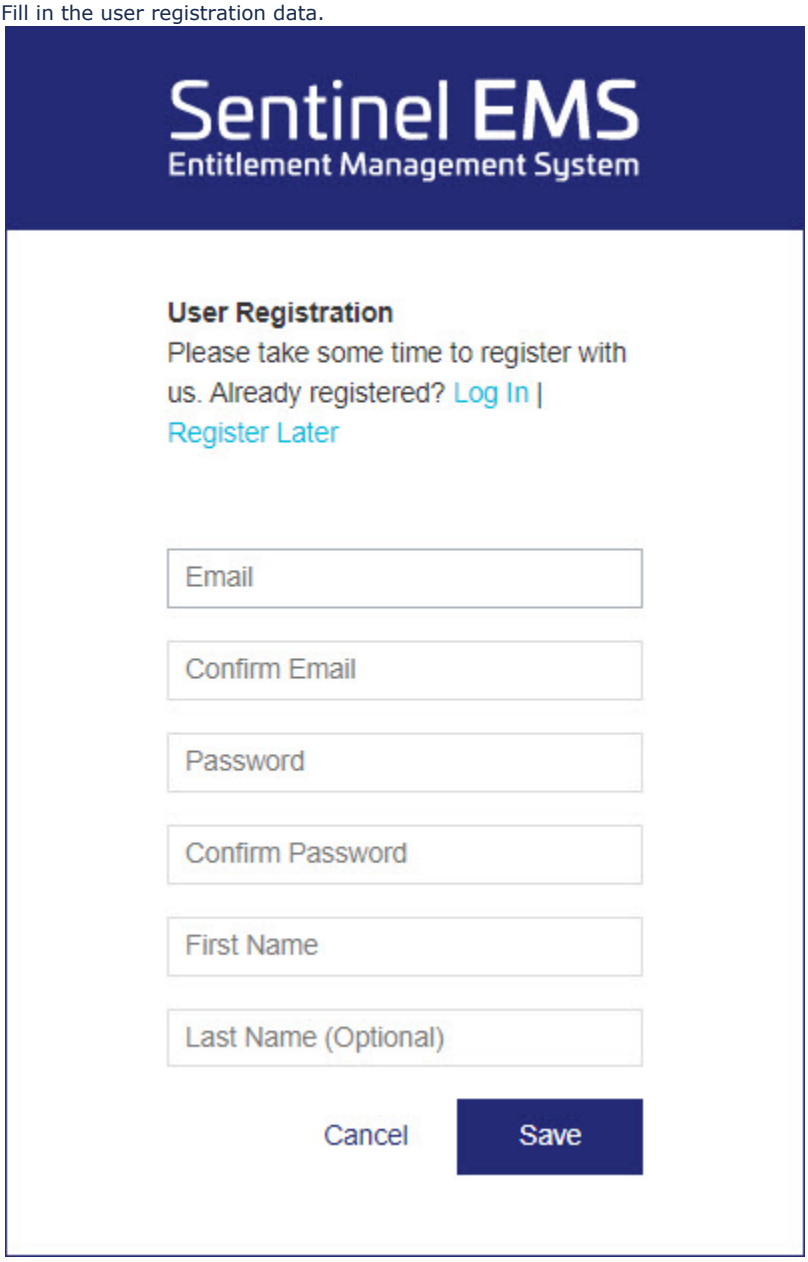
   > **Attention!**
   >
   > If you fail to log in to the website, contact the technical support.

> Guide to the Sentinel EMS Customer Portal

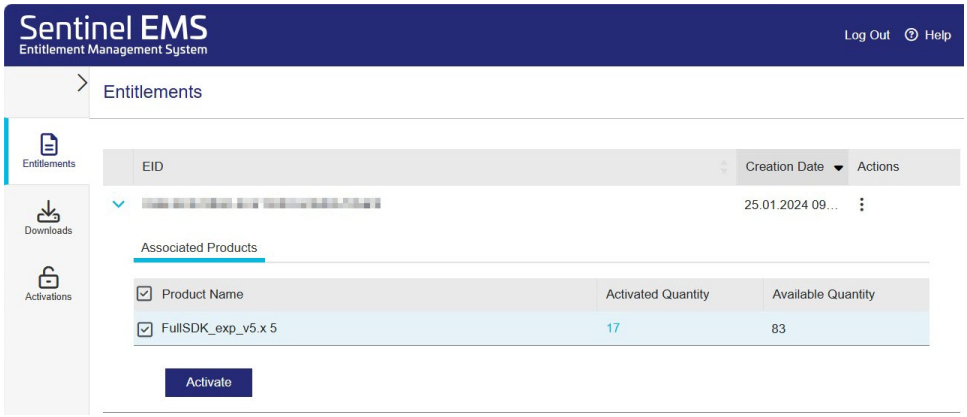
7. Log in using the received **EID**.



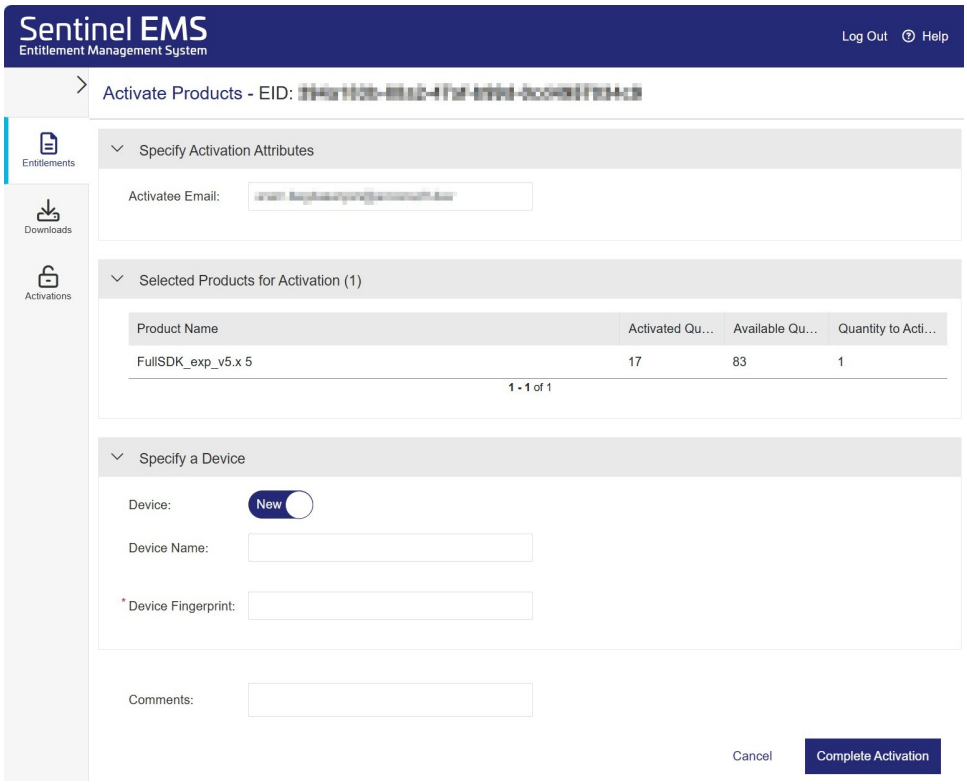
8. Fill in the user registration data.



9. Click the **Save** button.
10. Click the **Activate** button to activate the license.



11. In the **Activatee Email** field, specify the email address to confirm the license activation. The **licenseFile.v2c** file with license data will be sent to the specified email address.



12. In the **Device FingerPrint** field, specify the **FingerPrint** data.
13. Click the **Complete Activation** button.
14. Place the **licenseFile.v2c** in the required directory.

```
sudo cp /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data/licenses-archive/license.conf /opt/AxxonSoft
/DetectorPack/VLSdk/gpu/data/license.conf
```

15. Activate the license.

```
sudo /opt/AxxonSoft/DetectorPack/VLSdk/gpu/FingerprintViewer /opt/AxxonSoft/DetectorPack/VLSdk/gpu/data
/license.conf
```

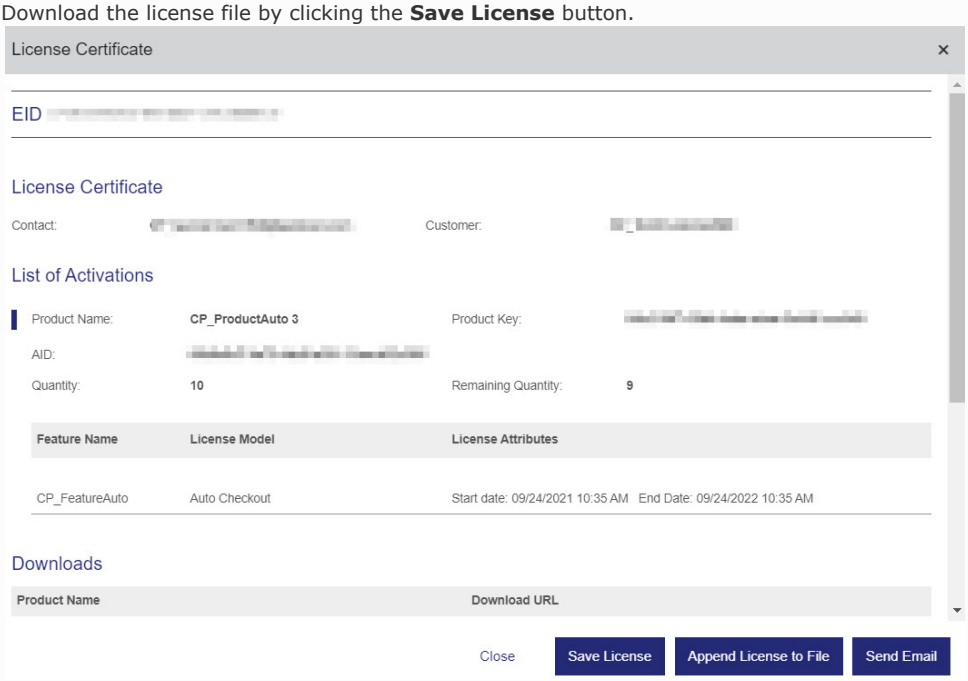
16. Make sure the license is successfully activated. If the Server is connected to the internet, the license will be checked automatically.

Note

If the Server doesn't have an Internet connection, do the following:

1. Do steps 2–5, 14 on the Server where the license will be used.
2. Do steps 1, 6–13, 15 on any computer connected to the internet.
3. Click the **View License Certificate** button.

4. Download the license file by clicking the **Save License** button.



The license is activated on the Server with no internet connection.

The **PPE detection VL** license is activated.

Configuring the PPE detection VL

Video stream and scene requirements for the PPE detection VL and its sub-tools

Image requirements for the PPE detection VL and its sub-tools

Hardware requirements for neural analytics operation

Activating the license for the PPE detection VL in Windows OS

Activating the license for the PPE detection VL in Linux OS

To configure the **PPE detection VL**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create...** **Category: Other** **PPE detection VL**.

By default, the detection tool is enabled and set to detect people who enter or stay in the protected area without the necessary equipment and personal protective equipment (PPE).

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

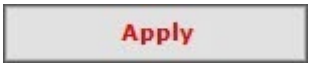
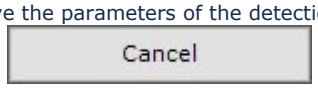
Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	The metadata is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**PPE detection VL**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei NPU	
Minimum authenticity threshold	**90**	Specify the minimum level of recognition accuracy for creating a track. You must select the appropriate value empirically. The higher the value, the fewer objects will be detected, but at the same time the recognition quality will be higher. The value must be in the range [1, 100]
Mode	**CPU**	Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools). **Attention!** • If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool. • It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS, Optimizing the operation of neural analytics on GPU in Linux OS).
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	

	Nvidia GPU 3	
Number of frames processed per second	**1**	Specify the number of frames that the neural network will process per second. If the detection tool recreates the track for the same object, which leads to incorrect counting, increasing the value can help eliminate false positives. The higher the value, the more accurate the tracking, but the higher the CPU load. The value must be in the range [0.016; 100]. **Attention!** To operate the detection in a "gateway", we recommend using the standard settings of the detection tool: **1** FPS and **10** FPS for output (see Functions of the PPE detection VL).
Number of measurements in a row to trigger detection	**10**	Specify the minimum number of frames with a violation for the detection tool to generate an event. The value must be in the range [2, 50]
One detection per track	**Yes** **No**	By default, the detection tool generates an event for each element of equipment once per track existence. If you want the detection tool to generate an event for each equipment violation, select the **No** value
Type	**PPE detection VL**	Name of the detection tool type (non-editable field)

By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- To hide detection area, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

The **PPE detection VL** will generate an event when a person is in the frame without the necessary equipment and personal protective equipment on the specified parts of the body or when equipment and personal protective equipment is improperly applied.

Category: Retail

Barcode Detection

Functions of the Barcode Detection

Description	The **Barcode Detection** is used to recognize and detect various types of barcodes. An event, based on which a macro can be started (see Examples of macros for barcode detection), can be generated if a barcode meets the conditions specified in the detection tool settings. Supported barcode types: • Aztec • DataMatrix • PDF417 • QR code (the maximum number of characters for recognition is 1000) • Linear (UPC-A, Code 39, UPC-E, Code 93, EAN-8, Code 128, EAN-13, Codabar, DataBar, DataBar Expanded, DX Film, Edge, ITF)
Licensing	To operate the detection tool, you need to contact a manager of AxxonSoft and get a license file (see Types of licenses)
Add-ons	For the detection tool to work, you must install the Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Barcode Detection and its sub-tools

Image requirements for the Barcode Detection and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the Barcode Detection and its sub-tools are given in the table:

Camera	• Resolution is at least 640x360 pixels • The FPS in the video stream from the camera must be at least 2 for typical tasks
Scene and camera angle	• Barcodes must be visually distinguishable from each other in the image • Background is mostly static and doesn’t change abruptly

Image requirements for the Barcode Detection and its sub-tools

Video stream and scene requirements for the Barcode Detection and its sub-tools

Hardware requirements for neural analytics operation

Requirements for the operation of the Barcode Detection and its sub-tools are given in the table:

Barcode images	• Image isn’t noisy or distorted by compression artifacts • For barcode detection, the duration of barcode visibility must be at least one frame

Configuring the Barcode Detection

Video stream and scene requirements for the Barcode Detection and its sub-tools

Image requirements for the Barcode Detection and its sub-tools

Hardware requirements for neural analytics operation

To create the detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Retail Barcode Detection**.

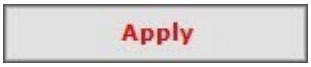
By default, the detection tool is enabled and configured for operation. Depending on the required tasks, you must select a specific type of barcode for detection.

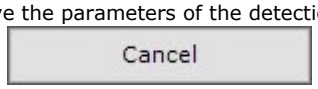
If necessary, you can change the settings of the detection tool parameters given in the table:

Parameter	Value	Description
Object features		
Record objects tracking	**Yes**	The metadata of the video stream is recorded to the database by default. To disable the parameter, select the **No** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Barcode Detection**	Enter the detection tool name or leave the default name
Barcode type	**Aztec**	Select the type of barcode that will generate events from the detection tool when detected
	DataMatrix	
	PDF417	
	QR code	
	Linear	
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	Huawei NPU	
Mode	**CPU**	Select a processor for the neural network operation (see Selecting Nvidia GPU when configuring detection tools)
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	

	Nvidia GPU 3	
	Intel NCS (not supported)	
	Intel GPU	
	Intel HDDL (not supported)	
	Huawei NPU	
Neural network file		If you use a custom neural network, select the corresponding file. **Attention!** • To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training). • A trained neural network for a particular scene allows you to detect only barcode of a certain type. • To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. • If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%. The standard neural networks are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory.
Number of frames processed per second	**20**	Specify the number of frames for the detection tool to process per second. The value must be in the range [0.016, 100]
Type	**Barcode Detection**	Name of the detection tool type (non-editable field)

By default, the entire frame is the detection area. If necessary, in the preview window, specify detection areas using the anchor points  (see Configuring a detection area).

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

The Barcode Detection is configured.



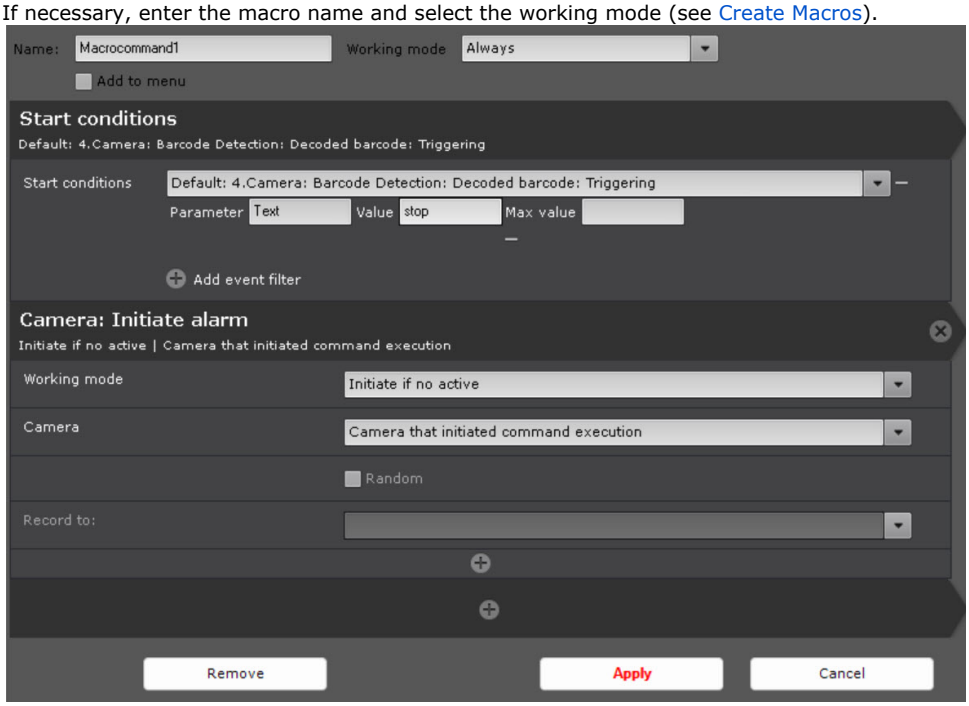
If necessary, you can search for a barcode in the archive. You can search by the text that was recognized during barcode detection (Search by barcode).

Examples of macros for barcode detection

You can configure macros for the barcode detection that will perform specific actions when a barcode is detected (see Settings specific to actions).

For example, you can configure a macro to initiate an alarm if a certain text is detected in a barcode. To configure this macro, do the following:

1. Create and configure the **Barcode Detection** beforehand (see Barcode Detection).
2. Go to the **Programming** tab **Event rules** **Create...**
3. If necessary, enter the macro name and select the working mode (see Create Macros).



4. In the Start conditions, specify the values:
    a. In the **Parameter** field, enter **Text**.
    b. In the **Value** field, enter the required text that will trigger an alarm when recognized.
5. Click the **Apply** button.

Configuring a macro to initiate an alarm when a specific text is detected in a barcode is complete.

Crowd Estimation VA

Functions of the Crowd Estimation VA

Description	The **Crowd Estimation VA** counts crowds of people and generates an event when a certain number of people in a specified area is exceeded. ⚠ **Attention!** • The **Crowd Estimation VA** is used to analyze scenes with the number of people from 10 to 10,000. • To analyze scenes with less than 10 people, we recommend using **Neurotracker** (see Neurotracker). An event on the basis of which a macro can be started (see Configuring start conditions for event-driven macros) can be generated if the number of objects in the frame meets the specified conditions
Licensing	To operate the detection tool, you need to contact a manager of AxxonSoft and get a license file (see Types of licenses)
Add-ons	For the detection tool to work, you must install the VA Crowd Estimation Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Crowd Estimation VA

Image requirements for the Crowd Estimation VA

Hardware requirements for neural analytics operation

Requirements for the operation of the Crowd Estimation VA are given in the table:

Camera	• Resolution of 256x256 pixels or higher • Color: analytics works with both gray and color images • No camera shake
Lighting	• The best performance of the detection tool is achieved under moderate lighting. In conditions of insufficient (night) or excessive (light-striking) lighting, the algorithm performance can decrease • No abrupt changes in lighting

Scene and camera angle	• The background is mostly static and doesn’t change abruptly
	• Analytics cannot work correctly:
	  ◦ on reflective surfaces and if there are sharp shadows from moving objects
	  ◦ if there is a repeating pattern in the scene (crosswalk)
	  ◦ if there are objects in the scene that look like people (monuments, animals)
	  ◦ if there are periodic movements of background objects in the camera FOV (trees, rain, and so on)

Image requirements for the Crowd Estimation VA

Video stream and scene requirements for the Crowd Estimation VA

Hardware requirements for neural analytics operation

Requirements for the operation of the Crowd Estimation VA are given in the table:

Object images	• Image quality: the image must be clear, without obvious defects from the compression algorithm

Configuring the Crowd Estimation VA

Video stream and scene requirements for the Crowd Estimation VA

Image requirements for the Crowd Estimation VA

Hardware requirements for neural analytics operation

To create the detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Retail Crowd Estimation VA**.

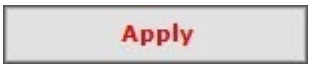
By default, the detection tool is enabled and set to count crowds of people.

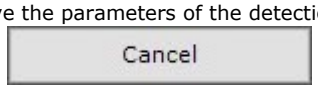
If necessary, you can change the settings of the detection tool parameters given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, the recording of the mask to the archive is disabled. To record the sensitivity scale of the detection tool to the archive (see Displaying information from a detection tool (mask)), select the **Yes** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Crowd Estimation VA**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Mode	**CPU**	Select a processor for the operation (see Selecting Nvidia GPU when configuring detection tools) **Attention!** If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
	Nvidia GPU 0	
	Nvidia GPU 1	
	Nvidia GPU 2	
	Nvidia GPU 3	
Number of alarm objects	**1**	Specify the number of objects at which an event occurs. The value must be in the range [0, 10000]
Number of frames processed per second	**0.017**	Specify the number of frames for the detection tool to process per second. The value must be in the range [0.016, 100]

Trigger upon count	**Greater than or equal to threshold value**	Select when you want to generate events. The **Crowd Estimation VA** will generate events from the threshold value set in the **Number of alarm objects** field
	Less than or equal to threshold value	
	Change in readings	
Type	**Crowd Estimation VA**	Name of the detection tool type (non-editable field)

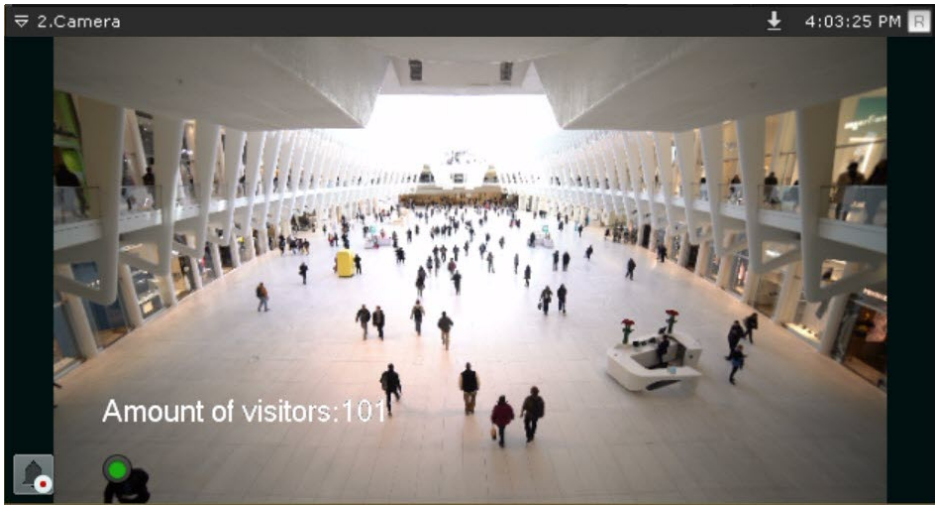
By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

It is possible to display the sensor and the number of objects in the monitored area in the Surveillance window on the layout (see Displaying the number of detected objects).



Neurocounter

Functions of the Neurocounter

Description	The **Neurocounter** counts the number of objects in a specified area using neural network. A event on the basis of which a macro can be started (see Configuring start conditions for event-driven macros), can be generated if the number of objects in the frame meets the specified conditions. Unlike the **Multiple Objects** detection tool (see Configuring Multiple Objects), **Neurocounter** generates events of one type—triggers. In addition, **Neurocounter** consumes fewer resources than the **Multiple Objects** detection tool on the basis of **Neurotracker**
Add-ons	For the **Neurocounter** to work, you must install Neuro Pack add-on (see Installing DetectorPack add-ons)

Video stream and scene requirements for the Neurocounter operation

Hardware requirements for neural analytics operation

Image requirements for the Neurocounter operation

Requirements for the operation of the **Neurocounter** are given in the table:

Camera	• Resolution must be at least 640x360 pixels. We also don't recommend using a resolution higher than 1920×1080, since higher resolution doesn't increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 (see Configuring the Neurocounter) • The frame rate per second in the video stream from the camera is at least 8 for solving typical tasks • Both colorless (gray) and color images **Attention!** The correct operation of the **Neurocounter** isn't guaranteed when you use a fisheye lens.
Lighting	• Lighting in the scene is at least 50 lux. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly • Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on) • The analyzed scene doesn't have reflective surfaces and sharp shadows from moving objects. If present, they must be masked • Camera shake doesn't result in image offsets greater than 1% of the frame size

Image requirements for the Neurocounter operation

Hardware requirements for neural analytics operation

Video stream and scene requirements for the Neurocounter operation

Requirements for the operation of the **Neurocounter** are given in the table:

Object images

- The detected object must be clearly distinguishable by the human eye
- Width and height of objects in the image must not exceed 75% of the frame size
- The image isn't noisy and not distorted by the artifacts of the compression algorithm
- The duration of the object visibility is at least six frames
- Between two frames, an object must move in the direction of a distance not exceeding its size. This condition is necessary for the correct calculation of an object track
- The minimum value of pixel density per meter is observed:

Image resolution	Object type	Minimum pixel density per meter (ratio of the object width in pixels to the object width in meters)	Minimum object size in pixels, width x height	Ratio of the object width to the frame width as a percentage
1920x1080	Human	55	~25x105	~3%
1280x720	Human	35	~17x70	~3%
640x360	Human	17	~10x42	~3%
1920x1080	Light vehicle (2 axles)	55	~354x300	~20%
1280x720	Light vehicle (2 axles)	35	~240x205	~20%
640x360	Light vehicle (2 axles)	17	~132x112	~20%

Configuring the Neurocounter

On the page:

- Configuring the detection tool
- Example of configuring Neurocounter for solving typical tasks

Video stream and scene requirements for the Neurocounter operation

Image requirements for the Neurocounter operation

Hardware requirements for neural analytics operation

Configuring the detection tool

To configure **Neurocounter**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Retail Neurocounter**.

By default, the detection tool is enabled and set to count the number of objects in a specified area using neural network.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, the recording of the mask to the archive is disabled. To record the sensitivity scale of the detection tool to the archive (see Displaying information from a detection tool (mask)), select the **Yes** v alue
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Neurocounter**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video streams. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**1**	Specify the number of frames for the detection tool to process per second. The value must be in the range [0.016, 100] **Note** The default values (**3** output frames and **1** FPS) mean that **Neurocounter** analyzes one frame once per second. If **Neurocounter** detects the specified number of objects (or more) on **3** frames, an event from the detection tool is generated.

Type	**Neurocounter**	Name of the detection tool type (non-editable field)
Advanced settings		
Detected objects	**Yes** **No**	By default, detected objects aren't highlighted in the preview window. If you want to highlight detected objects, select the **Yes** value
Neural network file		If you use a custom neural network, select the corresponding file **Attention!** • To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training). • A trained neural network for a particular scene allows you to detect only objects of a certain type (for example, a person, a cyclist, a motorcyclist, and so on). • If the neural network file is not specified, the default file will be used, which is selected automatically depending on the selected object type (**Object type**) and the selected processor for the neural network operation (**Decoder mode**). If you use a custom neural network, enter a path to the file. The selected object type is ignored when you use a custom neural network. • To ensure the correct operation of the neural network on Linux OS, the corresponding file must be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory. • If you use standard neural network (training wasn't performed in operating conditions), we guarantee the overall accuracy of 80-95% and the percentage of false positives of 5-20%. The standard neural networks are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory.
Number of measurements in a row to trigger detection	**3**	Specify the minimum number of frames on which the detection tool must detect a violation for the detection tool to generate an event. The value must be in the range [1, 20]
Object class		If necessary, specify the class of the detected object. If you want to display tracks of several classes, specify them separated by a comma with a space. For example, **1**, **10**. The numerical values of classes for the embedded neural networks: **1**—Human/Human (top-down view), **10**—Vehicle. a. If you leave the field blank, the tracks of all available classes from the neural network will be displayed (**Object type**, **Neural network file**). b. If you specify a class/classes from the neural network, the tracks of the specified class/classes will be displayed (**Object type**, **Neural network file**). c. If you specify a class/classes from the neural network and a class/classes missing from the neural network, the tracks of a class/classes from the neural network will be displayed (**Object type**, **Neural network file**). d. If you specify a class/classes missing from the neural network, the tracks of all available classes from the neural network will be displayed (**Object type**, **Neural network file**) **Note** Starting with *Detector Pack* 3.10.2, if you specify a class/classes missing from the neural network, the tracks won't be displayed (**Object type**, **Neural network file**).
Scanning window	**Yes** **No**	If detection of small objects or objects in areas far away from the camera is ineffective, you can use the scanning mode. The scanning mode doesn't provide absolute detection accuracy, but it can improve detection performance. To enable the scanning mode, select the **Yes** value (see Configuring the scanning mode)
Scanning window height	**0**	The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels

<table>
<tr><td>Scanning window step height</td><td>0</td><td rowspan="2">The scanning step determines the relative offset of the windows. If the step is equal to the height and width of the scanning window respectively, the segments will line up one after another. Reducing the height or width of the scanning step will increase the number of windows due to their overlapping each other with an offset. This will increase the detection accuracy, but will also increase the CPU load.

⚠ Attention!

The height and width of the scanning step must not be greater than the height and width of the scanning window—the detection tool will not operate with such settings.</td></tr>
<tr><td>Scanning window step width</td><td>0</td></tr>
<tr><td>Scanning window width</td><td>0</td><td>The height and width of the scanning window are determined according to the actual size of the frame and the required number of windows. For example, the real frame size is 1920×1080 pixels. To divide the frame into four equal windows, set the width of the scanning window to 960 pixels and the height to 540 pixels</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td>Detection threshold</td><td>30</td><td>Specify the Detection threshold for objects in percent. If the recognition probability falls below the specified value, the data will be ignored. The higher the value, the higher the accuracy, but some events from the detection tool may not be considered. The value must be in the range [0.05, 100]</td></tr>
<tr><td rowspan="9">Mode</td><td>CPU</td><td rowspan="9">Select a processor for the neural network operation (see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

⚠ Attention!

• If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
• It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU in Windows OS).
• Starting with Detector Pack 3.11, Intel HDDL and Intel NCS aren’t supported.</td></tr>
<tr><td>Nvidia GPU 0</td></tr>
<tr><td>Nvidia GPU 1</td></tr>
<tr><td>Nvidia GPU 2</td></tr>
<tr><td>Nvidia GPU 3</td></tr>
<tr><td>Intel NCS (not supported)</td></tr>
<tr><td>Intel HDDL (not supported)</td></tr>
<tr><td>Intel GPU</td></tr>
<tr><td>Huawei NPU</td></tr>
<tr><td>Number of alarm objects</td><td>5</td><td>Specify the number of objects at which an event occurs. The value must be in the range [0, 100]</td></tr>
<tr><td rowspan="3">Object type</td><td>Person</td><td rowspan="3">Select the recognition object.

• Nano—low accuracy, low processor load.
• Medium—medium accuracy, medium processor load.
• Large—high accuracy, high processor load.</td></tr>
<tr><td>Person (top-down view)</td></tr>
<tr><td>Person (top-down view Nano)</td></tr>
</table>

	Person (top-down view Medium)	
	Person (top-down view Large)	
	Vehicle	
	Person and vehicle (Nano)	
	Person and vehicle (Medium)	
	Person and vehicle (Large)	
Trigger to	**Greater than or equal to threshold value**	Select when you want to generate an event. The **Neurocounter** will generate events from the threshold value set in the **Number of alarm objects** field
	Less than or equal to threshold value	
	Change in readings	

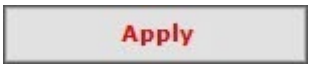
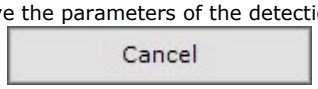
By default, the entire frame is the detection area. In the preview window, you can specify the detection areas using the anchor points  (see Configuring a detection area).



Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply**  button. To cancel the changes, click the **Cancel**  button.

It is possible to display the sensor and the number of objects in the monitored area in the Surveillance window on the layout (see Displaying the number of detected objects).

Example of configuring Neurocounter for solving typical tasks

By default, the **Neurocounter** is set to detect objects with a speed less than 0.3 m/s:

Parameter	Value
Other	
Number of frames processed per second	**1**
Advanced settings	
Number of measurements in a row to trigger detection	**3**
Neural network file	Path to the *.ann neural network file. You can also select the **Object type** value. In this case, this field must be left blank

Basic settings	
Detection threshold	**30**

To solve tasks in which object speed differs from 0.3 m/s, you must increase **Number of frames processed per second** or/and decrease **Number of measurements in a row to trigger detection**. You must select the values empirically depending on the task conditions.

Queue detection

Functions of the Queue detection

Description	The **Queue detection** generates an event when the specified number of people in the queue is exceeded

Video stream and scene requirements for the Queue detection

Image requirements for the Queue detection

Requirements for the operation of the Queue detection are given in the table:

Camera	• Resolution: 720x576 (CIF4), 360x288 (CIF1) is also allowed. Increasing the resolution above CIF4 doesn't improve the performance of the recognition algorithm • FPS is at least 6 • Color: analytics works with both gray and color images • No camera shake
Lighting	• The best performance of the detection tool is achieved under moderate lighting. In conditions of insufficient (night) or excessive (light-striking) lighting, the algorithm performance can decrease • Abrupt changes in lighting can lead to short-term incorrect operation of analytics
Scene and camera angle	• The best position is the camera looking down at the scene. The better this requirement is met, the more accurate the estimate is • Dimensions of the camera FOV: minimum 3x3 m (6x6 people), optimal 4x4 m (8x8 people), maximum 8x8 m (16x16 people) • The background is mostly static and doesn’t change abruptly • Analytics can work incorrectly on reflective surfaces, and if there are sharp shadows from moving objects • Analytics can work incorrectly if there are periodic movements of background objects in the camera FOV (trees, TV is on, and so on)

Image requirements for the Queue detection

Video stream and scene requirements for the Queue detection

Requirements for the operation of the Queue detection are given in the table:

Object images	• Image quality: image must be clear, without obvious defects from the compression algorithm • Allowable person size: the area of the rectangle around a person as a percentage of the frame area is from 0.25% to 10%

Configuring the Queue detection

Video stream and scene requirements for the Queue detection

Image requirements for the Queue detection

To configure the Queue detection, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Retail Queue detection**.

By default, the detection tool is enabled and set to count the number of people in a queue.

If necessary, you can change the settings of the detection tool parameters given in the table:

Parameter	Value	Description
Object features		
Record mask to archive	**Yes**	By default, the recording of the mask to the archive is disabled. To record the sensitivity scale of the detection tool to the archive (see Displaying information from a detection tool (mask)), select the **Yes** value
	No	
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Queue detection**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**1**	Specify the number of frames for the detection tool to process per second. The larger the value, the greater the load on the CPU. The value must be in the range [0.016; 100]
Type	**Queue detection**	Name of the detection tool type (non-editable field)
Advanced settings		
Current queue size report interval	**0**	The default value is **0** (no events are sent). To send events to *AxxonData* (see Queue length report), specify the interval of events transmission in seconds. The value must be in the range [0, 600]

<table>
<tr><td>Frame size change</td><td>1920</td><td>The analyzed frames are scaled down to a specified resolution (1920 pixels on the longer side) by default. The following algorithm is used:

1. If the longer side of the source image exceeds the value specified in the Frame size change field, it is divided by two.
2. If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further.
3. If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution.

Note

For example, the source image resolution is 2048*1536, and the specified value is set to 1000. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td>Person size</td><td>10</td><td>Note

It is better to specify the minimum size of a person graphically, the number in the Person size fi eld is a conditional value. The value must be in the range [0.25, 10]

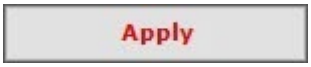
Click the min button and specify the minimum size of a person. To do this, move the anchor points of the rectangular area:

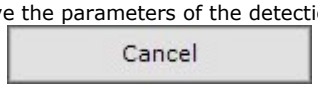
 
</td></tr>
<tr><td>Queue size</td><td>5</td><td>Specify the number of objects in a queue. When the number is exceeded, an event is generated. The value must be in the range [2, 20]</td></tr>
<tr><td>Sensitivity</td><td>0.5</td><td>Specify the sensitivity of the detection tool. The higher the sensitivity, the better the algorithm reacts to minor motion. If you specify the minimum sensitivity value, only significant scene changes can be analyzed by the Queue detection.
You must specify the sensitivity value empirically based on the data from the motion mask (see Displaying information from a detection tool (mask)) in the preview window</td></tr>
</table>

In the preview window, you can specify the detection area by moving the anchor points (see Configuring a detection area).

Note

- For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.
- The detection area is displayed by default. To hide it, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Configuration of the Queue detection is complete. The detection tool will generate events of the following type:

```
Camera. Detection "Queue detection" triggered, queue (min.: 10, max.: 10)
```

where min. and max. is estimated queue length.

Visitors Counter

Functions of the Visitors Counter

Description	The **Visitors Counter** counts visitors of the monitored object and generates an event when the specified number of people at the object is exceeded

Video stream and scene requirements for the Visitors Counter

Image requirements for the Visitors Counter

Requirements for the operation of the **Visitors Counter** are given in the table:

Camera	• Resolution: 720x576 (CIF4), 360x288 (CIF1) is also allowed. Increasing the resolution above CIF4 doesn't improve the performance of the recognition algorithm • FPS is 25 • Color: only color camera • No camera shake
Lighting	• The best performance of the detection tool is achieved under moderate lighting. In conditions of insufficient (night) or excessive (light-striking) lighting, the algorithm performance can decrease • Abrupt changes in lighting can lead to short-term incorrect operation of analytics
Scene and camera angle	• The best position is the camera looking down at the scene. The better this requirement is met, the more accurate the estimate is • Dimensions of the camera FOV: minimum 2x2 m, optimal 4x4 m • The background is mostly static and doesn’t change abruptly • There are no moving objects in the counting area except for people • Analytics can work incorrectly on reflective surfaces, and if there are sharp shadows from moving objects • Analytics can work incorrectly if there are periodic movements of background objects in the camera FOV (trees, TV is on, and so on) • People are minimally obscured by static objects in the scene (columns, trees, and so on) • People must not move in solid stream. Groups of a few people are counted correctly

Image requirements for the Visitors Counter

Video stream and scene requirements for the Visitors Counter

Requirements for the operation of the **Visitors Counter** are given in the table:

Object images	• Image quality: image must be clear, without obvious defects from the compression algorithm

- Allowable person size:
  Person size is an area of the rectangle around a person as a percentage of the frame area. For the correct operation of the detection tool, you must select person size in the range from the minimum value depending on the frame width to 75% of the frame width.

  > **Note**
  >
  > Frame width isn't the original resolution of the video image, but the size of the frame based on the **Frame size change** parameter (see Configuring the Visitors Counter).

  The minimum size of a person, depending on the frame width, is given in the table:

Frame width, px	Minimum size of a person in %
320	18.8
360	16.7
384	15.7
400	15
426	14.1
512	11.8
640	9.4
800	7.5
832	7.3
854	7.1
960	6.3
1024	5.9
1120	5.4
1152	5.2
1280	4.7
1440	4.2
1600	3.8
1792	3.4
1856	3.3
1920	3.2
2048	3.0
2304	2.7
2560	2.4
2732	2.2
2800	2.2
3200	1.9
3840	1.6
4096	1.5
6400	1
8192	0.8

Configuring the Visitors Counter

Video stream and scene requirements for the Visitors Counter

Image requirements for the Visitors Counter

Attention!

- The **Visitors Counter** detection tool can have a margin of error and is suitable for counting the average number of visitors.
- We cannot guarantee the correct operation of the detection tool with a fisheye lens.

To configure the **Visitors Counter**, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Retail Visitors Counter**.

By default, the detection tool is enabled and set to count the number of people in a queue.

If necessary, you can change the settings of the detection tool parameters given in the table:

Parameter	Value	Description
Object features		
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Visitors Counter**	Enter the detection tool name or leave the default name
Decoder mode	**Auto**	Select a processing resource for decoding video. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	
Number of frames processed per second	**25**	Specify the number of frames for the detection tool to process per second. The larger the value, the greater the load on the CPU. The value must be in the range [0.016; 100]
Type	**Visitors Counter**	Name of the detection tool type (non-editable field)
Advanced settings		

Frame size change	**640**	The analyzed frames are scaled down to a specified resolution (by default, **1920** pixels on the longer side) by default. The following algorithm is used: 1. If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two. 2. If the resulting resolution falls below the specified value, the algorithm stops and this resolution will be used further. 3. If the resulting resolution still exceeds the specified value, it is divided by two until it is less than the specified resolution. **Note** For example, the source image resolution is 2048*1536, and the specified value is set to **1000**. In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, we recommend reducing the compression.
Number of people indoor	**0**	Enter the number of people indoor at the time you are configuring the detection tool. The value must be in the range [0, 100000]
People indoor counter	**Yes** **No**	By default, the parameter is disabled. The detection tool generates events: Camera. Visitor access in the direction of "Entrance" and Camera. Visitor access in the direction of "Exit". If you also want to count visitors at the facility and generate an event when the threshold value is exceeded, select the **Yes** value
People indoor counter threshold	**10000**	Specify the threshold value of the number of people indoor. If this value is exceeded, the detection tool generates an event. The value must be in the range [0, 100000]
Basic settings		

Person size	**20**	**Attention!** You must specify the size of a person taking into account Video stream and scene requirements for the Visitors Counter and Image requirements for the Visitors Counter. Specify the area of the rectangle around a person as a percentage of the frame area. Note that the size is calculated based on the compressed frame size, not the original size of the video stream. The value must be in the range [1, 75]. **Note** It is better to specify the minimum size of a person graphically, the number in the **Person size** field is a conditional value. Click the  button in the preview window and specify the size of a person. To do this, move the anchor points of the rectangular area: 

In the preview window, specify the detection area. The detection area is divided into two sectors—area 1 and area 2. The transition from area 1 to area 2 is the visitor's passage in the "Exit" direction. The transition from area 2 to area 1 is the visitor's passage in the "Entrance" direction. If the **People indoor counter** parameter is enabled:

- Transition from area 1 to area 2—minus one to the visitors counter.
- Transition from area 2 to area 1—plus one to the visitors counter.

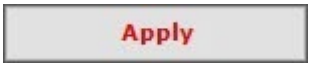
You can configure the sectors, using the anchor points  or lines. To swap sectors, click inside one of them.

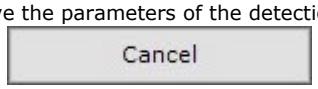


Note

For convenience of configuration, you can "freeze" the frame. Click the  button. To cancel the action, click this button again.

Sectors are displayed by default. To hide them, click the  button. To cancel the action, click this button again.

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Category: Service

Audio Loss

Functions of the Audio Loss

Description	The **Audio Loss** detection tool analyzes audio signal from the camera microphone and generates an event when the line from the microphone to the **Server** breaks (complete absence of sound) ⚠ **Attention!** The **Audio Loss** detection tool doesn't operate with cameras emitting a background signal with a non-zero volume, even if the integrated microphone is physically disabled.

Configuring the Audio Loss

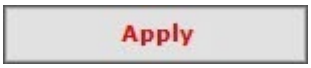
To create the detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Service Audio Loss**.

By default, the detection tool is enabled and set to detect audio loss when the line from the microphone to the **Server** breaks (complete absence of sound).

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Audio Loss**	Enter the detection tool name or leave the default name
Type	**Audio Loss**	Name of the detection tool type (non-editable field)

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Noise Detection

Functions of the Noise Detection

Description	The **Noise Detection** analyzes audio signal from the camera microphone and generates an event when noise is detected

Configuring The Noise Detection

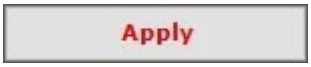
To create the detection tool, do the following:

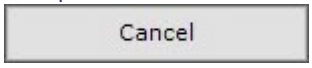
1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Service Noise Detection**.

By default, the detection tool is enabled and set to detect noise.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Noise Detection**	Enter the detection tool name or leave the default name
Type	**Noise Detection**	Name of the detection tool type (non-editable field)
Basic settings		
Alarm end delay	**10**	Enter the time in seconds during which the generation of an event won't stop after the noise stops. If noise is detected again within the specified time, it will be considered as one event
Percentage of noise in audio stream	**2**	Specify the threshold value of noise in the audio stream as a percentage. If the value is exceeded, the detection tool will generate an event. You must select the value empirically in the range [0, 100]

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Signal Detection

Functions of the Signal Detection

Description	The **Signal Detection** analyzes audio signal from the camera microphone and generates an event when an audio signal is received from an audio device

Configuring the Signal Detection

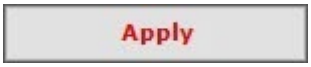
To create the detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Service Signal Detection**.

By default, the detection tool is enabled and set to detect signals.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Other		
Enable	**Yes**	The detection tool is enabled by default. To disable the detection tool, select the **No** value
	No	
Name	**Signal Detection**	Enter the detection tool name or leave the default name
Type	**Signal Detection**	Name of the detection tool type (non-editable field)
Basic settings		
Alarm end delay	**10**	Enter the time in seconds during which the generation of an event won't stop after the noise stops. If noise is detected again within the specified time, it will be considered as one event
Percentage of noise in audio stream	**2**	Specify the threshold value of noise in the audio stream as a percentage. If the value is exceeded, the detection tool will generate an event. You must select the value empirically in the range [0, 100]

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Tampering Detection

Functions of the Tampering Detection

Description

The **Tampering Detection** analyzes video image to determine the nature of its change

Type of analysis	Description
Blurred image analysis	The detection tool generates an event when image borders aren't clear. For example, the detection tool can generate an event when the image is blurred because of a dirty lens
Compression artifacts analysis	The detection tool generates an event when compression artifacts appear in the image
Image noise analysis	The detection tool generates an event when noise appears in the image. For example, the detection tool can generate an event when the bitrate is low, or the image is rippled (snow)
Quality degradation analysis	The detection tool generates an event when there is a degradation in the quality of the image received from the camera. For example, the detection tool can generate an event when there is lens flare, severe defocusing, when camera lens closes, or when there is an abrupt decrease in image lighting
Scene change analysis	The detection tool generates an event when the background of the image changes, indicating a change in the position of the camera in space

Video stream and scene requirements for the Tampering Detection

Image requirements for the Tampering Detection

Requirements for the operation of the **Tampering Detection** are given in the table:

Camera	• Resolution is at least 320x240 pixels • FPS is at least 1 • Camera shake doesn't result in image offsets greater than 1% of the frame size
Lighting	• Moderate lighting. In conditions of insufficient (night) or excessive lighting (light-striking), stable operation of the analytics isn't guaranteed • No abrupt changes in lighting

Scene and camera angle	• Moving objects are visually separable from each other
	• Background is mostly static and doesn't change abruptly
	• Moving objects are minimally obscured by static objects in the scene (columns, trees, and so on)
	• Analytics can work incorrectly
	  ◦ on reflective surfaces, and if there are sharp shadows from moving objects
	  ◦ on long monochrome objects

Image requirements for the Tampering Detection

Video stream and scene requirements for the Tampering Detection

Requirements for the operation of the **Tampering Detection** are given in the table:

Object images	• Image isn't noisy and not distorted by the artifacts of the compression algorithm
	• The width and height of objects in the image must not:
	  ○ be less than 1% of the frame size (at resolutions of at least 1920x1080 pixels) or 15 pixels (at lower resolutions)
	  ○ exceed 75% of the frame size
	• Speed of object movement in the image must be at least one pixel per second
	• To detect an object, the duration of its visibility must be at least eight frames
	• Between two frames, an object must move in the direction of a distance not exceeding its size. This condition is necessary for the correct calculation of an object track

Configuring the Tampering Detection

Video stream and scene requirements for the Tampering Detection

Image requirements for the Tampering Detection

To create the detection tool, do the following:

1. Go to the **Detection Tools** tab.
2. Below the required camera, click **Create... Category: Service Tampering Detection**.

By default, the detection tool is enabled and set to respond to all types of video analysis.

If necessary, you can change the detection tool parameters. The list of parameters is given in the table:

Parameter	Value	Description
Object features		
Video stream	**Main stream**	If the camera supports multistreaming, select the stream for which detection is needed. Selecting a low-quality video stream reduces the load on the Server
Other		
Enable	**Yes**	By default, the detection tool is enabled. To disable, select the **No** value
	No	
Name	**Tampering Detection**	Enter the detection tool name or leave the default name
Decode key frames	**Yes**	By default, the **Decode key frames** parameter is enabled. In this case only key frames are decoded. To disable the parameter, select the **No** value. This parameter reduces the load on the Server, but at the same time the detection quality decreases. We recommend enabling this parameter for "blind" (without video image display) Servers, on which you want to perform detection. For the MJPEG codec decoding isn't relevant, as each frame is considered a key frame. **Attention!** The **Number of frames processed per second** and **Decode key frames** parameters are interrelated. If a local Client isn't connected to the Server, the following rules work for remote Clients: • If the key frame rate is less than the value specified in the **Number of frames processed per second** field, the detection tool will work by key frames. • If the key frame rate is greater than the value specified in the **Number of frames processed per second** field, the detection will be performed according to the set period. If a local Client is connected to the Server, the detection tool will always work according to the set period. After disconnecting the local Client, the above rules will be relevant again.
	No	
Decoder mode	**Auto**	Select a processing resource for decoding video. When you select a GPU, a stand-alone graphics card takes priority (when decoding with Nvidia NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding
	CPU	
	GPU	
	HuaweiNPU	

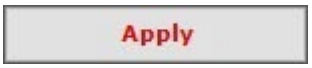
<table>
<tr><td>Number of frames processed per second</td><td>25</td><td>Specify the number of frames for the detection tool to process per second. The value must be in the range [0.016; 100]</td></tr>
<tr><td>Type</td><td>Tampering Detection</td><td>Name of the detection tool type (non-editable field)</td></tr>
<tr><td colspan="3">Advanced settings</td></tr>
<tr><td rowspan="2">Blurred image analysis</td><td>Yes</td><td rowspan="8">  Functions of the Tampering Detection

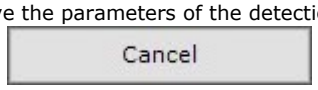
By default, all types of analysis are applied to the video image. Select the No value for unnecessary types of analysis.

 Attention!

If you select Compression artifacts analysis, Image noise analysis and Blurred image analysis, you must specify the values for the Event duration to trigger detection (sec), Sensitivity parameters.</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Compression artifacts analysis</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Image noise analysis</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Quality degradation analysis</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Scene change analysis</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td colspan="3">Basic settings</td></tr>
<tr><td>Event duration to trigger detection (sec)</td><td>20</td><td>Specify the maximum time of event duration for the response in seconds, after which the detection tool generates an event. The value must be in the range [5, 1200].

• If the algorithm definetely detects a defect in the frame, the response from the detection tool comes before the specified time.
• If after the specified time, the defect hasn't been detected, you must increase the Sensitivity of the detection tool</td></tr>
<tr><td>Sensitivity</td><td>50</td><td>Specify the sensitivity of the detection tool as a percentage. The higher the sensitivity, the smaller change in the frame is detected. The value must be in the range [0, 100]</td></tr>
</table>

To save the parameters of the detection tool, click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

Scene Analytics detection tools

Functions of Scene Analytics detection tools

The following detection tools enable analysis of the situation in a video camera's field of view.

Name of a Detection Tool object	Detection description
Motion in area	Motion in Area detection tool. **Important!** This tool is not triggered if an object enters the area (refer to **Appearance in area**).
Stop in area	Non-activity detection tool. **Important!** This tool is not triggered if an object exits the area (refer to **Disappearance in area**).
Appearance in area	Entry into Area detection tool. **Important!** This tool is not triggered if an object appears inside the area without crossing its perimeter (refer to **Motion in Area**).
Disappearance in area	Exit from Area detection tool. **Important!** This tool is not triggered if an object disappears (or becomes idle) inside the area without crossing its perimeter (refer to **Stop in Area**).
Loitering	Detection tool triggered by the lengthy presence of an object in an area of a video camera's field of view.
Abandoned object	Detection tool triggered by the appearance of an abandoned object in an area of a video camera's field of view.
Line crossing	Detection tool triggered by the trajectory of an object crossing a virtual line.
Multiple objects	Detection tool is triggered when the number of objects within the designated area exceeds a predefined value.
Move from area to area	Detection tool is triggered when an object moves from one pre-specified area to another within the scene.

Attention!

To detect any motion within an area, you need to apply two detection tools: **Motion in Area** and **Appearance in area**.

Note

Neural filter and Neural Tracker require Addon Neuro Pack to be installed (see Installing DetectorPack add-ons).

Video requirements for scene analytics detection tools

Video requirements for object tracker-based scene analytics detection tools

For video analytics to work correctly, the following requirements must be met:

1. Camera requirements:
    a. Resolution min. 640x360 pixels.

    > ⚠ **Attention!**
    >
    > Pixel resolutions over 800x600 are not recommended for this detection tool. Higher resolutions lead to increased RAM consumption and CPU load with no significant increase in tracker's performance.

    b. Frames per second: min. 6 fps.
    c. Color: video analytics work with both black-and-white and color images.
    d. Camera shaking must not cause image shifting of more than 1% of the frame size.
2. Lighting requirements:
    a. Moderate lighting. Lighting that is too little (night) or too much (bright sunlight) may impact the quality of video analytics.
    b. No major fluctuations in lighting levels.
3. Scene and camera angle requirements:
    a. Moving objects must be visually separable from each other in the video.
    b. The background must be primarily static and not undergo sudden changes.
    c. Minimal obscuration of moving objects by static objects (columns, trees, etc.).
    d. Reflective surfaces and harsh shadows from moving objects can affect the quality of analytics.
    e. Long single-color objects may not be tracked properly.
4. Object requirements:
    a. There is no noise on the video image and there are no artifacts caused by the compression algorithm.
    b. The width or height of the objects in the image must be not less than 1% of the frame size (if resolution is over 1920 pixels) or 15 pixels for lower resolution.
    c. The width or height of the objects in the image must not exceed 75% of the frame size.
    d. The speed of objects in the frame must be at least 1 pixel per second.
    e. In order to detect the object it is to be visible at not less than 8 frames.
    f. Within two adjacent frames the object cannot move in the movement direction for the distance that is longer than its size. This condition is essential for correct calculation of the object’s trajectory (track).

Video requirements for object tracker (with neural filter)-based scene analytics detection tools

For video analytics to work correctly, the following requirements must be met:

1. Camera requirements:
    a. Resolution min. 640x360 pixels.
    b. Frames per second: min. 6 fps.
    c. Color: video analytics work with both black-and-white and color images.
    d. Camera shaking must not cause image shifting of more than 1% of the frame size.
2. Lighting requirements:
    a. Moderate lighting. Lighting that is too little (night) or too much (bright sunlight) may impact the quality of video analytics.
    b. No major fluctuations in lighting levels.
3. Scene and camera angle requirements:
    a. Moving objects must be visually separable from each other in the video.
    b. The background must be primarily static and not undergo sudden changes.
    c. Minimal obscuration of moving objects by static objects (columns, trees, etc.).
    d. Reflective surfaces and harsh shadows from moving objects can affect the quality of analytics.
    e. Long single-color objects may not be tracked properly.
4. Object requirements:
    a. There is no noise on the video image and there are no artifacts caused by the compression algorithm.
    b. The width or height of the objects in the image must be not less than 1% of the frame size (if resolution is over 1920 pixels) or 15 pixels for lower resolution.
    c. The width or height of the objects in the image must not exceed 75% of the frame size.
    d. The speed of objects in the frame must be at least 1 pixel per second.
    e. In order to detect the object it is to be visible at not less than 8 frames.
    f. Within two adjacent frames the object cannot move in the movement direction for the distance that is longer than its size. This condition is essential for correct calculation of the object's trajectory (track).
5. Camera requirements for neural filter operation.

Video requirements for VMD-based scene analytics detection tools

To ensure the correct operation of scene analytics, it is necessary to meet the general requirements for video motion detection and some special requirements for VMD-based scene analytics detection tools, which are listed on the page Video stream and scene requirements for the Motion detection and its sub-tools.

Camera requirements for abandoned objects detection

Make sure the following requirements for abandoned object detection are met:

1. Camera requirements:
    a. Resolution must be not less than 640x480 pixels.
    b. Color: analytics works both with color and monochromatic images.
    c. It is not allowed to the image shift be more than 1% from the frame size due to camera shake.
2. Lighting requirements:
    a. Moderate lighting. The quality of analytics performance can be lower in case of low lighting (night) or over lighting (overexposure).
    b. There must be no dramatic changes in lighting.
3. Scene and camera angle requirements:
    a. Background is mostly static and is not changed.
    b. Incorrect analytics performance can be caused by reflective surfaces.
    c. Abandoned objects are hidden by moving objects not longer than 10% of the time.
4. Object images requirements:
    a. An abandoned object must be visible on the image.
    b. The digital noise and compression-related artifacts are minimal.
    c. The width and height of the objects in the image must be not less than 1% of the frame size (if resolution is over 1920 pixels) or 15 pixels for lower resolution.
    d. The width and height of the objects in the image must not exceed 25% of the frame size.

If these conditions are in place, the abandoned object detection tool is guaranteed to:

- detect 92 items out of 100;
- keep false positives to 20 out of 100.

Camera requirements for neural filter operation

To operate the neural filter, a camera must match the following requirements:

1. Use color cameras. Monochrome image may noticeably decrease the detection quality.
2. Video resolution is no less than 640x360.
3. Frame rate is no less than 6 fps.
4. An object must occupy no less than 5% of the FoV width/height.
5. Objects must be visually separated from the background as well as from each other.

> ⚠ **Attention!**
>
> We cannot guarantee normal operation of the neural filter with a fisheye camera.

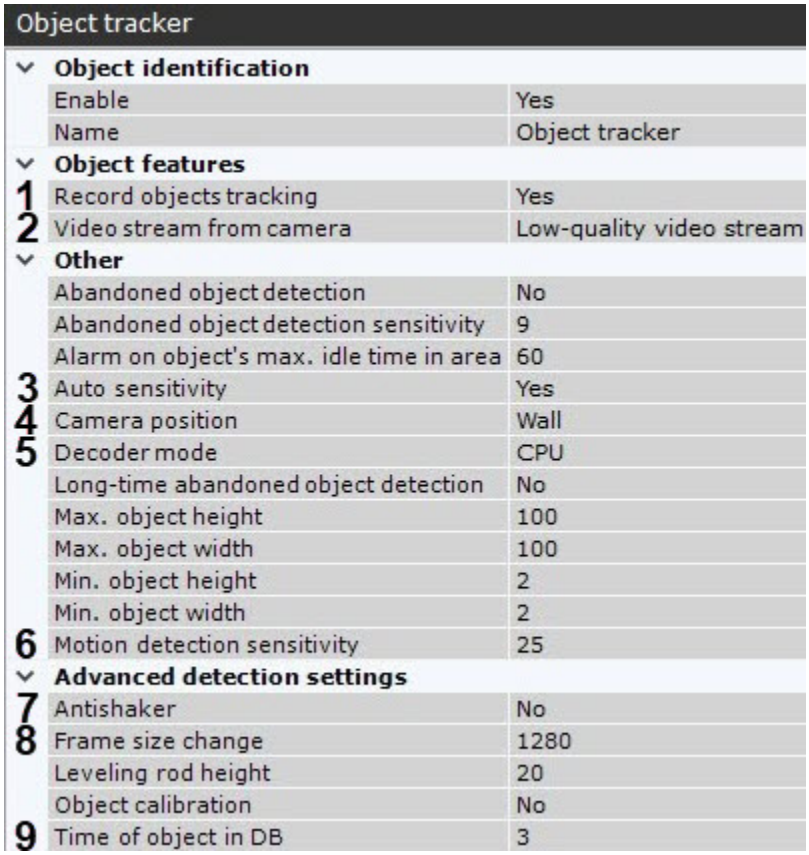
Configuring Scene Analytics Detection Tools

Setting up Tracker-based Scene Analytics detection tools

Setting general parameters of Tracker-based Scene Analytics detection tools

Some parameters can be configured for Scene Analytics detection tools simultaneously. To configure them, do as follows:

1. Select the **Object tracker** object.



Object tracker	
Object identification	
Enable	Yes
Name	Object tracker
Object features	
1 Record objects tracking	Yes
2 Video stream from camera	Low-quality video stream
Other	
Abandoned object detection	No
Abandoned object detection sensitivity	9
Alarm on object's max. idle time in area	60
3 Auto sensitivity	Yes
4 Camera position	Wall
5 Decoder mode	CPU
Long-time abandoned object detection	No
Max. object height	100
Max. object width	100
Min. object height	2
Min. object width	2
6 Motion detection sensitivity	25
Advanced detection settings	
7 Antishaker	No
8 Frame size change	1280
Leveling rod height	20
Object calibration	No
9 Time of object in DB	3

2. By default, video stream metadata are recorded to the database. You can disable the recording by selecting **No** in the **Record objects tracking** list (**1**).

> **Attention!**
>
> Video decompression and analysis are used to obtain metadata, which causes high Server load and limits the number of video cameras that can be used on it.

3. If the video camera supports multistreaming, select the stream for which detection is needed (**2**). Selecting a low-quality video stream allows reducing the load on the Server.

> **Attention!**
>
> To display the object tracks properly, make sure that all video streams from multistreaming camera have the same aspect ratio settings.

4. If you need to automatically adjust the sensitivity of the scene analytics detection tools, select **Yes** in the **Auto sensitivity** list (**3**).

> **Note**
>
> It is recommended to enable this option if the lighting fluctuates significantly in the course of the video camera operation (for example, in outdoor conditions).

5. To reduce the number of false positives from a fish-eye camera, you have to position it properly (**4**). For other devices, this parameter is not valid.

6. Select a processing resource for decoding video streams (**5**). When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding.
7. In the **Motion detection sensitivity** field (**6**), set the sensitivity of the scene analytics detection tools to motion in the range [1, 100].
8. To smooth camera shake, set **Yes** for the **Antishaker** parameter (**7**). This parameter is recommended to use only when the camera shake is evident.
9. Analyzed framed are scaled down to a specified resolution (**8**, 1280 pixels on the longer side). This is how it works:

    a. If the longer side of the source image exceeds the value specified in the **Frame size change** field, it is divided by two.
    b. If the resulting resolution falls below the specified value, it is used further.
    c. If the resulting resolution still exceeds the specified limit, it is divided by two, etc.

    > **Note**
    >
    > For example, the source image resolution is 2048*1536, and the specified value is set to **1000**.
    >
    > In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the limit (1024 > 1000).

    > **Note**
    >
    > If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.

10. Enter the time interval in seconds, during which object properties will be stored in the **Time of object in DB** field (**9**). If the object leaves and enters the FOV within the specified time, it will be identified as one and the same object (same ID).
11. If necessary, configure the neural network filter (see Hardware requirements for neural analytics operation). The neural network filter processes the results of the tracker and filters out false positives on complex video images (foliage, glare, etc.).

    > **Attention!**
    >
    > A neural network filter can be used either for analyzing moving objects, or for analyzing abandoned objects only. You cannot operate two neural networks simultaneously.

    a. Enable the filter by selecting **Yes** (**1**).

	Neural network filter	
2	Abandoned object filter file	
	Abandoned object filter mode	Nvidia GPU 0
1	Enable filter	**Yes**
3	Moving object filter file	**D:/human_car.ann**
	Moving object filter mode	Nvidia GPU 0

    b. Select the processor for the neural network—CPU, one of NVIDIA GPUs, or one of Intel GPUs (**2**, see Hardware requirements for neural analytics operation, Selecting Nvidia GPU when configuring detection tools).

    > **Attention!**
    >
    > - If you specify other processing resource than the CPU, this device will carry the most of computing load. However, the CPU will also be used to run the detection tool.
    > - It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU).
    > - Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

    > Camera requirements for neural filter operation

    c. Select a neural network (**3**). To access a neural network, contact AxxonSoft technical support. If no neural network file is specified, or the settings are incorrect, the filter will not operate.
12. Click the **Apply** button.

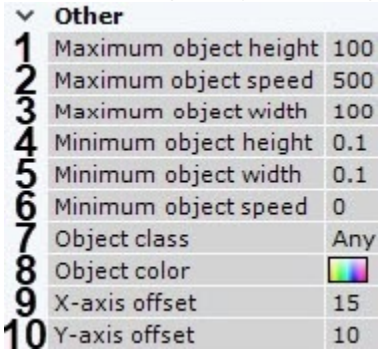
The general parameters of the Scene Analytics detection tools are now set.

Configuring detected objects

You can set a number of parameters that describe the objects that should cause a trigger for each Scene analytics detection tool.

To configure the settings of the detected objects, do the following:

1. Select the corresponding Scene analytics detection tool.

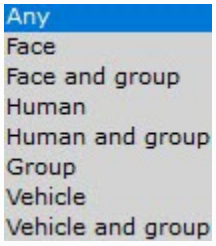


2. Set the maximum and minimum height of the object that should cause a trigger as a percentage of the frame size (**1**, **4**). The values should be in the range [0,05; 100].
3. Set the maximum and minimum speed per second of the object that should cause a trigger as a percentage of the frame size (**2**, **6**). The values should be in the range [0; 500].

> **Note**
>
> In *Axxon One* speed is a conditional value. It is calculated using the values of different dimensions. The speed calculation algorithm takes into account both the frame width and the frame height.
>
> For visual understanding of the speed values, it is recommended to go to the speed configuration when searching in the archive (see Configuring minimum and maximum object speed).

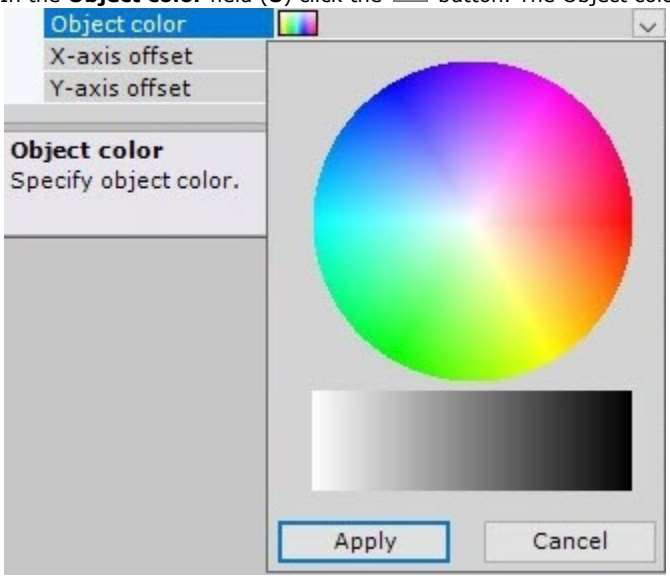
> **Note**
>
> These parameters are not set for the Abandoned object detection tool.

4. Set the maximum and minimum width of the object that should cause a trigger as a percentage of the frame size (**3**, **5**). The values should be in the range [0,05; 100].
5. Select the class of the object that should cause a trigger (**7**).

> **Note**
>
> A **Group** is a group of two or more people moving beside each other for some time. If you select this class of object, the detection tool will not trigger, if it detects the movement of one person. If you select the **Human** class, the detection tool will not trigger, if it detects the movement of several people beside each other.
>
> 
>

6. Set a color (or color range) of the object that should cause a trigger:

a. In the **Object color** field (**8**) click the button. The Object color dialog box opens.



b. Set the color range of the object with drag-and-drop on the RGB or black-and-white color palette.



> **Note**
>
> Any click on the palette is interpreted as the beginning of a new range. The previous range will disappear.
>
> To cancel a selected color, click on any palette, save the changes, and click the **Apply** button.

> **Attention!**
>
> *Axxon One* logic treats all objects as monochrome. The object color in *Axxon One* is an average of all object colors on the video image.
>
> All objects of the specified colors will be detected. If no object color is set, the detection tool will trigger to objects of any color.

7. Set the X-axis offset and Y-axis offset as a percentage of the track area to specify the detection tool triggering area (**9**, **10**). The values should be in the range [1; 50].
8. Click the **Apply** button.

Configuring the detected objects is complete.

Setting up VMD-based Scene Analytics detection tools

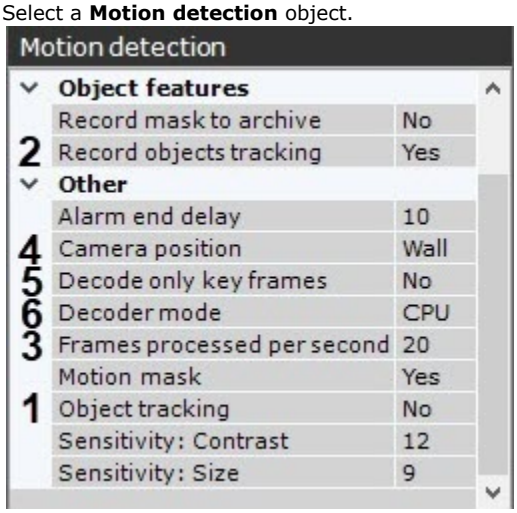
Video requirements for scene analytics detection tools

Attention!

- If you plan to use the metadata from the VMD for MomentQuest (see Forensic Search for Fragments (MomentQuest)), you may need to update the license file. Contact an AxxonSoft manager for detailed information and license file.
- The Abandoned object detection works only with the basic Object tracker (see Abandoned Object detection).
- It is not possible to determine the object type and color based on metadata from VMD.

To configure Scene Analytics detection tools based on VMD, do the following:

1. Select a **Motion detection** object.



2. Select **Yes** in the **Object tracking** field (**1**).
3. By default, metadata are not recorded into the database. To enable metadata recording, select **Yes** from the **Record objects tracking** list (**2**).
4. For a proper operation of VMD-based Scene Analytics detection tool, it must analyze a frame at least every 500 milliseconds (see Configuring the Motion detection for the **Frames processed per second** and **Decode only key frames** parameters description).
5. Select a processing resource for decoding video streams (**6**). When you select an NVIDIA GPU, priority is given to a discrete graphics card (when decoding on NVIDIA NVDEC chips). If there's no appropriate GPU, then decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding.
6. To reduce false alarms rate from a fisheye camera, you must position it properly (**4**). For other devices, this parameter is not valid.
7. Click the **Apply** button.
8. Next, you must create and configure the necessary VMD-based detection tools. The configuration procedure is the same as for the basic tracker (see Setting up Tracker-based Scene Analytics detection tools).

Category: Embedded

General information about embedded detection tools

Axxon One integrates embedded analytics for multiple cameras. You can find analytics in the list of supported devices in the **Analytics** column.

Camera embedded analytics is the ability to process a video stream directly on the camera to identify specific events or objects. For example, this can include face recognition, motion detection, person or vehicle counting, detection of an entrance or exit area, and so on.

If *Axxon One* supports the device embedded analytics, you can create detection tools from that camera (see Configuring detection tools and their sub-tools).

Note

- Some devices have interdependent embedded analytics that cannot work together with other detection tools. For example, if **Embedded Face Detection** is created for a camera in the *Axxon One* configuration, you can create the **Face Detection VL** for the same camera, but it won't work.
- Some camera manufacturers restrict the use of multiple embedded detection tools at the same time. If such a restriction exists, it won't be displayed in *Axxon One*. You can create multiple embedded detection tools for one camera, but the functionality of these detection tools can be limited by the manufacturer.

If the camera supports Motion Mask, it is displayed in the preview window when you configure the embedded detection tool. If there is motion, but it doesn't exceed the threshold value (because of the sensitivity parameters of the detection tool), the mask cells are colored green. If there is motion and it generates an event, the cells are colored red.



AxxonSoft Tracker in Axis devices

Attention!

Tracker isn't supported since DriverPack 3.76 (see Documentation Drivers Pack).

You can use analytics from AxxonSoft (Configuring Scene Analytics Detection Tools) on Axis devices.

Note

This option is available for all Axis devices on the following hardware platforms:

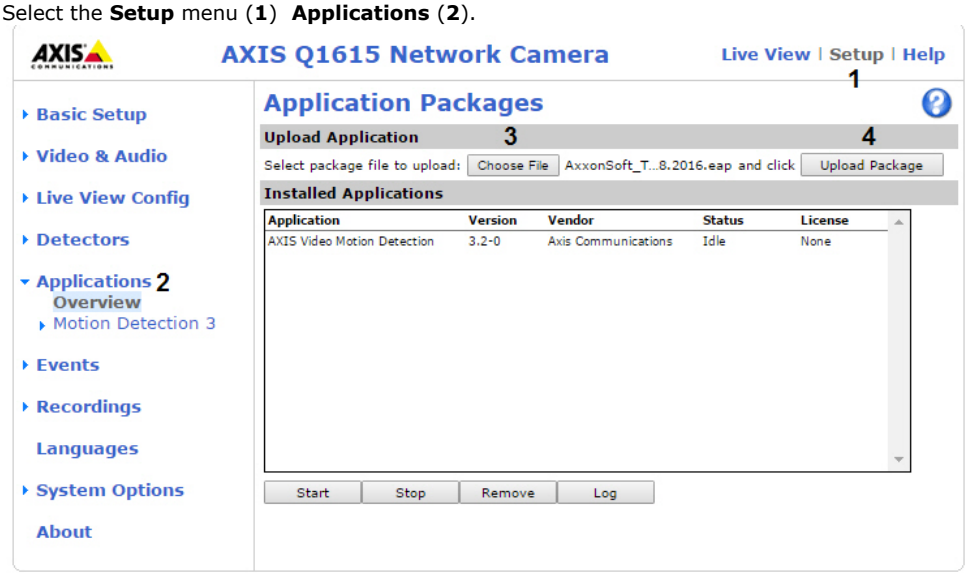
- MIPS (ARTPEC-4 and ARTPEC-5 CPUs),
- ARMv7 (ARTPEC-6 and ARTPEC-7 CPUs).

For full list of setup parameters, refer to the AxxonSoft Tracker help.

All CPU heavy analytics and metadata generation tasks are delegated to the camera in this case.

To do this:

1. Go to the device's web interface.
2. Select the **Setup** menu (**1**) **Applications** (**2**).

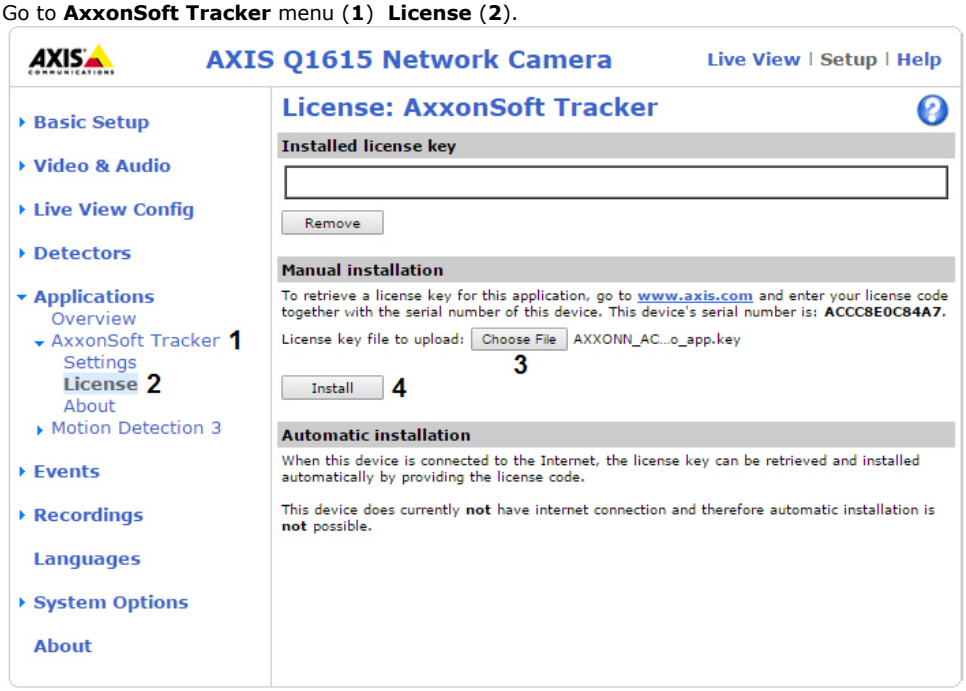


3. Select the ACAP application (**3**) and click the **Upload Package** button (**4**).

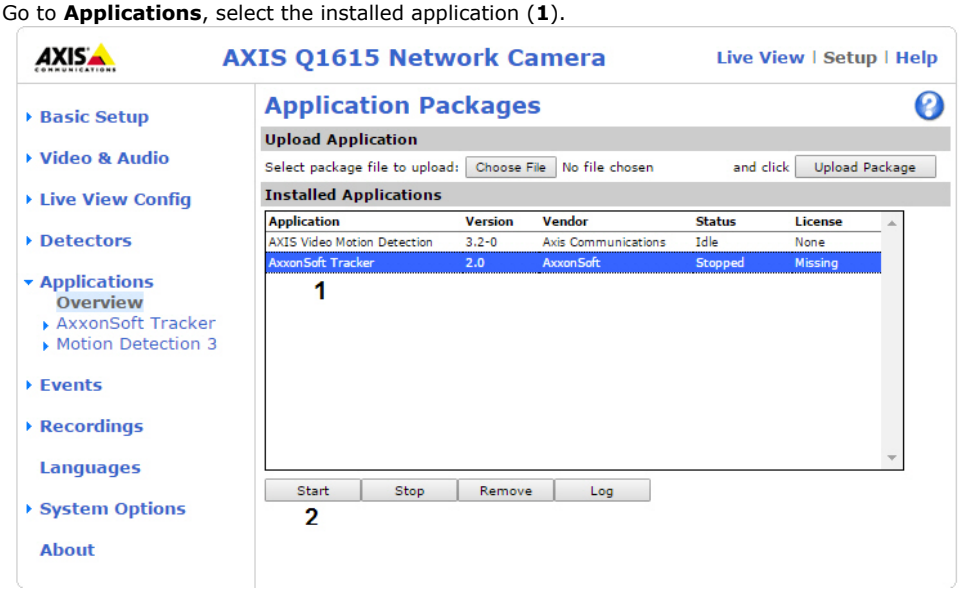
Attention!

For application, contact AxxonSoft help-desk. You will be given a license code that you must register along with camera's MAC address on Axis website in order to get the license file.

4. Go to **AxxonSoft Tracker** menu (**1**) **License** (**2**).

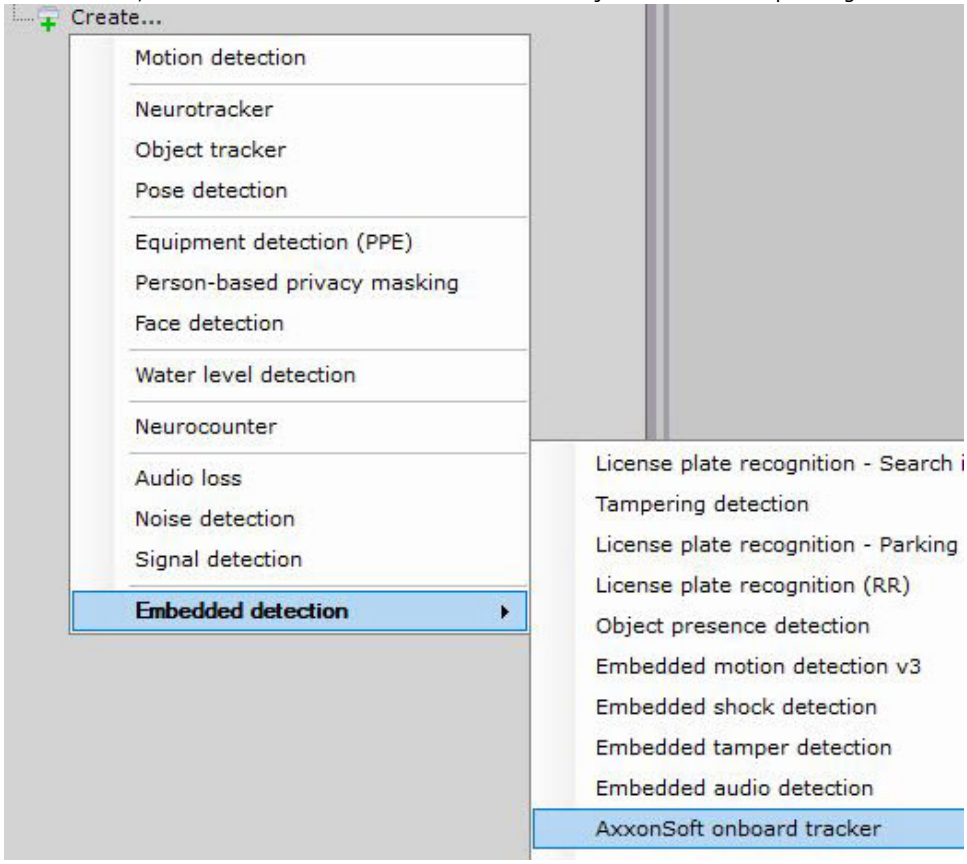


5. Select the license file (**3**).
6. Click the **Install** button (**4**).
7. Go to **Applications**, select the installed application (**1**).



8. Click the **Start** button (**2**).

9. In *Axxon One*, create the **AxxonSoft onboard tracker** object for the corresponding camera.



10. Configure the tracker and create the required detection tools.

> **Note**
>
> You can configure the **AxxonSoft onboard tracker** object similar to General information on the standard detection sub-tools.
>
> You cannot configure perspective for solution based on Axis devices.

Face Detection and Temperature Control with Mobotix M16 TR cameras

Functional parameters of the Face Detection and Temperature Control

When working with Mobotix M16 TR cameras, the standard face detection algorithm (see Functions of the Face Detection VA) is used along with an additional option of temperature measurement.

For each recognized face, the following is performed:

1. Temperature measurement.
2. Display the measurement result next to the face bounding box.
3. Recording the temperature value into the system log along with the face recognition event (see The System Log).

You can as well set the system to launch a macro if temperature readings exceed the maximum permitted value (see Specific parameters for triggering a face recognition macro).

Camera requirements for face detection and temperature control

Face detection with temperature control works properly if cameras are installed and set up as follows:

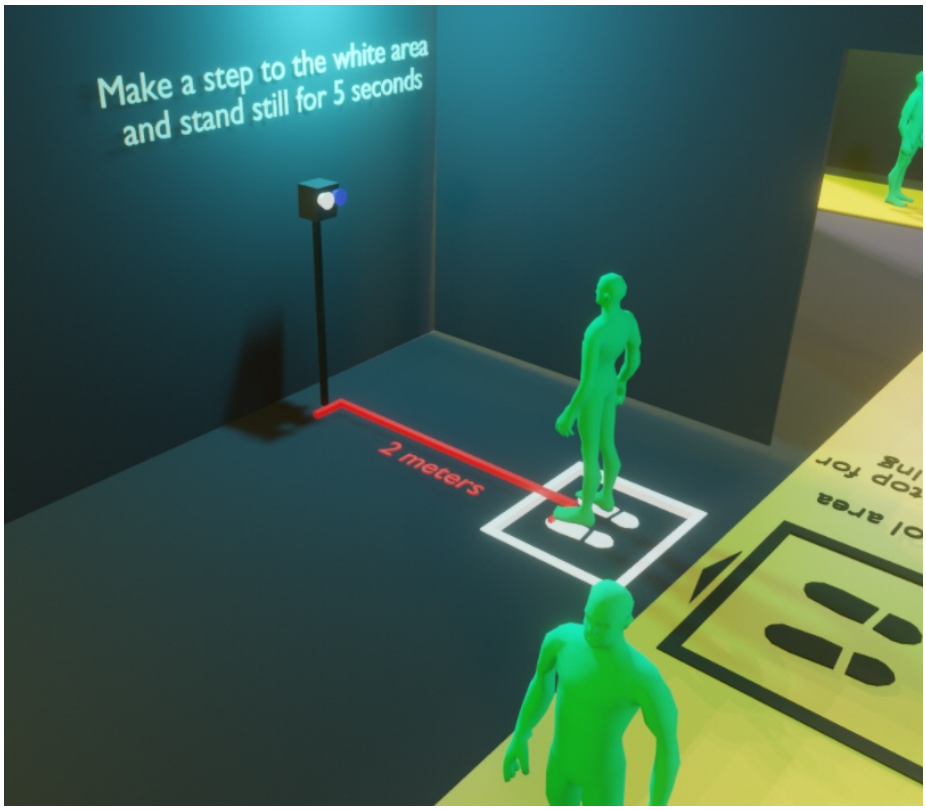
1. At least 8 frames per second.
2. Minimum resolution is at least 1280 x 960 pixels.
3. Indoor installation only.
4. To establish maximum measurement accuracy, avoid installing cameras near exits to street, in direct sunlight, and close to HVAC outlets.
5. Keep the distance from camera to the subject of measurement within the range of 1-2 meters.
6. For best accuracy, install the Electromagnetic Radiation Absorber (BB) at the same distance from camera as the subjects of measurement.
7. The maximum angle of incidence should not exceed +/- 15° off the ground level.
8. Distance between pupils on the received photos of face must be not less than 32 pixels.
9. There should be minimum mutual overshadowing of the captured faces.
10. The faces should be evenly illuminated with a diffused light of at least 200 lux. Directional side lighting is not allowed.
11. The sharpness of the captured faces on the received photos must be over 64 grayscale. Deficient or exceeding illumination is not allowed.
12. There should be no back light and sharp gradients of light and shade.
13. The photos of the captured faces received from video cameras should be clear. Image blurring caused by motion is not allowed.

> **Note**
>
> The required distance between the camera and the face can be set using a lens with required focal length.

Temperature screening protocol

For maximum measurement accuracy, please make sure that:

1. Subjects of measurement must have their body temperature normalized. To do this, please avoid their exposure to direct sunlight, incoming air flow from street or HVAC, and exclude any other factors that may cause momentary changes in body temperature.
2. The measurement area may contain only one individual.
3. No headgear, medical mask or glasses may be worn in the area.
4. The subject should dwell in the control area no less than 3 seconds, standing/sitting still, facing the camera.



Pre-configuration of the Mobotix M16 TR camera

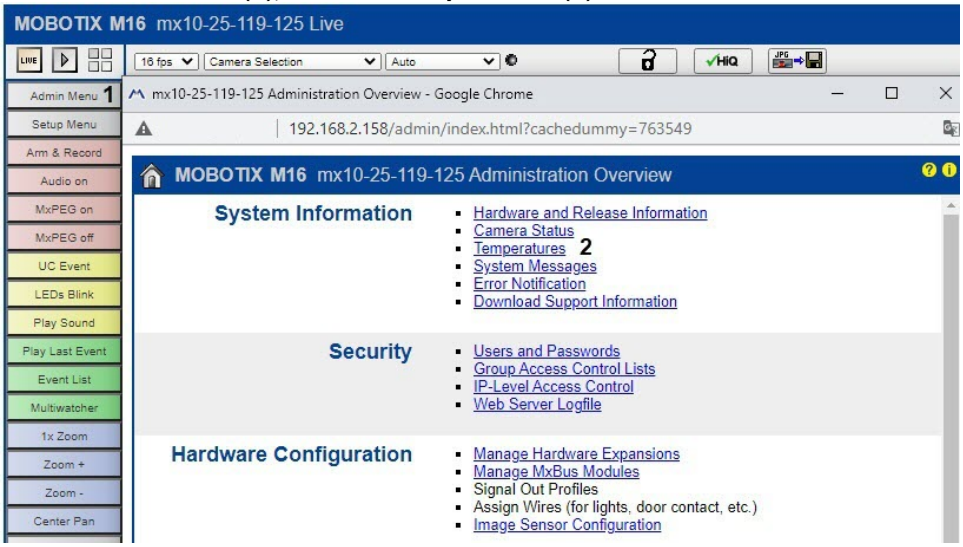
Attention!

Install MX-V5.2.6.7 (2020-06-16) or later firmware.

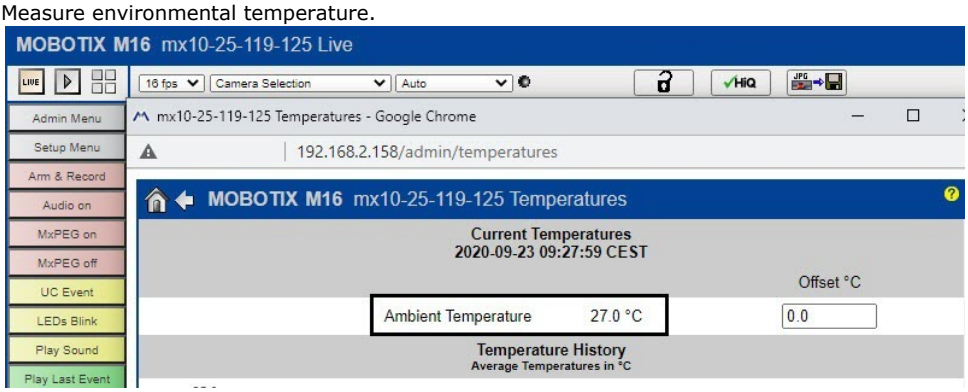
For detailed configuration via the web interface, refer to manufacturer's instructions.

Before starting *Axxon One*, please configure the camera via the web interface:

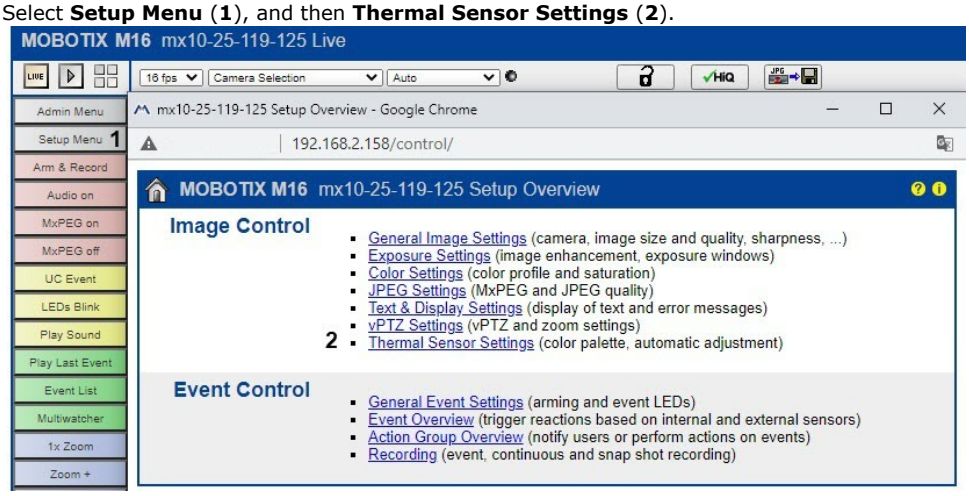
1. Proceed to admin menu (**1**), and select **Temperatures** (**2**).



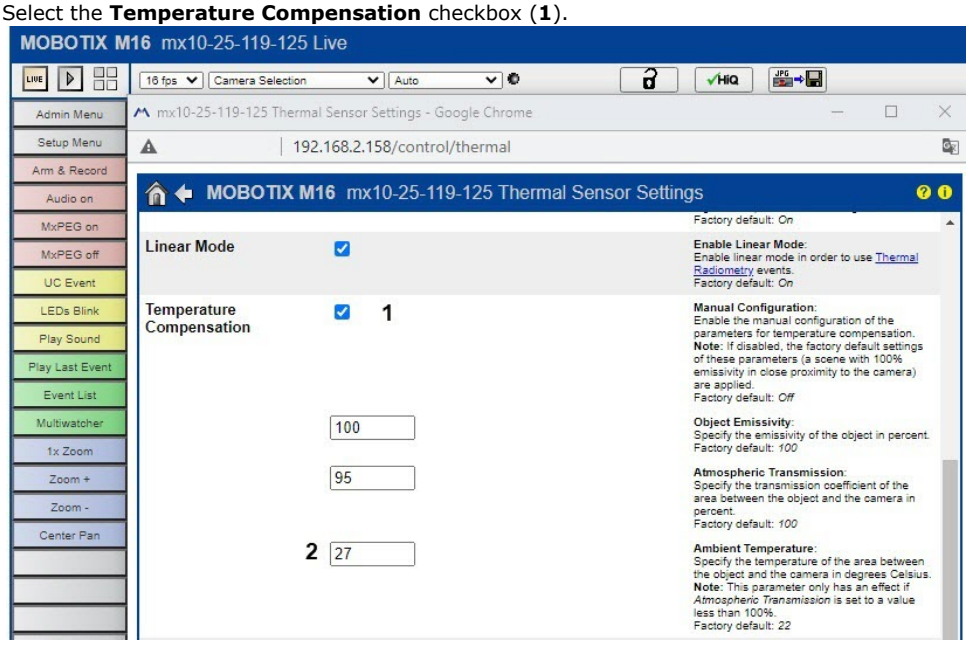
2. Measure environmental temperature.



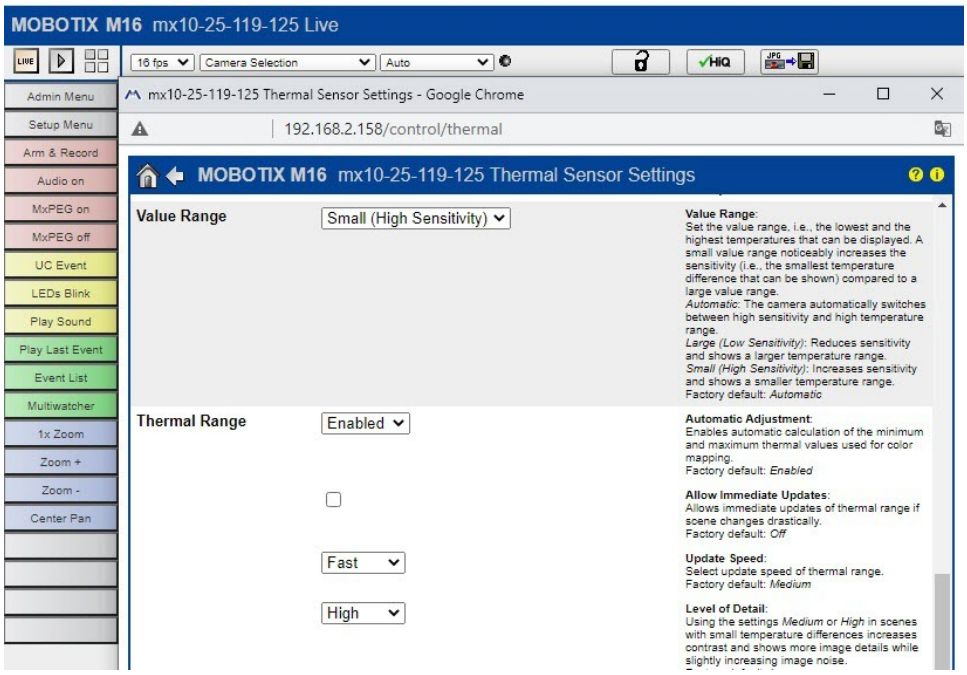
3. Select **Setup Menu** (**1**), and then **Thermal Sensor Settings** (**2**).



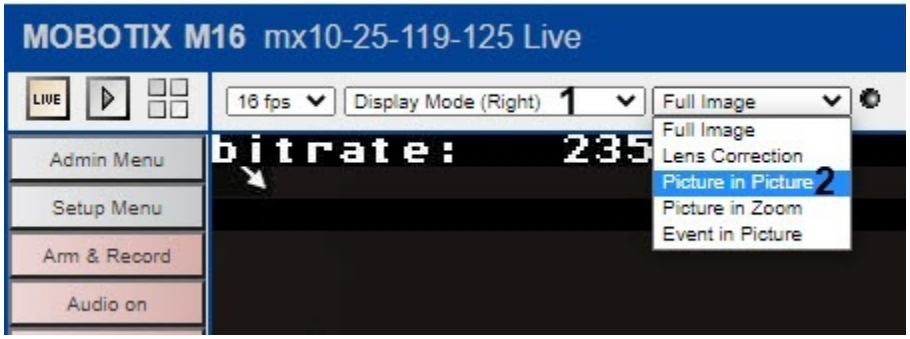
4. Select the **Temperature Compensation** checkbox (**1**).



5. Enter the environmental temperature value (**2**, see point 2).
6. Specify the **Value Range** and **Thermal Range** parameters as shown on the screenshot.



7. To caption video with temperature readings, select **Display Mode (Right)** (**1**), and then **Picture in Picture** (**2**) checkboxes.



8. Save the settings.

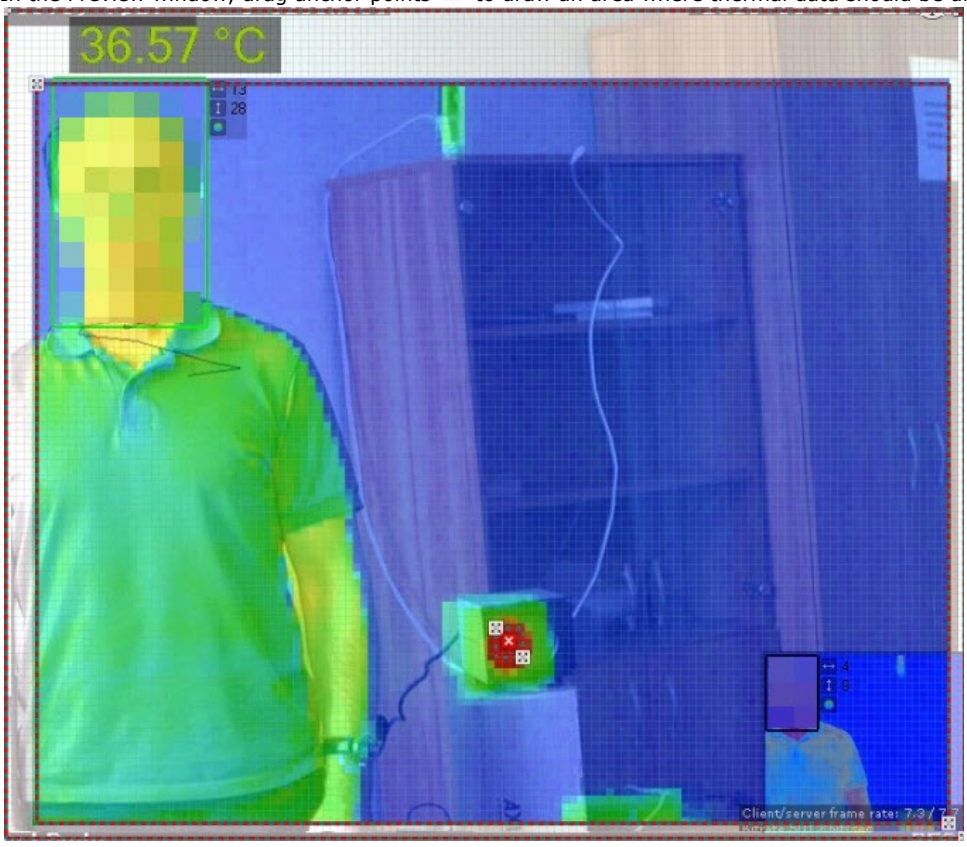
Configuring Face Detection and Temperature Control

To configure face detection and temperature control, do the following:

1. Add a **Temperature Matrix Data** object in the **Embedded Detection** group**.**
2. Under the newly added object, create a **Face Detection and Temperature Control**.
3. Select temperature unit (**1**).

	Face detection and temperature control	
	Frame size change	1920
	Maximum face height	100
	Maximum face width	100
	Minimum face height	2
	Minimum face width	2
	Minimum threshold of face authenticity	90
	Mode	CPU
	Period of face search	250
	Send face images	No
2	Show thermal overlay	No
1	Temperature unit	Degree Celsius (°C)
	Track loss time	500

4. To caption video with thermal data, do the following:
   a. Select **Yes** for the **Show thermal overlay** parameter (**2**).
   b. In the Preview window, drag anchor points to draw an area where thermal data should be displayed.



5. If you use an Electromagnetic radiation absorber (BB), do the following:

a. Specify its temperature (**3**). If temperature readings in this point are different, the bias will be used to re-calculate readings across all measurement points.

	Advanced detection settings	
3	Electromagnetic radiation absorber (BB) temperature	37.5
	Face detection algorithm	ALG1
	Maximum face deflection rate	15
	Minimum face recognition quality	50
	Minimum filtering threshold	50
4	Temperature value offset	0

b. In the Preview window, double click to add anchor points at the position of the electromagnetic radiation absorber (BB).



6. If you have discovered that your readings differ from actual temperature values, add the offset value into the **Temperature value offset** field (**4**). Bias values may be positive or negative.

> **Note**
>
> The rest of this detection tool parameters are identical to those of the basic face detection tool (see Configuring the Face Detection TV).

7. Click the **Apply** button.

You have configured detection tool now.

Embedded vehicle speed measurement radar

On this page:

- General information
- Configuring the Embedded vehicle speed measurement radar detection tool
- Search the archive by vehicle speed

General information

Some video cameras feature built-in analytics for license plate recognition and vehicle speed detection. IP devices that support this analytics are listed in the list of supported IP devices in the **Analytics** column.

Embedded vehicle speed measurement radar is a built-in detection tool which is used to determine the vehicle speed. Based on events received from the embedded radar, you can configure macro commands in *Axxon One* and search the archive by vehicle speed.

Configuring the Embedded vehicle speed measurement radar detection tool

In general, the **Embedded vehicle speed measurement radar** is configured as follows (as an example, the GIT-CNW25060/BUR(L) video camera is used):

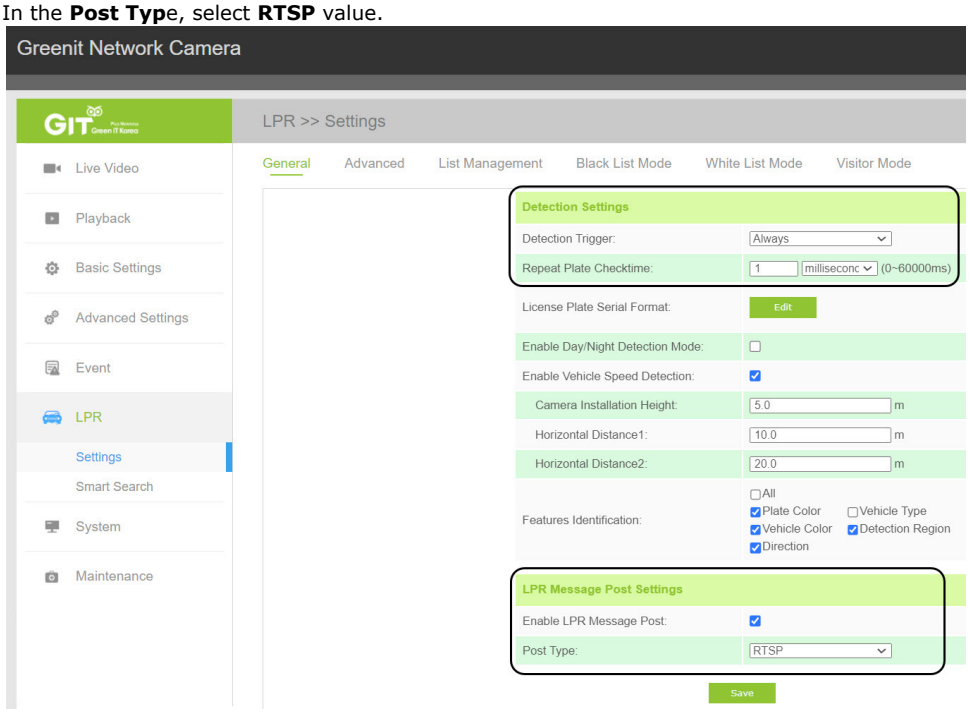
1. Configure the detection tool in the web interface of the IP device.

   ⚠ **Attention!**

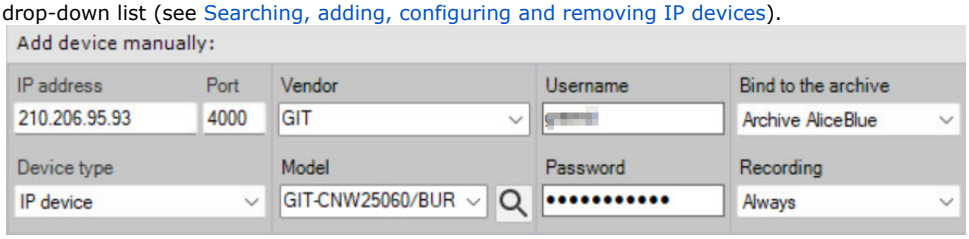
   - Settings for embedded detection tools are described in the official documentation of the corresponding IP devices.
   - To receive alarms from the embedded detection tool in *Axxon One*, set up a schedule in the web interface of the IP device:
     a. Go to the **Configuration** **LPR** **Settings** **General** tab.
     b. In the **Schedule settings** section, select the operation time of the embedded detection tool.

   a. In the **Detection Settings** group:
      i. In the **Detection Trigger** field, select **Always**.
      ii. In the **Repeat Plate Checktime** field, specify the value **1 millisecond**.
   b. In the **LPR Message Post Settings** group:
      i. Set the **Enable LPR Message Post** checkbox.

ii. In the **Post Type**, select **RTSP** value.

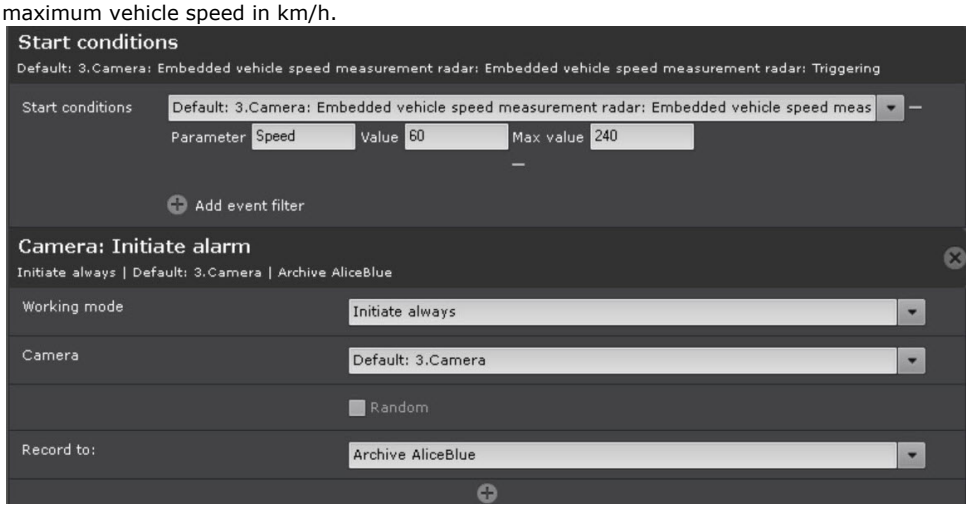


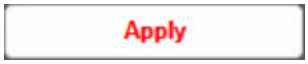
2. To save the changes, click the **Save** button.
3. Add this IP device to *Axxon One* by setting up permanent recording to the archive and selecting **Always** from the **Recording** drop-down list (see Searching, adding, configuring and removing IP devices).



4. On the **Detection Tools** tab, below the required IP device, click **Create... Category: Embedded Embedded vehicle speed measurement radar**.
5. Configure a macro command when the **Embedded vehicle speed measurement radar** detection tool is triggered (see Create Macros). If necessary, you can configure a macro to trigger an alarm when the vehicle speed is exceeded (see Initiating an alarm in the system). To do this:

   a. Click the  button under the condition for macro.
   b. In the **Parameter** field, specify the **Speed** value; in the **Value** and **Max value** fields, specify the minimum and maximum vehicle speed in km/h.

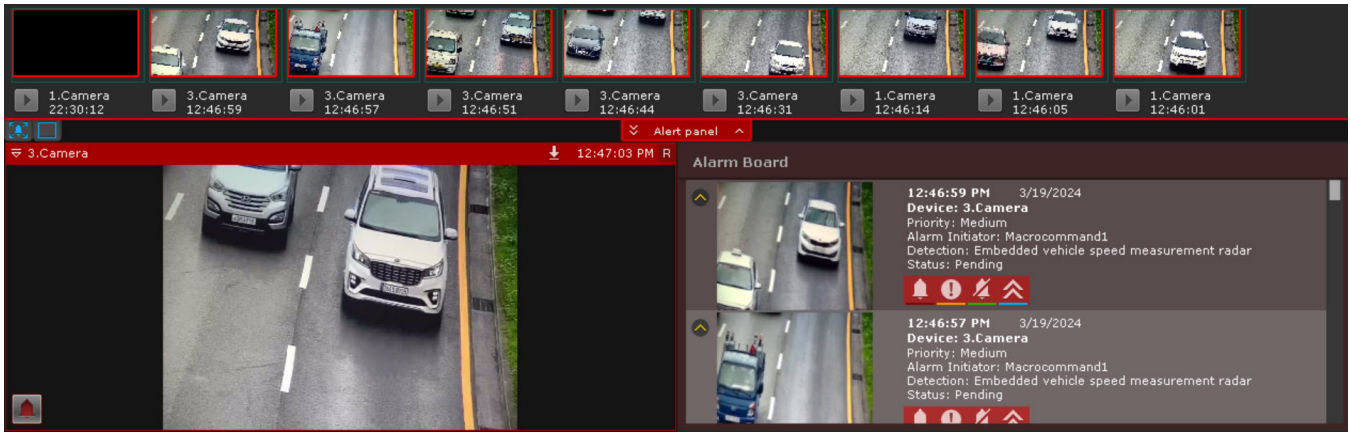


6. Click on the **Apply** button 

.

The **Embedded vehicle speed measurement radar** detection tool is configured.

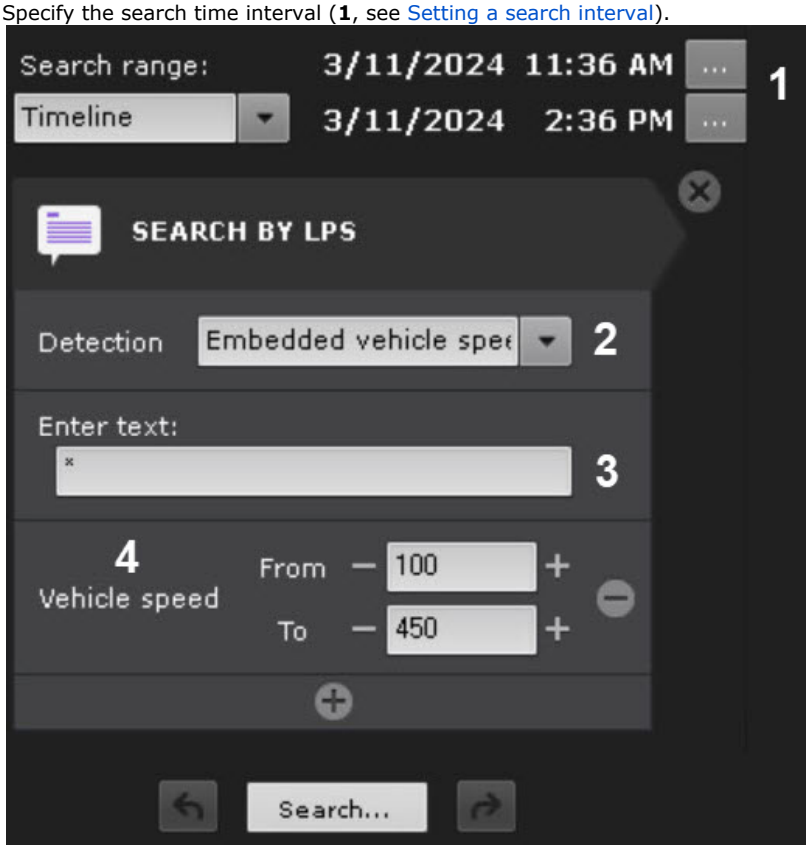
When the vehicles moving at speed that exceeds the values specified in the macro command are detected, an alarm will be triggered and displayed on the alarm panel (see Alert panel, Working with an Alarm Board).



Search the archive by vehicle speed

You can search in the archive for events from the **Embedded vehicle speed measurement radar** detection tool based on vehicle speed. To do this:

1. Switch to the archive search mode of the video camera on the basis of which the **Embedded vehicle speed measurement radar** was created (see Switching to Archive Search mode).
2. Specify the search time interval (**1**, see Setting a search interval).



3. From the list of search types, select **Search by LPs** (see Search by LPs).
4. From the list of detection tools, select **Embedded vehicle speed measurement radar** (**2**), the alarms from which should be used as a search source.
5. Specify the license plate number of the vehicle to search in the archive (**3**).

> **Note**
>
> To search by all recognized license plates, enter * (asterisk).

6. Add an additional **Vehicle speed** criterion (**4**): in the **From** and **To** fields, specify the vehicle speed range in km/h. The search results will only display events where the vehicle speed matches or is within the specified range.
7. Click the **Search** button.

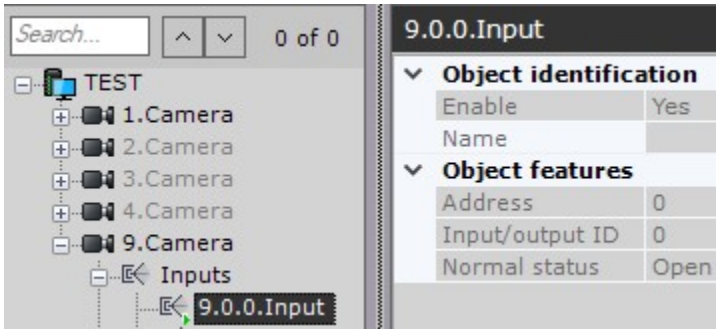
This starts a search based on the selected criteria.

The search results panel displays frames with vehicles whose license plates contain the text from the search query and also meet the specified additional parameters.

Configuring Inputs

After becoming enabled on the **Devices** tab, the **Input** object appears on the **Detection Tools** tab (see the section The Input Object**).**

Check the functioning of the Input in the **Devices** tab (see the section The Input Object). The **detection properties** field in the **Detec tion Tools tab** duplicates the settings entered in the **Devices** tab under **Settings** and is not editable.



Perform the follow actions for the **Input detection tool**, on the **Detection Tools tab**:

1. Check triggering of the detection tool with the help of the Triggers ribbon (optional) (see the section Checking the triggering of a detection tool).
2. Set the rules to be automatically executed when the detection tool is triggered (see the section titled Automatic Rules).

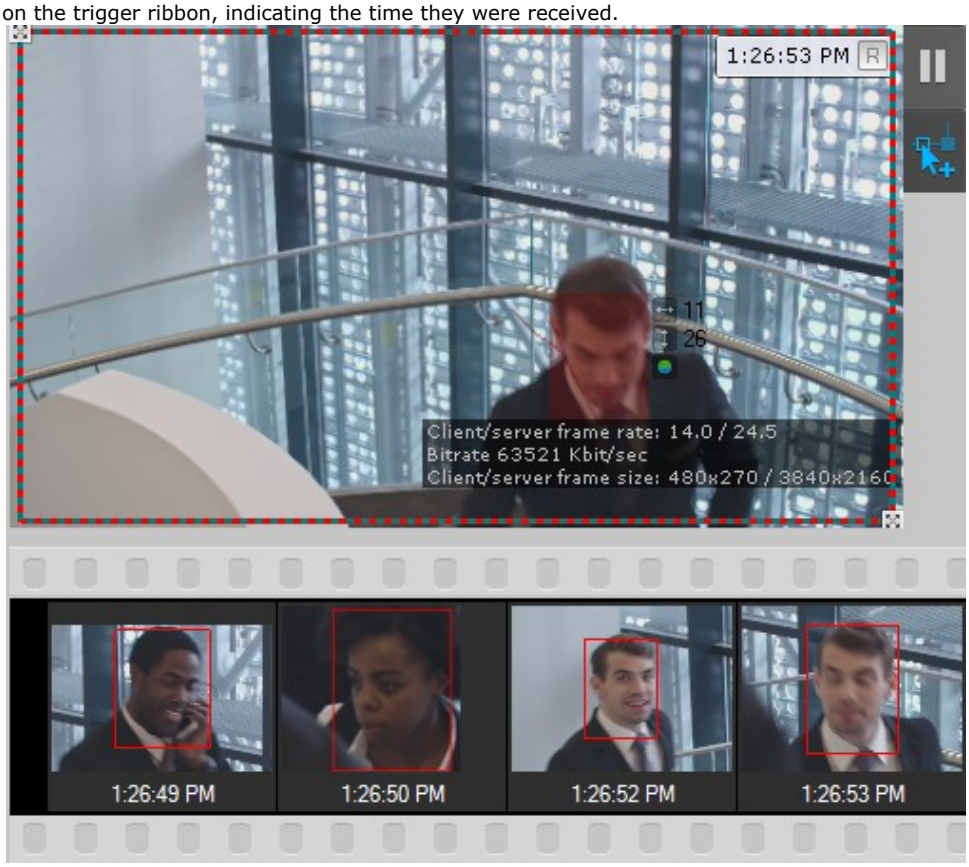
Checking the triggering of a detection tool

On the **Detection Tools** tab, you can check whether the detection tools are being triggered. To do this:

1. In the list of detection tools, select the one that you want to check.

   > **Attention!**
   >
   > The detection tool should be enabled and configured.

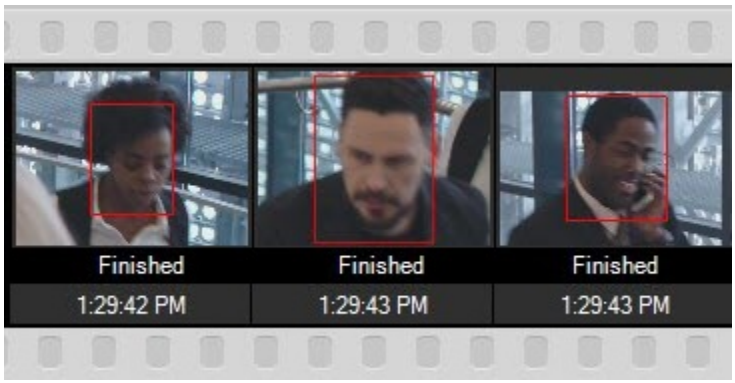
2. Reproduce an event upon the occurrence of which the detection tool should be triggered: the start of movement in the frame, turning the video camera, sending sound to an audio device, etc.
3. If the detection tool is configured correctly, video frames from the camera corresponding to the detection tool will be displayed on the trigger ribbon, indicating the time they were received.



> **Note**
>
> If the archive recording is not configured for the camera corresponding to the detection tool (see Configuring recording to an archive), then the trigger ribbon will not contain video frames, because they are taken from archive recordings.

VMS checks the on/off status of detection tools when they triggered and stopped. Not applicable to detection of: quality loss, position change, disappearance of an object, motion stop and ANPR.

After the end of triggering, the **Finished** message is displayed.

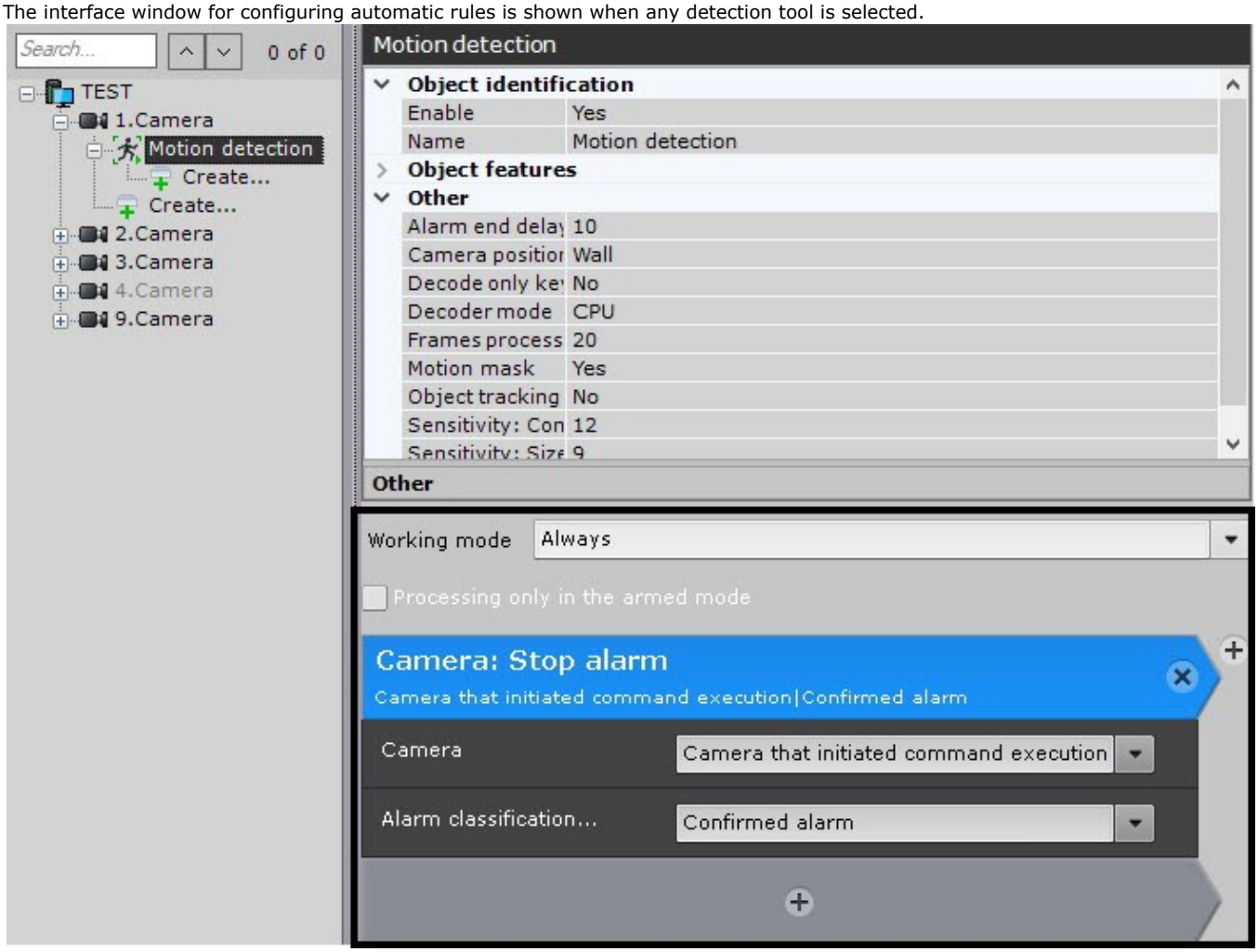


Checking the triggering of a detection tool is now complete.

Automatic Rules

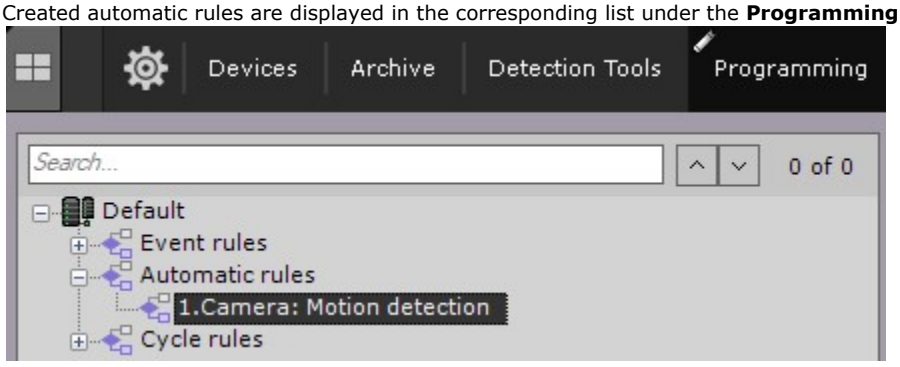
Automatic rules are basic macros: particular actions that are performed when a detection tool is triggered (see Configuring macros). One or multiple automatic rules can be set for each detection tool.

The interface window for configuring automatic rules is shown when any detection tool is selected.



Configuring automatic rules and their mode of operation is the same as configuring macros (see Configuring macros).

Created automatic rules are displayed in the corresponding list under the **Programming** tab.



Note

When you create the Record to archive automatic rule, the recording stops when VMD (see Configuring Scene Analytics Detection Tools) triggering stops.

Configuring macros

General information about the macros

Macro is a tool used to configure system responses to certain events. System response may include one or several different actions.

You can configure *Axxon One* to perform certain actions if any events occur in the system. For example, when a fire is detected—to activate voice notification, when the camera is disarmed—to send an email notification and initiate an alarm, etc. To perform such actions, you need macros.

> **Attention!**
>
> Macros work within a single Axxon-domain only. Macro conditions and actions cannot include objects from another Axxon-domain.

Types of macros



There are three types of macros:

1. Event-driven (**1**). These macros can run automatically on detecting the specified events or initiated manually by the operator. When triggered, the actions in the macro are executed once.
2. Automatic Rules (**2**). These macros run every time when the detection tool triggers.
3. Cycle (**3**). These macros can run automatically after a set period of time, or at a random time within a set interval. Cycle macros are run on the first Server in the Axxon-domain (alphabetical order) available at the time of launching the macro. Cycle macros are executed immediately after you save them in the system, unless they have been created outside the time schedule (see Create Macros). After completing all actions, the macro is automatically restarted. Additionally, a cycle macro can be launched at a specified time interval, or at a random moment within the specified time interval. In this case, all actions in the macro will be executed once.

   > **Attention!**
   >
   > If, during the response of a cycle macro to a certain event, another event that should also be processed by this macro occurs, it will be skipped.
   >
   > If another event occurs during an event-driven macro response, this event will be processed according to the specified parameters.

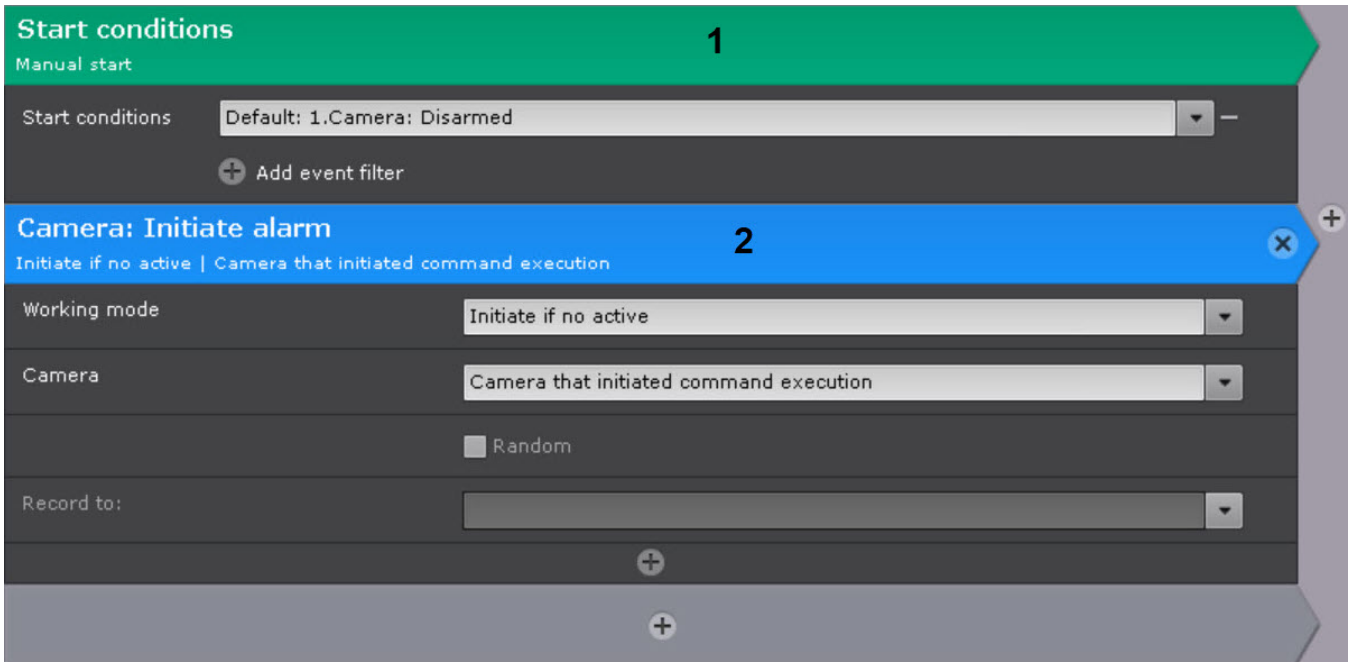
Unless the macro has standby commands (see Wait for event, Wait for timeout, Wait till previous action finishes), all actions are performed simultaneously.

> Macros control

Configuring macros

You can create and configure macros on the **Programming** tab (see Create Macros).

To configure macros, do the following:



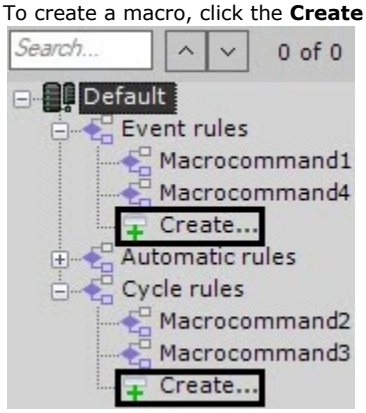
1. Specify the green section of the setting **Start conditions** (**1**). These are the events in the system that will trigger a macro (see Configuring start conditions for event-driven macros).
2. Specify the blue section of the setting that is the system actions (**2**). These are the actions that the system should perform after an event occurs (see Settings specific to actions). Several system actions can be configured.

There is also an orange setting section in cycle macros. It sets the system wait time between the actions. For more information on configuring the cycle macros, see Cycle macros.

You can find examples of macros on these pages: Configuring macros when working with vehicles lists, Examples of macros used when working with face lists.

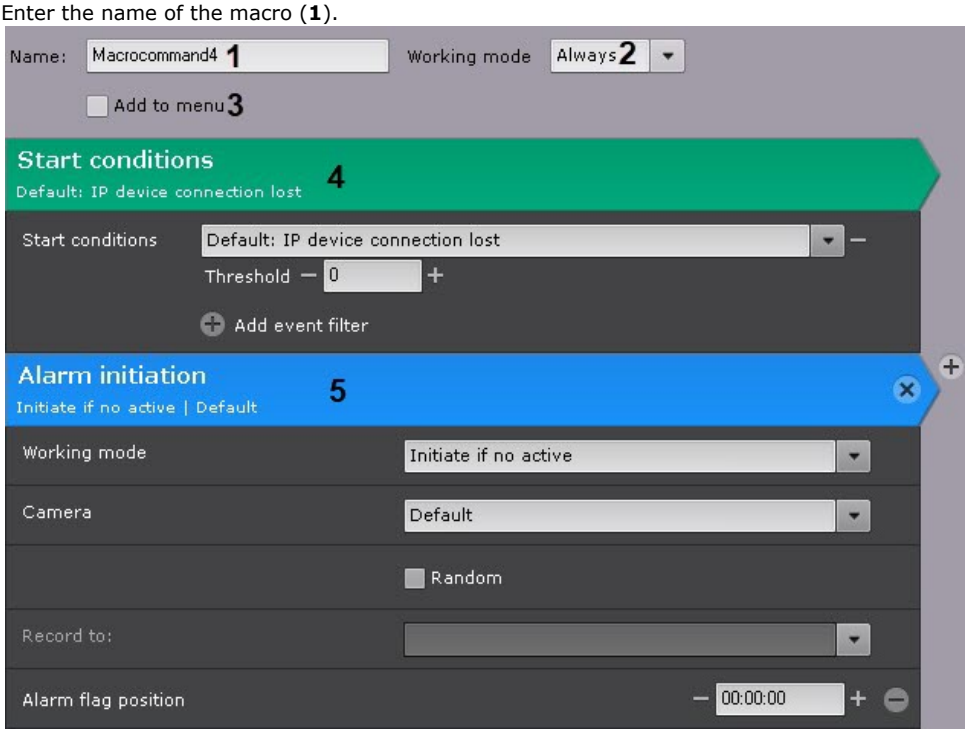
Create Macros

To create a macro, click the **Create** button in the required list.



Then do as follows:

1. Enter the name of the macro (**1**).



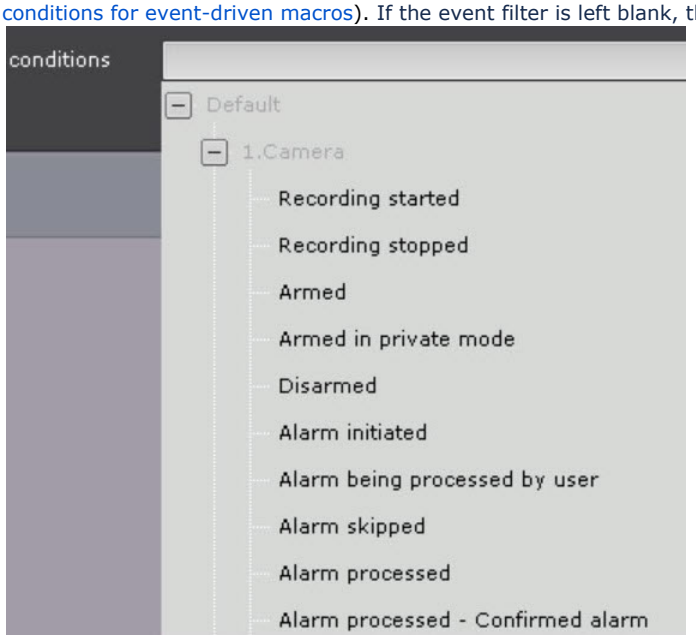
2. Select the macro working mode (**2**):

Mode	Event-driven	Cyclic
Never	Manual execution only (see Working with Dialog Board, Macros control)	Disabled, manual execution is possible (see Macros control)
Always	Always on	Always on
Time schedule	Runs within the selected time schedule (see Creating schedules). Manual execution is possible at any time	Runs within the specified time schedule

> **Note**
>
> When creating a macro, the **Always** mode is used by default.

3. If you need to add a macro to the control menu on the layout (see Macros control), set the corresponding checkbox (**3**).

4. To configure event-driven macros, click the button and select one or more trigger events (**4**, see Configuring start conditions for event-driven macros). If the event filter is left blank, the macro can be executed only manually.



> **Note**
>
> To delete an event from the filter, click the button.

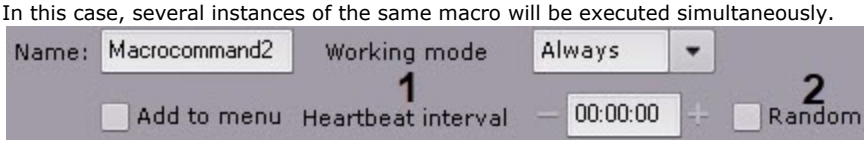
5. Add one or more actions to the macro (**5**, see Settings specific to actions). Click the button to do this. To delete an action, click the button.

> **Note**
>
> The macro can be executed for a group of cameras (see Creating a system of groups and subgroups).

> **Note**
>
> To hide the start conditions and action for the macro, click the action name.

6. A cyclic macro can be launched automatically at a specified time interval, or at a random moment within the specified time interval. To configure this action, do as follows:

   a. In the **Heartbeat Interval** field, specify the time interval in the HH:MM:SS format (**1**). For example, if you set the interval to 8 hours and leave the **Random** checkbox clear (see 6b), the macro will be launched every 8 hours strictly. The macro will be launched according to cycle settings even if the actions from its previous launch are not completed. In this case, several instances of the same macro will be executed simultaneously.



   b. Set the **Random** checkbox (**2**), if you need to launch the macro at a random moment set by the **Heartbeat interval** p arameter. For example, if the interval is set to 8 hours, then once every 8 hours at a random moment, the macro will be launched.

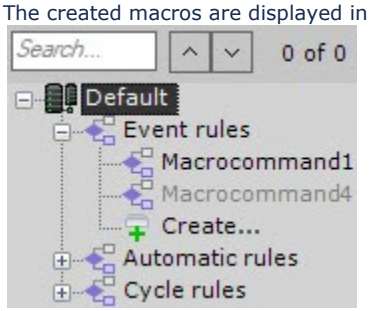
> **Attention!**
>
> If the macro working mode is linked to a time schedule, and the launch time falls out of the schedule, the macro will not be launched.

7. To save the macro, click the **Apply** button.

Attention!

By default, the created macros are available only to the users from the admin group (see Creating and configuring roles).

The created macros are displayed in the list. If the **Never** mode is selected for the macro, it is grayed out.



You can copy macros. To do it, do the following:

1. Select the macro to copy.
2. Click the **Create** button.

A new macro with the similar parameter will be created.

Note

To create an empty macro with no parameters specified, select any of the common macros groups, and click the **Create** button.

To delete a macro, select it in the list and click the **Remove** button.

Configuring start conditions for event-driven macros

When creating event macros, you can select one or more events which will trigger the macro.

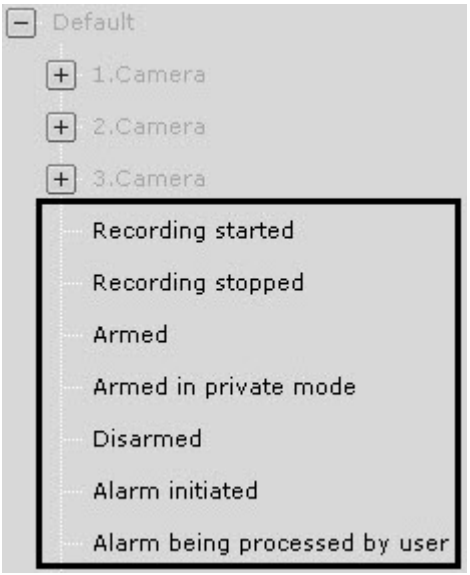
In addition, the macros can be triggered when specified statistical conditions are met (see Triggering macros by statistical data).

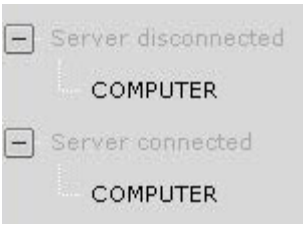
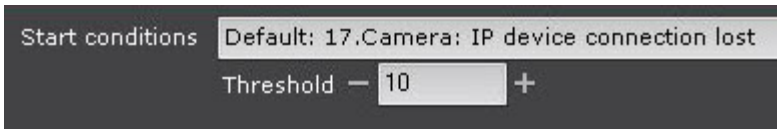
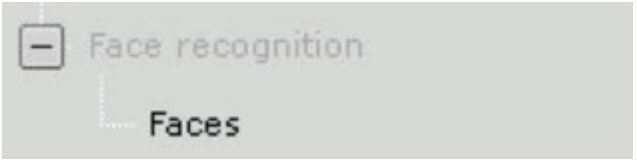
If several conditions are set, the macro will be triggered when any of these conditions are met.

You can also filter events:



The following events are available for selection:

Object	Event	Image
Axxon-domain	A string of events. If you select an event from an Axxon-domain, the macro will be launched when this event is received from any object in the Axxon-domain	
Server	Server disconnected	

	Server connected	
Camera	Recording started	
	Recording stopped	
	Armed	
	Armed in private mode	
	Disarmed	
	Alarm initiated	
	Alarm being processed by user	
	Alarm skipped	
	Alarm processed	
	Alarm processed—Confirmed alarm	
	Alarm processed—Suspicious situation	
	Alarm processed—False alarm	
	Connected	
	Disconnected	
	Motion: Triggering start	
	Motion: Triggering end	
	Signal lost	 You can set a threshold for these type of events: the time in seconds (0 to 3600) between switching from **Signal Lost** to **Signal Restored** state. For example, if a 10-second threshold is set for the **Signal Lost** condition, then at least 10 seconds should pass between the last **Signal Restored** event and the new **Signal Lost** event to start the macro
	Signal restored	
	Face recognition It is necessary to select the list from which the macro will be triggered when recognizing a face	

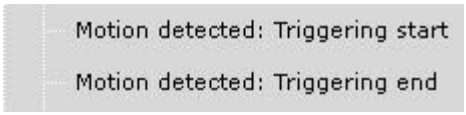
<table>
<tr>
<td>Group of cameras</td>
<td>A string of events.

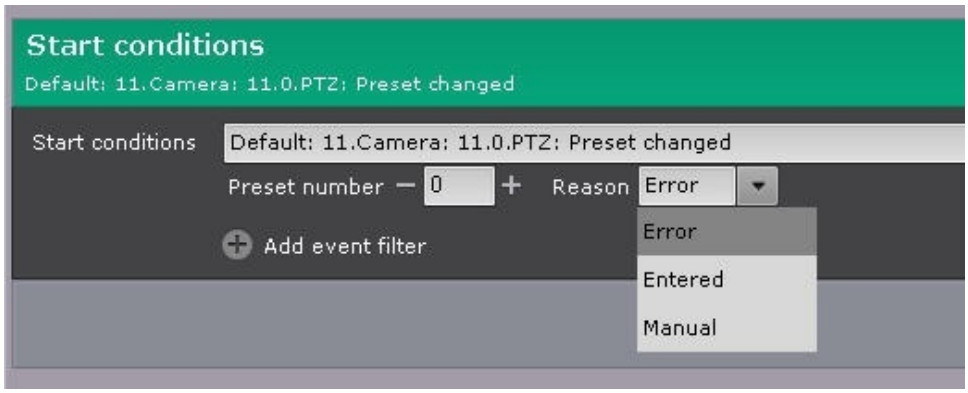
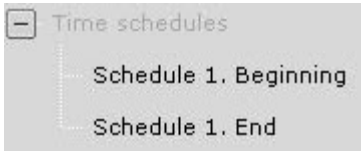
If you select an event from a group of cameras, the macro will be launched when this event is received from any camera in the group.</td>
<td> 
</td>
</tr>
<tr>
<td>Detector, Input and Output</td>
<td>Triggering start

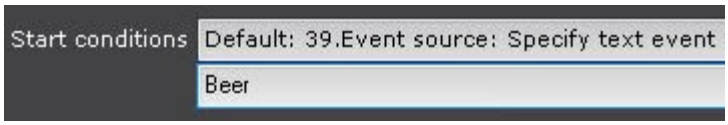
Attention!

If triggering conditions for a macro include a Triggering start event, any changes in macro's settings that have been saved while the detection tool is triggered (before the Triggering end event) will lead to re-executing the macro.

The same logic is applied when you create a macro. If you are creating a macro, and the detection tool is triggered, the macro will be executed immediately after the creation is complete.

Triggering end</td>
<td> 
</td>
</tr>
</table>

	Triggering (for detection tools, which do not have the start and end of the triggering, see Checking the triggering of a detection tool)	
	Specified Triggering (for face detection only, see Specific parameters for triggering a face recognition macro)	
	Preset change	 For these events, you should specify the preset number and the reason for the action: 1. Error. 2. Entered: the action occurs if you select a preset (see Creating and editing presets) with the selected number while controlling the camera (see Controlling a PTZ Camera). 3. Manual: the action occurs when you manually change the position of the camera when a preset is selected (see Control using step buttons and virtual joystick)
Neurocounter	Triggering	
Archive	Archive partition error	
	Archive partition restored	
Time schedules	Beginning	
	End	

Event source	Description: for the **Event source** object, you should specify the trigger word or phrase. When it comes up in the captions, the macro starts. For example, this filter triggers the macro when the word "Beer" appears in the captions. If a macro is triggered by a simultaneous combination of words and/or values, use curly braces for logical AND. For example, {Beer} {Belgium}	

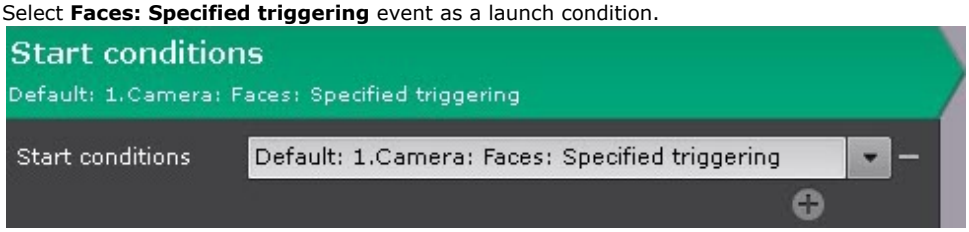
Specific parameters for triggering a face recognition macro

You can set a number of specific parameters which affect triggering a face recognition macro:

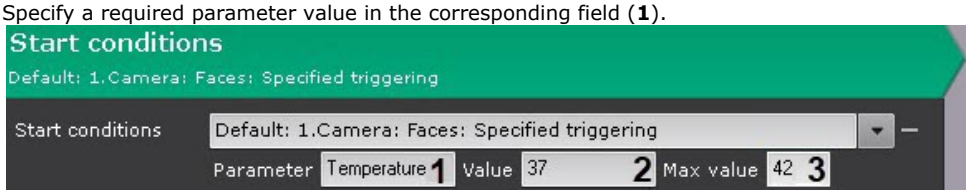
1. **Age** of the individual (requires activation of the **Gender and Age** parameter, see Configuring the Face Detection TV).
2. **Gender** of the individual (requires activation of the **Gender and Age** parameter, see Configuring the Face Detection TV). Value: **1** = female, **2** = male.
3. **TemperatureValue**: body temperature of the individual (requires the **Face Detection and Temperature Control**, see Face Detection and Temperature Control with Mobotix M16 TR cameras).

To set specific parameters, do the following:

1. Select **Faces: Specified triggering** event as a launch condition.



2. Click  .
3. Specify a required parameter value in the corresponding field (**1**).



> **Attention!**
>
> The parameter is case-sensitive.

4. In the **Value** (**2**) and **Max value** (**3**) fields, set the range of parameter values within which the macro will be triggered.

> **Note**
>
> Examples.
>
> If you set **Age** to [18, 100], the macro will be triggered only if the detection tool returns the age value of 18 or more.
>
> If you set **Gender** to [1, 1], the macro will be triggered only if the detection tool returns the individual's gender as female.
>
> If you set **Gender** to [2, 2], the macro will be triggered only if the detection tool returns the individual's gender as male.
>
> If you set **TemperatureValue** to [37, 100], the macro will be triggered only if the detection tool returns the temperature value of 37 or more.

5. Add one or more actions into the macro (see Settings specific to actions).
6. Click the **Apply** button.

Triggering macros by statistical data

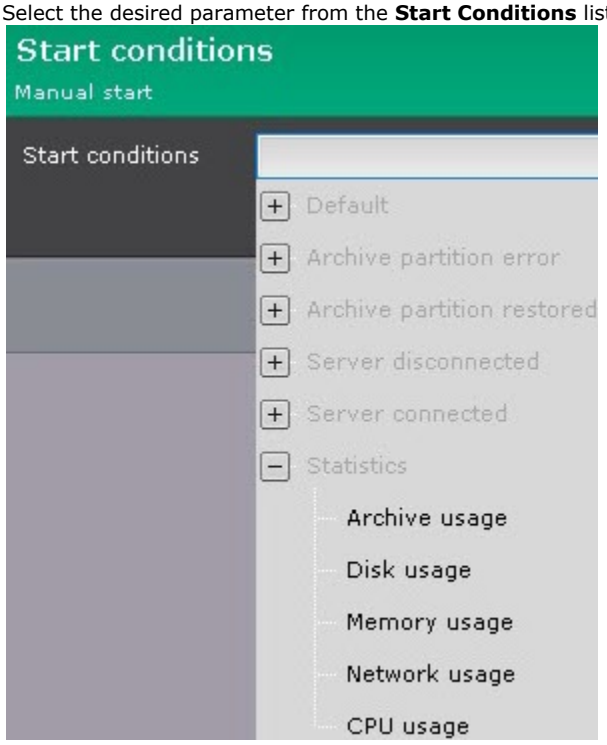
Event-triggered macros can be launched not only by events of particular type (see Configuring Filters for Event-driven Macros) but also by statistical parameters.

A macro can be initiated by the following parameters reaching pre-defined criteria:

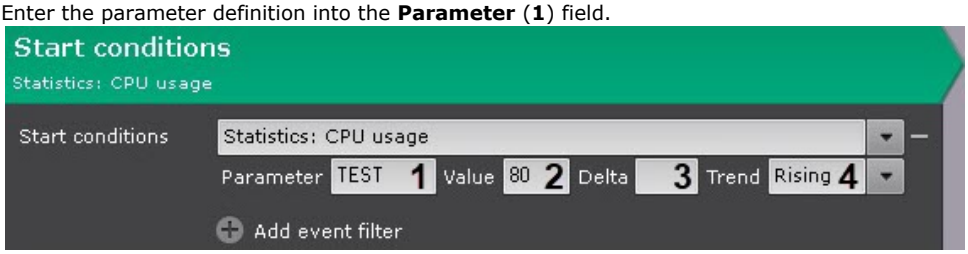
1. The percentage of used space in Archive.
2. The percentage of used space on a volume.
3. The percentage of used RAM on a Server.
4. The percentage of used network bandwidth on a Server.
5. The percentage of CPU load on a Server.

To set up triggering macros by statistics, do as follows:

1. Select the desired parameter from the **Start Conditions** list in the **Statistics** group.



2. Enter the parameter definition into the **Parameter** (**1**) field.



Archive usage	Archive in the following format: hosts/TEST/MultimediaStorage.AliceBlue/MultimediaStorage.
Disk usage	**TEST@C:**, where TEST is the name of a Server within the Axxon-domain, C:\ is the volume name. **Important!** You cannot monitor storage capacity of a disk fully allocated for Archive.
Memory usage (RAM)	The name of a server within the Axxon-domain.
Network usage	The name of a server within the Axxon-domain.
CPU usage	The name of a server within the Axxon-domain.

3. Enter the threshold value into the **Value** (**2**) field.
4. For **Leaving** condition, enter the range into the **Delta** (**3**) field (see section 5).
5. From the **Trend** (**4**) list, select a triggering condition for the macro.

Leaving	The macro is triggered if a parameter value goes out of the specified range [**Value** – **Delta**; **Value**].

Rising	The macro is triggered if the parameter value exceeds the threshold specified in the **Value** field.
Falling	The macro is triggered if the parameter value falls behind the threshold specified in the **Value** field.

> **Attention!**
>
> The triggering conditions are set not for current but for future events. For instance, if the current CPU load is 85%, and you set the triggering condition to exceeding 80%, the macro will be launched only when the CPU load exceeds 80% value next time.

6. If necessary, you can set several event and/or statistical conditions for triggering macros.

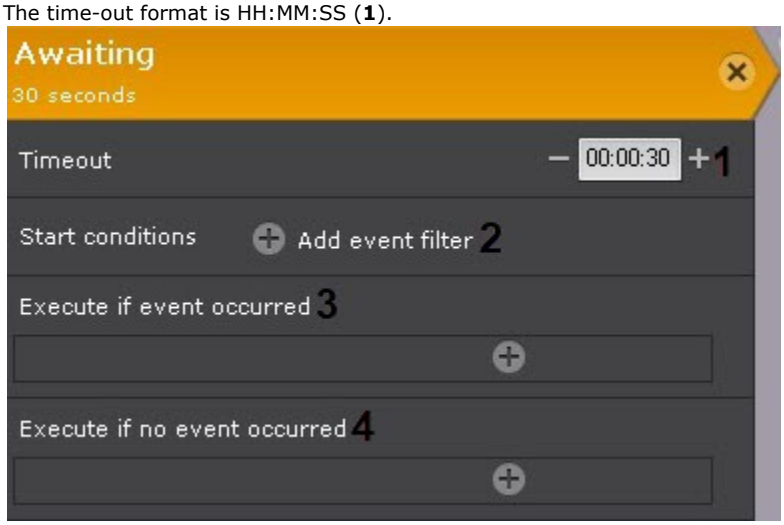
Settings specific to actions

Wait for event

This is the IF condition for running a command (only after the specified events occur). You must configure the conditions to start a macro beforehand (see Configuring filters for event-driven macros).

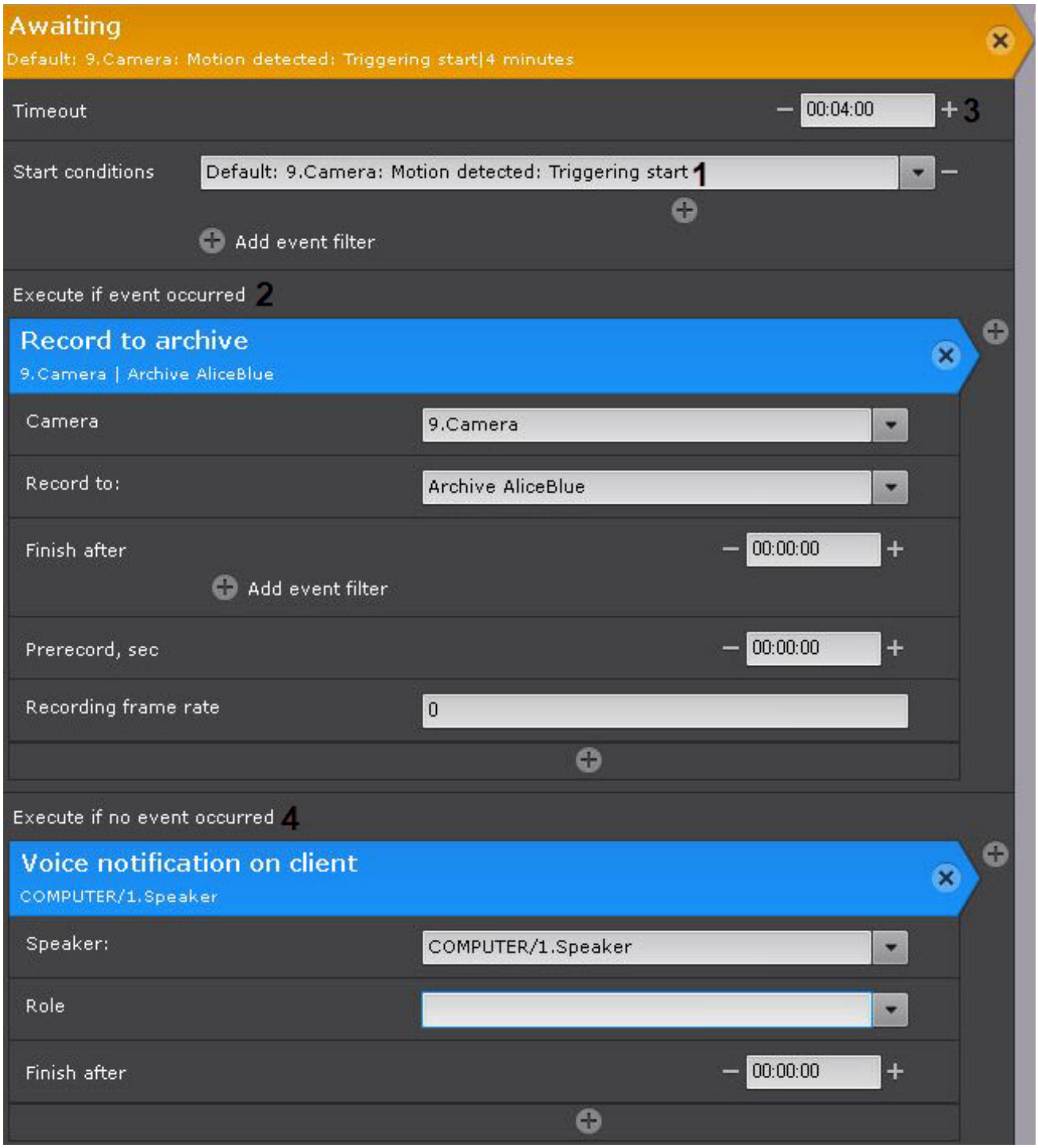
You can enter the following parameters in the **Awaiting** command:

1. The time-out format is HH:MM:SS (**1**).



2. Break command—here you enter one or more events that override the Awaiting command (**2**). If you do not specify events, the time-out applies.
3. If necessary, select and configure the action to perform when an event from Break Command occurs. A new **Awaiting** instance is also an option (**3**)**.**
4. If necessary, select and configure the action to perform if none of the events that were set in Break Command occurred during the time-out. A new **Awaiting** instance is also an option (**4**)**.**

Example 1. The macro is conditioned by the **Motion detected event** on **Camera 9** (**1**).

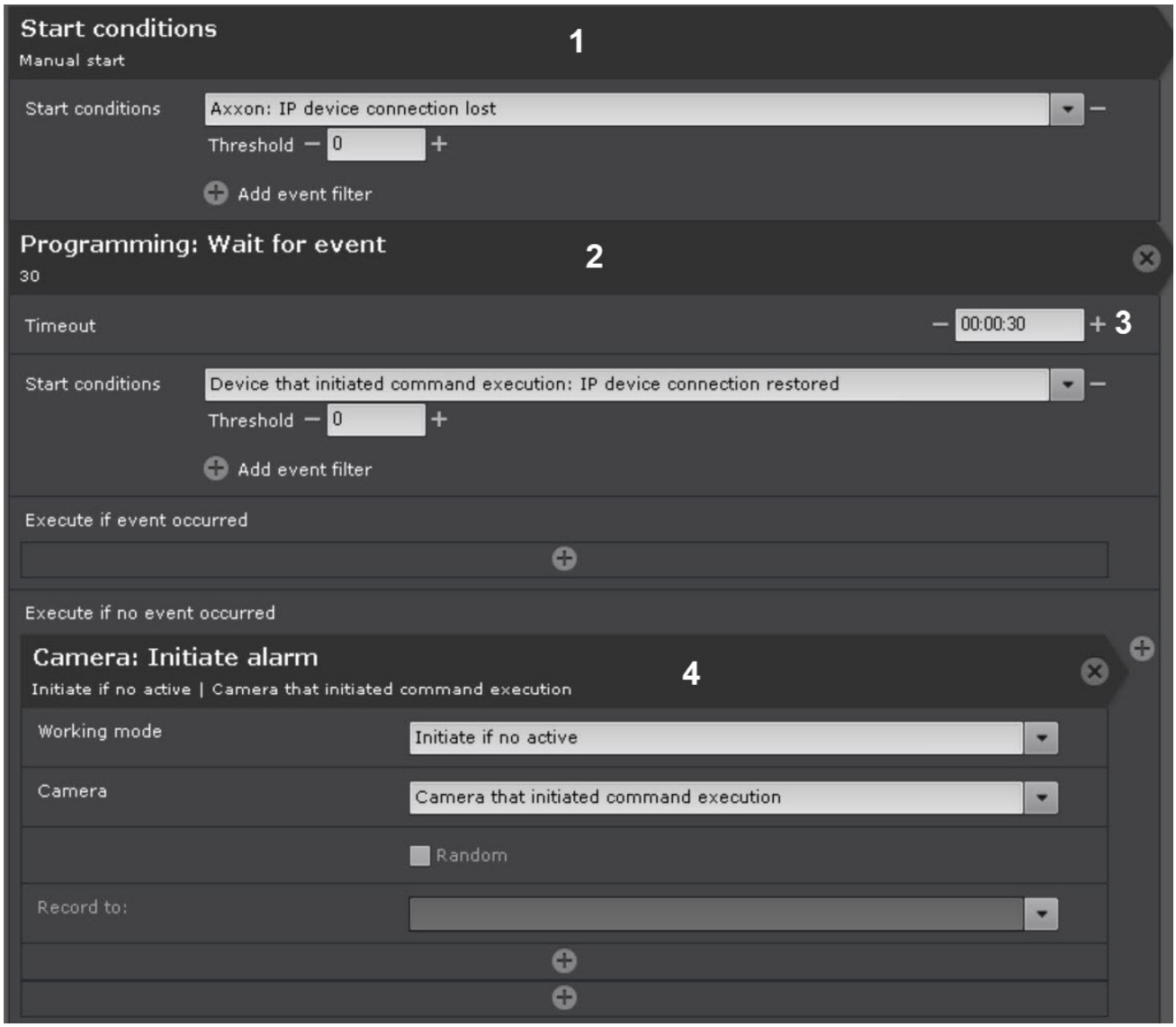


When it occurs, the macro continues. This also starts recording (**2**). Further macro actions are executed, if any.

If this event does not occur, the time-out is 4 minutes (**3**). After this time, a sound notification (**4**) plays.

> **Attention!**
>
> The **Awaiting** command does not affect the commands below (outside of) it.

Example 2. The macro checks the connection with the IP device.



If connection with the IP device is lost (**1**), the waiting time (**2**) for restoring the connection with the device is 30 seconds (**3**). The awaiting ends as soon as the connection with the IP device is restored.

If the connection is not restored, then after the awaiting time, an alarm is initiated (**4**).

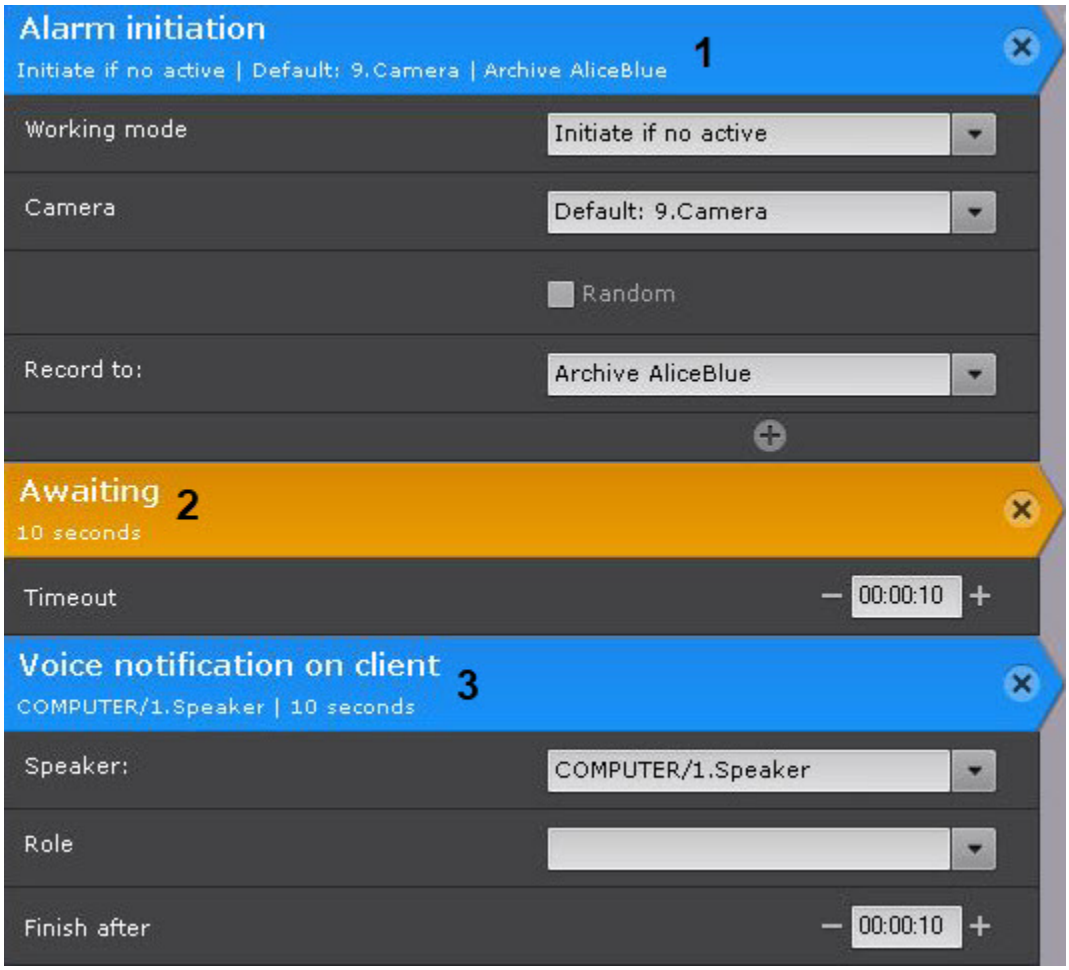
Wait for timeout

This command delays launch for downstream macros. You must configure the conditions to start a macro beforehand (see Configuring filters for event-driven macros)

The time-out format is HH:MM:SS.



For example, when performing that macro, an alarm will be initiated in the system (**1**), and then after 10 seconds (**2**)—an audio alert (**3**).



Wait till previous action finishes

This is the IF condition for running a command (only if the previous steps are completed/not completed in the specified time).

To configure, set up the following parameters:

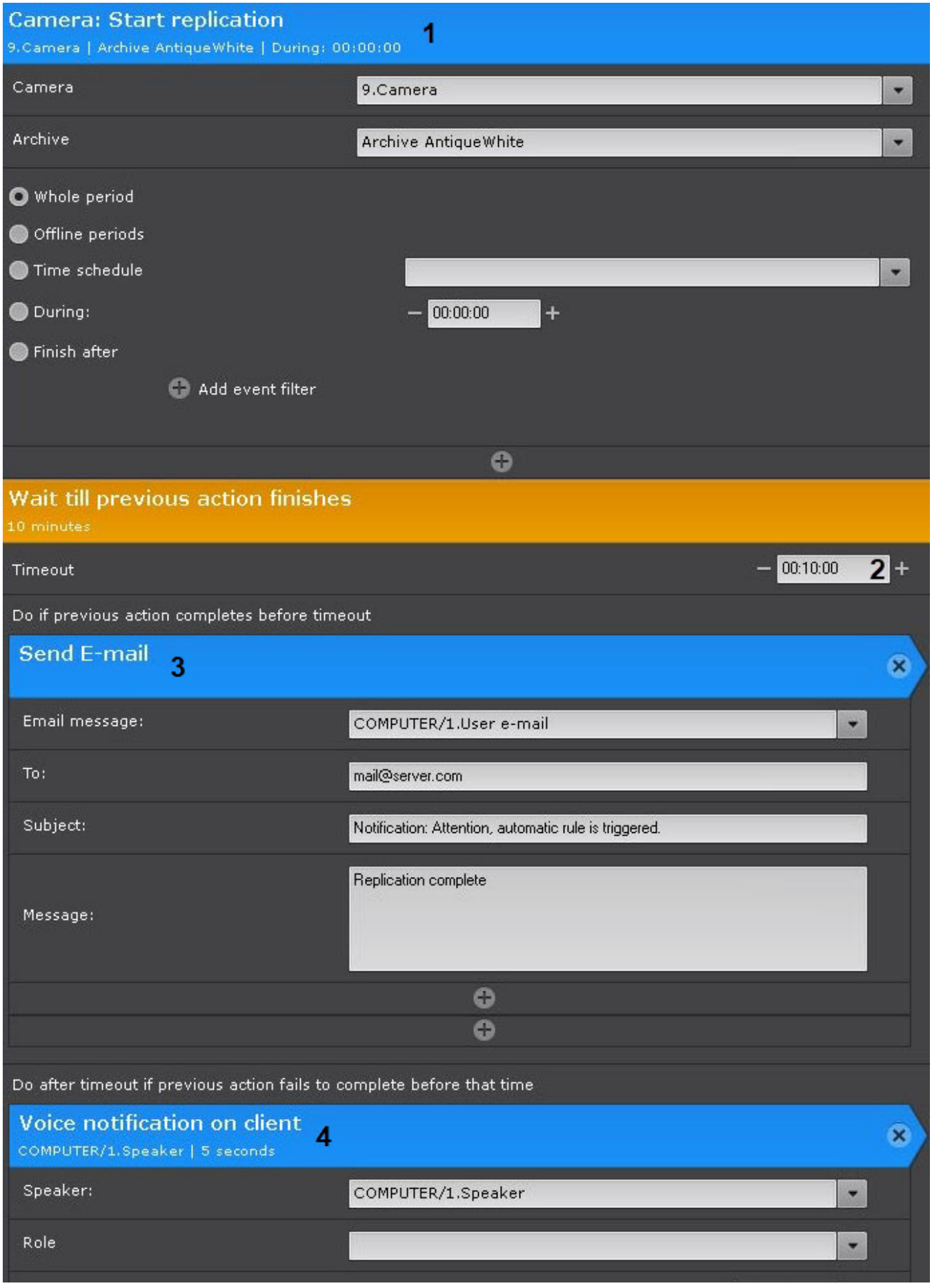
1. Set waiting period in HH:MM:SS format for previous action to be performed (**1**). If 00:00:00 is set, then waiting will last forever.



2. Specify the action to perform if the previous command was completed within the specified timeout (**2**).
3. Specify the action to perform if the previous action was **not** completed within the specified timeout (**3**). If the timeout is **00:00:00**, this setting is not applicable.

> **Attention!**
>
> This command does not affect the commands below (outside of) it.

Example: In this macro, replication (**1**) and the program on the Client (**5**) start at the same time. If replication is completed within 10 minutes (**2**), an Email message (**3**) is sent. Otherwise, a voice alert (**4**) is played.

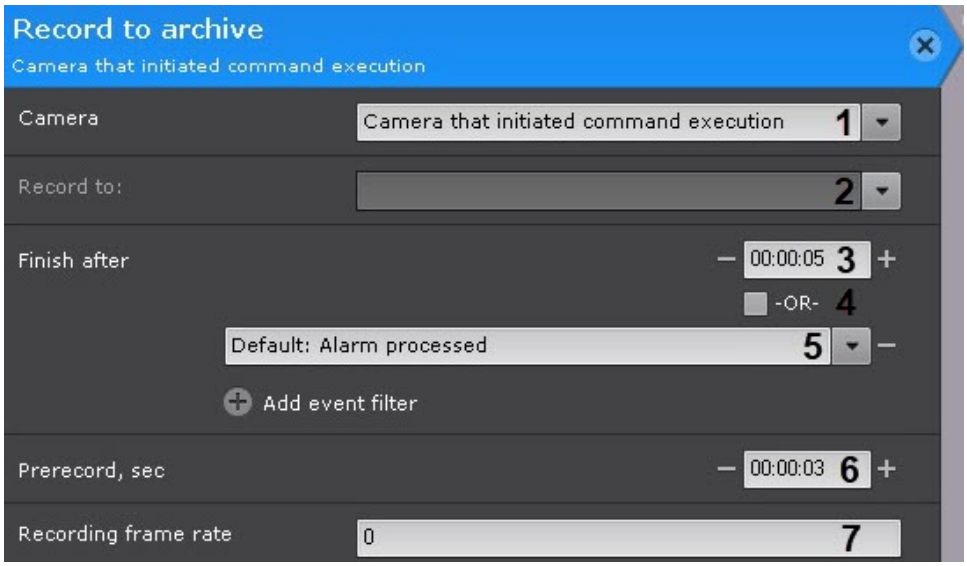

Camera: Start replication
9.Camera | Archive AntiqueWhite | During: 00:00:00
1
Camera
9.Camera
Archive
Archive AntiqueWhite
Whole period
Offline periods
Time schedule
During:
00:00:00
Finish after
Add event filter
Wait till previous action finishes
10 minutes
Timeout
00:10:00
2
Do if previous action completes before timeout
Send E-mail
3
Email message:
COMPUTER/1.User e-mail
To:
mail@server.com
Subject:
Notification: Attention, automatic rule is triggered.
Message:
Replication complete
Do after timeout if previous action fails to complete before that time
Voice notification on client
COMPUTER/1.Speaker | 5 seconds
4
Speaker:
COMPUTER/1.Speaker
Role


Finish after
00:00:05
Launch external program on client
5
Path to file:
"C:\Windows\System32\cmd.exe"
...

Record to archive

To configure **Record to archive**:

1. Selecting a camera or group of cameras for recording (**1**). An implicit selection of a video camera is also allowed – **Camera that initiated command execution**.



> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered the command, the action will not start.

2. Select an archive to write to (**2**).
3. Configuring conditions that end recording.

Condition	Description
Timer (**3**)	Only a timer value is set. Recording stops according to the time setting.
Event filter (**5**)	One or several events are set, the timer is set to 00:00:00. Recording stops on any IF event.
Timer (**3**) + Intelligent event filter (IF) (**5**)	One or several events are set, the timer is set to non-zero. Recording stops when the set time interval expires after any IF event (trigger) occurs.
Timer (**3**) + **OR** flag (**4**) + IF (**5**)	One or several events are set, the timer is set to non-zero, the **OR** flag is set. In this case, the recording stops on any of the two conditions: after the time interval expires or if an IF event (trigger) occurs.

> **Note**
>
> The **OR** flag can be set only if the timer setting is not 00:00:00.

> **Note**
>
> An implicit selection of an event is allowed – **Last event for condition that initiated execution**.
>
> For example, if the event that triggered the execution of the command was the **Start time of detection tool trigger** from any type of detection tools, then the end event will be the **End time of detection tool trigger** from the same tool.

4. Set the pre-alarm recording time (**6**). The maximum pre-alarm recording time is 30 seconds.

Attention!

By default, the pre-alarm recording time interval is set to the value specified in Archive settings (see Configuring recording to an archive).

The longest pre-alarm recording time available in the Archive settings is used.

Changing this value in a specific macro does not affect the Archive settings.

5. If you have cameras in continuous recording mode (see Configuring recording to an archive) and you want to record with specified fps (see example 2) change the frame rate, enter the required frame rate (**7**). After the macro command completes, recording resumes at the frame rate specified in the archive settings. You can use special codes:

   a. **0** – do not change the current frame rate (default).
   b. **-1–** record only I-frames.
   c. **1000** – record at the standard fps of the camera.

Attention!

Fps for pre-recording will not change.

If the macro command is set to complete some time after a specified event has been received (see p. 3), the frame rate will change for this Check-in Event-time.

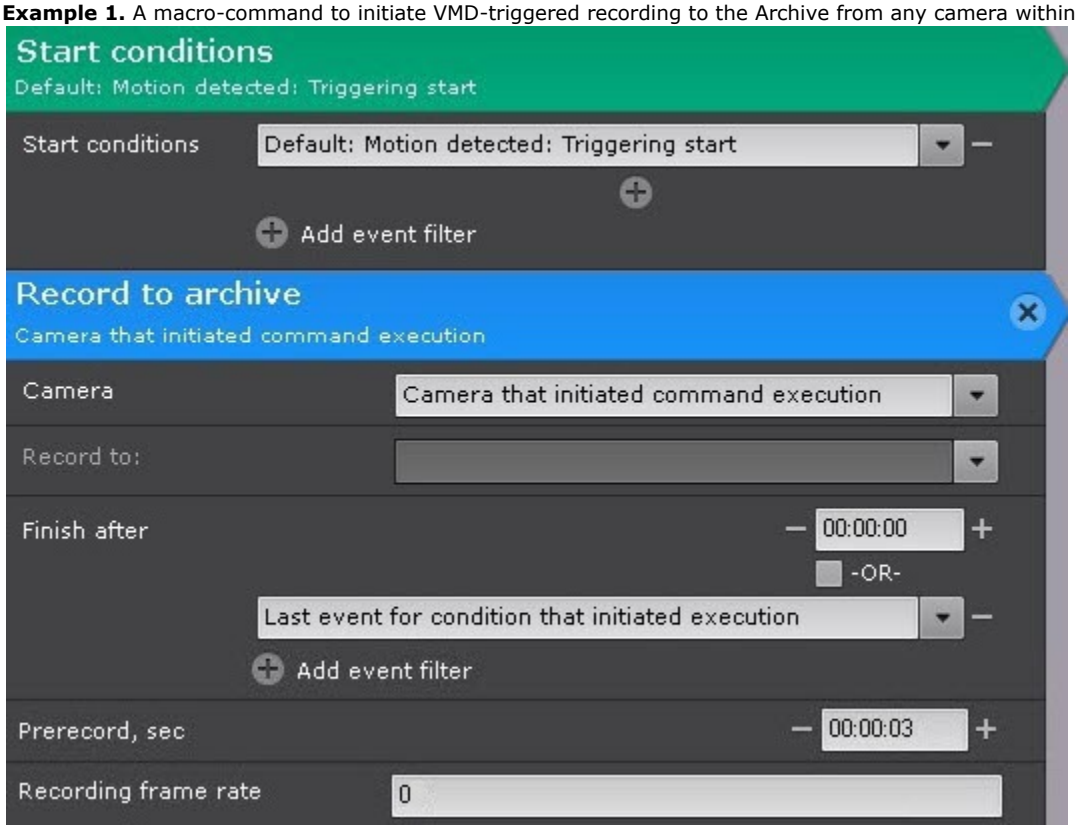
Attention!

When you prune by frame dropping, in all video streams except MJPEG, only I-fames (Intra-Coded Frame or Key Frames) are saved, so please use codes: **-1** and **1000**.

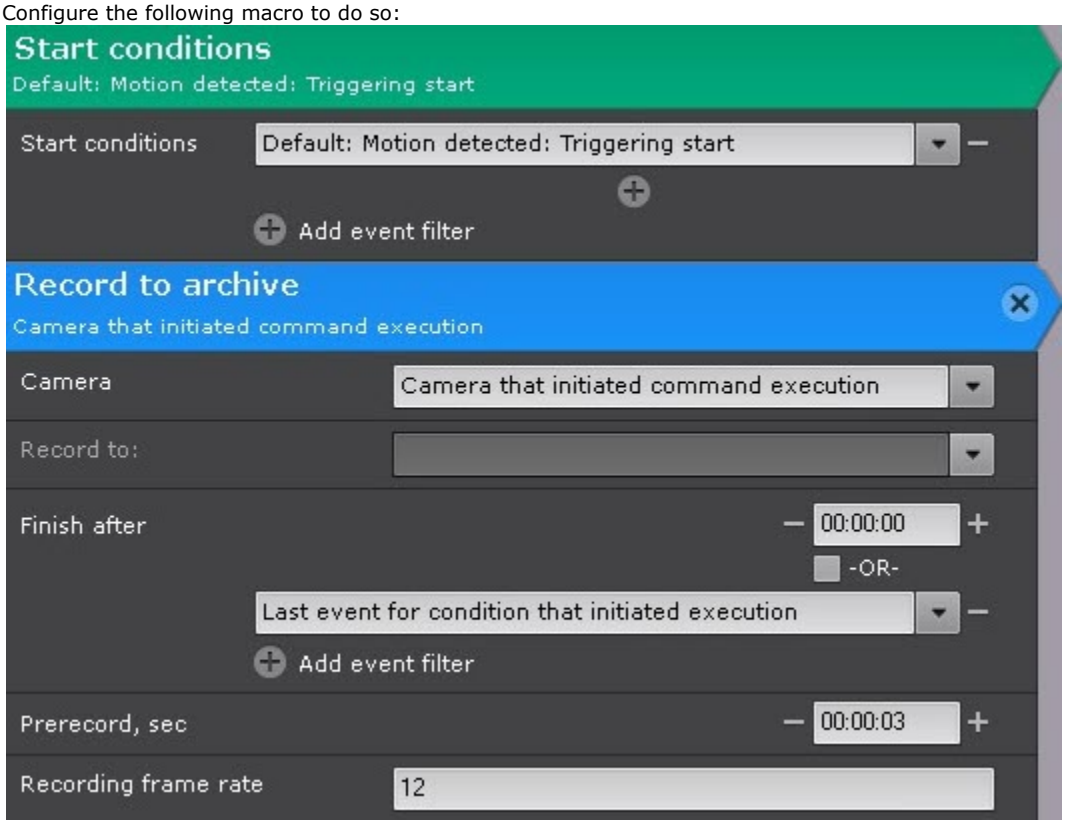
If you go for a custom frame rate this will lead to dropping some key frames.

MJPEG video contains only Iframes (Intra-coded pictures with a complete image), so it makes sense to set a desired frame rate here.

Example 1. A macro-command to initiate VMD-triggered recording to the Archive from any camera within **Default** Axxon domain.



Example 2. All video cameras from the **Default** Axxon Domain are set to continuously record video at the specified fps by dropping frames (see Configuring recording to an archive). When you have a motion detection event, you need to switch to full fps recording. Configure the following macro to do so:

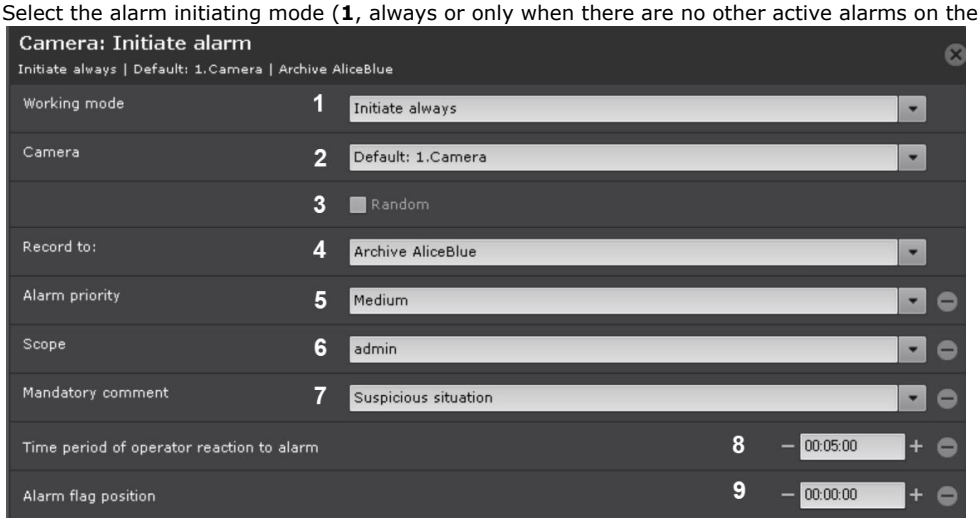


Initiating an alarm in the system

This action initiates an alarm in the system and starts recording to the archive.

To configure the action, do the following:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the alarm initiating mode (**1**, always or only when there are no other active alarms on the specified camera).



3. Select a camera or group of cameras, on which you want to initiate an alarm (**2**). An implicit selection of a camera is also allowed—**Camera that initiated command execution** (see Configuring start conditions for event-driven macros).

> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera for this action. If you select a group of cameras or a camera that initiated the macro, the action will not start.

4. If you selected a group of cameras or an Axxon-domain in the previous step, set the **Random** (**3**) checkbox to initiate an alarm on a random camera from this group/Axxon-domain.
5. Select an archive to record to (**4**).
6. Select the alarm priority (**5**). The higher the priority of the alarm, the higher it will be placed in the list on the Alarms Panel.
7. Select the scope of roles, the users of which will be able to see the alarm initiated by the macro (**6**). If you don't specify any role in the **Scope** field, the alarm will be displayed for all users.
8. Select alarm assessments, after receiving which the operator must enter a comment (**7**).
9. In the **Time period of operator reaction to alarm** field, specify the time within which the alarm must be taken into processing, otherwise it will be assigned the **Skipped** status (**8**). The minimum value is 2 minutes.

> **Note**
>
> You can configure the **Mandatory comment** and **Time period of operator reaction to alarm** fields in the system settings (see Configuring Alarm processing). If you specify these fields in the macro settings, the system settings will be ignored only for the alarms initiated by this macro.

10. Enter the time in seconds by which the alarm flag will be shifted back relative to the time when the event that started the macro was received (**9**).

> **Note**
>
> If the alarm flag position is set, the event that was just taken into processing will be played back from the moment corresponding to the flag position, and not from the alarm start.

Stopping alarm

This action allows you to process and assess an alarm.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a video camera or a group of cameras on which you want to stop an alarm (**1**). You can also implicitly select a camera—**Camera that initiated command execution**.



> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered the command, the action will not start.

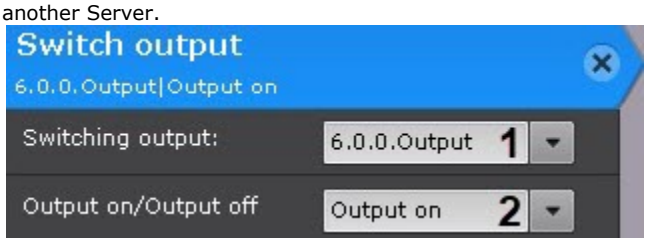
3. Select the alarm status (**2**).

Switch output

This action switches a output to a pre-selected state.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a output to switch by the macro (**1**). You can select any active output within your system, including outputs linked to another Server.

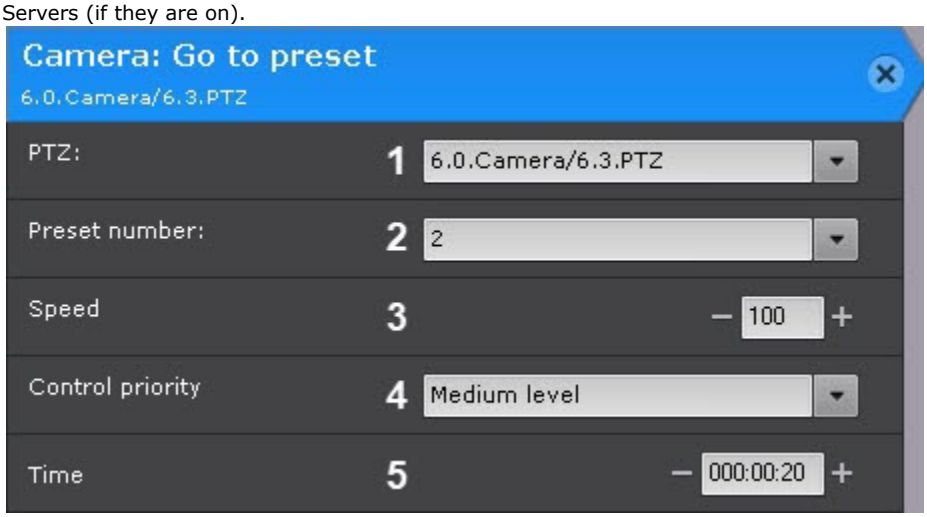


3. Outputs switch back after On-time (**2**), or after Check-in Event-time for any specified events**.**

Switching to a PTZ camera preset

To configure the action, do the following:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a PTZ device that you want to use from the **PTZ** list (**1**). Any PTZ cameras can be used, including those from other Servers (if they are on).



3. Select the preset (**2**) to which you want to switch when a macro is triggered.
4. Set the rotation speed of the camera (**3**). The value should be in the range [1; 100].
5. Set the control priority of the camera (**4**). The priority determines the user with which access level (see Creating and configuring roles) will take over the control of the camera when the macro is running.
6. Set time (**5**). If the macro is running and the user has a lower access level than the macro, the user will be able to control the PTZ camera only after this time has elapsed.

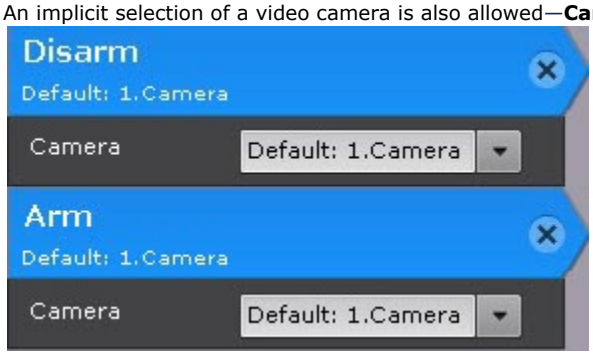
Note

In order to create a sequential switching to specified presets at selected time intervals (**5**), set Wait till previous action finishes between the switching actions. You can also set Wait for timeout. In this case, the switching between the presets will take place after the timeout time.

Arm /disarm a camera

To configure these actions, select a camera or group of cameras that you want to arm or disarm. You must configure the conditions to start a macro beforehand (see Configuring filters for event-driven macros).

An implicit selection of a video camera is also allowed—**Camera that initiated command execution**.



Attention!

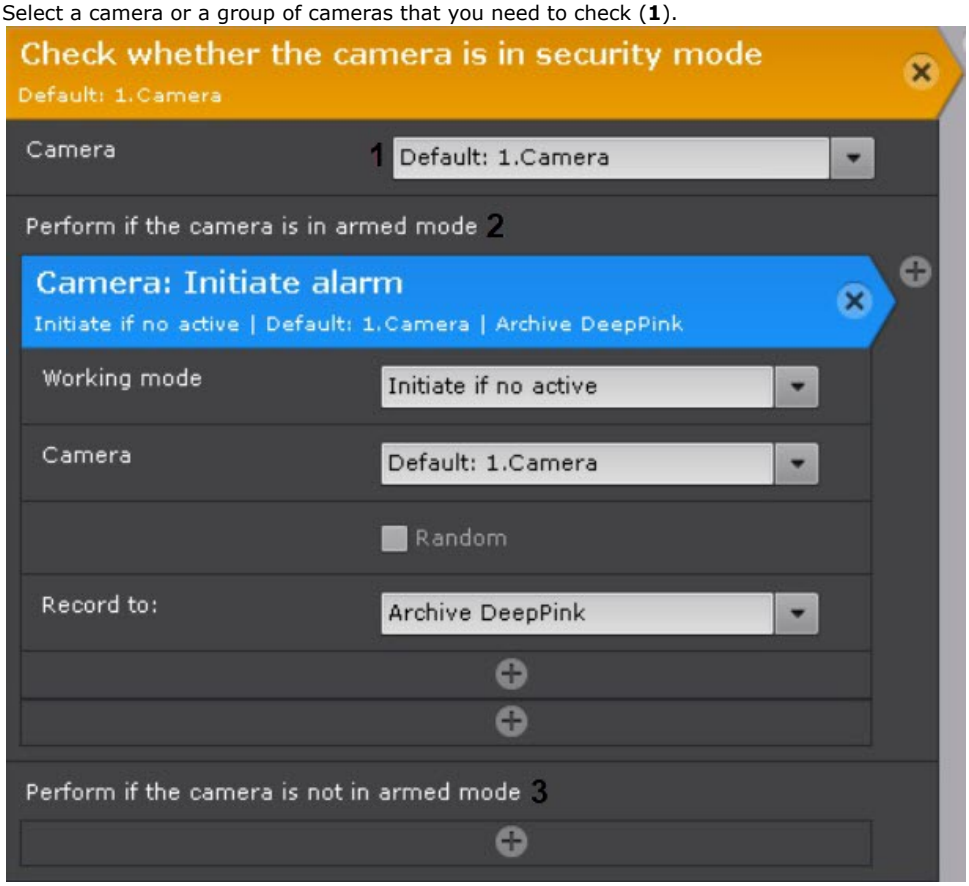
If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered the command, the action will not start.

Checking whether the camera is in armed mode

This command allows you to check whether a camera or a group of cameras is armed (see Arming and Disarming a Video Camera).

To configure this command, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros.
2. Select a camera or a group of cameras that you need to check (**1**).



3. Select the response scenario if the camera checked is armed (**2**).
4. Select the response scenario if the camera checked is not armed (**3**).

View camera

It is possible to open the layout with the specified camera.

The **View camera** macro uses the following algorithm:

1. Searches for the layouts available to the current user that contain the selected camera.
2. Selects the layout with the minimum number of cells to display the selected camera.
3. If the required layout does not exist, creates a new layout with the selected camera.
4. Switches to the selected layout or the created layout.
5. Performs the specified action.

To configure the **View camera** macro, do the following:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the camera to be displayed (**1**) or **Camera that initiated command execution** (see Configuring start conditions for event-driven macros). You can select a group of cameras for the **Switch to archive** mode (see step 2).

   > **Attention!**
   >
   > If the macro was triggered by a sensor or a relay (see Configuring start conditions for event-driven macros) that are not associated with the camera, the action will not be triggered.



3. Select the display mode (**2**).

Display mode	Description
Select camera	The camera is highlighted on the layout
Zoom in camera	The camera is highlighted on the layout, the viewing tile takes up 98% of the screen
Zoom in and show map	The camera is highlighted on the layout, the viewing tile takes up 50% of the screen, the map under the tile shows the camera
Switch to immersion mode	Immersive mode is on, the viewing tile takes up 50% of the screen
Switch to archive mode	The camera is highlighted on the layout and it is in archive mode. If a group of cameras is specified, then a layout is created with all the cameras in archive mode
Mark camera	The camera is added and highlighted on the **Marked cameras** layout (see Creating special layouts)
Unmark camera	The camera is deleted from the **Marked cameras** layout (see Creating special layouts)

4. Specify the number of the monitor on which the camera should be displayed (**3**).
5. Select the user roles, for which this macro will be available (**4**).

The configuration of the **View camera** macro is complete.

Open layout

You can open any layout you created (the **Open layout** macro) or restore the previous one (the **Restore layout** macro).



To configure the **Open layout** macro, do the following:

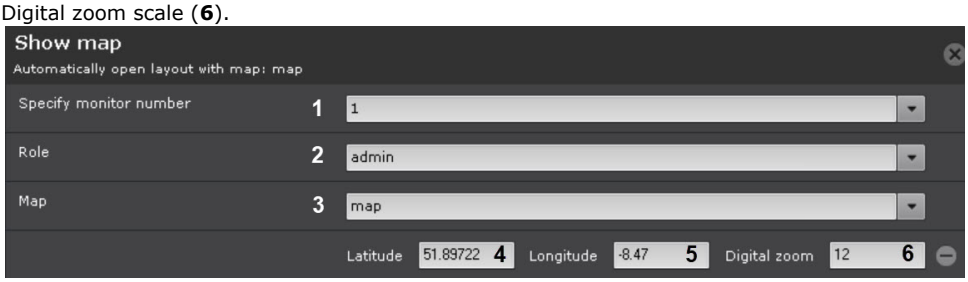
1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the layout (**1**).
3. Specify the number of the monitor on which you want to open the selected layout (**2**).
4. Select the role of users who can access this macro (**3**).

Show map

You can display any map added to the system on the required monitor (see Adding a new map).

To configure the **Show map** macro, do the following:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Specify the number of the monitor on which you want to display the selected map (**1**).
3. Select the role of users who can access this macro (**2**).
4. Select the map (**3**). When selecting a geomap, it is necessary to specify the following parameters to display the required area:
    a. Latitude (**4**).
    b. Longitude (**5**).
    c. Digital zoom scale (**6**).



5. Click the **Apply** button.

The **Show map** macro is now configured.

The selected map will be displayed on the specified monitor.

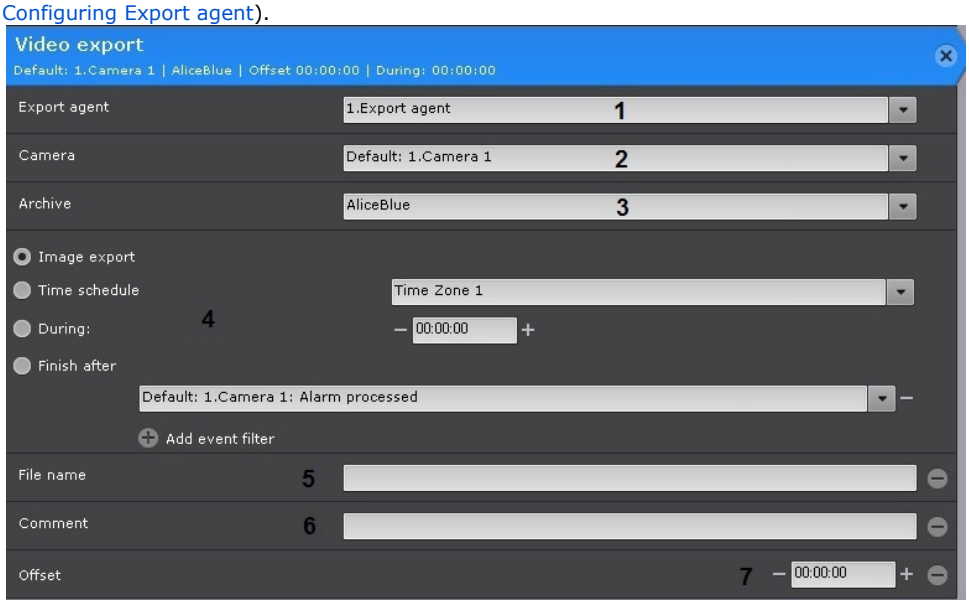


Starting export

This action starts the export of a snapshot or a video. You must configure the conditions to start a macro beforehand (see Configuring filters for event-driven macros).

To configure, set up the following parameters:

1. **Export agent** (**1**)—select the Server (formally the **Export agent** object) to which you want to export the video recording (see Configuring Export agent).



2. **Camera** (**2**)—select a camera for export. An implicit selection of a video camera is also allowed—**Camera that initiated command execution**.

> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered the command, the action will not start.

3. **Archive** (**3**)—select an archive for export.
4. Set the export interval (**4**).

Option	Description
Image export	Exports a snapshot with the time stamp identical to the start time of action. **Important! The image cannot be exported if the video camera does not have an archive**
Time schedule	You need to select a time schedule. Exports images from within time schedule. Video recording interval – [Beginning of the specified time slot; the end of the specified time slot]
During:	You should set the export duration in HH: MM: SS. The starting point of the exported video is the command start. End point is defined on the basis of the specified duration – (Interval [command start; command start + duration])
Finish after	Select one or more events that will trigger export stop. The starting point of the exported video will be the command start, the end point – the moment of receiving any these events

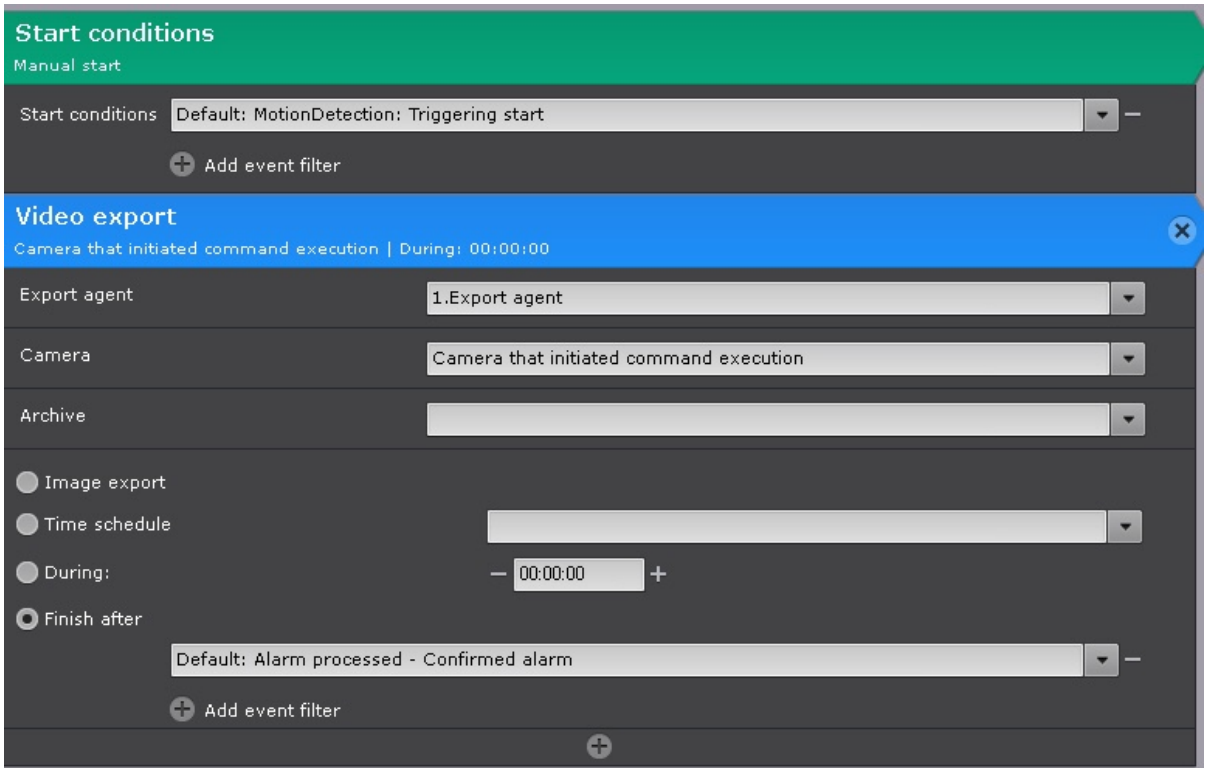
5. You can click the button to add additional parameters:
   a. File name (**5**).

> **Attention!**
>
> You can use the following templates for file names and text comments:
>
> - **%startTime%** , or **[START_TIME]**, or **{startTime}**: the starting time of exported interval.
> - **%finishTime%** , or **[FINISH_TIME]**, or **{finishTime}** : the finishing time of exported interval.
>
> You may use the following templates for macros triggered by a text message from an event source (see Configuring start conditions for event-driven macros):
> - **%startEvent%**, or **[START_EVENT]**, or **{startEvent}**: an event that triggered exporting.
> - **%finishEvent%** , or **[FINISH_EVENT]**, or **{finishEvent}**: an event that stopped the export.

b. Comments superimposed as captions over the exported video (**6**).
c. **Offset** (**7**) is a time period used to roll back the start time of exported video. If you set this this parameter to non-zero, the time interval of the exported video will be as follows:

   [action start − (duration + offset); action start − offset].
   If exported video(s) fall into a specific slot on Time schedule, this parameter is used to define the start time for video retrieval. For example, if you set the Offset (GUI: Buffer) to 48 hours, all videos from the given Time schedule slot recorded within 48 hours before the action start will be exported.

Example: A macro command for automatically exporting video recordings of all alarm events evaluated by operators as "confirmed".

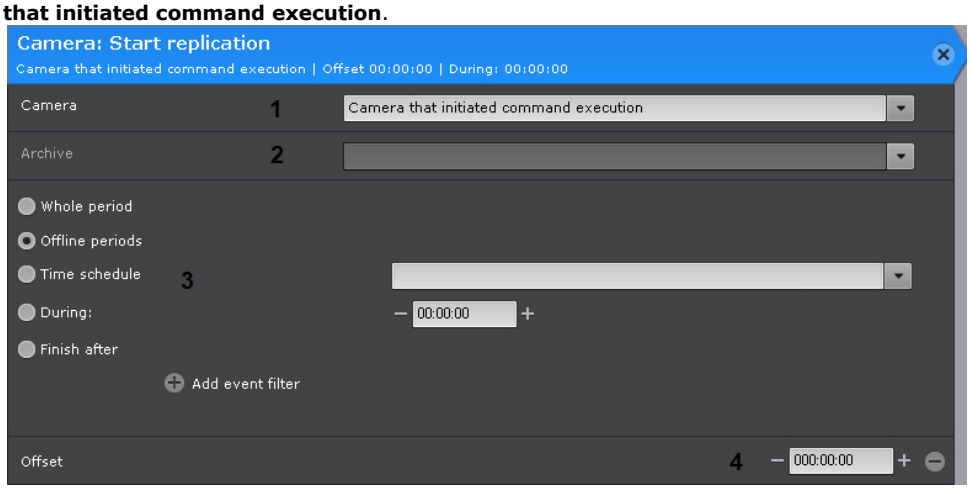


Start replication

This command starts the replication process.

To configure the command, perform the following:

1. Configure on-demand replication if replication is performed from the archive (see Configuring data replication). To replicate from the on-board storage (SD card or other storage embedded in the video camera), enable the corresponding object (The Embedded storage object).
2. Select a video camera or a group of cameras to replicate (**1**). An implicit selection of a video camera is also allowed – **Camera that initiated command execution**.



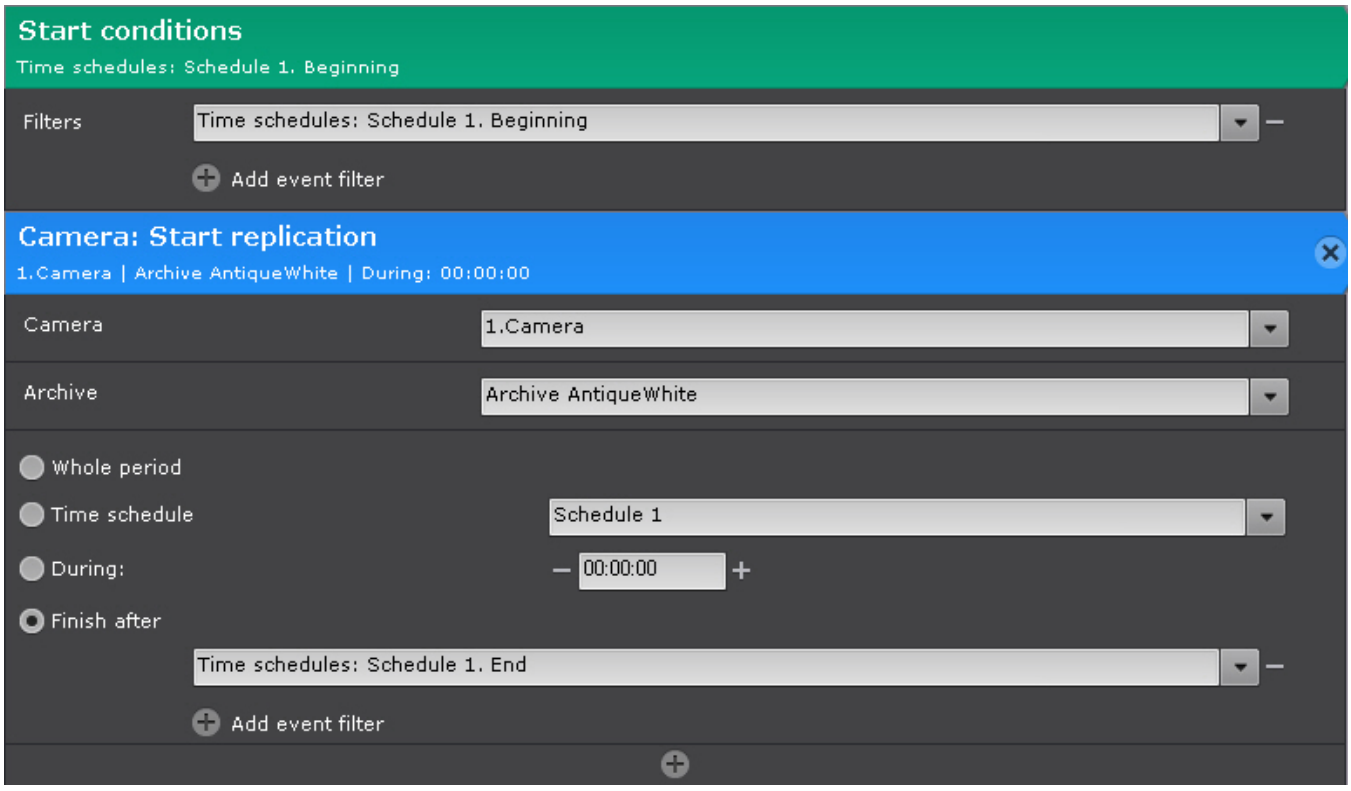
> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered the command, the action will not start.

3. Select an archive file to which video recordings will be replicated (**2**).
4. Select the replication period (**3**).

Option	Description
Whole period	All missing video recordings made **prior** to the command start time will be copied.
Offline periods	The system copies footage recorded to embedded storage (camera's SD card) during offline periods (between consecutive **Signal lost** and **Signal restored** events). If no **Offset** parameter (see paragraph 5) is specified, the replication covers offline footage recorded during the last 24 hours.
Time schedule	Select a time schedule (see Creating schedules). All recordings made according to the time schedule settings for the last 24 hours prior to the command start time will be copied.
During:	Set the replication duration in HH:MM:SS. Video recordings from the period [start action, start action + duration] will be copied. An additional **Offset** parameter can be specified as needed (see 5).
Finish after	Select one or more end events. All video recordings between the start point (when the action starts) and the end point (when the event is received) will be copied. **Important! Replication will not start until the end event is received.**

5. Specify **Offset**(**4**), if you specified the parameter **During:** for replication in previous step. Video recordings from the period [start action – offset, start action **+** duration **–** offset] will be copied.

To run replication on schedule (corresponding to **Time schedule 1**), configure the macro as follows:


Start conditions
Time schedules: Schedule 1. Beginning
Filters
Time schedules: Schedule 1. Beginning
Add event filter
Camera: Start replication
1.Camera | Archive AntiqueWhite | During: 00:00:00
Camera
1.Camera
Archive
Archive AntiqueWhite
Whole period
Time schedule
Schedule 1
During:
00:00:00
Finish after
Time schedules: Schedule 1. End
Add event filter

Notifications

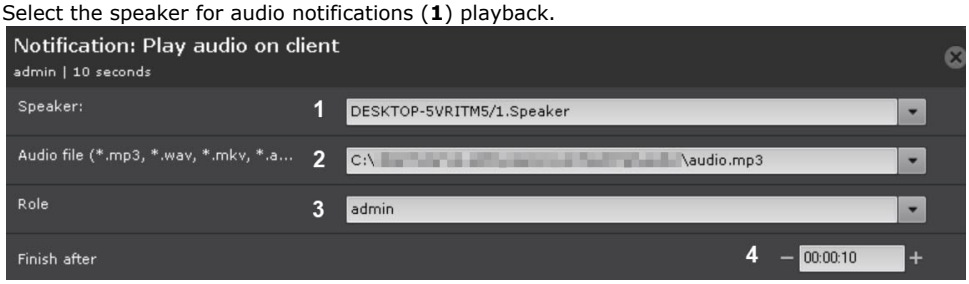
Audio notification on Client

You can playback audio via Client's speakers.

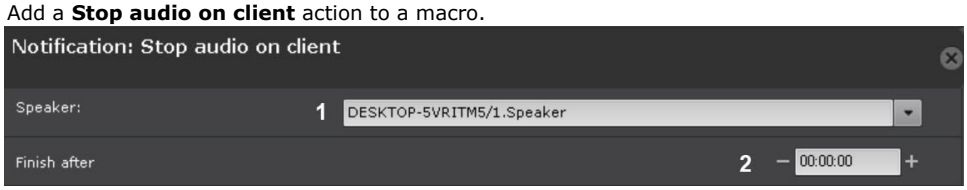
> **Attention!**
>
> To make the Client-side audio playback possible, you have to create a **Speaker** object allowing **Play on client** playback mode (see The Speaker object).

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the speaker for audio notifications (**1**) playback.



3. Select an audio file that you want to play as a notification (**2**).
4. Select a role to address notification to specific users (**3**).
5. If you need to cancel audio notification after some time, set the required time interval (**4**).
6. For event-triggered audio notification cancellation, do the following:
   a. Create a new event macro with all required events filtered (see Create Macros, Configuring start conditions for event-driven macros).
   b. Add a **Stop audio on client** action to a macro.



   c. Select the speaker on which you want to cancel audio notification (**1**).
   d. If you need to cancel notification after a certain amount of time, set the required time interval (**2**).

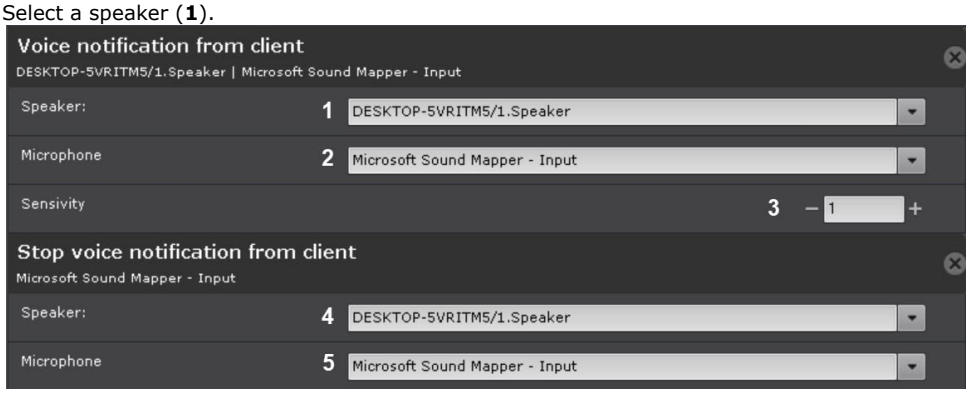
Voice notification from Client

Use this action to transmit audio from the Client's microphone to the selected speaker.

> **Attention!**
>
> If a Client is behind the NAT, you have to specify the external IP address of the switch for this Client with a port range of at least 1000 (see Network settings utility).

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a speaker (**1**).



3. Select a microphone (**2**).
4. Specify sensitivity from 0 to 100 (**3**).

To stop sound, use the **Stop voice notification from client** command on the Client.

To configure this command, select a speaker (**4**) and a microphone (**5**).

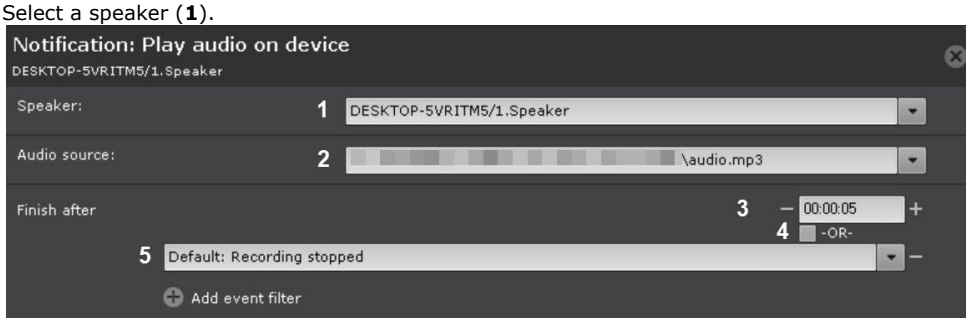
Play audio on device

This action allows you to play audio on a Server speaker.

> **Attention!**
>
> To make the Client-side audio playback possible, you have to create a **Speaker** object allowing **Play on Server** playback mode (see The Speaker object).

To configure the action, set up the parameters:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a speaker (**1**).



3. In the **Audio file** field (**2**), select the audio notification file.
4. Configure a condition (IF event, trigger) that will cancel the notification:

Condition	Description
Timer (**3**)	Only a timer value is set. Alerts are cancelled according to the time setting
Event filter (**5**)	One or several events are set, the timer is set to 00:00:00. Alerts are cancelled according to the IF event (trigger)
Timer (**3**) + Intelligent event filter (IF) (**5**).	One or several events are set, the timer is set to non-zero. Alerts are cancelled in a given time after the selected IF event (trigger) occurs
Timer (**3**) + **OR** checkbox (**4**) + IF (**5**).	One or several events are set, the timer is set to non-zero, the **OR** checkbox is set. In this case, the alert is cancelled on any of the two conditions: after the time interval expires or if an IF event (trigger) occurs

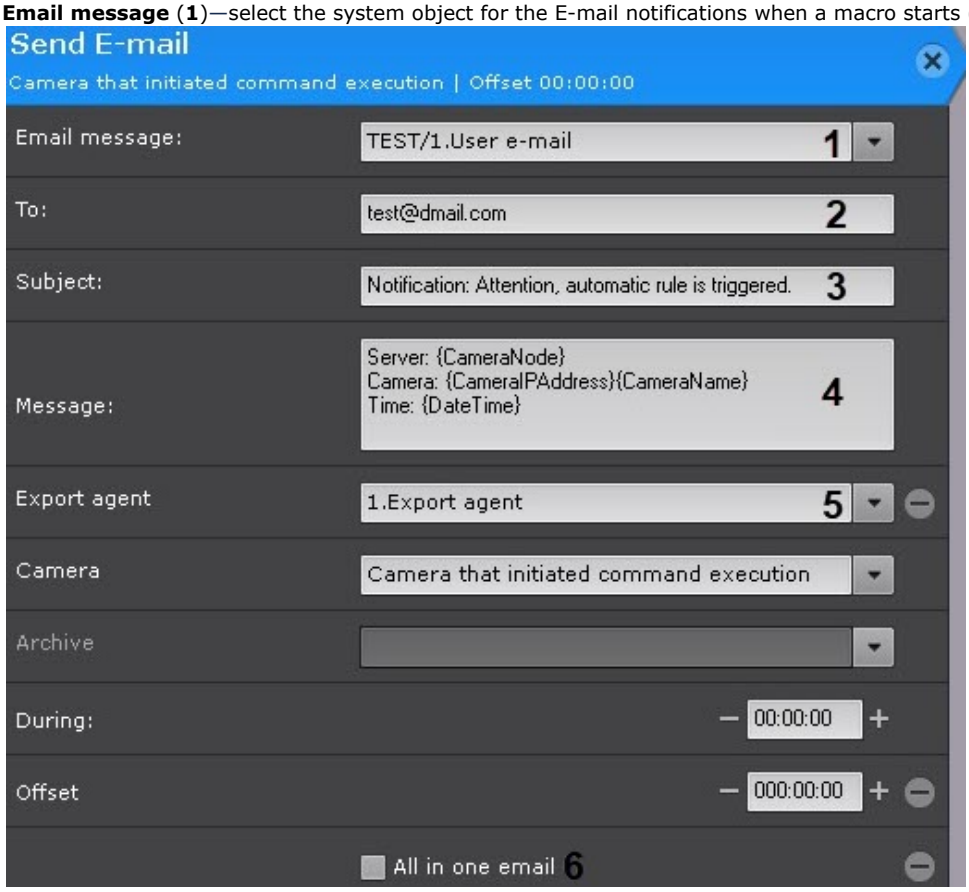
> **Note**
>
> The **OR** checkbox can be set only if the timer setting is not 00:00:00.
>
> An implicit selection of an event is allowed—**Last event for condition that initiated execution** (see Configuring filters for event-driven macros).
>
> For example, if the event that triggered the execution of the command was the **Start time of detection tool trigger** from any type of detection tools, then the end event will be the **End time of detection tool trigger** from the same tool.

E-mail notification

This action sends E-mails to the specified addresses. Exported videos or frames can be attached. You must configure the conditions to start a macro beforehand (see Configuring filters for event-driven macros).

To configure the E-mail notification, specify the following parameters:

1. **Email message** (**1**)—select the system object for the E-mail notifications when a macro starts (see The Email notifier object).



2. **To** (**2**)—enter the E-mail address to which you want to send the message.

> **Note**
>
> Multiple E-mail addresses can be specified. Separate them with comma (,) or semicolon (;).
>
> Notifications will also be sent to the addresses you specified when configuring the **E-mail** object (see The Email notifier object).

3. **Subject** (**3**)—the subject of the E-mail notification that will be sent when a macro starts.
4. **Message** (**4**)—enter the text that should be sent in the E-mail notification when a macro starts.

> **Note**
>
> You can use templates in the message (see Text templates in macros).

5. If necessary, you can attach exported video or a frame to your message. Click the button (**5**) to add and configure additional parameters. Configuration of these parameters is identical to configuration of export (see Starting export).

> **Note**
>
> If the **During** is not specified, the frame is sent. You can set the format of video and frame export in the Export agent settings (see Configuring Export agent).

6. If a macro is launched from a group of cameras (see Configuring start conditions for event-driven macros), you can send the frames from all cameras in the group in a single E-mail message. To do this, set the **All in one email** checkbox (**6**). If this checkbox is not set, there will be a separate E-mail for each camera in the group.

The Email notifier object

On this page:

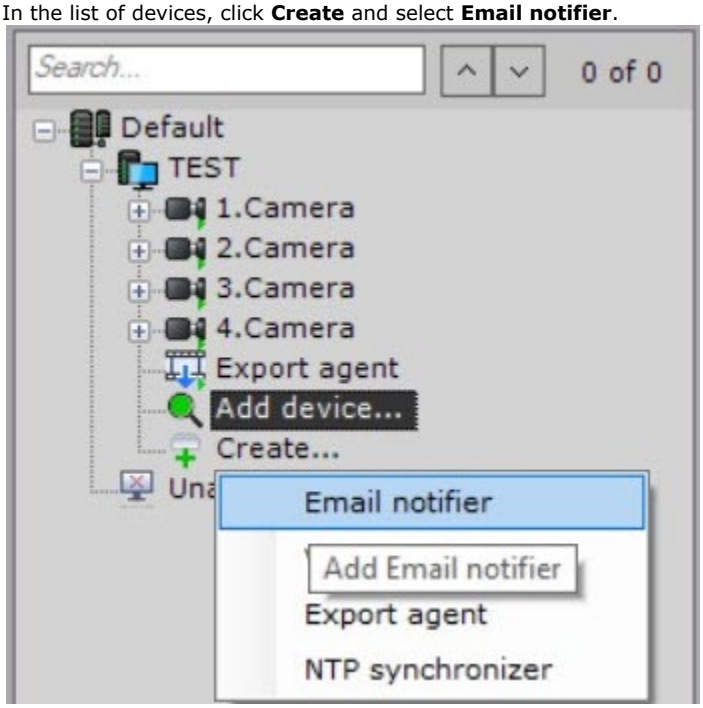
- Creating the Email notifier object
- Configuring the Email notifier object
- Checking Email notification

The **Email notifier** object is used to configure the electronic messages, which then can be sent to the user when a macro or an automatic rule is triggered.

Creating the Email notifier object

To create the **Email notifier** object, do the following:

1. In the list of devices, click **Create** and select **Email notifier**.



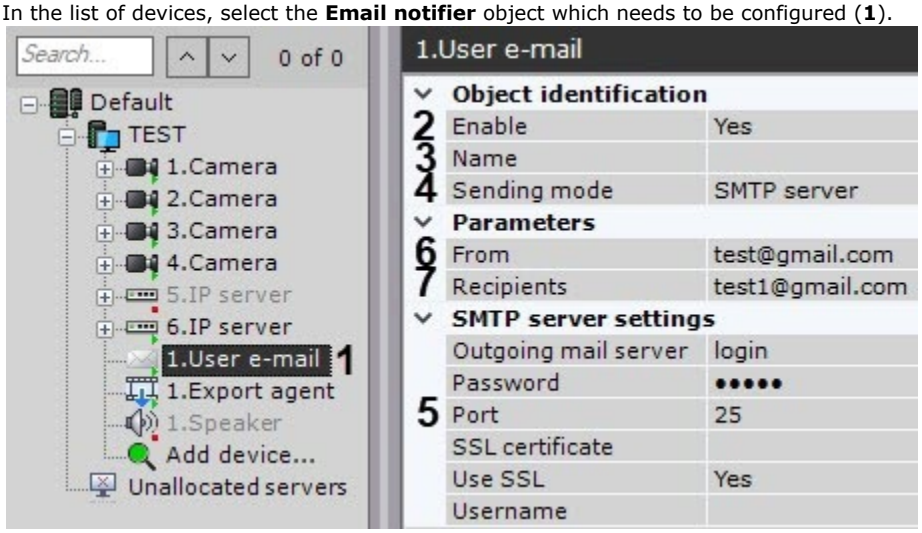
2. Click the **Apply** button.

The **E-mail notifier** object will appear in the list of devices.

Configuring the Email notifier object

To configure the **Email notifier** object, do the following:

1. In the list of devices, select the **Email notifier** object which needs to be configured (**1**).



2. Activate the **Email notifier** object by selecting **Yes** in the **Enable** list (**2**).
3. In the **Name** field (**3**) enter the required name of the **Email notifier** object.
4. Select the mode for sending the Email notifications: through *AxxonNet* or through the specified SMTP Server (**4**).

> **Attention!**
>
> To send notifications through *AxxonNet*, you should connect to it (see Configuring a domain in AxxonNet).
>
> *AxxonNet* has a limit of 10 messages a day.

> **Note**
>
> Message through *AxxonNet* will be sent within a minute.

5. Configure the SMTP Server, if this mode was selected (**5**):
   a. In the **Outgoing mail server** field, enter the outgoing Email SMTP Server.
   b. In the **Password** field, enter the password of the user account on the outgoing Email Server.
   c. In the **Port** field, enter the number of the port used by the outgoing Email Server.
   d. In the **SSL certificate** field, specify the path to the SSL certificate file, if you use this protocol. If no certificate is specified, but the **Use SSL** parameter is enabled, then the Email Server certificate will be used.
   e. If you need to use SSL-encrypted connection when connecting to the outgoing Email Server, select **Yes** from the **Use SSL** list.
   f. In the **Name** field, enter the name of the user account used to send messages on the outgoing Email Server.
6. In the **From** field, enter the Email address from which the messages will be sent (**6**).

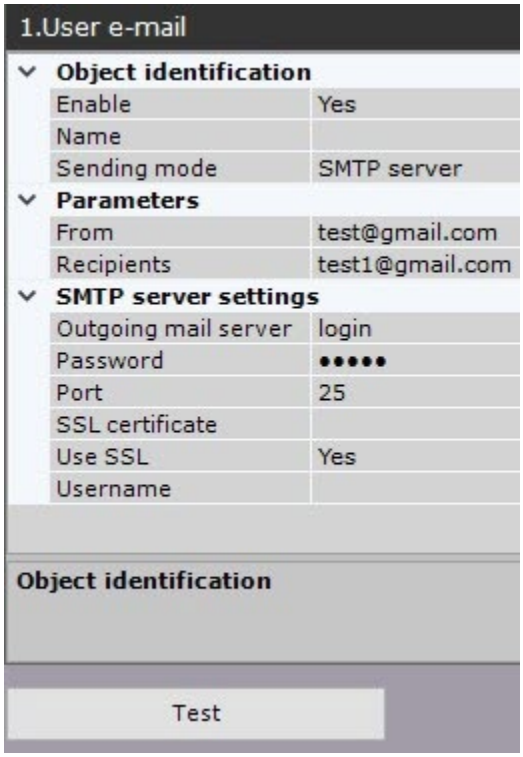
> **Attention!**
>
> When using email notification, Email Servers may disable the user account or deny authentication in some cases. We recommend you to disable all security parameters in your email account beforehand.

7. In the **Recipients** field (**7**), enter one or several Email addresses to which messages will be sent.
8. Click the **Apply** button.

Configuration of the **Email notifier** object is now complete.

Checking Email notification

To check the Email notification from the **Email notifier** object, send a test message by clicking the **Test** button.



When you do this, the following message will be sent to the Email address specified in the **Recipients** field (see Configuring the E-mail notifier object): "Test message".

Push notification

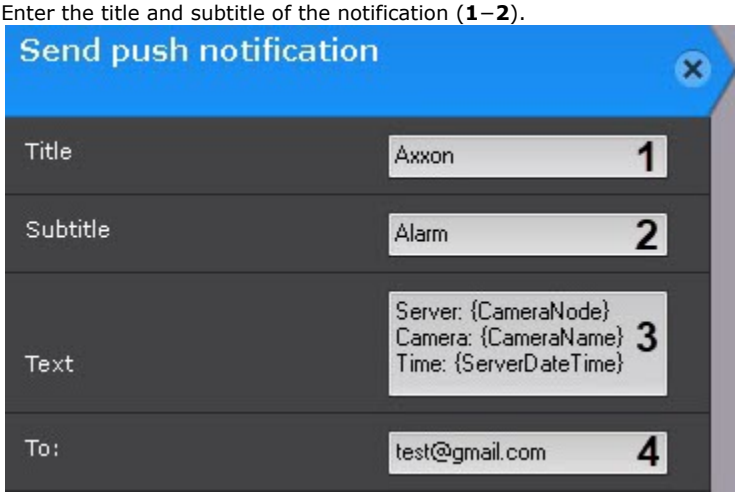
This action sends a push notification to the device with the *AxxonNet* app installed.

To run the action, make sure the following requirements are met:

- the Axxon-domain must be connected to *AxxonNet* (see Configuring a domain in AxxonNet);
- the person who is notified must log in with *AxxonNet* cloud credentials in the *AxxonNet* app.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Enter the title and subtitle of the notification (**1**–**2**).



3. Enter the main text of the notification (**3**). Text templates may be used (see Text templates in macros).
4. Enter the e-mail address of the user who will be notified (**4**). Only one address is allowed.

Telegram bot notification

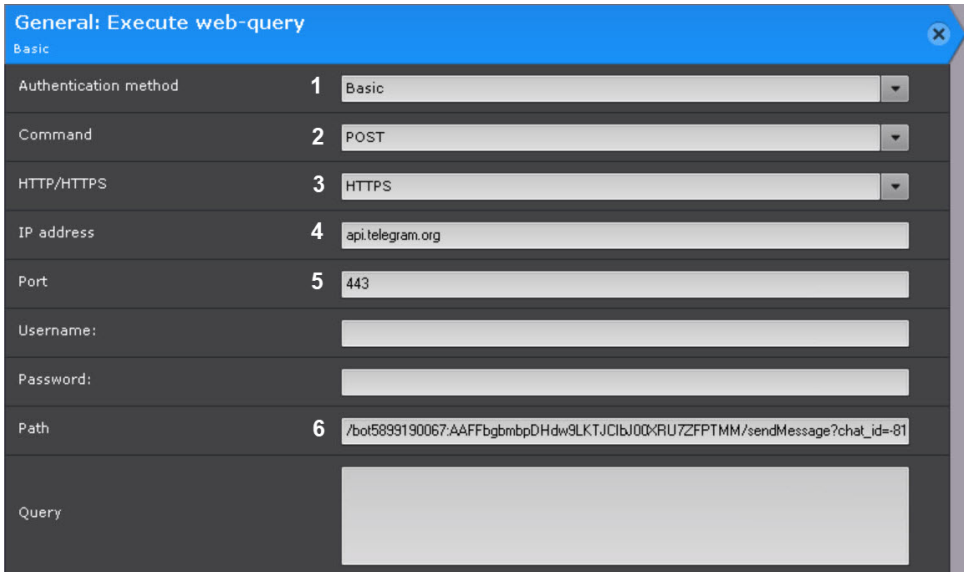
Axxon One allows you to send text notifications to Telegram chat when any event occurs from the objects registered in the *Axxon One* objects tree. Once configured, the notification sending is initiated by the *Axxon One* macro.

Before configuring notifications sending from *Axxon One* to Telegram, create a bot and a group chat with this bot in Telegram. For the distribution package and manuals on working with Telegram, see the developer's official website telegram.org.

> **Note**
>
> For the correct operation of Telegram bot and notification sending, the user who created the bot must have @username specified in Telegram.

To configure notification sending in Telegram bot, do the following:

1. Configure the conditions to start a macro (see Configuring start conditions for event-driven macros).
2. Select the **"General: Execute web-query"** action.
3. Select the authentication method: Basic or Digest (**1**). By default, the Basic authentication method is selected.



4. Select the query type (**2**). Four types are supported: POST, GET, PUT, DELETE. By default, the POST query type is selected.
5. Select the server protocol: HTTP or HTTPS (**3**). For the correct notifications sending, select the HTTPS protocol.
6. Enter the IP address of the server (**4**). The address of the Telegram server is api.telegram.org.
7. Enter the port of the server (**5**). The port of the Telegram server is 443.
8. Enter the path of the query (**6**). The path of the query should look like this: /bot<BOTToken>/sendMessage?chat_id=<ChatID>&&text=<Text>, where <BOTToken> is an ID of the bot in Telegram;

   > **Note**
   >
   > The ID is provided when you create the bot

   <ChatID> is the ID of the chat;

   > **Note**
   >
   > To learn the ID of the chat, add the @RawDataBot bot to the chat. After adding, the bot will send a message to the chat that will contain the result of the execution of the getUpdates function. Find ChatId in the message. Then remove the @RawDataBot bot from the chat.

   <Text> is a notification text. You can enter the set of US-ASCII characters (Latin characters and digits) in the notification text. For the notification text to display correctly with other characters and punctuation marks, you need to encode them. The encoding is described in the RFC 3986 standard and called URL-encoding, URLencoded, or percent-encoding. For example, a space character is encoded as %20.

When using the "**General: Execute web-query**" action, all fields for sending a web-query to the specified server can be filled in (see Executing a web query). However, the **Username, Password** and **Query** fields are not required for sending a notification via Telegram bot.

Starting an external program on Clients

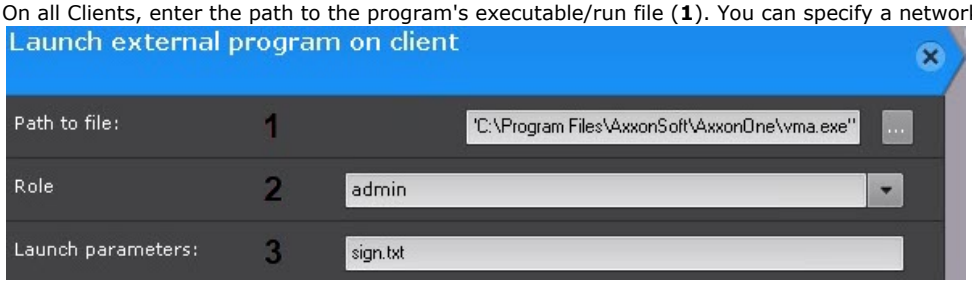
This starts an external program on your *Axxon One* client.

The external program is started on all Clients that are connected to the domain.

> **Attention!**
>
> The external program is not started on a computer that is an *Axxon One* Server, if the Client is not running on the computer when a macro is triggered.

To configure, do the following:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. On all Clients, enter the path to the program's executable/run file (**1**). You can specify a network path.



3. Select users of the (external) program (**2**).
4. You can also add command-line options (**3**). When you start an external program, its directory matches the one in which the executable file is located. If there is a file in the startup parameters and it is located in the directory with the program's executable file, you do not need to specify the path to it.

> **Attention!**
>
> To run the program, you need administrator permissions. You have to disable UAC (in Windows 10 OS, you need to edit the registry), or start *Axxon One* with administrator rights.

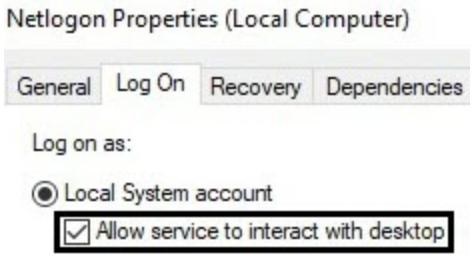
Starting an external program on Servers

This starts an external program on your Axxon domain.

> **Attention!**
>
> Any software containing a GUI is not recommended to be executed on the Server. If you encounter a problem launching interactive services, please refer to the Windows OS user manual.

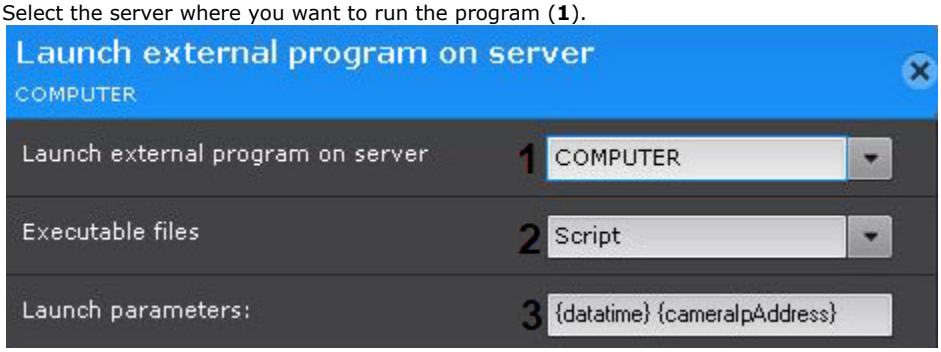
To configure, do the following:

1. Allow interaction of the server **NGP Host service** with the desktop: Start Control Panel Administrative Tools Services Net Logon Properties Log On.



> **Note**
>
> For **Failover server and client** installation type (see Installation), you have to allow the **NGP RaFT supervisor service** to interact with desktop.

2. Add to folder <Directory where *Axxon One* is installed>\UserScripts\ one or more .bat files with the application startup command.
   The command should include a path to the executable file. You can specify a network path and command-line options (see Starting an external program on Clients).
3. Select the server where you want to run the program (**1**).



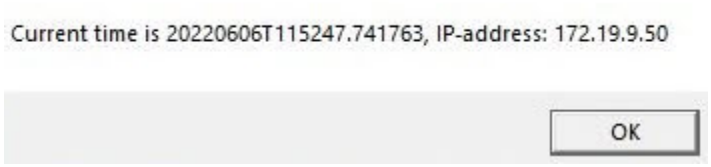
4. Select a .bat file with the run command (**2**).
5. Enter templates, if they were set via a .bat file (**3**).

Example 1: If you apply the following bat file:

```
SET "datatime=%1"
SET "cameraIpAddress=%2"

msg * Current time is %datatime%, IP-address: %cameraIpAddress%
```

executing the macro will lead to the following message:



Example 2: Exporting camera connection status events (offline/online) to a csv.bat file containing the following:

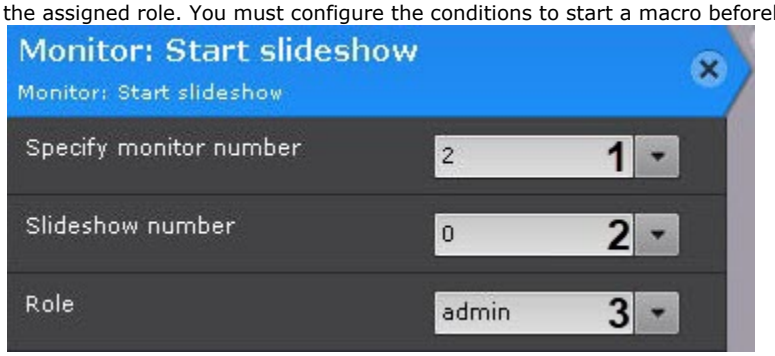
```
SELECT "timestamp"
    ,REGEXP_REPLACE("object_id", 'hosts/', '') as device,
    CASE
                                WHEN ("any_values"::json->>'state') = '4' THEN 'Signal Lost'
                                WHEN ("any_values"::json->>'state') = '3' THEN 'Signal Restored'
                                ELSE ''
        END as state
FROM public."t_json_event"
WHERE type = '0' AND ("any_values"::json->>'state'='3' OR "any_values"::json->>'state'='4') AND timestamp >=
'20200211T0000'
ORDER by timestamp DESC
```

Example 3: Exporting detection tools triggering events to a csv.bat file containing the following:

```
SELECT "timestamp",
        REGEXP_REPLACE("object_id", 'hosts/', '') as device,
        CASE
                                WHEN ("any_values"::json->>'phase') = '1' THEN 'Closed'
                                WHEN ("any_values"::json->>'phase') = '2' THEN 'Opened'
                                ELSE ''
        END as state
FROM public."t_json_event"
WHERE type = '1' AND timestamp >= '20200209T110000' AND "object_id" LIKE '%ray%'
ORDER by timestamp DESC
```

Start/stop slideshows of layouts

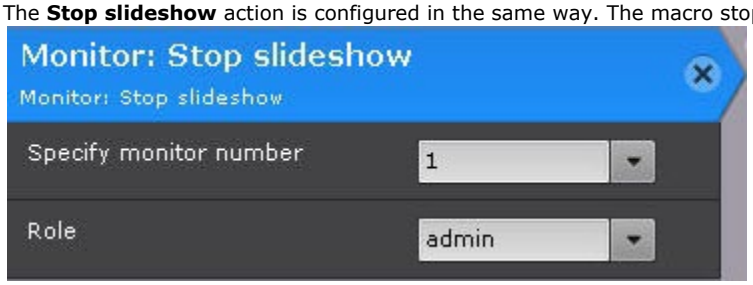
These actions start and stop a specific layout slideshow (see Selection and Slideshow of Layouts) on the selected operator monitor for the assigned role. You must configure the conditions to start a macro beforehand (see Configuring filters for event-driven macros).



To configure the **Start slideshow** action, set the following parameters:

1. Select the monitor number from the **Specify monitor number** drop-down list (**1**). If you select a dash (−) when selecting a monitor, the slideshow will run for the active monitor.
2. Select the number from the **Slideshow number** drop-down list (**2**). The list starts with a zero. For example, **Slideshow #1** in the **Layouts** interface will have the number 0.
3. Select the role for which the macro will function from the **Role** drop-down list (**3**). If you leave the **Role** field empty, the macro will function for all roles that have access to this rule.

The **Stop slideshow** action is configured in the same way. The macro stops the slideshow being played.



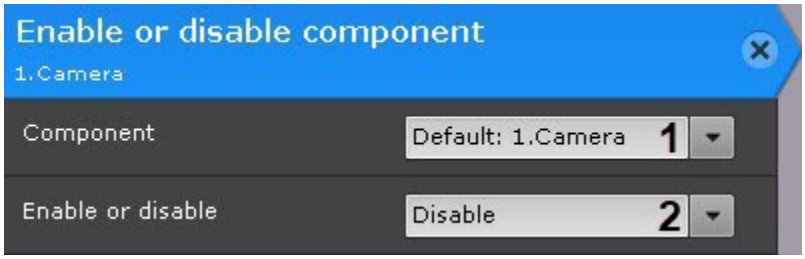
To stop the slideshow of the layouts, you can also select any video surveillance window by clicking the left mouse button. After restarting the Client, the slideshow resumes.

Enable/disable a component

This action enables or disables the selected camera, detection tool or input.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the required object (**1**).



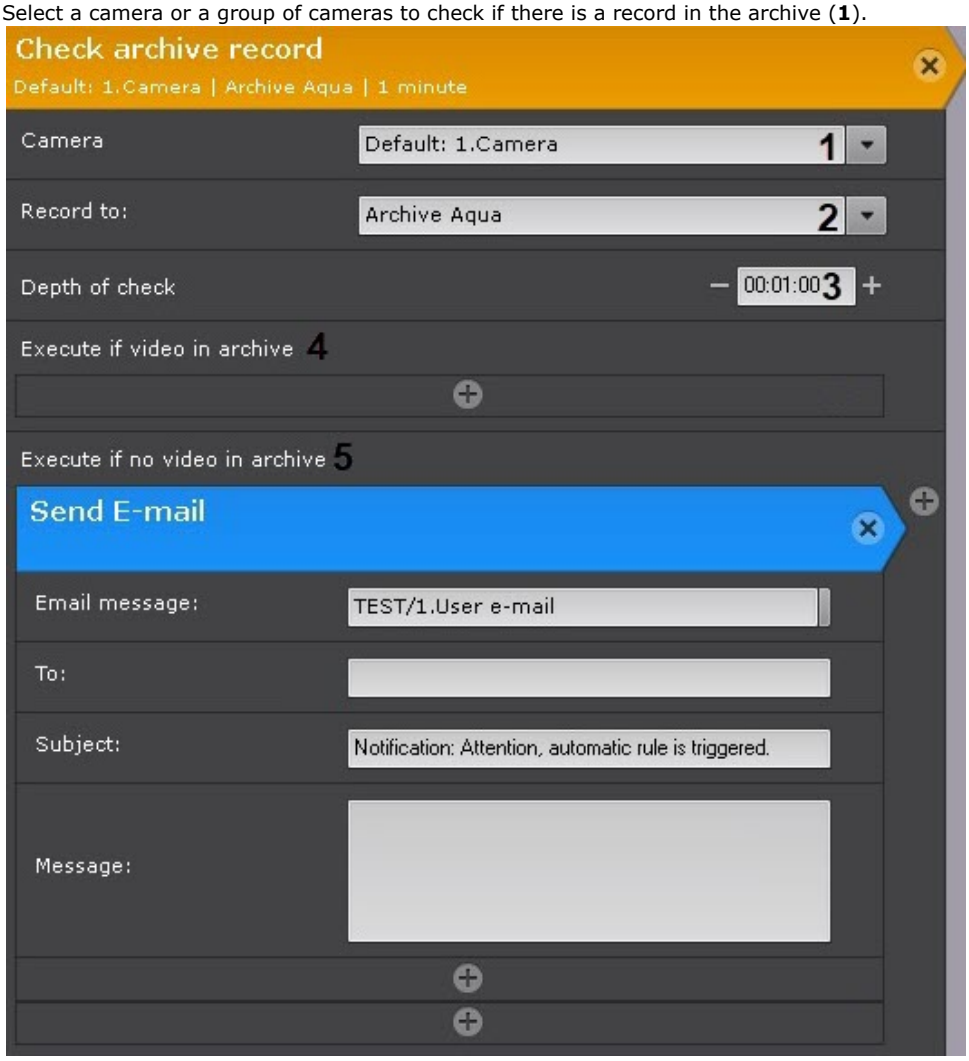
3. Select the required command (**2**).

Checking for archive video recordings

This action checks recorded video from a specific camera or group of cameras for the specified period.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a camera or a group of cameras to check if there is a record in the archive (**1**).



> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring start conditions for event-driven macros) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered the command, the action will not start.

3. Select an archive where you want to check if recorded video is available (**2**). If you leave the field empty, all recorded video in this camera archives will be checked.
4. Specify the depth of check (**3**). The check time period covers: [the time of the action start - (minus) the depth of the check; start time of the action].
5. Select an action if the archive record for the specified period is found (**4**).
6. Select an action if the archive records for the specified period are not found (**5**).

Note

If E-mail is selected as a reaction, then the target cameras will be indicated in the message (if a group of cameras was selected) for which there are no entries in the archive for the specified period.

You can also use two special purpose templates in the message:

- {failureRecordCheck}—failed check of a record in an archive (format: Server Name|Camera Name|Archive Name);
- {successRecordCheck}—successful check of a record in an archive (format: Server Name|Camera Name|Archive Name).

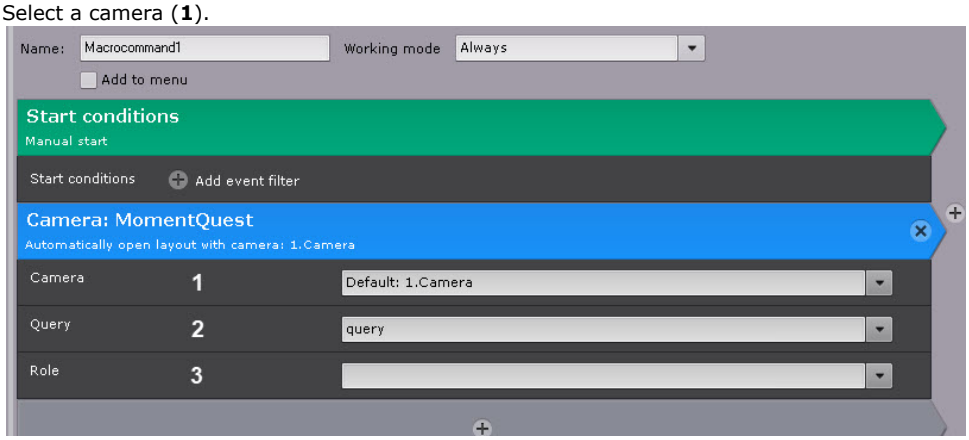
Attention! For the correct execution of the macro, synchronize the time across all Servers within the Axxon-domain.

Switching to MomentQuest search results in archive

This action allows you to open the results of a previously saved MomentQuest search in the archive.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select a camera (**1**).



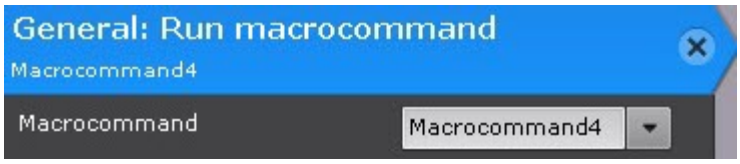
3. Select a previously saved search query (**2**, see Saving search queries).
4. Select a role for users of which this action must be performed (**3**).

Executing a macro

This action launches another macro.

To configure this action, do the following:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the necessary macro.



Attention!

This action launches only event-related macros.

Checking protected video records in the archive

This action checks if there are protected video records in the specified archive and performs the specified actions if they are present or absent, and participates in the mechanism of protecting video records from FIFO overwriting (see Protecting video footage from FIFO overwriting). To configure this action, see Setting up a macro for automatic copying of protected records.

Executing a web query

This action sends a web query to a specified Server.

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros).
2. Select the authentication method: Basic or Digest (**1**).



3. Select query type (**2**). Four types are available: POST, GET, PUT, DELETE.
4. Select HTTP or HTTPS Server protocol (**3**).
5. Enter the IP address of the Server (**4**).
6. Enter the port number of the Server (**5**).
7. Enter the username (**6**) and password (**7**) to be used for authorization on the Server.
8. Enter query path (**8**).
9. If necessary, enter a query body (**9**).

> **Note**
>
> You can use templates to build a query body (see Text templates in macros).

Text templates in macros

You can use message templates in commands (see E–mail notification, Executing a Web-query) that involve sending notifications:

- {cameraNode} – Server name;
- {eventNode} – Server name (used if the macro launching condition is not linked to a particular camera);
- {cameraName} – name and short name of the camera that initiated the macro;
- {cameraLabel} – just the camera's name;
- {cameraIpAddress} – camera's IP address;
- {cameraId} – camera's ID;
- {cameraRef} – the VIDEOSOURCEID identifier;
- {list} – name of the List of Facial Templates or ANPR list;
- {plate} – recognized vehicle number;
- {plateDirection} – the direction of movement of the vehicle in the frame;

> **Note**
>
> Possible values:
>
> **1** – from top to bottom;
>
> **2** – from bottom to top.

- {name} – name of the recognized person from Lists of Facial Templates;
- {age} – age of the recognized individual;
- {gender} – gender of the recognized individual;

> **Attention!**
>
> The {age} and {gender} templates can be applied when the following conditions are met:
>
> 1. The **Gender and Age** parameter is activated in facial detection tool settings (see Configuring the Face Detection TV).
> 2. The **Face Appeared: Specified Triggering** event is selected as a launch condition for this macro (s).

- {appearedTime} – UTC time of object detection;
- {dateTime} – date and UTC time of triggering the macro in ISO format;
- {serverDateTime} – local Server time of triggering the macro in ISO format;
- {rectangles} – coordinates and size of the object that triggered the detection tool;
- statistics templates:
  - {cpuUsage} – percentage of CPU load on a Server;
  - {netUsage} – percentage of used network bandwidth on a Server;
  - {memoryUsage} – percentage of used RAM on a Server;
  - {diskUsage} – percentage of disk usage;
  - {archiveUsage} – percentage of Video Footage usage.

> **Attention!**
>
> You can apply statistics templates only if you launch a macro by a corresponding statistical condition (see Trig gering macros by statistical data).

> **Note**
>
> Templates allow {} and %%. For example, %cameraId%.

Note

Date/time templates (such as dateTime, serverDateTime, appearedTime and serverAppearedTime) offer an extended input option which allows you to set date and time in arbitrary format. A format description parameter must be contained within a pair of @ symbols.

Here's an example: {dateTime@%Y–%m–%d %H:%M:%S@}. In this case, the actual format is presented as 2020–10–04 18:43:23.

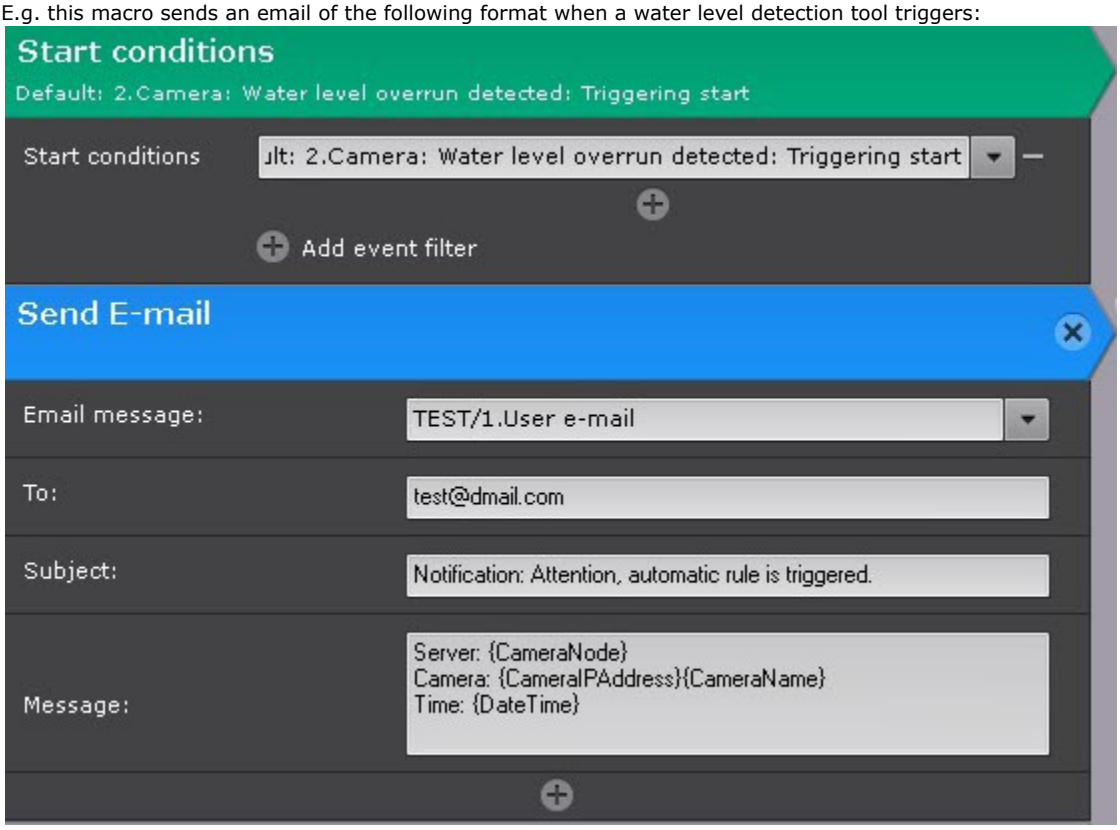
Available parameters:

Parameter	Description
%a	Abbreviation for the day of the week
%A	Full name of the day of the week
%b	Abbreviation for the month
%B	Full name of the month
%y	Last two digits of the year
%Y	Full number of the year
%m	Month of the year
%d	Day of the month
%H	Hour in 24h format
%M	Minute as a decimal number
%S	Second as a decimal number
%F	Fractions of second

Combined parameters:

Parameter	Description
%D	Equivalent to %m/%d/%y
%T	Equivalent to %H:%M:%S

E.g. this macro sends an email of the following format when a water level detection tool triggers:



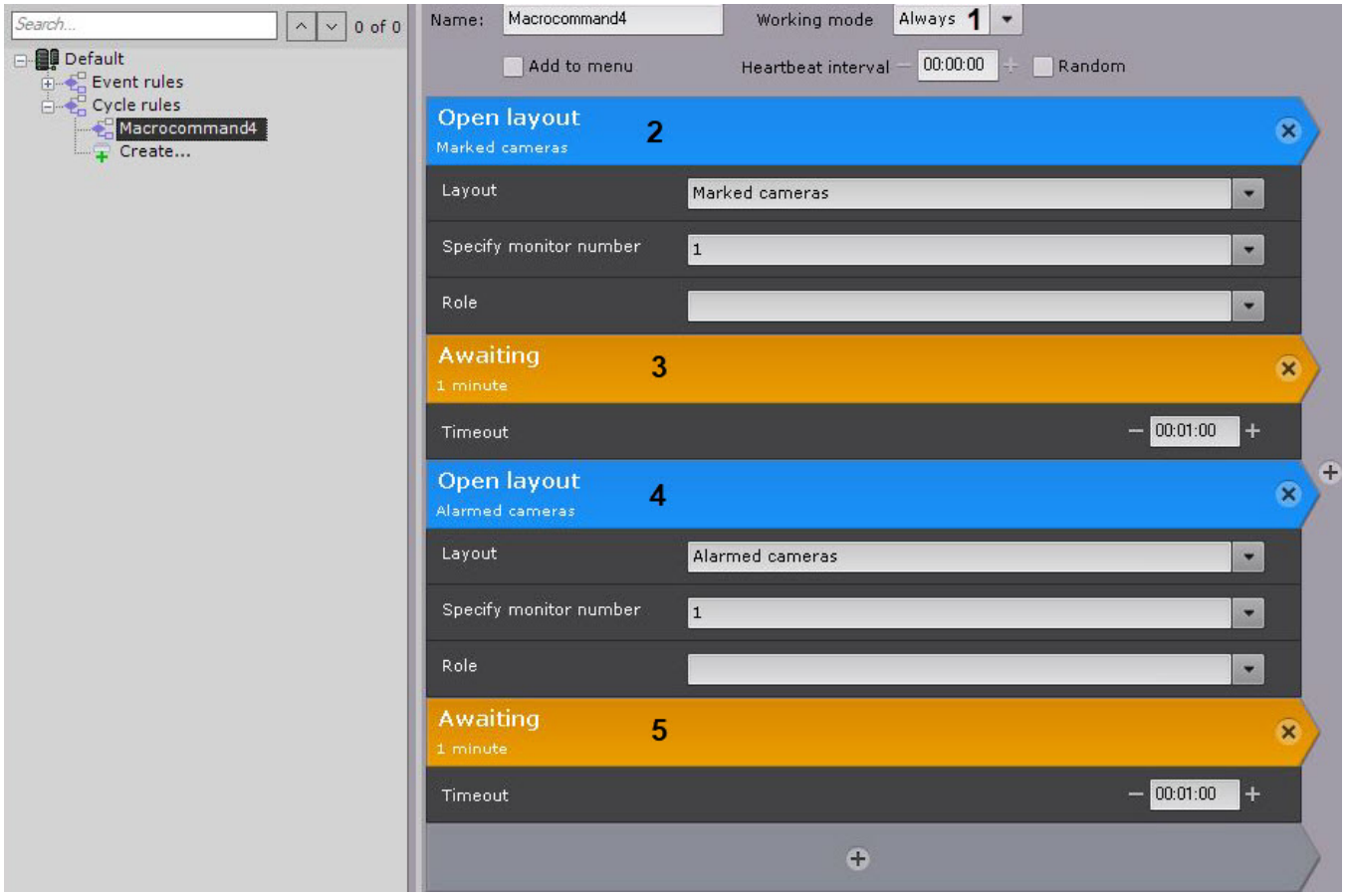

```
Subject: Notification: Attention, water level detection is triggered.

Server: Server1
Camera: 10.0.11.36 34.Camera
Time: 20190812T085517.926430
```

Cyclical macros

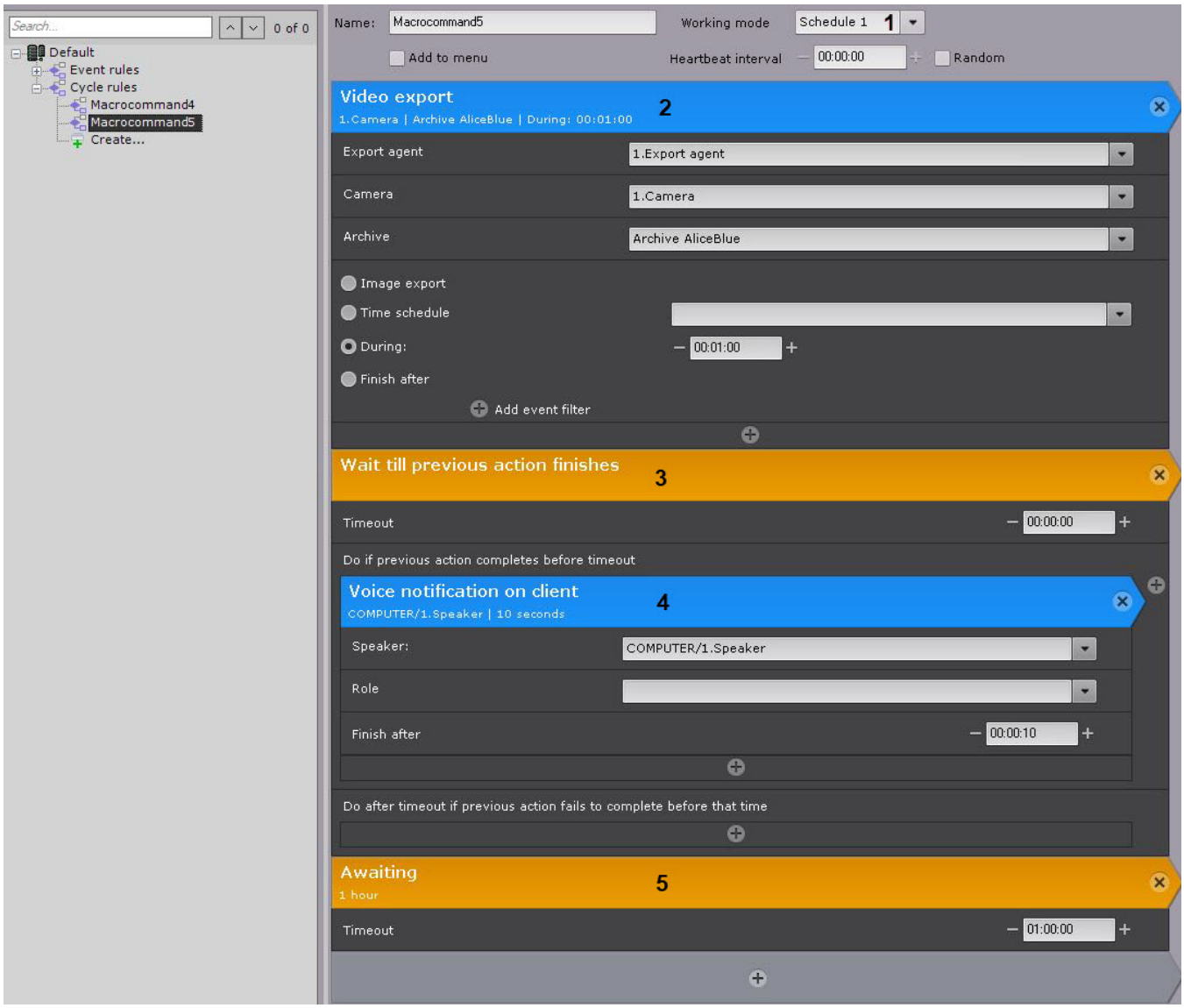
> **Attention!**
>
> If you do not have the **Wait** command in a cyclic macro, the time-out between cycles is 1 second.

Example 1. This macro runs continuously (**1**), starting from the moment that you saved it.



The cycle consists of alternating layouts with marked cameras (**2**) and layouts with alarmed cameras (**4**). interval – 1 minute (**3**, **5**).

Example 2. This macro runs continuously within the time schedule 1 (**1**).



Every hour (**5**) video from camera 1 is exported (**2**). After the export is completed (**3**), an audio alert is sounded (**4**).

Wait for timeout

Wait till previous action finishes

Configuring user permissions

On this page:

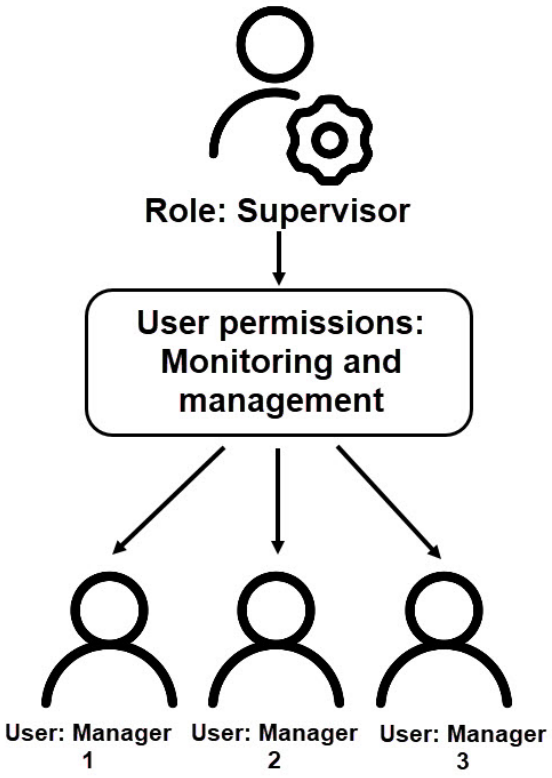
- General information about Roles, Users, and Permissions
- Common algorithm for setting permissions
- Types of permissions to access hardware, archives and macros

General information about Roles, Users, and Permissions

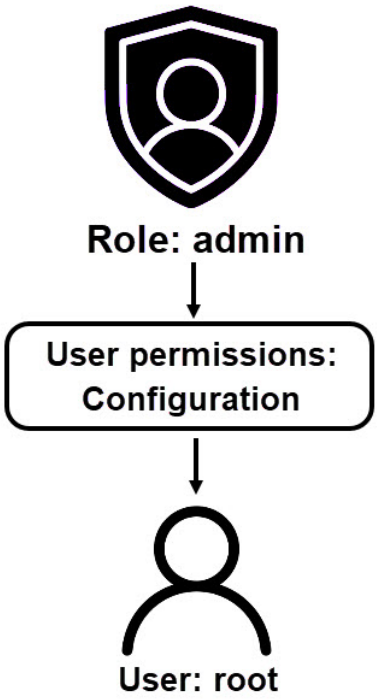
In *Axxon One*, every user has permissions based on his role.

Term	Description
Role	Defines a set of permissions for users in *Axxon One*. Several users can have the same role in *Axxon One*.
User	An account in *Axxon One*. Each user can be assigned to one or more roles. In this case, the user's permissions are summed up from all the roles which the user has, i.e., the permissions with the widest access to configuring the components of *Axxon One* are selected from all user roles. The user logs into the system using a unique username and password.
Permissions	Determine what actions a user can perform in the system. These actions may include administering, managing and monitoring the components of a video surveillance system. Permissions are configured along with roles and are granted to users assigned to the corresponding roles.

For example, three **Manager** users are assigned the **Supervisor** role. Users have permissions to monitor and manage video surveillance system components. User permissions are configured when creating a role.



By default, there is one role (**admin**) and one user (**root**). The **root** user belongs to the **admin** role and has rights to configure all components of the video surveillance system. To add a user with individual permissions, create a new role with the necessary permissions and then create a new user account.



Note

Only **admin** users can create other **admin** role users.

Common algorithm for setting permissions

To register users with individual permissions, it is necessary to create a new role with these permissions and a new user account. To do this:

1. Create a new role on the **Users** tab (see Creating and configuring roles).
2. Configure permissions for the new role.
3. Register new users for the role (see Creating local users).
4. Enter additional information about users.

There are two types of users: local (stored in the Server database) and LDAP (see Connecting LDAP users).

To enable LDAP users, you must configure access to LDAP catalogs.

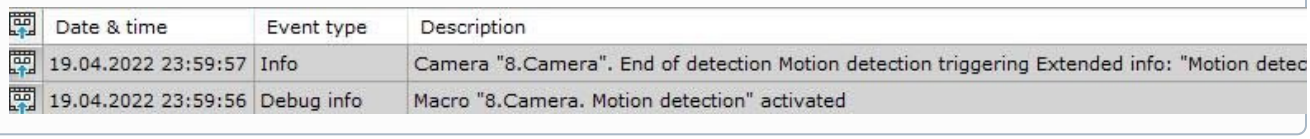
The actions of all system users are recorded in the system log (see The System Log).

Note

The following user actions are logged:

- login and log out of the Client;
- unsuccessful login attempt;
- adding, editing and removing hardware settings, archive or detectors;
- creating, editing and removing macros;
- adding, editing and removing user permissions;
- alarm initiation triggered by video camera;
- arming and disarming the video camera;
- controlling a PTZ camera;
- creating and editing comments;
- exporting frames and video recordings.

In all user-specific events, the user IP address is indicated.



Date & time	Event type	Description
19.04.2022 23:59:57	Info	Camera "8.Camera". End of detection Motion detection triggering Extended info: "Motion detec
19.04.2022 23:59:56	Debug info	Macro "8.Camera. Motion detection" activated

Types of permissions to access hardware, archives and macros

In *Axxon One*, it is possible to set user permissions both for a specific device (object) and for a group of devices. Specifics of object and group permission types are described in the table below.

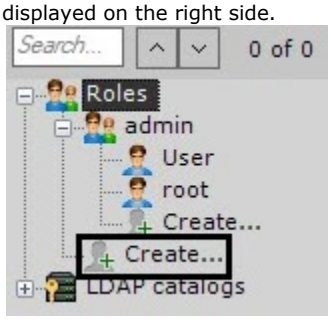
User permission type	**Usage**	**Priority**
Object	Configuring access to a specific device, archive or macro in the system	Highest
Group	Configuring access to all cameras added to a group (see Creating a Group object).	Priority below Object permissions **Note** • If the camera belongs to several groups with different access levels assigned to them, the user permissions with the highest access level are used. • If the camera belongs to a child group, then the permissions defined for the child group will take precedence when determining access to the camera
Default	Configuring access to all devices, archives or macros that will be created in the system. If Group or Object rights are not assigned to the device after its creation, then the default permissions are applied.	Priority below Group permissions

Creating and configuring roles

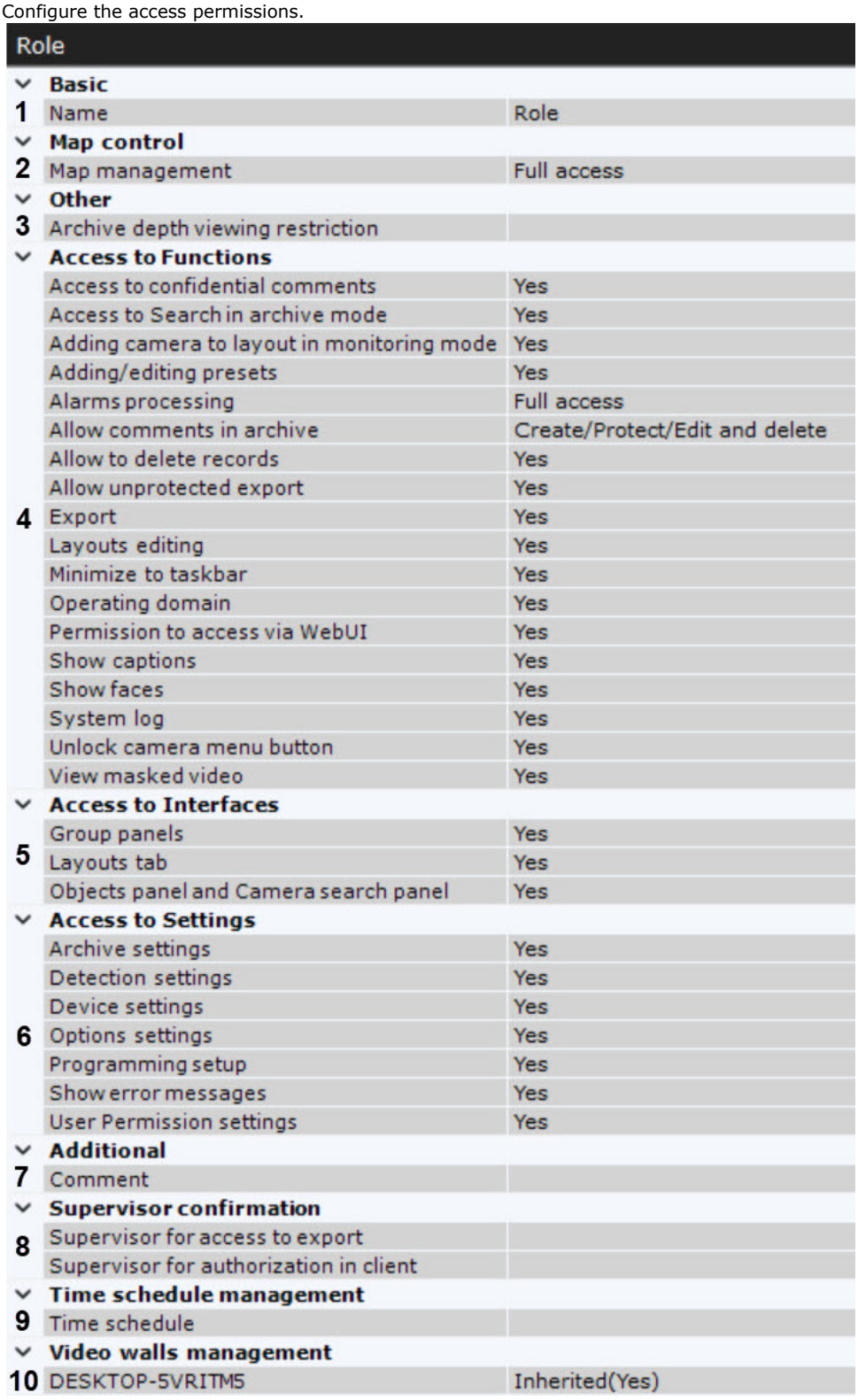
A role is intended for assigning a group of users individual rights and permissions for administration, management and/or monitoring of individual components of *Axxon One*.

To create a new role, do the following:

1. At the end of the list of system roles, click the **Create** link. The new role will be added to the system, with its properties displayed on the right side.

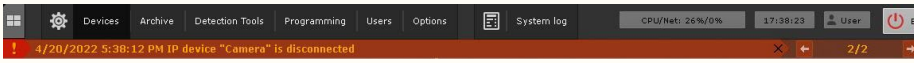


2. Configure the access permissions.



Parameters	Access level	Description
Basic		
Name	–	Enter a name for the role (**1**)
Map control		Select the access level to the maps for users with the current role (**2**)

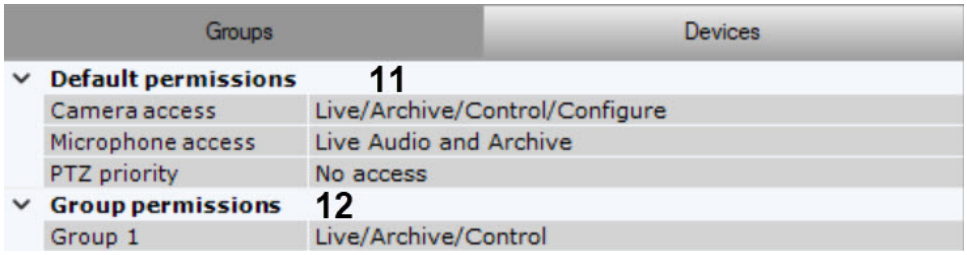
Map management	**No access**	Users cannot view maps
	View only	Users can only view maps
	View /move /scale	Users can views, move, and scale maps
	Full access	All operations with map are available
Other		
Archive depth viewing restriction	**–**	If you need to limit the access of users of a given role to all system archives, you can specify the a
Access to Functions		Set access permissions to *Axxon One* functions (**4**)
Access to confidential comments	**Yes**	Add and view confidential comments
	No	
Access to Search in archive mode	**Yes**	Archive search (see Video surveillance in archive search mode)
	No	
Adding camera to layout in monitoring mode	**Yes**	Add a camera to a layout in live video mode (see Adding cameras to cells)
	No	
Adding /editing presets	**Yes**	Add and edit presets for PTZ cameras (see Selecting a preset)
	No	
Alarms processing	**–**	Alarms management (see Video surveillance in alarm management mode)
	No access	Users have no access to alarm videos
	View only	Users can view alarm videos, but they can't assess alarms
	Full access	Users can view alarm videos and assess alarms
Allow comments in archive	**–**	Create comments in the archive (see Operator comments) and protected records (see Protecting v
	No access	No comments allowed
	Create	Add comments to the archive
	Create /Protect	Add comments to the archive, create protected records
	Create /Protect / Edit and delete	Add comments to the archive, create and edit protected records
Allow to delete records	**Yes**	Remove video recordings from the archive (see Delete a part of an archive)
	No	
Allow	**Yes**	

unprotected export	**No**	Export frames and video recordings without password protection (see Frame export, Standard vid g frames and video recordings)
Export	**Yes**	Export frames and video recordings (see Exporting frames and video recordings)
	No	
Layouts editing	**Yes**	Edit layouts (see Editing layouts)
	No	
Minimize to taskbar	**Yes**	Minimize the Client to the tray (see Interface of the Axxon One Software Package)
	No	
Operating domain	**Yes**	Manage Axxon domain (see Operations with domains)
	No	
Permissions to access via WebUI	**Yes**	Access to the Web-Server (see Working with Axxon One through the Web-Client)
	No	
Show captions	**Yes**	Display captions (see Viewing titles from POS terminals)
	No	
Show faces	**Yes**	Showing faces (see Masking faces)
	No	
System log	**Yes**	View the system log (see The System Log)
	No	
Unlock camera menu button	**Yes**	Context menu of a video camera (see Viewing Tile Context Menu)
	No	
View masked video	**Yes**	View masked video (see Setting up privacy masking in Video Footage, Configuring the People mas
	No	
Access to Interfaces		Configure the access permissions to the interfaces (**5**)
Group panels	**Yes**	Configure the access permissions to video camera groups in the **Hardware** tab and to the video c
	No	
Layouts tab	**Yes**	Configure the access permissions to the **Layouts** tab. This parameter applies to both the Client ar
	No	
Objects panel and Camera search panel	**Yes**	Configure the access permissions to the Objects panel (see Objects Panel) and the Camera search
	No	
Access to Settings		
Archive settings	**Yes**	Configure the access permissions to the **Settings** tabs and to the system error messages (**6**).
	No	**Attention!** • Error messages are displayed in real-time in the **Layouts** interface.  • If you set the **User Permission settings** parameter to **Device access rights only**, a connected devices. • If the **Programming setup** is not available for the user role, the user will not be able • Critical error messages in the system are displayed regardless of the **Show error mes**
Detection settings	**Yes**	
	No	
Device settings	**Yes**	
	No	
Options settings	**Yes**	
	No	

Programming settings	**Yes**	
	No	
Show error messages	**Yes**	
	No	
User Permission settings	**Yes**	
	No	
Additional		
Comment	**–**	Specify additional information about the user, if necessary (**7**). If no value is specified, users can
Supervisor confirmation		Set the parameters to apply the four-eye principle (**8**)
Supervisor for acccess to export	**–**	If the administrator has to confirm the launch of export for users of this role (see Exporting frame
Supervisor for authorization in client	**–**	If the administrator has to confirm the login of users of this role (see Starting the Axxon One Clier
Time schedule management		
Time schedule	**–**	If you need to grant the users in this role permissions only for a certain period of time, select a tir outside of the selected time schedule
Video walls management		
Server	**Yes**	Configure the rights to manage the connected Clients' monitors by setting permissions for each Se of a particular Server can manage monitors of any Client connected to that Server
	No	

3. On the **Groups** tab, configure the default permissions (**11**, see Configuring user permissions).

> **Note**
>
> When you create a new role, you cannot go to another tab until the role is saved. If you change any access permissions on any tab, you cannot go to another tab until the settings are saved.



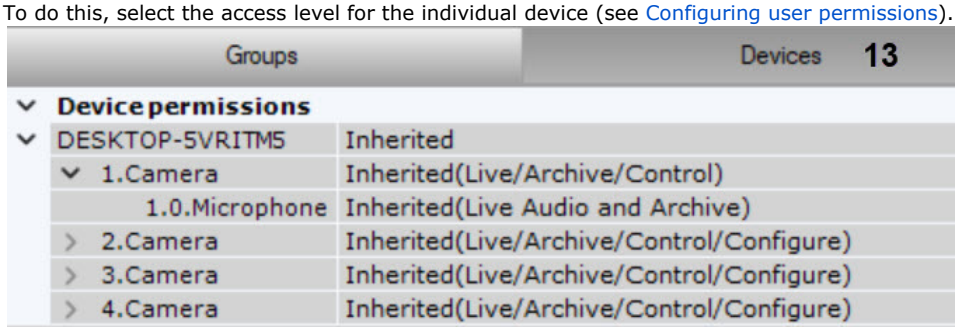
Device	Access level	Description
Default permissions		Configure the default permissions to devices
Camera access	**No access**	No access to the device
	Archive only	User can view only the archive
	Live in Armed mode	User can view video from the camera only when the camera is armed
	Live	User can view live video from the camera. Other functions and device configuration are not available
	Live/Archive	User can view live and recorded video from the camera. User cannot arm/disarm /configure the camera

	Live/Archive /Control	All functions available. User cannot configure the device
	Live/Archive /Control /Configure	All functions and device configuration available
Microphone access	**No access**	User cannot listen to live audio from the camera. User cannot listen to audio in the archive. Audio recording to an exported file is not available
	Live Audio	User can listen to live audio from the camera (the microphone must be turned on). User cannot listen to audio in the archive
	Live Audio and Archive	All functions are available
PTZ priority	**No access**	User cannot control the PTZ device
	Minimum level	User can control the PTZ device with the corresponding priority (see Controlling a PTZ Camera)
	Low level	
	Medium level	
	High level	
	Maximum level	

4. On the **Groups** tab, configure the group permissions if there are camera groups (**12**, see Configuring video camera groups).

Device	Access level	Description
Group permissions		Configure group access permissions to cameras (see Configuring user permissions)
Camera group	**Inherited**	Access permissions are inherited from the **"Default permissions"** tab **Camera access** (see the previous step)
	No access	No access to the device
	Archive only	User can view only the archive
	Live in Armed mode	User can view video from the camera only when the camera is armed
	Live	User can view live video from the camera. Other functions and device configuration are not available
	Live/Archive	User can view live and recorded video from the camera. User cannot arm/disarm /configure the camera
	Live/Archive/Control	All functions available. User cannot configure the device
	Live/Archive/Control /Configure	All functions and device configuration available

5. If necessary, configure the access permissions to a specific device (the **Devices** tab, **13**).
To do this, select the access level for the individual device (see Configuring user permissions).



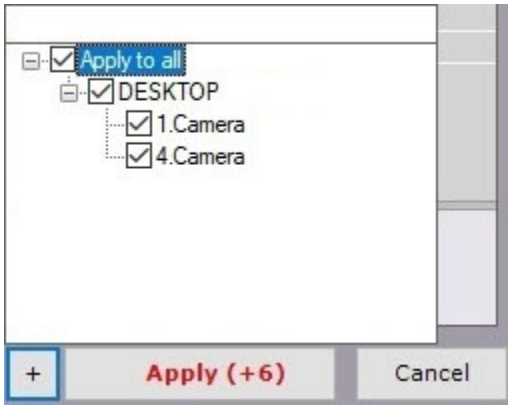
Access level	Device	Access level to device
Inherited	**Camera**	Access levels are inherited from the **Groups** tab **"Default permissions"** or from the group permissions

	Microphone	Access levels are inherited from the **Groups** tab **"Default permissions"**
	PTZ	
Archive only	**Camera**	Archive only
	Microphone	Live audio and archive
	PTZ	Medium level
Live in Armed mode	**Camera**	View in armed mode
	Microphone	Live audio
	PTZ	Medium level
Live	**Camera**	View live video
	Microphone	Live audio
	PTZ	Medium level
Live/Archive	**Camera**	View live video and archive
	Microphone	Live audio and archive
	PTZ	Medium level
Live/Archive/Control	**Camera**	All functions, configuration isn't available
	Microphone	Live audio and archive
	PTZ	Medium level
Live/Archive/Control /Configure	**Camera**	All functions, configuration is available
	Microphone	Live audio and archive
	PTZ	Maximum level

You can specify the access level to an individual camera and extend it to other cameras. To do it, do the following:

a. Select the access level to a camera from a drop-down list on the **Devices** tab.

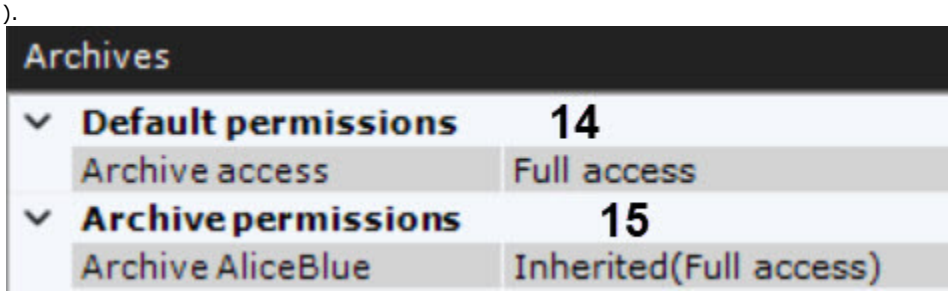
b. Click the + button and select the cameras to which you want to specify the same access level.



c. Click the **Apply** button.
As a result, the the specified access level will be extended to the selected cameras.
To quickly select multiple cameras, hold down the **Shift** key, select the first and last camera to which you want to specify the same access level. The checkbox will set for all selected cameras when you select any of them.

> **Note**
>
> Similarly, you can extend the access levels to microphones, PTZ devices and archives.

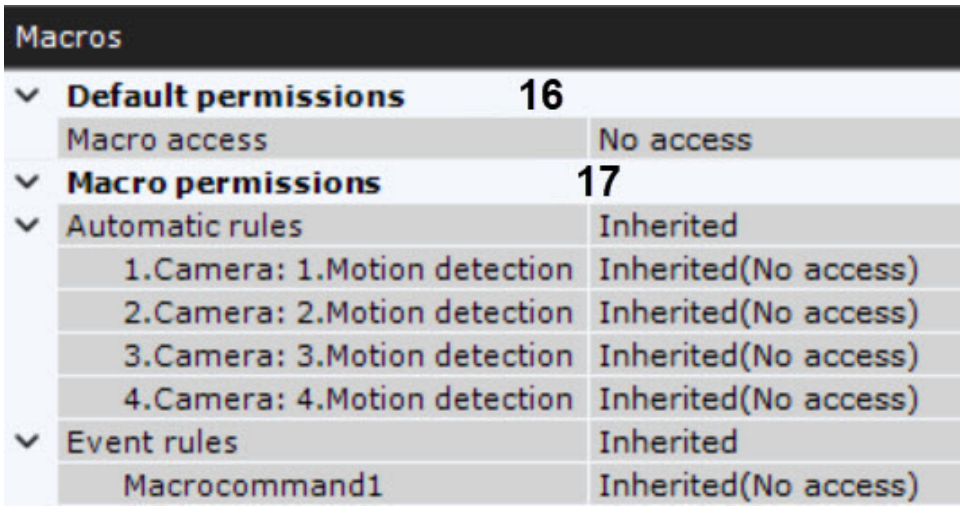
6. Configure the access permissions to domain archives. You can set the permissions to all archives (**14**) or to a specific archive (**1**).



Device	Access level	Description
Default permissions		Configure the default access permissions to the archive (see Configuring user permissions)
Archive access	**No access**	No access to this archive
	Full access	Full access to the archive
Archive permissions		Configure the permissions to a specific archive (see Configuring user permissions)
Archive	**Inherited**	Access level is inherited from the **Default permissions** tab
	No access	No access to this archive
	Full access	Full access to the archive

7. Set the possibility to manually run all or some macros (see Configuring macros) from the **Layouts** interface by selecting the corresponding access level.

> **Attention!**
>
> Users outside the **admin** group can create macros, if they have the permissions to create them. They cannot use them until they have the permissions to use them.



Macro type	Access level	Description

Default permissions		Configure the default permissions to macros (**16**, see Configuring user permissions)
Macro access	**No access**	No access to macros
	Full access	Full access to macros
Macro permissions		Configure the access permissions to a specific macro (**17**, see Configuring user permissions)
Automatic rules	**Inherited**	Access level is inherited from the **Default permissions** tab
	No access	No access to macros
	Full access	Full access to macros
Event rules	**Inherited**	Access level is inherited from the **Default permissions** tab
	No access	No access to macros
	Full access	Full access to macros
Cycle rules	**Inherited**	Access level is inherited from the **Default permissions** tab
	No access	No access to macros
	Full access	Full access to macros

8. Click the **Apply** button to save the role.

The new role has been created.

You can copy a role. To do it, do the following:

1. Select the role to copy.
2. Click the **Create** button.

A new role will be created with the same parameters as the selected role.

> **Note**
>
> To create an empty user role with no parameters specified, select the **Roles** common group, and click the **Create** button.

To delete a role, do the following:

1. Select the role to delete.
2. Click the **Delete** button.

> **Note**
>
> You cannot delete a role if the user who is logged in belongs to that role.

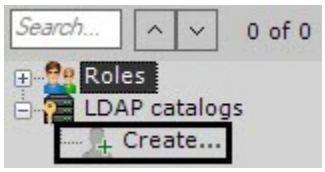
3. Click the **Apply** button to save the changes.

The role has been deleted. All users who belong to this role will also be deleted.

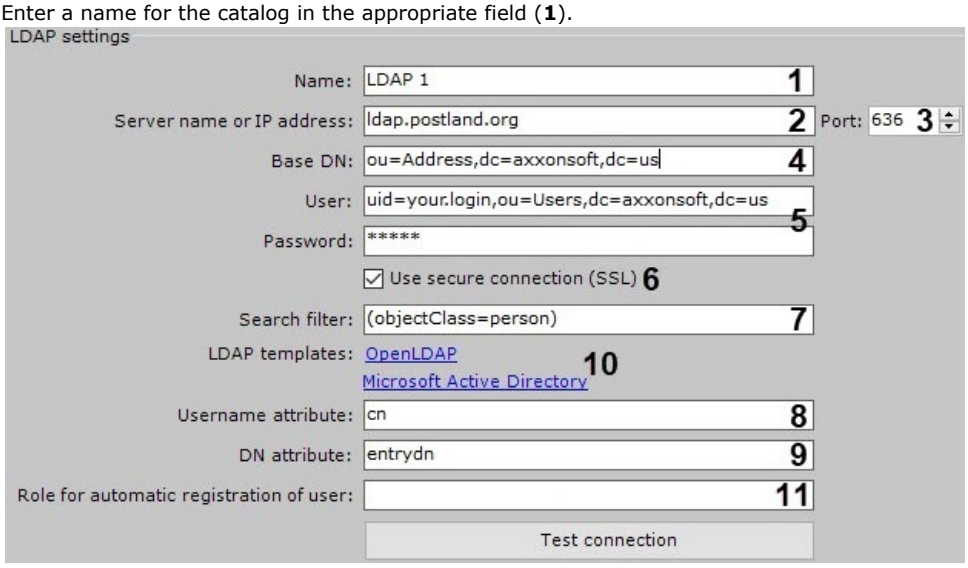
Connecting to an LDAP catalog

To connect to an LDAP catalog:

1. In the **LDAP catalogs** group, click **Create...**.



   An **LDAP** object is added in the system. On the right, a panel displays configuration settings for the **LDAP** catalog.
2. Enter a name for the catalog in the appropriate field (**1**).



3. Enter the address of the LDAP catalog server (**2**) and port (**3**).
4. In the **Base DN** field, enter the Distinguished Name of the branch from which to start search (**4**).

> **Attention!**
>
> If LDAP users are located in multiple directories with a tree-like structure, you cannot establish instant synchronization across all users.
>
> To synchronize each user group within a DN branch, you have to specify the path to the corresponding directory.
>
> For example, LDAP contains a directory **Employees** including subdirectories **Managers**, **Cashiers** and **Salesmen.**
>
> DN branches for synchronizing users within **Managers** directory: ou=Managers,ou=Employees,dc=example,dc=com.
>
> DN branches for synchronizing users within **Cashiers** directory: ou=Cashiers,ou=Employees,dc=example,dc=com.
>
> DN branches for synchronizing users within **Salesmen** directory: ou=Salesmen,ou=Employees,dc=example,dc=com.

5. Enter the name of a user who has write access to the base DN, in LDAP format (RDN + DN) with password (**5**).
6. If encryption (SSL) is required for connecting to the LDAP server, select the corresponding check box (**6**).
7. In the **Search filter** field, enter a string for filtering catalog entries (**7**).

> **Attention!**
>
> To upload users by groups, not by directories, you should use the Member Of filter attribute. For example:
>
> `(&(objectClass=user)(memberof=CN=YourGroup,OU=Users,DC=YourDomain,DC=com).`

8. In the **Username attribute** field, enter the field from which the user's login is obtained (**8**).

> **Note**
>
> To search users by attribute **sAMAccountName**, enter their names in small letters – **samaccountname**.

9. In the **DN attribute** field, enter the field from which the user's DN is obtained (**9**).

> **Note**
>
> To set a login and DN attribute, you can use Microsoft Active Directory and OpenLDAP LDAP templates. To use a template, click the relevant link (**10**).

10. Specify a default user role for users created via LDAP (**11**). If no role is specified, no automatic user creation will be possible for this catalog.
11. Click the **Apply** button.

The LDAP catalog is now added to the system.

To test the connection, click the **Test connection** button. If connection is successful, the form on the lower part of the screen displays information about the catalog users. Otherwise, an error message appears.

cn	entrydn
name1 surname1	cn=name1 surname1,ou=load,ou=Groups,dc=example,dc=com
name2 surname2	cn=name2 surname2,ou=load,ou=Groups,dc=example,dc=com
name3 surname3	cn=name3 surname3,ou=load,ou=Groups,dc=example,dc=com

Working with users

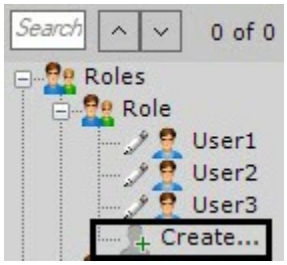
In *Axxon One*, multiple users can be assigned to the same role. A user will be granted the permissions for administration, management and/or monitoring that are indicated in the settings of the user's role. When adding a new user, the name and password necessary for that user to log in to the system are specified.

Creating local users

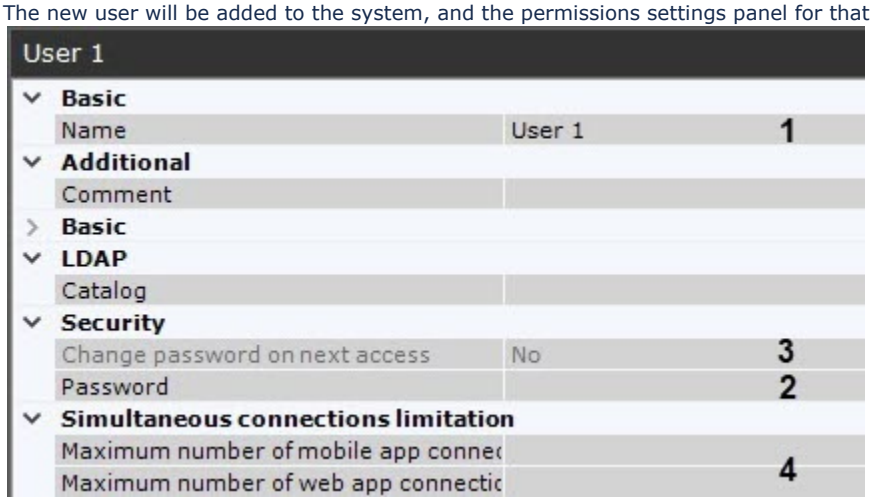
Registering local users

To register a local user, do the following:

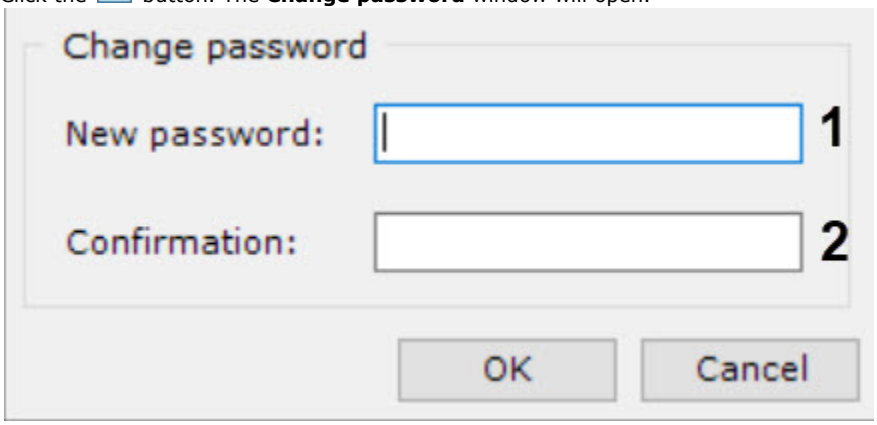
1. Click the **Create** link at the end of the list of a role to which you want to add a user.



The new user will be added to the system, and the permissions settings panel for that user will open on the right.



2. Enter a user name (**1**).
3. In the **Security** settings group, enter a password (**2**).
   a. Click the button. The **Change password** window will open.



   b. In the **New password** field (**1**), enter a new password assigned to the user.

> Configuring the user security policy

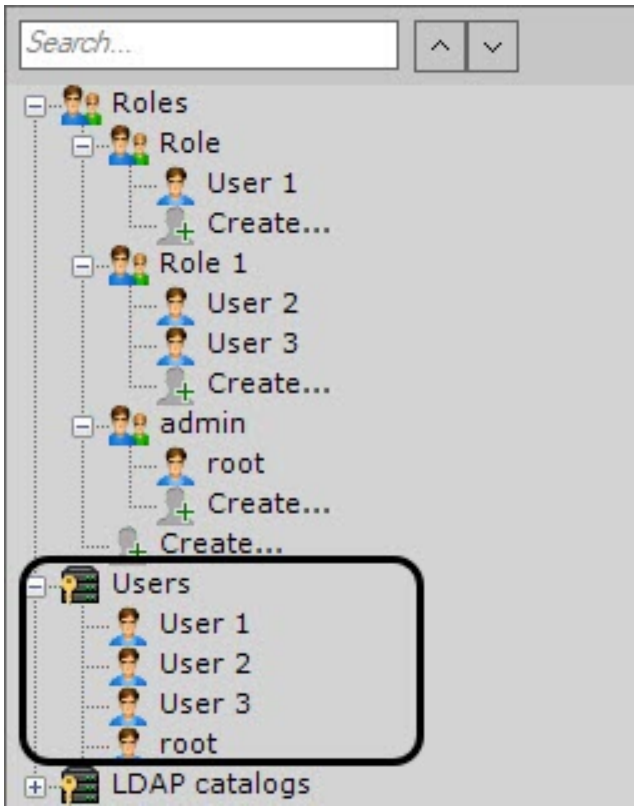
   c. In the **Confirmation** field (**2**), reenter the password.
   d. Click the **OK** button to save the settings.
4. In order for the user to change the password upon the next connection to the Client, set the corresponding parameter (**3**) to **Ye**
   .
5. If you want to limit the number of connections for a user through Web or mobile Clients, specify a maximum number of connections (**4**). The **Maximum number of web app connections** parameter also sets a maximum number of rtsp streams requests for a particular user.

> **Attention!**
>
> The limit on the number of connections will take effect after the Server is restarted (see Launching and closing the Axxon One software package).

6. If necessary, enter additional information about the user (e-mail, IP address, personal and company ID, etc.) in the corresponding fields.
7. Click the **Apply** button.

The user has been registered and added to a role.

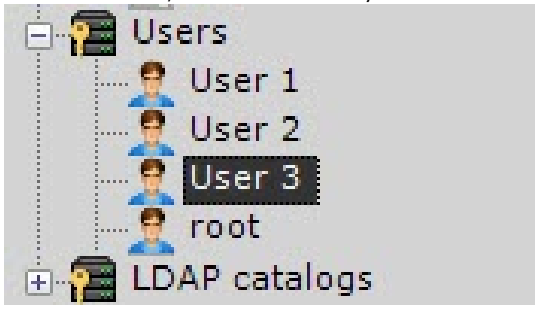
All created users are displayed in the **Users** list.



Adding users to a role

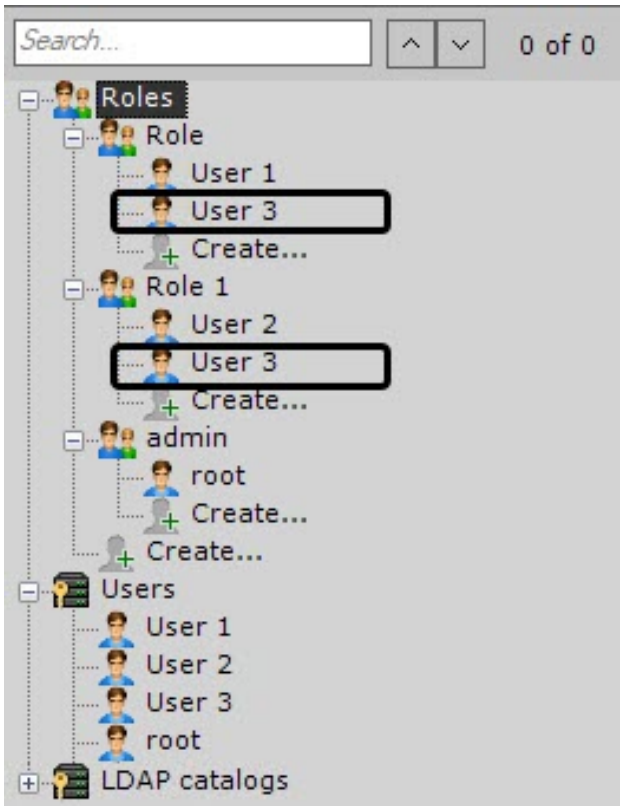
In *Axxon One*, you can add a user to several roles. To do this, do the following:

1. In the **Users** list, select a user who you want to add to a different role.



2. Move the user to the required role by dragging and dropping.
3. Repeat steps 1-2 if you want to add the user to another role.
4. Click the **Apply** button.

As a result, the user will be added to several roles.



User access permissions are summarized from all roles to which the user belongs, i.e. from all roles the rights with the highest access to the configuration of *Axxon One* components are selected.

You can also move users from one role to another. To do this, do the following:

1. Select the user in the role from which you want to move them.
2. Move the user to another role by dragging and dropping.
3. Click the **Apply** button.

As a result, the user will be moved from one role to another.

Configuring user permissions

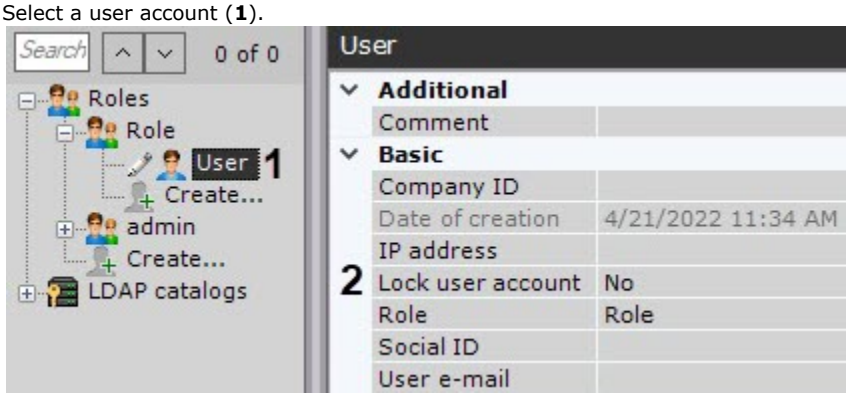
Deleting users

Locking a user account

You can lock user accounts to prevent unwanted logins.

To do this:

1. Select a user account (**1**).



2. In the **Lock user account** field, select **Yes** (**2**).
3. Click **Apply**.

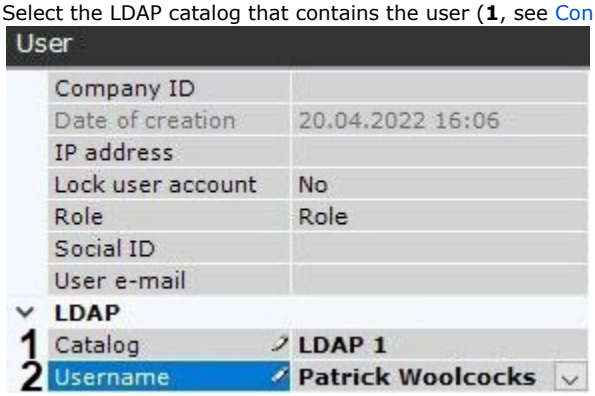
To unlock an account, select **No** in the **Lock user account** field.

Creating LDAP connections

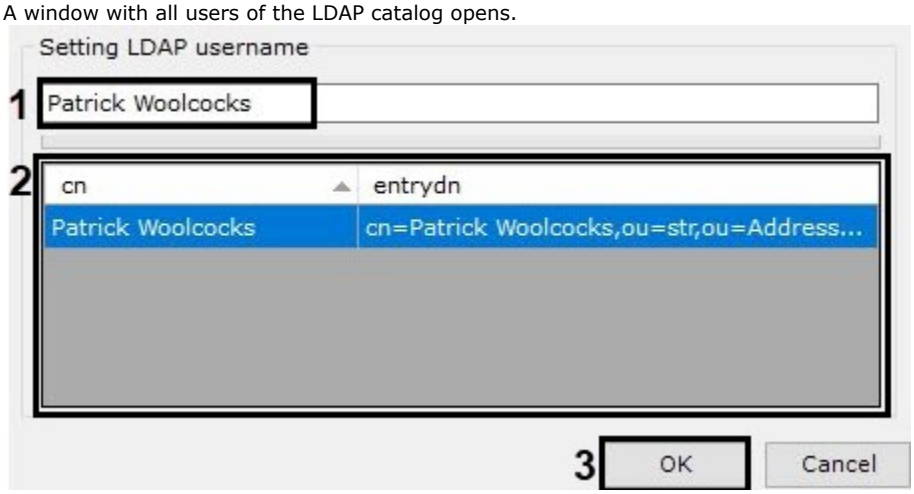
When adding an LDAP user, the user's login is selected from the specified LDAP catalog. No password is required.

To add an LDAP user:

1. Add the user to the system (see Creating local users).
2. Select the LDAP catalog that contains the user (**1**, see Connecting to an LDAP catalog).



3. In the **Username** field, click the button (**2**).
   A window with all users of the LDAP catalog opens.



4. Find a user via search (**1**) or manually select a user from the list (**2**). Click **OK** (**3**).
5. Specify the other user settings (see Creating local users).
6. Click the **Apply** button to save the settings.

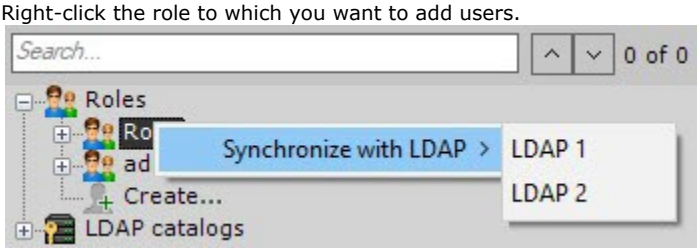
The user has now been added and assigned a role.

When an LDAP user connects, the user's login from Server settings is used with the password from the LDAP catalog.

Synchronize LDAP users

To add users from an LDAP directory to a specific role, do as follows:

1. Right-click the role to which you want to add users.



2. Choose **Synchronize with LDAP** and then the required LDAP directory (see Connecting to an LDAP catalog).

All users in the selected directory will be added to this role. By default, the user name will match the login in the LDAP directory.

Deleting users

To delete a user from the tree:

1. Select the user to delete.
2. Click **Delete**.

> **Note**
>
> You cannot delete the user through which you logged into the system.

3. Click the **Apply** button to save the settings.

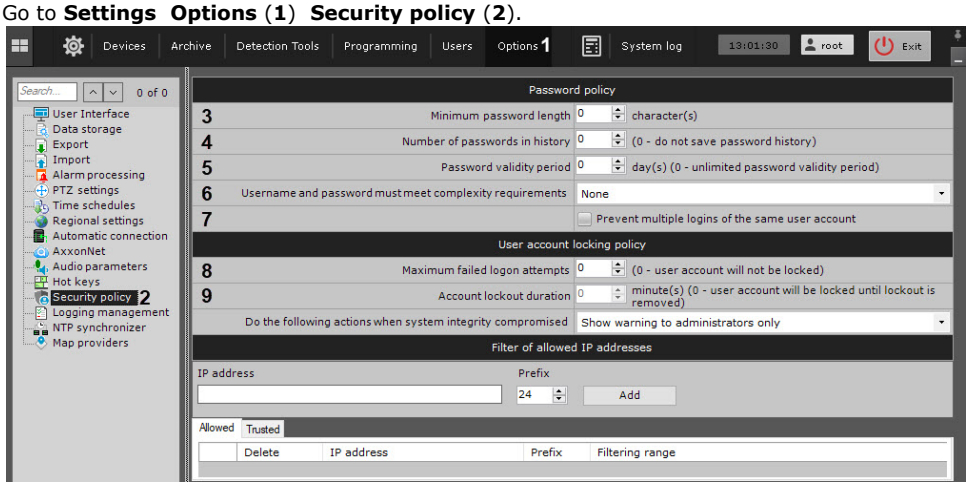
The user has now been deleted from the tree.

> **Attention!**
>
> If you delete a user account on the LDAP server, it will be automatically deleted from *Axxon One* VMS.

Configuring the user security policy

To configure the user security policy, do as follows:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **Security policy** (**2**).



2. Set the minimum password length (**3**).
3. Set the number of the most recent passwords for each user to be stored in history (**4**). **0**—do not store password history. If this value is different from **0**, the passwords that are stored in history cannot be used when setting a new password.
4. Set the password validity period in days (**5**). After the validity period expires, the user will be prompted to set a new password. —the password validity period never expires.
5. Select the positions to meet complexity requirements: nothing, password only, username and password (**6**).
   The requirements:
   a. Username:
      i. should contain at least six characters and at least two digits;
      ii. should not include common role names, such as: user, admin, administrator, administrator1, root, super, superuser, supervisor.
   b. The password must contain at least eight characters that must meet at least three requirements for passwords containing less than 10 characters and at least two requirements for passwords containing 10 or more characters:
      i. At least one uppercase letter;
      ii. at least two lowercase letters;
      iii. at least three digits;
      iv. at least four special characters: **. , : ; ! ? \ | / ( ) [ ] { } + − = < >" @ ' # * $ ` % ^ & _ ~**.
6. If you need to limit the number of sessions per user to one, set the corresponding checkbox (**7**). This requirement also applies to Web-Clients and mobile Clients.
7. Set the number of failed logon attempts to lock a user's account (**8**). **0**—no account locking on incorrect passwords. If this value is different from **0**, when a new user is created, they will be given the name User with a random number from 10000 to 99999. The name can be changed in the user settings.

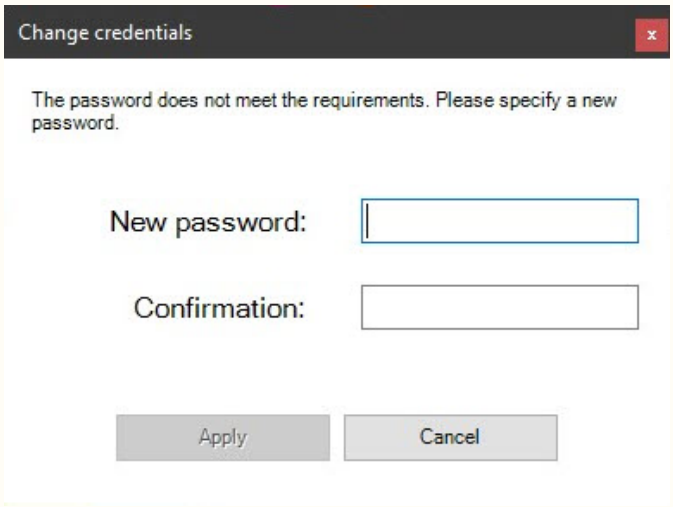
> **Attention!**
>
> When unblocked, the user is offered only one authentication attempt. A successful authentication will reset the failed attempts counter to zero, otherwise the user account will be blocked again.

8. Set the duration of user account lockout on failed login attempts in minutes (**9**). **0**—the account can be unlocked by the administrator only (see Locking a user account).
9. Click the **Apply** button.

Configuring the user security policy is complete.

Attention!

If any user accounts created in your system before you applied changes in security policy are incompatible with the new requirements, the users will be prompted to change their credentials upon their next login.



Configuring automatic response when Axxon One integrity check fails

IP address filtering configuration

Configuring layouts

Axxon One allows users to configure custom layouts.

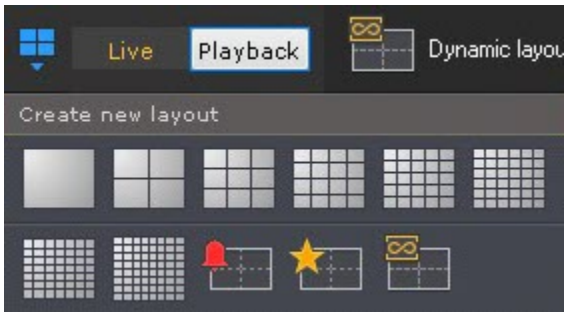
Separate layouts are configured for each user of the system. To configure layouts, log into any Server of Axxon-domain under the appropriate user name and configure the layouts for that user. Layouts created for the user will be available when you connect from any Client to any Server in the Axxon-domain. The layout is selected for display and editing only for a specific user – other users of the system will not see any changes on their screen.

> **Note**
>
> Creation, editing, copying, and deletion of layouts are available to users that belong to roles with the **Changing custom layouts** component activated (see Configuring user permissions).

After you configure user's layouts, you may limit user's privileges.

Creating and deleting layouts

Layouts are created based on standard layout types. To create a new layout, click the  button in the context menu and select one of the standard layouts.



This takes you to layout editing mode (see Switching to layout editing mode).

> **Note**
>
> A new layout is also created when you select a video camera that is not displayed in any previously created layout (see Objects Panel, Camera Search Panel).
>
> If you do this, layout editing mode does not start and the layout will not be saved.

The newly created layout will be named automatically. You can rename it later.

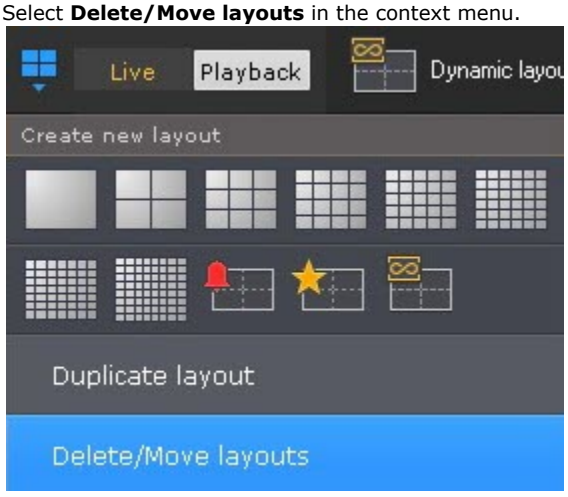
To save the layout, exit layout editing mode and save changes (see Exiting Layout Editing mode).

The layout will then be placed at the beginning of the list in the layout panel.

If you do not save changes and exit, the layout will not be saved.

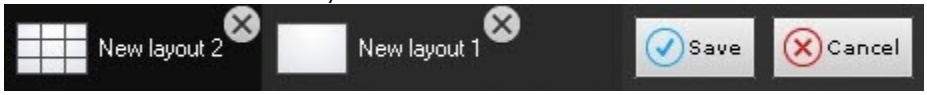
To delete layouts:

1. Select **Delete/Move layouts** in the context menu.



> **Note**
>
> You can not access it in the Layout Editing mode though.

2. Click the  button to delete layouts.



3. Click **Save**.

You will exit Manage Layouts mode and save changes.

The layouts have now been deleted.

Rename Layouts

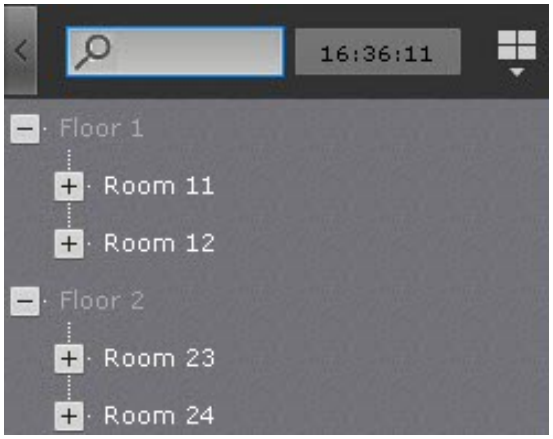
To rename a layout, double left-click and enter a new name.



You can rename layouts in Manage Layouts mode either.

Using the "\" symbol in the layout name, you can build a layout tree in the Object Panel (see Objects Panel).





Reorder Layouts

To reorder layouts in the ribbon:

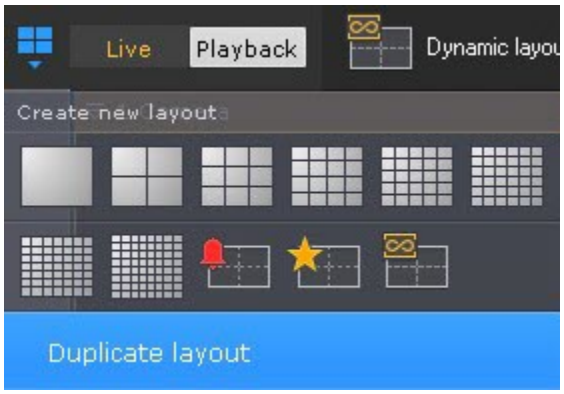
1. Go to Manage Layouts mode (see Creating and deleting layouts).
2. Drag & drop layouts.
3. Click **Save**.

You have now reordered layouts.

Layout copying

You can copy existing layouts.

Select the layout that you want to copy. Click the  button to open the context menu and select **Duplicate layout**.



An identical layout is then created.

> **Note**
>
> Layouts cannot be copied while in editing mode.

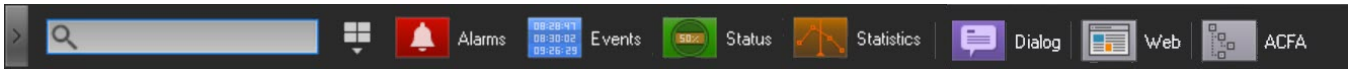
Editing layouts

Every layout consists of cells that are windows in which either video cameras or information boards can be placed.

In *Axxon One*, there are 7 types of information boards that can be added to the layout:

1. Alarms Board.
2. Events Board.
3. Status Board of the Servers and cameras.
4. Statistics Board.
5. Dialog Board.
6. Web Board.
7. Devices Board.

Information boards are available on the layouts panel in the editing mode.

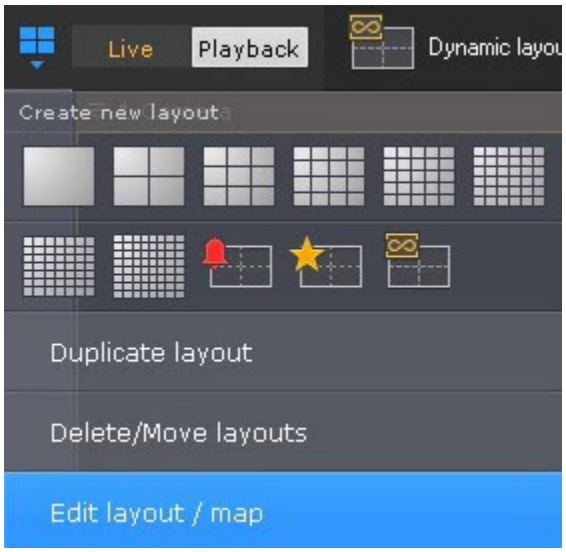


When a camera is added to a cell, a surveillance window appears.

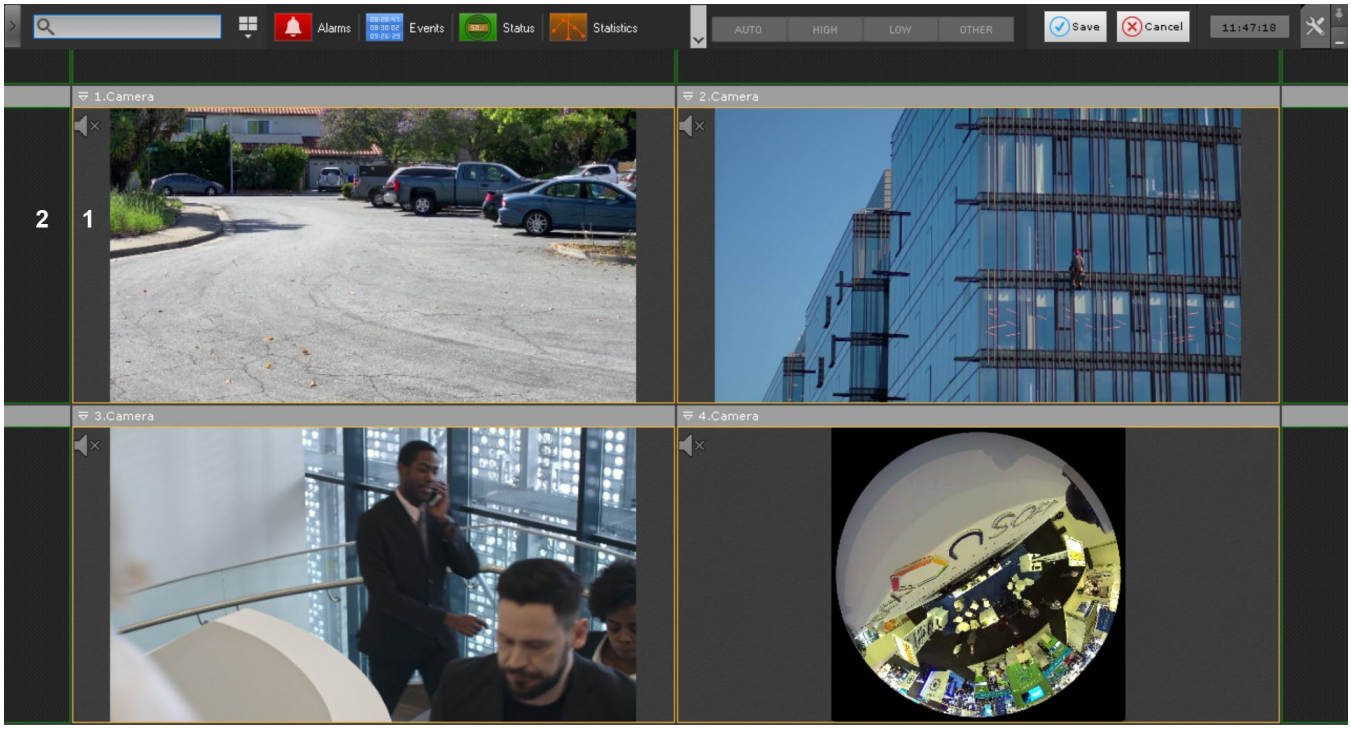
Switching to layout editing mode

You can switch to the layout editing mode either automatically when creating a new layout (see Creating and deleting layouts), or manually using the **Edit layout/map** item of the context menu of the layouts panel. The context menu is opened when you click the  button.

> **Note**
>
> To use the layout editing mode, you must have the required permissions (see Configuring user permissions).



In the layout editing mode, the space is divided by a grid into cells of the surveillance windows (**1**).



On the edge of the layout there are fragments of cells (**2**), which are parts of the ordinary empty cells and allow adding new cells to the layout (see Adding new cells to a layout).

Selecting a layout for editing

To edit a layout, do as follows:

1. Go to the layout you want to change (see The Layouts panel).
2. Switch to the Layout Editing mode (see Switching to layout editing mode).

As a result, an interface for editing the selected layout will be displayed.

Configuring layout cells

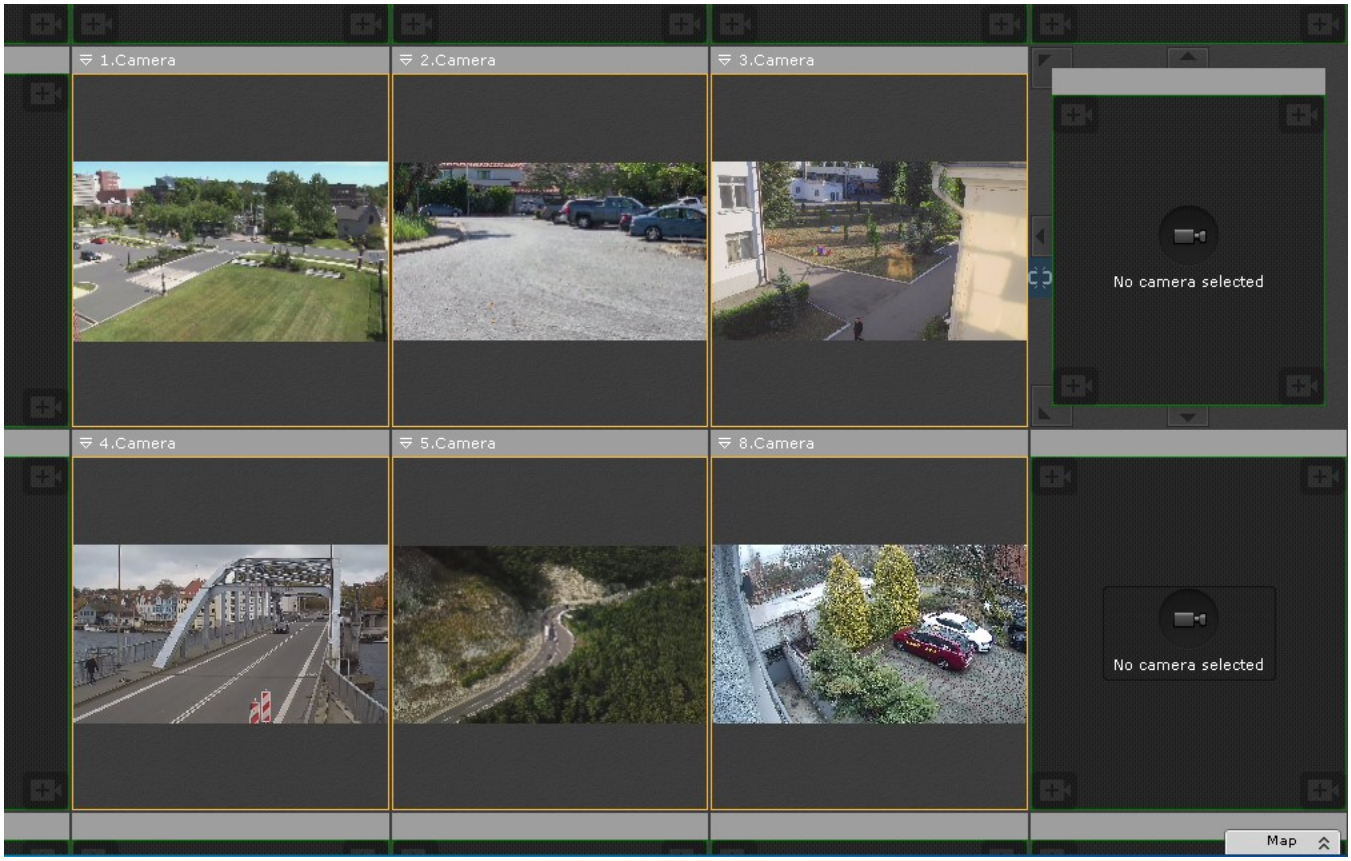
Adding new cells to a layout

Switching to layout editing mode

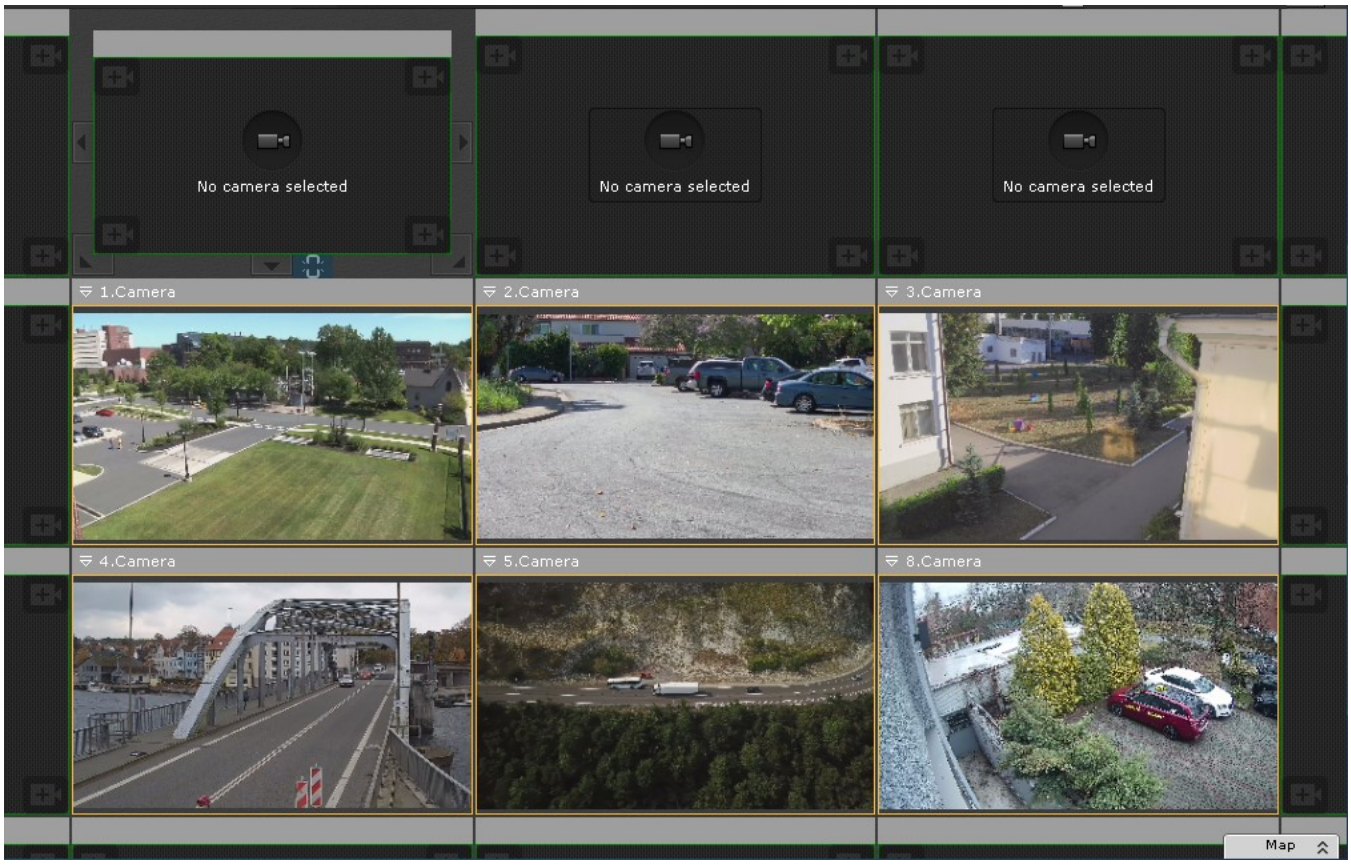
You can add new cells to a layout in one of three ways:

1. Drag a non-empty cell onto a grid square fragment (see Moving cells).
2. Left-click a grid square fragment and resize it (see Resizing cells).
3. Left-click a grid square fragment and select a video camera or information board in it (see Adding cameras to cells).

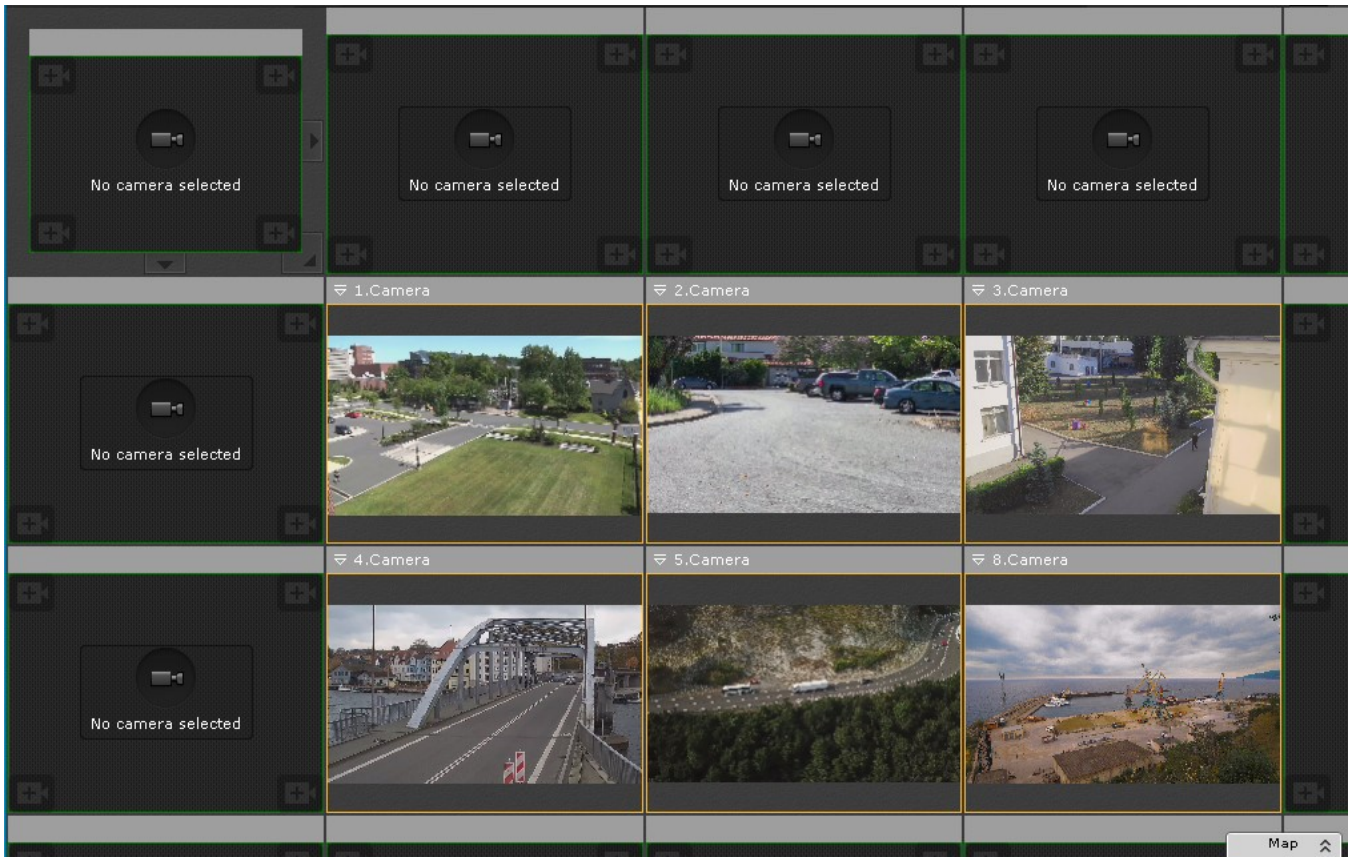
Cells are added in rows. For example, when editing a six-square (3*2) layout, a column of two grid squares is added when a fragment is chosen on the left or right side of the screen.



A row of three squares is added when you select a fragment from the upper or lower part of the screen.



When you select a corner fragment, both a row and column are added.



Resizing cells

Switching to layout editing mode

To resize a cell, use the buttons on its edges.

Button	Action	Button	Action
	Increases the cell by a column to the left and row above		Increases the cell by a column to the right and row below
	Increases the cell by a column to the left		Increases the cell by a column to the right
	Increases the cell by a column to the left and row below		Increases the cell by a column to the right and row above
	Increases the cell by a row below		Increases the cell by a row above

When you point the cursor at any button, a darkened area that shows the size of the cell after resizing is displayed.



You can also select and resize any tile. To resize, click the button on the cell border and expand/contract the cell as you wish. You can resize the cell only in one direction. You cannot resize the cell in two directions with the corner buttons.

If you expand a tile, the neighboring tiles contract and vice versa.

Note

If the cell is in the outermost top/bottom row or left/right column, you cannot resize it by clicking and dragging the borders. You should add an extra cell to the current row or column first.

Attention!

If you expand the cell over the next one or several cells, they are deleted.

Moving cells

Switching to layout editing mode

To move a cell, left-click the frame of the grid square fragment and drag it to the necessary position.

The cells are then switched: the contents of the previously occupied cell are moved to the location of the cell being moved.

If a cell is moved to a grid square fragment, new cells are added to the layout (see Adding new cells to a layout).

Adding cameras to cells

Switching to layout editing mode

You can add a camera to a cell in one of three ways:

1. Using the **Objects Panel**.
2. Using the **Camera Search Panel**.
3. Using an interactive map.

You can add a camera to an empty cell or to a cell containing an information panel or another camera.

Note

You can add cameras from any domain to the layout (see Camera Search Panel).

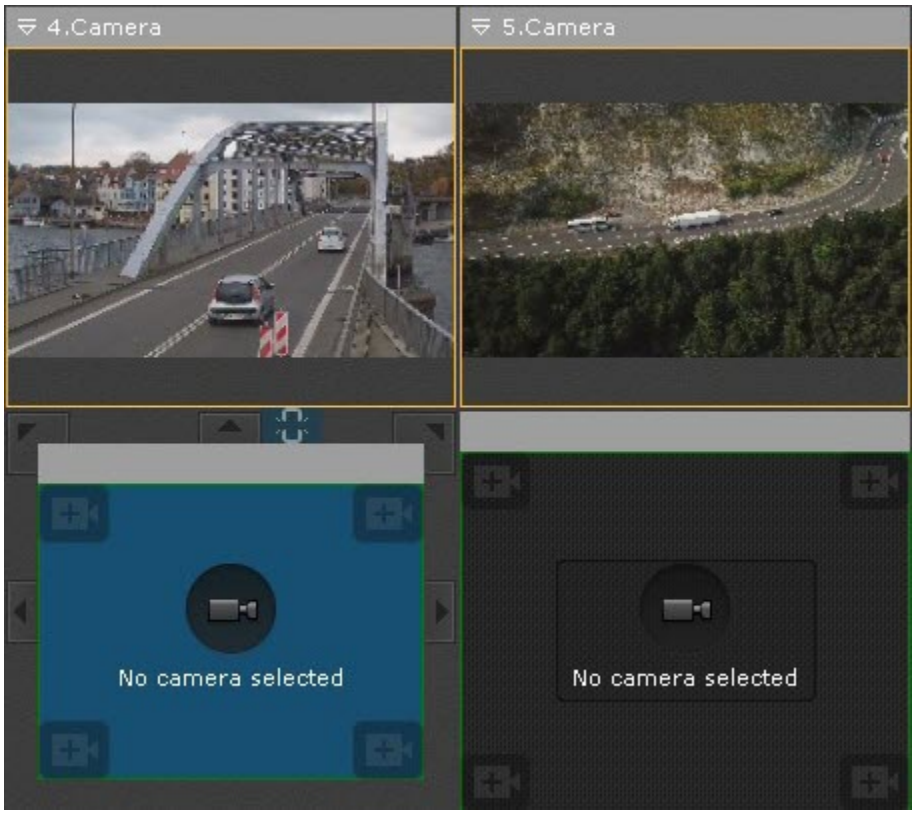
You can add the same camera to several cells of the same layout.

Adding a camera using the Objects Panel

To add a camera using the **Objects Panel**, do the following:

1. Click the mouse button to switch the cell to the active mode.
2. Click a camera in the **Objects Panel** (see Objects Panel).

You can also drag a camera to a cell. An empty cell with a cursor in it is highlighted when you drag the camera.



To add multiple cameras to a layout, do the following:

1. In the **Objects panel**, use the **Ctrl** or **Shift** key to select several cameras.
2. Drag the cameras to the layout.

You can use the **Objects Panel** for adding all cameras within a group or a domain to the layout. To do it, do the following:

1. Left-click the group/domain on the panel.
2. Drag the group/domain to the layout.

> **Note**
>
> Cameras that are currently disabled won't be added to the layout.

Adding a camera using the Camera Search Panel

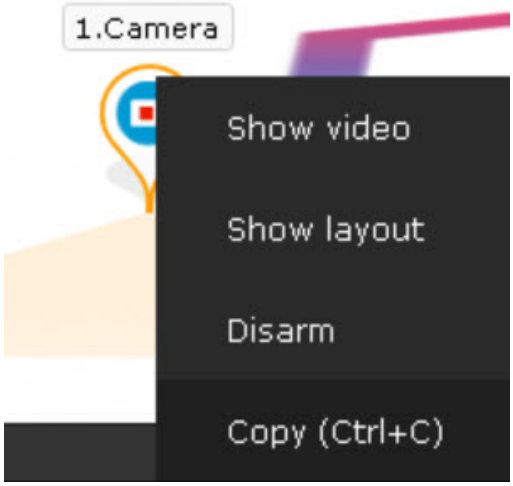
To add a camera to a cell, do the following:

1. Click the mouse button to switch the cell to the active mode and select a camera from the list in the **Camera Search Panel** (see Camera Search Panel).
2. Select a camera from the list in the **Camera Search Panel** and drag it to the layout.

Adding a camera using an interactive map

You can add a camera to a cell in one of the following ways:

1. Select a camera icon on the map and drag it to a cell (see Adding video cameras).
2. In live mode, right-click the camera icon and click the **Copy** button.



Then click an empty cell or a cell containing an information panel or another camera.

> **Note**
>
> Changes aren't saved and the original layout will be available when you switch layouts or the next time you start the Client.

Adding information boards to cells

Switching to layout editing mode

You can add information boards to cells in two ways:

1. Activate the cell (by clicking it) and select the information board that you want to add to the cell.
2. Click an information board to select it. Drag the information board to the layout cell and then release the mouse.

You can add an information board to an empty cell or to a cell that contains a camera or other information board.

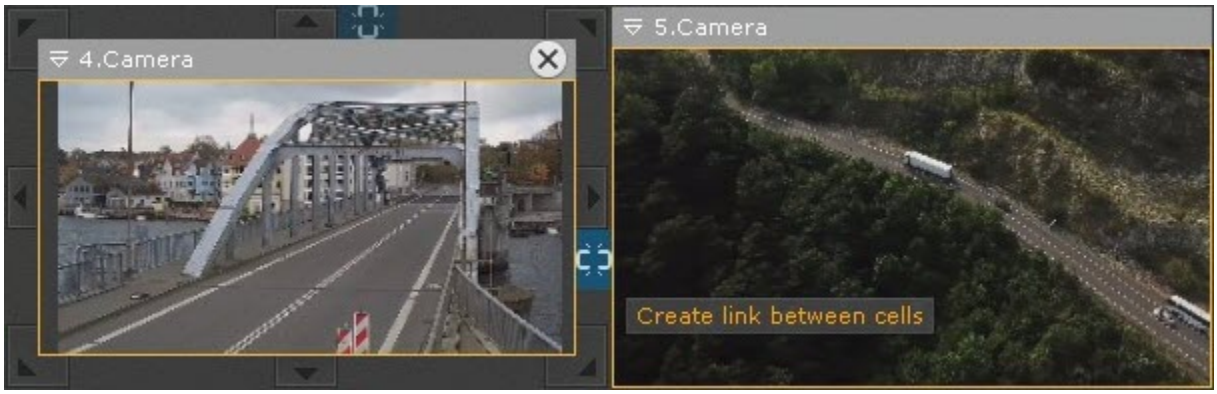
Note

After you add an information board to the cell, you should configure it (see Configuring information boards).

Linking cells

Switching to layout editing mode

You can link cells. To create a link, select cells and click the button on the border. To delete the link, click .



You can create the following links:

1. A viewing tile to a viewing tile. You can link cells from the same row only.
   This way you can hide cell borders in live view and have a virtually merged FoV from several cameras.
   

2. An information board to viewing tile. This way you can link adjacent cells, up/down and across. A single information board can be linked with multiple cameras. If the viewing tile is linked to **Event Board**, you can click an event and switch to the Archive mode (see Switching a camera linked to an Event Board to the archives).
3. Also, you can link 2 information panels or empty cells to panels (see Configuring Alarmed cameras layout).

All linked cells have a different scaling logic (see Scaling the surveillance window).

Merging videos from adjacent cameras (FrameMerge)

Switching to layout editing mode

FrameMerge stitches video feeds from neighboring cameras into a single panoramic view.

The resulting video is available:

- as live video feeds,
- as recorded footage,
- as exported video files.

> **Attention!**
>
> The maximum horizontal resolution of exported video is 8184 pixels.

To use this option, cameras and their video feeds must match the following conditions:

1. Install cameras as close to each other as possible.
2. No more than 3 cameras' feeds can be merged horizontally.
3. The cameras must have:
    a. pixel resolution of no less than 640 * 480;
    b. identical aspect ratio for the high and low bitrate streams;
    c. identical parameters of lenses.
4. You have to synchronize time on all cameras (for example, via NTP protocol).
5. Camera jitter must not result in more than 1% image shift in both directions.
6. The recommended image overlap across adjacent cameras is 20–25 percent of image width.
7. Camera images must be aligned vertically.

For best results in merging, ensure the following:

1. Daylight illumination.
2. Sufficient light to capture small details.
3. No over-exposed areas within the scene.
4. Minimum video noise and compression artifacts.
5. Moving objects must be visually separated within the FOV.
6. Same set of objects in overlapping areas.

> **Attention!**
>
> If overlapping areas are plain monochrome (e.g. the sky), no merging is possible.

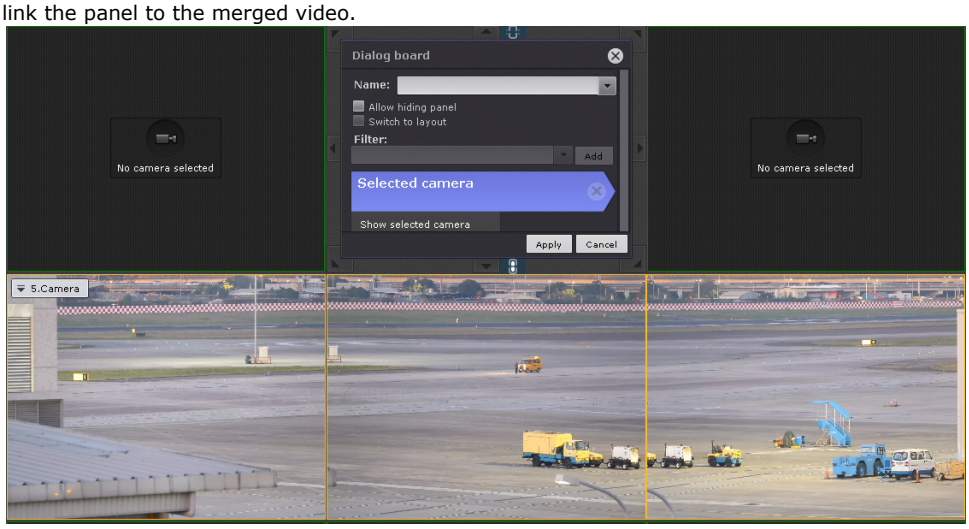
To configure video merging, do the following:

1. Place the cameras horizontally within the layout.
2. Link the corresponding cells to each other (see Linking cells).



3. If you need to display a sub-area of the merged video in a separate window, do the following:
    a. add a dialog board to the layout (see Configuring a Dialog Board);
    b. configure the panel to display the selected camera;

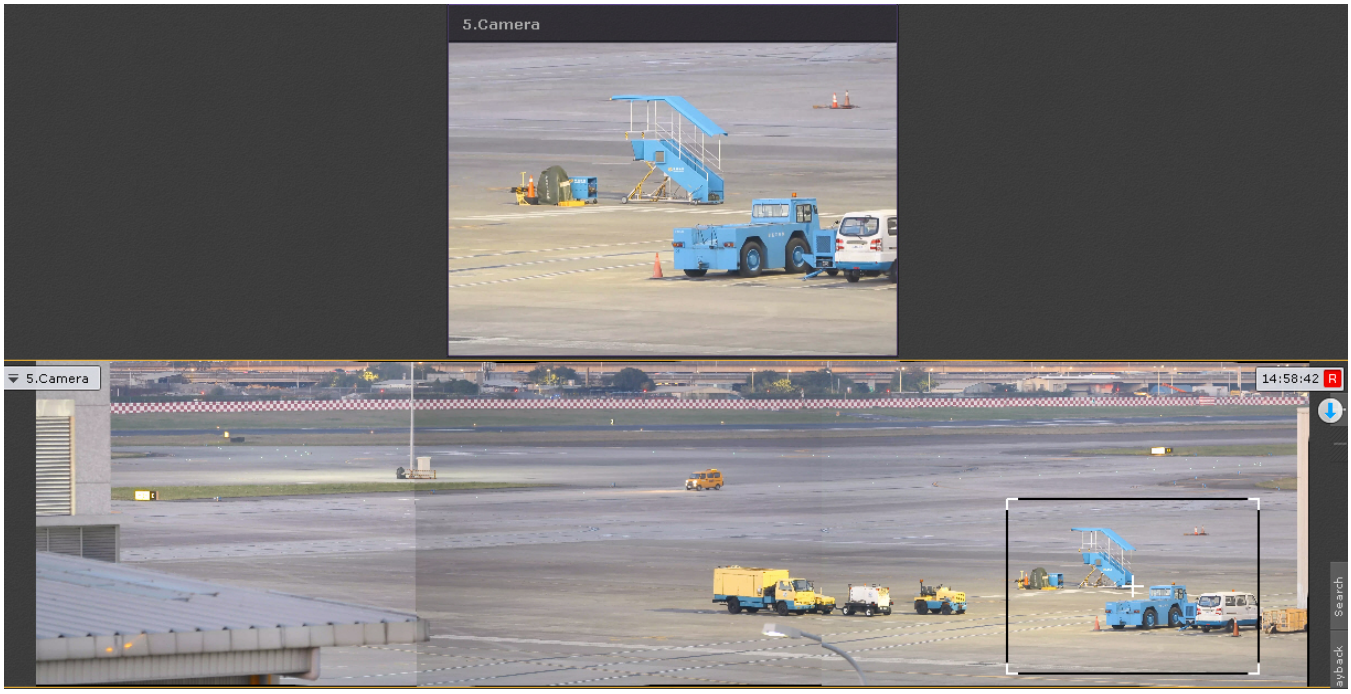
c. link the panel to the merged video.



4. Save the layout.

While merging video feeds, the system automatically scans images from adjacent cameras for appropriate stitching points.

The resulting image will be displayed in a single viewing window. If you select a rectangular area within the video image (as for Area zoom function, see Control using Areazoom), the cropped image appears in the dialog board.



Attention!

Do not move or reposition cameras after merging their video feeds. If any of the cameras change its position, you have to reconfigure the merging.

Clearing cells

Switching to layout editing mode

To remove an information board or camera from a cell, in the upper-right corner, click the  button.

If clearing cells in a row or column removes content from all of these cells, the entire row and/or column is removed from the layout.

Configuring viewing tiles

Selecting default functions for viewing tiles

Switching to layout editing mode

Default values for video stream quality, object tracking, autozoom, and video display (contrast, focus, deinterlacing and flip) functions can be set for viewing tiles.

After the user switches to a layout, these functions are activated automatically.

To set a function as a default one, activate it during Layout Editing mode (see Selecting video stream quality in a viewing tile, Tracking objects, Autozoom, Video image processing, Selecting viewing mode for videos from a fisheye camera) and save changes before exiting the mode.

Selecting the default video stream for all cameras on the layout

Switching to layout editing mode

You can select the defaut video stream (see The Camera object) for all video cameras on the layout on the top panel:



When you switch to the layout editing mode, buttons for selecting the quality of the video stream will be displayed on the top panel. The number of cameras with the selected video stream quality is displayed above each button.

When you click the buttons, all multi-stream video cameras switch to the selected video stream quality, except the **Other** quality (see Selecting video stream quality in a Surveillance window (GreenStream)).

Also in the editing mode, the selected quality of the video stream is displayed in the upper right corner of the video surveillance window.



Note

Information about the quality of the video stream in the video surveillance window is displayed only for multi-stream video cameras.

Selecting the default video mode for a camera

Switching to layout editing mode

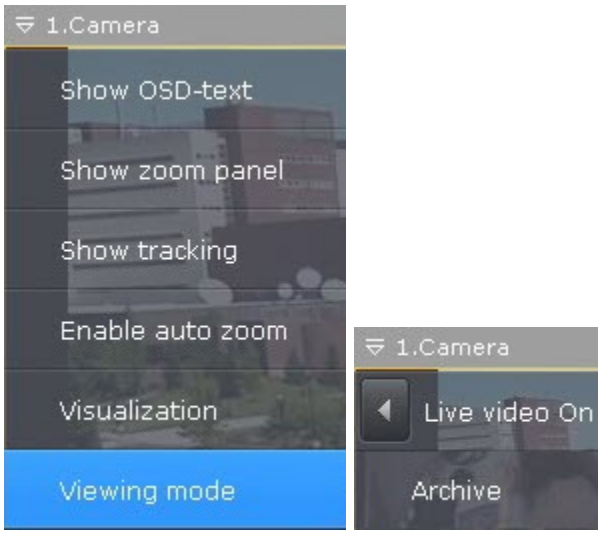
By default, when you switch to a layout, all video cameras are in Real-time/Live viewing mode.

You can select a default video mode for each camera: Real-time mode or Archive mode.

Note

This function is not available if the camera is not attached to an archive.

To select a default video mode, in the context menu of the viewing tile, select **Viewing mode** and select the necessary mode.



If Archive mode is selected, when you switch to the layout, the camera is immediately in Archive mode.

Moving input and output icons in a viewing tile

Switching to layout editing mode

You can move input and output icons in a viewing tile.

To do so, left-click the input or output icon and drag it to the place in the viewing tile where you want to put the icon.

Configuring default zoom levels (the Fit screen function)

Switching to layout editing mode

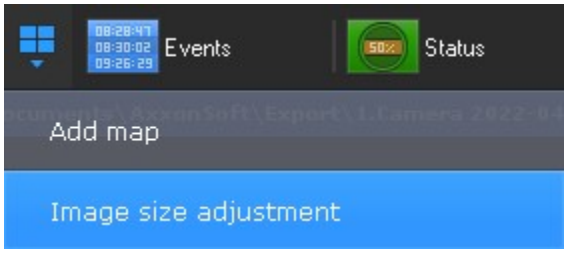
The Fit screen function allows displaying a viewing tile by default so that it occupies all of the available space on the screen (full screen). The default zoom level for full screen display is calculated automatically as a minimum zoom value thal allows filling the available screen space with the viewing tile contents.

To enable the Fit screen function for a specific video tile, display the digital zoom controller (see Digitally Zooming Video Images), click the  button on it, and save changes when exiting editing mode.

Note

To disable the Fit screen function, click the  button again.

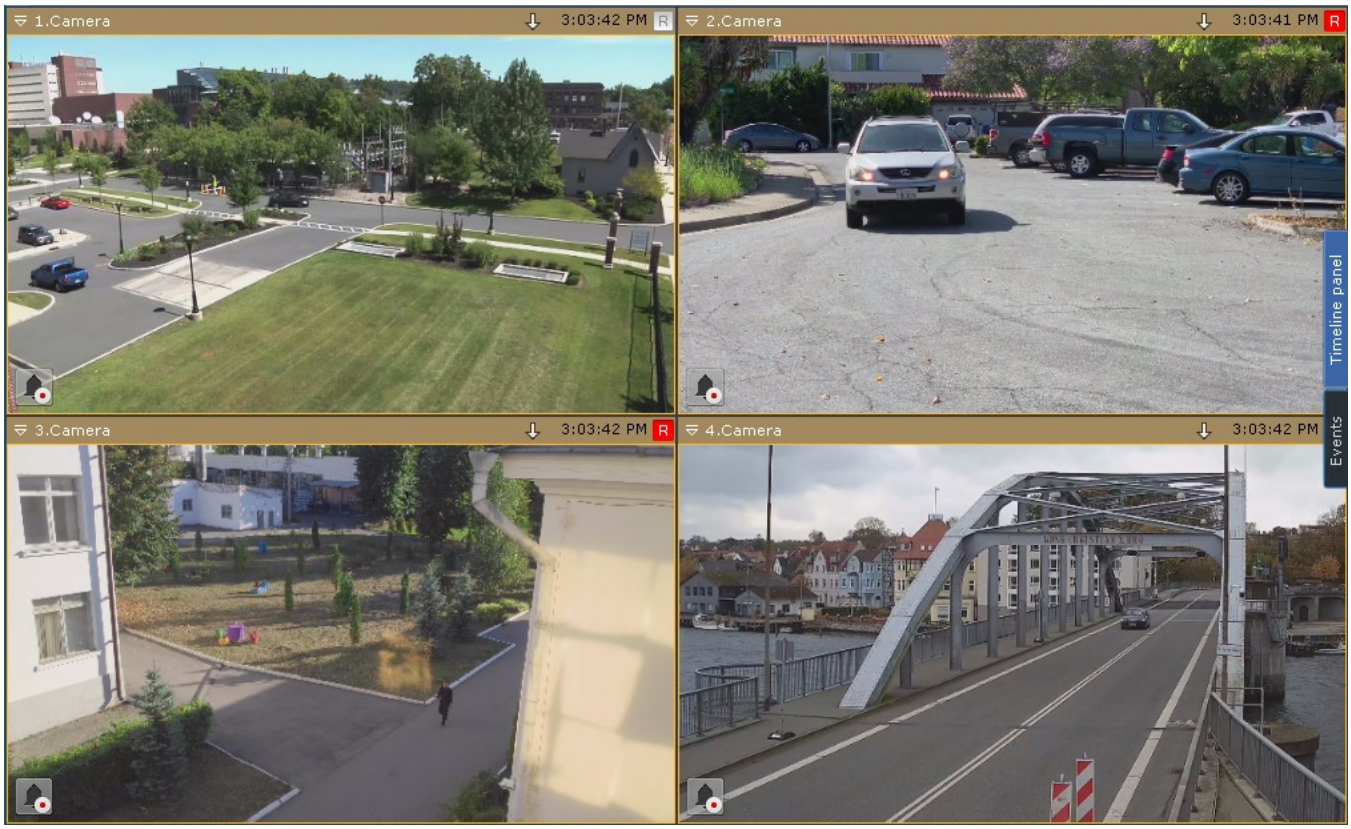
To enable the Fit screen function for all video tiles on the layout open the context menu and select **Image size adjustment**.



Note

To disable Fit screen across all layouts reselect **Image size adjustment**.

Now when a user switches to this layout, the video in the viewing tile is displayed at the calculated minimum necessary level of digital zoom and the viewing tile occupies all available space.


1.Camera
3:03:42 PM
2.Camera
3:03:41 PM
3.Camera
3:03:42 PM
4.Camera
3:03:42 PM
Timeline panel
Events

Configuring pan/tilt angle for video cameras with Immervision lenses in 180o Panorama display format

Switching to layout editing mode

You can set the pan/tilt angle for fisheye cameras in 180° Panorama display format when switching to a layout.

This is useful when needing to display the entire viewable area in the layout (two areas of 180° each). In this case, the video camera is added twice but with different viewing angles.



To set the viewing angle, click and hold the  button (see 180 degree Panorama).

Configuring display of water level detection

Switching to layout editing mode

If you have created a water level detector for a camera (see Configuring the Water Level Detection), you can see the water level sensor in the camera window.

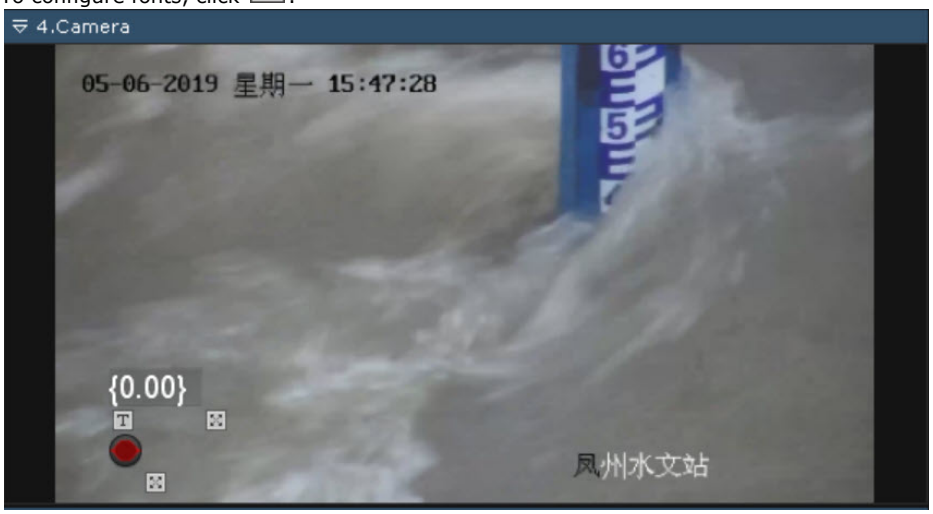
You can also display numerical value of current water levels for the detector. To do it, follow the steps below:

1. In the text field, enter "{0.00}" and additional text if necessary. For example, "Water level: {0.00}".

   Note

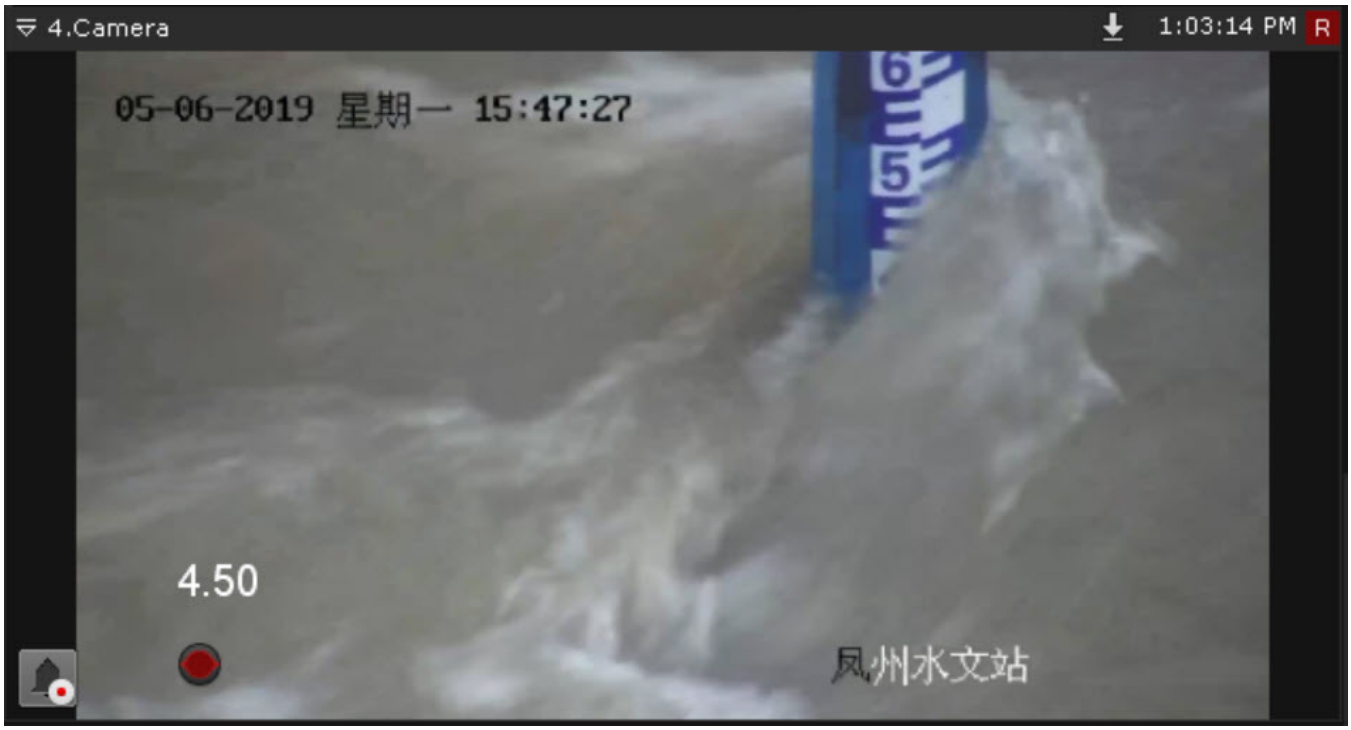
   If you enter "{0.00}", then a fractional number with 2 digits after the point will be displayed (see Displaying the number of detected objects).

2. To configure fonts, click T.



3. Use buttons to scale up/down the text and the sensor icon.
4. You can move the sensor just as any other object (see Moving input and output icons in a viewing tile).

When the layout is saved, you see the information displayed in the camera window.


4.Camera
1:03:14 PM
R
05-06-2019 星期一 15:47:27
4.50
凤州水文站

Adding links to other cameras to the Camera Window

Switching to layout editing mode

You can add links to other cameras to the Camera Window. If you click on such a link, you go to the corresponding camera's window (see Switching to other camera via a link in the Camera Window).

To add a link, do the following:

1. While holding the Ctrl button on your PC keyboard, left-click the camera icon on the **Objects Panel** (see Objects Panel), and drag it into the Camera Window.

   A link will be added to a window as a thumbnail  .
2. To rotate the thumbnail, click . Each click rotates the thumbnail by 45°.

   Note

   If you add a text note to the link (see 3), the thumbnail disappears after you rotate it by 360°, and you will have just the text to switch to another camera.

   To bring back the thumbnail, click .

   Note

   To remove the link, click the button.
3. If required, you can add a text comment to a link via the appropriate text field. To set font attributes, click the button.
4. Use buttons to scale up/down the text and the thumbnail.
5. You can move the link just as any other object (see Moving input and output icons in a viewing tile).

When the layout is saved, you see the newly created link in the Camera Window.



Configuring information boards

Configuring information board templates

Switching to layout editing mode

To save information board parameters as a template, specify a name when configuring an information board.



If a name is not specified for the information board (it is not necessary to specify one), no template with the information board parameters is saved or made available when creating new information boards.

When configuring a new information board, you can use previous templates for the type of information board in question by selecting one from the **Name** list.



If you save the new information board with the same name, the template parameters are updated and all information boards based on the template are updated as well.

To delete a template, in the **Name** list, click the button across from the template. The parameters of information boards based on the deleted template are saved, but their names are discarded.

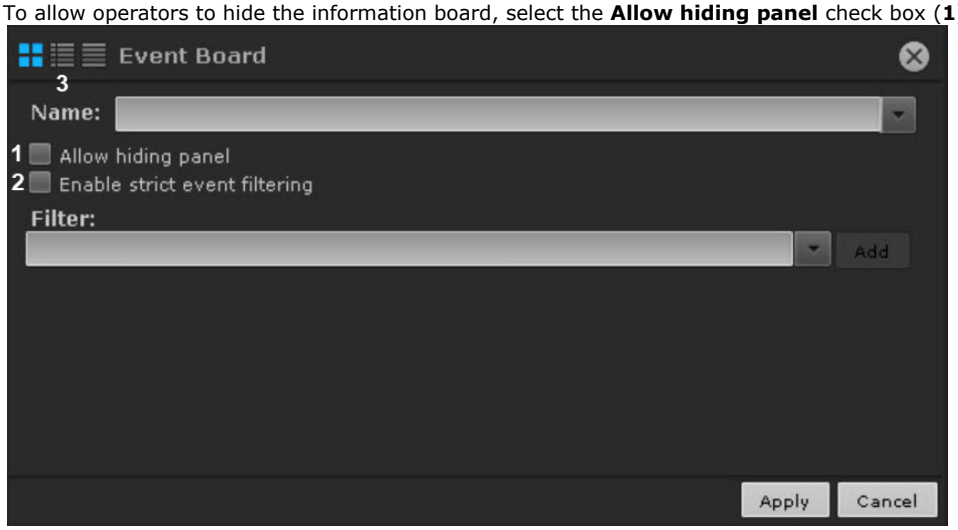
Configuring an Event Board

Switching to layout editing mode

Event Boards display some or all system events.

To configure an **Event Board**:

1. Add an information board to the layout (see Adding information boards to cells).
2. In the upper-right corner, click the  button.
3. To allow operators to hide the information board, select the **Allow hiding panel** check box (**1**).



4. By default, some events on the **Event board** come with audit events. If no display of audit events is required, select the **Enable strict event filtering** checkbox (**2**).
5. In the list, select the event types that you want to display on the board and click **Add**.



To add events of the same type from different devices, enter the name of the event in the **Filter** field. This will list only the events of the chosen type. To list all events, clear the **Filter** field.

Note

To remove an added event type, click the  button.

If no event type is selected, all system events are displayed on the information board.

Note

You can also add any text to the filter. For example, if you add **Signal lost** filter, **Event Board** will display event data from all devices in the system.

> **Note**
>
> To display facial detection tool triggering, we recommend that you select 2 events: **Triggered detection "Face appeared"** and **Triggered specified detection "Face appeared"**.

6. Select the default view for information on the **Event Board** (see Options for displaying information on Events Boards): the first frame of the event and time, first frame and text, or text only (**3**).
7. Click the **Apply** button to save changes.

Configuration of the **Event Board** is complete.

Configuring a Health Board

Switching to layout editing mode

System Health Boards display the status of selected system servers and connected cameras.

To configure a Health Board:

1. Add an information board to the layout (see Adding information boards to cells).
2. In the upper-right corner, click the button.
3. To allow operators to hide the information board, select the **Allow hiding panel** check box (**1**).



4. Select the Servers you want to monitor. To do so, select one server (**3**) or all servers from the Axxon domain (click **All selected servers**) and click the **Add** button (**2**).

> **Note**
>
> To remove the selected server, click the button.

5. To display the status of only distressed servers out of those selected, select **Distressed servers only** (**3**).
   A server is classified as distressed if any of the following are true:
   a. Any components (CPU, hard disk, or network connection) are in critical condition.
   b. There is no connection to the Server.
   c. Any video cameras of the Server are in critical condition.

> **Note**
>
> Information about the status of Servers and cameras is given in the section Working with System Health Boards.

6. Select the default view for display of information on the Health Board (see Working with System Health Boards): diagram, diagram with text, or table (**4**).
7. Click the **Apply** button to save changes.

Configuration of the Health Board is complete.

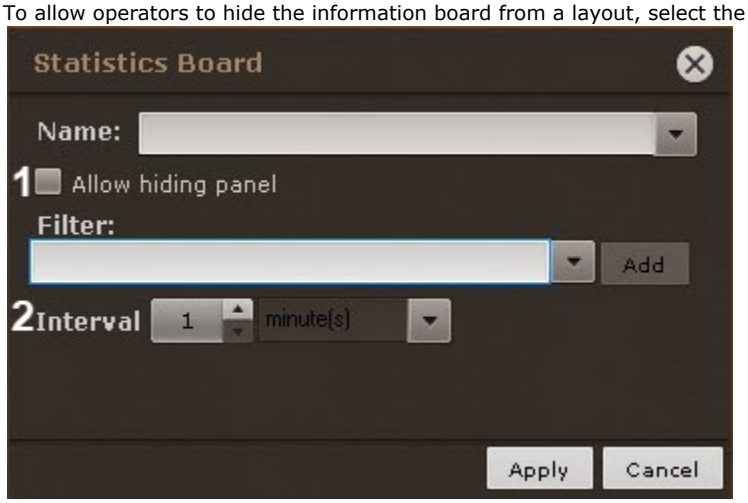
Configuring a Statistics Board

Switching to layout editing mode

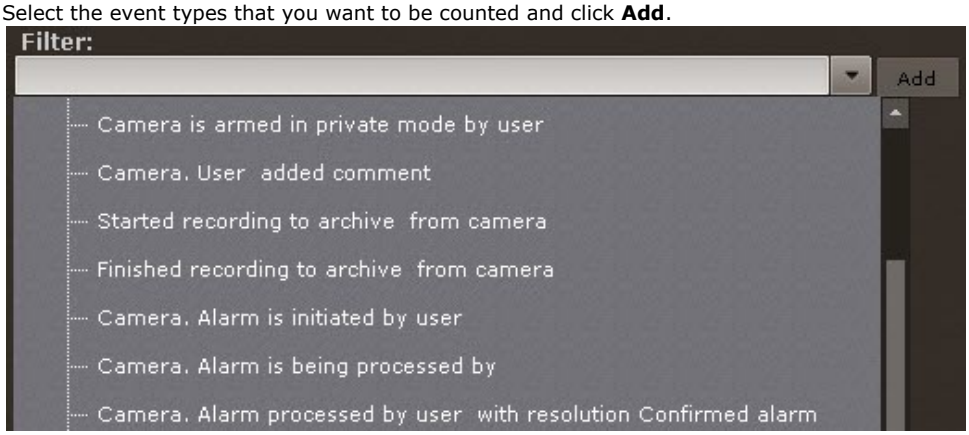
Statistics Boards display information on the number of events of the selected type or types, as a number and graph.

To configure a Statistics Board:

1. Add an information board to the layout (see Adding information boards to cells).
2. In the upper-right corner, click the button.
3. To allow operators to hide the information board from a layout, select the **Allow hiding panel** check box (**1**).



4. Select the event types that you want to be counted and click **Add**.



To add events of the same type from different devices, enter the name of the event in the **Filter** field. This will list only the events of the chosen type. To list all events, clear the **Filter** field.

Note

To remove an added event type, click the button.

If no event type is selected, all system events are counted.

5. Select the time period for display of statistics on the graph (**2**).
6. Click **Apply** to save the changes.

Configuration of the Statistics Board is complete.

Configuring a Web Board

Switching to layout editing mode

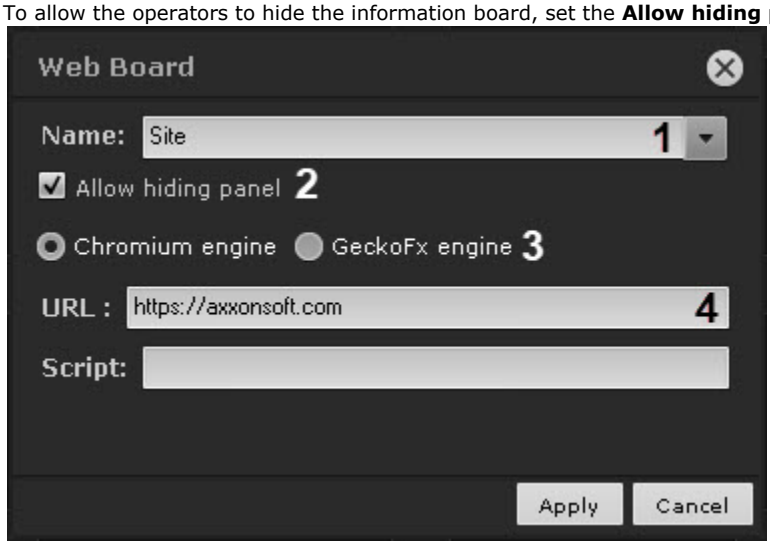
The **Web Board** allows you to view a specific web page on the layout.

Note

Starting with *Axxon One* 2.0, web pages in the *Axxon One* interface are displayed via Chromium or Gecko browser. When upgrading from previous versions that support the Internet Explorer engine, the engine will be automatically replaced with Chromium, which you can manually replace with Gecko.

To configure the **Web Board**:

1. Add an information board to the layout (see Adding information boards to cells).
2. In the upper-right corner, click the  button.
3. Enter the name of the **Web Board** or select it from the list (**1**).
4. To allow the operators to hide the information board, set the **Allow hiding panel** check box (**2**).



5. Select the web page output: Chromium or Gecko (**3**).
6. Enter the address in the **URL** field (**4**).

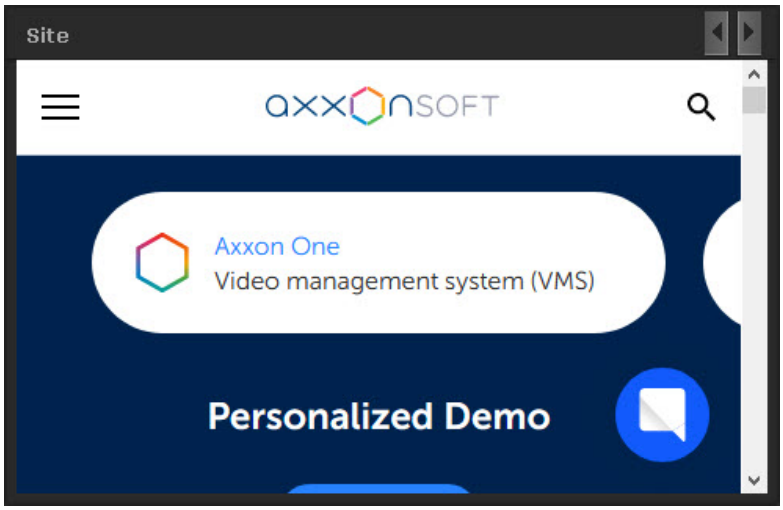
Note

The **URL** field supports addresses in the following formats:

- http://www.site.com
- http://site.com
- https://www.site.com
- https://site.com
- www.site.com
- site.com
- [IP-address]
- [IP-address]:[Port]
- http://[IP-address]
- http://[IP-address]:[Port]

7. To save the changes, click the **Apply** button. To discard the changes, click the **Cancel** button.

Configuration of the **Web Board** is complete. The specified page will be displayed on the **Web Board**.


Site
Axxon One
Video management system (VMS)
Personalized Demo

Configuring a Dialog Board

Switching to layout editing mode

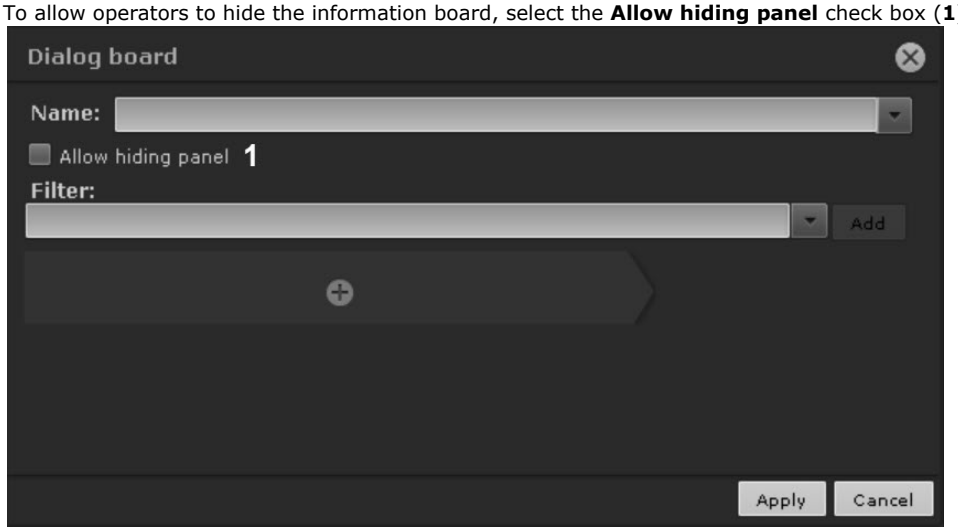
Dialog board allows users to view info about alerts/detection events and quickly start macros to respond.

In addition, the panel can display:

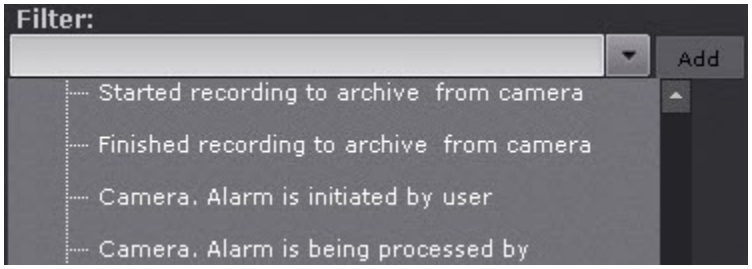
- video from the selected camera on the layout;
- video from the Related camera for the selected camera on the layout;
- video from the Related camera for the camera linked to the panel;
- alarm event from the selected or linked camera;
- still image.

You can configure Dialog board as follows:

1. Add an information board to the layout (see Adding information boards to cells).
2. In the upper-right corner, click the button.
3. To allow operators to hide the information board, select the **Allow hiding panel** check box (**1**).



4. Select the event types that you want to display on the board and click **Add**.



To add events of the same type from different devices, enter the name of the event in the **Filter** field. This will list only the events of the chosen type. To list all events, clear the filter field.

Note

To remove an added event type, click the button.

Note

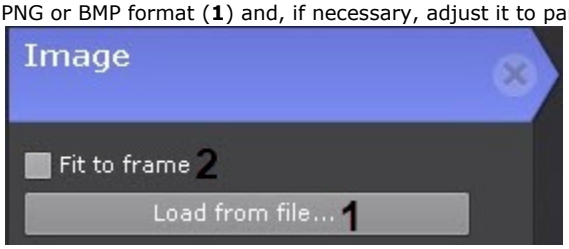
If the board has video, the event filter is not required.

If no event type is selected, all system events are displayed on the information board.

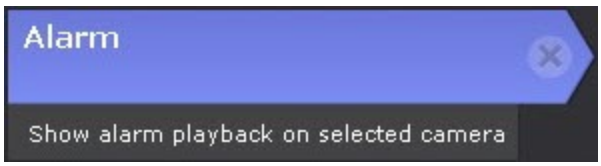
5. Configure the information board:
    a. If you want video on the board, then click the button and select the item in the menu. You cannot add other elements if you have video here.
        i. **Selected camera** – if you want to display video from the selected camera (**1**).



        ii. **Related camera of selected camera** – if you want to display video from the related (alternative, see The Camera object) camera of the selected camera (**2**).
        iii. **Related camera of linked camera** – if you want to display video from the related (alternative, see The Camera object) camera of the linked camera (**3**). In this case, the panel must be connected to some camera window.
    b. If you want to display a still image on the panel, select the **Image** element. To do this, select a desired image in JPEG, PNG or BMP format (**1**) and, if necessary, adjust it to panel size (**2**).



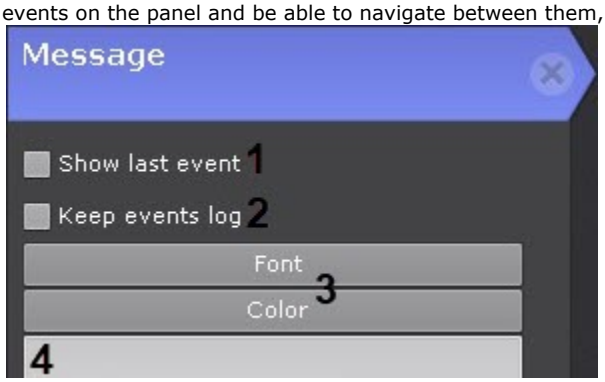
    c. If you want to display an alarm event in the panel from the selected or linked camera, select **Alarm**. If the panel is linked to any camera window, then alarms from this camera will be displayed. If the panel is not linked to any tile, then alarms from any selected camera will be displayed.



When you add the **Alarm** item to the message panel, you can also add pre-programmed buttons to evaluate the alarm event. It is color-coded as follows: green – **False alarm**, yellow – **Non-critical alarm**, red – **Critical alarm**.



d. If necessary, add a message that will be displayed on the panel in case of event (**4**). You can select the font and color (**3**) of the message. If it is necessary to display the event text, set the **Show last event** checkbox (**1**). To keep all events on the panel and be able to navigate between them, set the **Keep events log** checkbox (**2**).



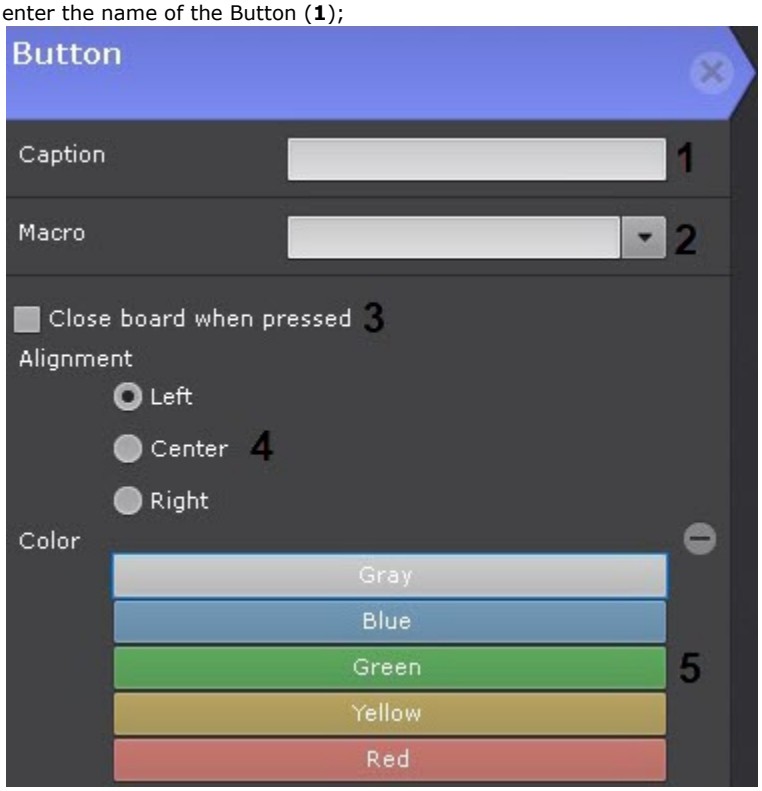
e. If necessary, add the comments field. Select the appropriate check box to make comments mandatory.



f. Add one or more Response Buttons.

To configure Response Buttons, you should set the mandatory and optional parameters (by clicking):

- enter the name of the Button (**1**);



- select a macro that will start when you click the Button (**2**);
- if you want to hide the board after pressing the Response Button, select the checkbox (**3**);
- select location for the Button: on the left, in the center, on the right (**4**);
- select a color (**5)**.

6. Click **Apply** to save the changes

Configuration of the Dialog board is complete.

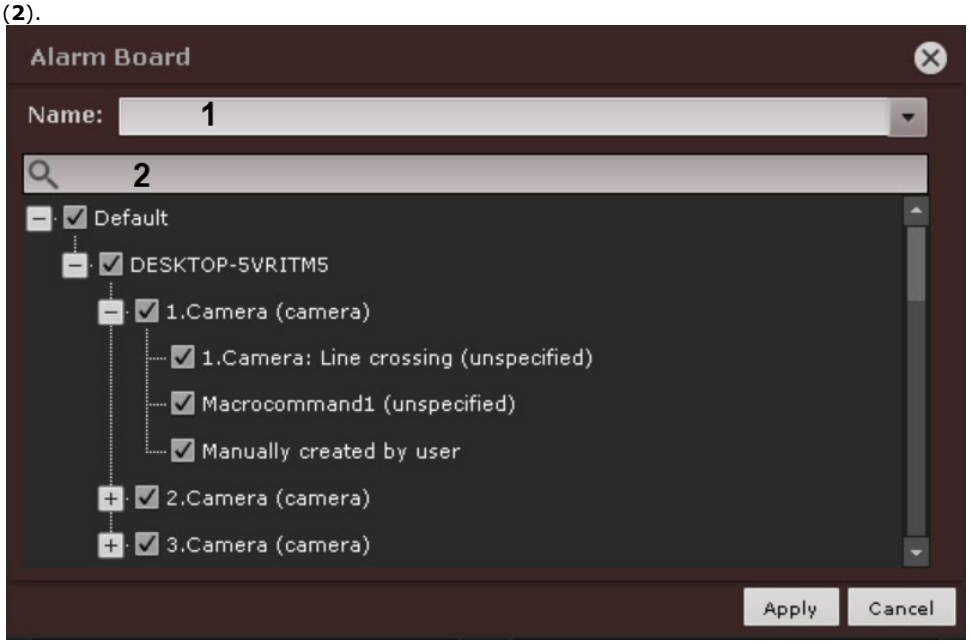
Configuring an Alarm Board

Switching to layout editing mode

Alarm Board is used to display alarm events and work with them. The board displays video clips of all alarm events of the system.

To configure an **Alarm Board**, do the following:

1. Add the board to the layout (see Adding information boards to cells).
2. In the upper right corner of the board, click the  button.
3. Enter or select the name of the Alarm Board from the list (**1**).
4. Set the checkboxes next to the devices and types of commands that can trigger an alarm and should be displayed on the board (**2**).



5. To save the changes, click the **Apply** button. To cancel the changes, click the **Cancel** button.

Configuring an **Alarm Board** is complete.

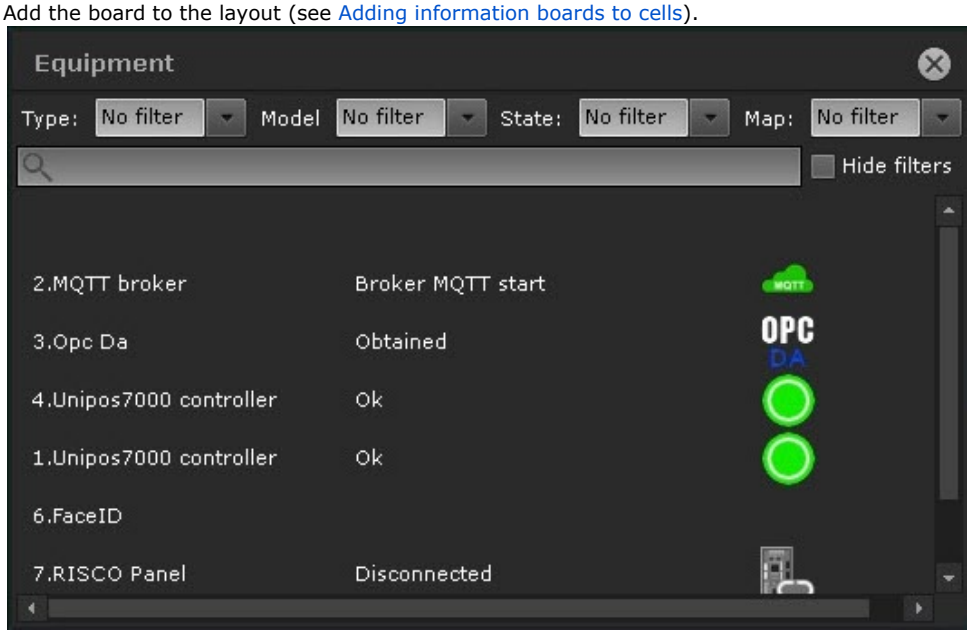
Configuring an Equipment Board

Switching to layout editing mode

The **Equipment Board** is used to display information about *ACFA* integration modules.

To configure the **Equipment Board**, do the following:

1. Add the board to the layout (see Adding information boards to cells).



2. If necessary, configure the filters that you want to display on the board by setting the ☑ checkbox next to the required option in the drop-down list. Types of filters, options and their description are presented in the table:

Type of filter	Option	Description
Type	• No filter • ACFA • Controller • Loop • Reader • Sensor • Relay • Lock • Area • Group area • Fence	Equipment type
Model	• No filter • Lock • Fence • Sensor • Reader • *ACFA* integration module	Equipment model

State	• No filter • start • stop • Tamper • Obtained • Locked • Closed • AUX trouble • Arm • Ok • Unknown • Cracked • Opened • Normal • Unlocked • Disarm • Disconnected • Connected • Alarm	Equipment state
Map	• No filter • Any • Not on map • Map	Display equipment on the map

> **Note**
>
> If you don’t specify any filters, the board will display all available information about *ACFA* integration modules.

3. If you want to hide filters on the layout, set the ☑ **Hide filters** checkbox.
4. Click the **Save** button to save the changes (see Creating and deleting layouts).

Configuring Alarms Panel on a layout

You can configure the size of Alarms Panel (see Alert panel) with included videos for each layout separately.

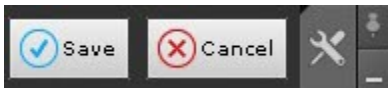
To do it, follow the steps below:

1. Go to the desired layout.
2. Open the Alarms Panel and set desired sizes of videos, and of the panel itself (see Alert panel).
3. Switch to the Layout Editing mode (see Switching to layout editing mode).
4. Exit the Layout Editing mode and save changes (see Exiting Layout Editing mode).

The Alarms Panel will always open as you have specified it for this layout.

Exiting Layout Editing mode

To exit Layout Editing mode and save changes, click **Save** in the upper panel.



To exit Editing mode without saving changes, click **Cancel**.

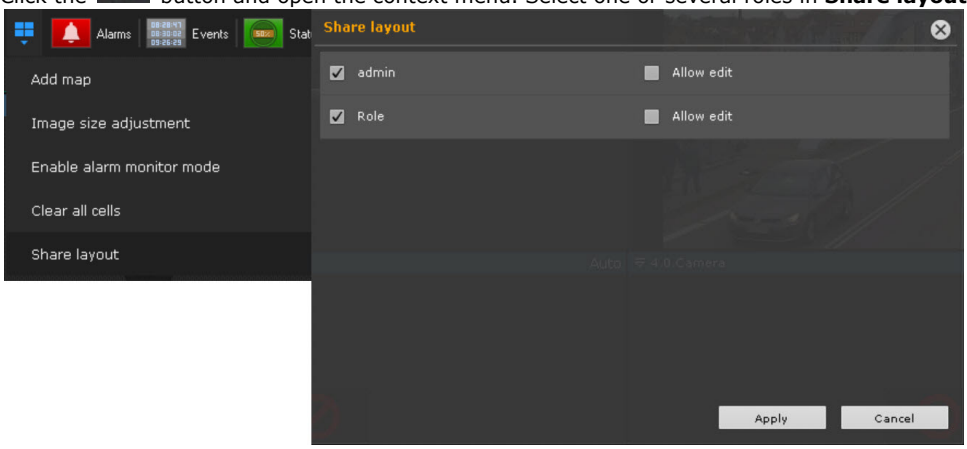
Share Layouts

You can share custom layouts with other users. The user can share only his/her custom layouts.

> **Note**
>
> This feature comes in handy, when it is only the administrator's job to create and edit layouts. After configuring, the administrator can assign the layouts to users/roles.

To share a layout, complete the following steps:

1. Select a layout (see Selecting a layout for editing) and go to Layout Editing mode (see Switching to layout editing mode).
2. Click the  button and open the context menu. Select one or several roles in **Share layout**.



> **Note**
>
> You can select the roles of the selected Axxon domain. Axxon domain can be selected on the Camera Search Panel.

3. If you want to grant rights to edit layouts, select the **Allow edit** checkbox for the required user role.
4. Click the **Apply** button.
5. Exit layout editing mode (see Exiting Layout Editing mode).

This layout is shared with other users.

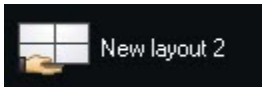
These users can not edit and share this layout. They can:

1. Work with layout (see The Layouts panel).
2. Delete it from their list (see Creating and deleting layouts).

> **Note**
>
> Only the layout owner can completely remove it from the VMS.
>
> Upon removal, the layout becomes unavailable to all users. If the removed layout was open on some user's monitor, it is immediately replaced by another layout.

3. Copy the layout (see Layout copying). If you copy the layout, you are the owner of your copy. You can edit it.

Shared layouts are sealed with the following sign:



Configuring special layouts

Creating special layouts

There are three special layouts available in *Axxon One*:

1. Marked cameras layout displays all marked cameras  .
2. Alarmed cameras layout displays all cameras with alarms  .
3. Dynamic layout displays the cameras added from the **Object Panel** in Live video mode  .

To create a special layout, do the following:

1. Click the  button to open the **Layouts** context menu.
2. Select the required layout.



The layout is created and added to the panel.

By default, the **Marked cameras** layout and the **Alarmed cameras** layout are 3*3. The **Dynamic** layout is created empty.

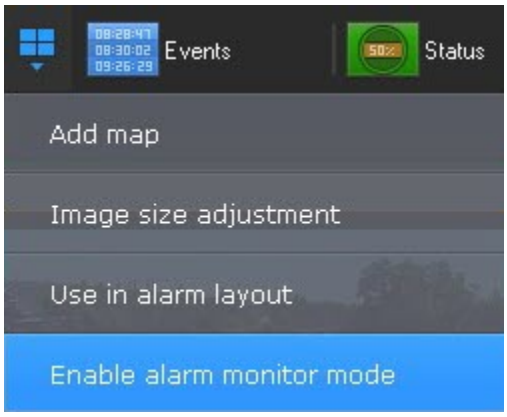
The number of cameras on the **Marked cameras** layout and the **Alarmed cameras** layout can be limited by the layout template—1, 4, 9, 16, 25, 36, 49, 64. To set the layout template, do the following:

1. Click the  button to open the context menu of the layouts.
2. Set the required template.



> **Note**
>
> To return to automatic change of the **Alarmed cameras** layout, click the format that you selected again.

You can change any standard layout to an **Alarmed cameras** layout. To do this, in the layout editing mode, open the menu and select **Enable alarm monitor mode**.



In this mode, only alarmed cameras will be displayed.

If the alarm monitor mode is enabled, the layout will be marked with the following sign 

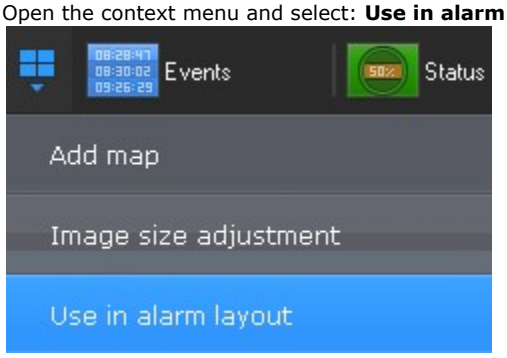
.

Configuring Alarmed cameras layout

By default, special layout display alerts from all cameras. You can limit this: alerts only from the selected layouts.

To do this:

1. Select the layout (see Selecting a layout for editing).
2. Open the context menu and select: **Use in alarm layout**.

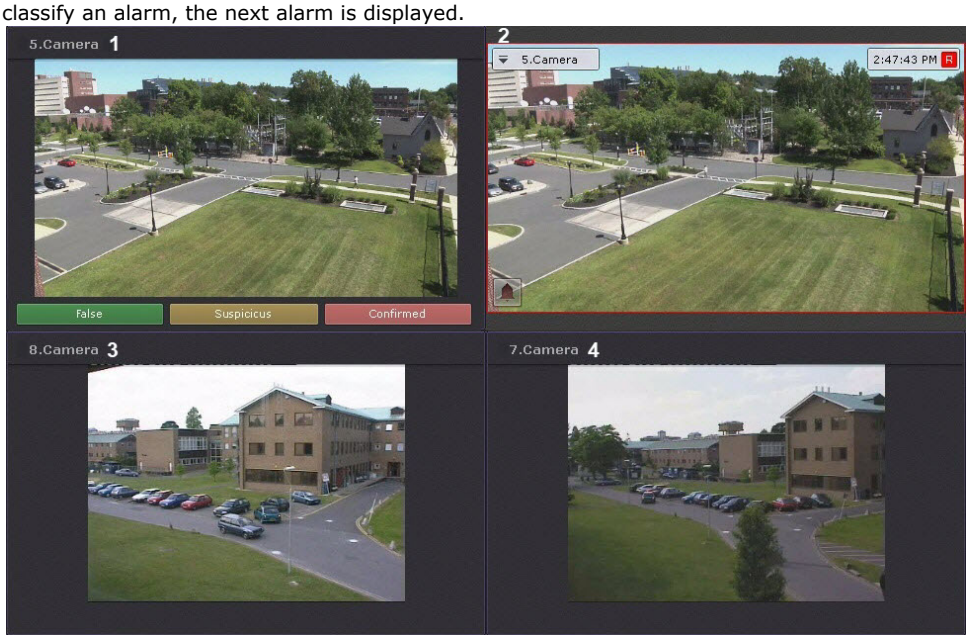


3. Save changes (see Exiting Layout Editing mode).

> **Note**
>
> To undo, select: **Disable use in alarm layout.**

Also, you can customize the layout with active alarms to show:

1. An alarm and the Alarm Management option (**1**). If there are several alarms, the longest-standing alarm is displayed. If you classify an alarm, the next alarm is displayed.

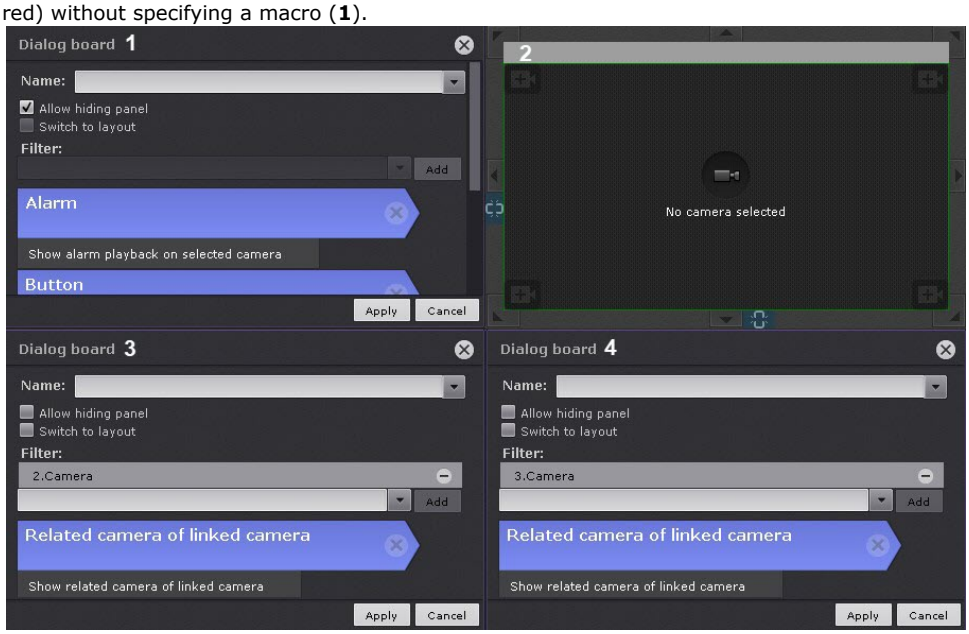


2. An alerted camera in Live Video mode (**2**).
3. 2 additional cameras (**3**, **4**) in Live Video mode (for example, the 2 nearest ones to the alarmed one).

Do the following:

1. Switch to the Layout Editing mode (see Switching to layout editing mode).

2. In the first cell, add a Dialog board (see Configuring a Dialog Board) with the **Alarm** element and 3 buttons (green, yellow and red) without specifying a macro (**1**).



3. Leave the second cell empty (**2**).
4. In the third and fourth cells, add a message panel with **Related camera of linked camera** (**3**, **4**).
5. Link cells as follows: 1 with 2, 2 with 4, 3 with 4 (see Linking cells).
6. Save the layout.
7. For each camera, select 2 stand-by cameras (for example, those closest to it, see The Camera object).

> **Note**
>
> In cell **4**, the first stand-by camera will be displayed, in cell **3** – the second.

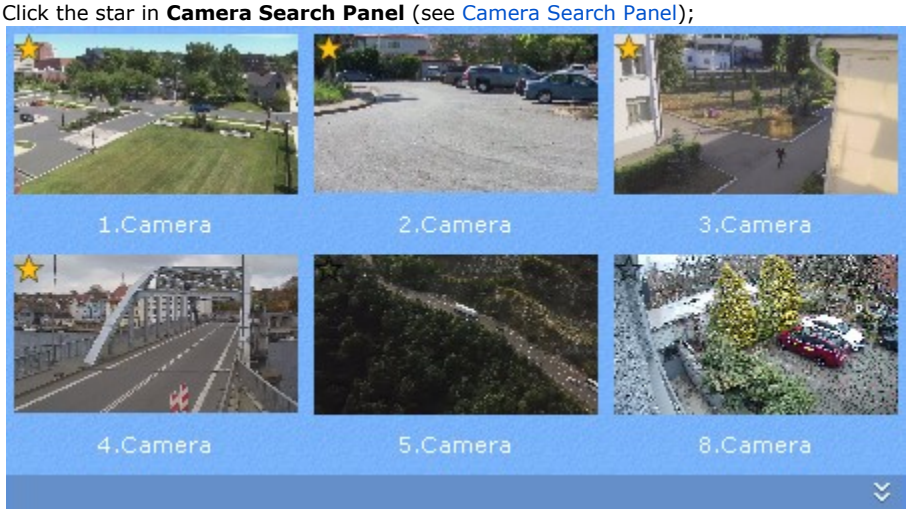
Configuring Marked cameras layout

To add a tag to a video camera, do one of the following actions:

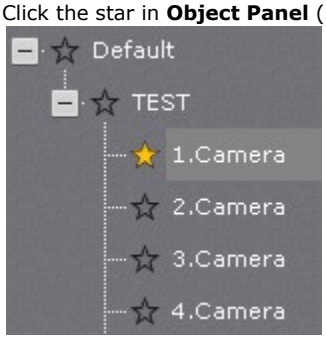
- Click the star  in the top left corner of the camera window;



- Click the star in **Camera Search Panel** (see Camera Search Panel);



- Click the star in **Object Panel** (see Objects Panel);



Attention!

You can add tags to cameras on any video wall (see Managing monitors on a local Client).

If you exceed the maximum number of cameras allowed, only the cameras most recently selected remain on the layout.

Note

To remove the tag, click the star again  .

You can move cameras around on layouts by drag-and-drop.

Attention!

Camera windows are not saved on the layout. After restarting the Client or Server, you should add them again.

Note

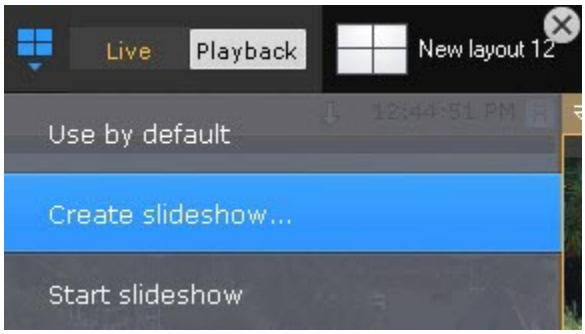
You can use Duplicate layout to create a copy of the current special layout.

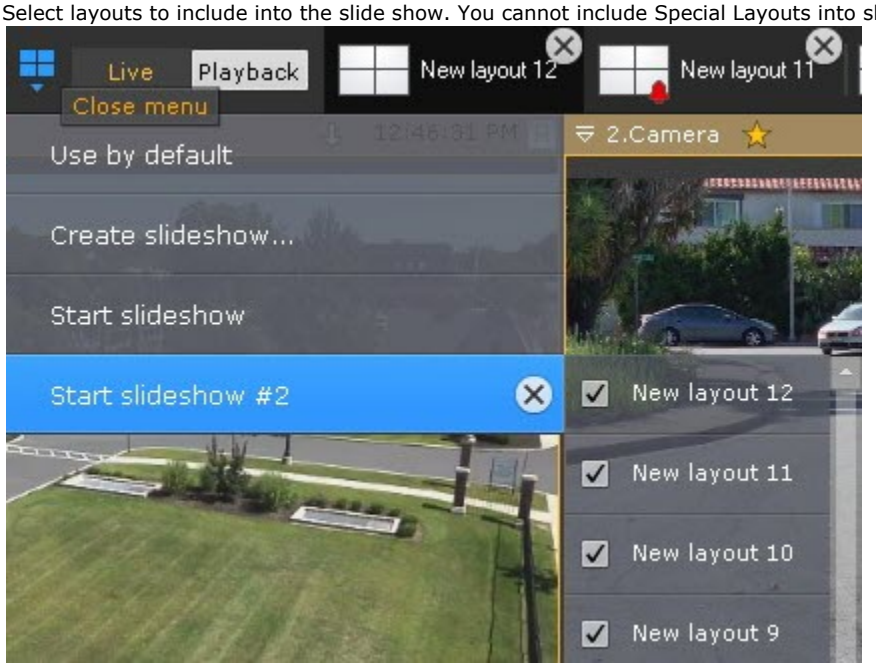
Configuring user-defined slide shows

A slide show is a set of layouts displayed on the operator's screen in a specified order for a specified dwelling time (see Configuring the slideshow parameters).

By default, the system includes only one slide show that includes all available layouts.

To create a user-defined slide show, do the following:

1. Go to Manage Layouts mode (see Creating and deleting layouts).
2. Click  and select **Create slideshow...** .


3. Select layouts to include into the slide show. You cannot include Special Layouts into slide show.


4. Click **Save**.

To remove a user-defined slide show, click the  button.

Setting the default layout

You can set a default layout to be displayed after you launch the Web Client.

To set the default layout, do the following:

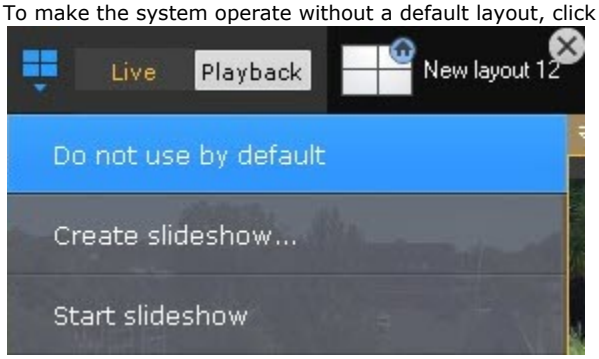
1. Go to Manage Layouts mode (see Creating and deleting layouts).
2. Go to the desired layout.
3. Click  and select **Use by default**.



Now, the current layout is assigned as default.

To assign another layout as default, repeat the steps above.

To make the system operate without a default layout, click  and select **Do not use by default**.



Setting a layout ID

You can set an ID for a layout. This may appear useful for calling layouts with hotkeys (see Notes regarding hot key actions).

To specify an ID, do the following:

1. Double click on a layout thumbnail.


2. Enter an ID.


3. Click anywhere in the Client UI.

Now, the ID is added and displayed before the layout name.



Note

When you hover the mouse cursor over a layout, the name and ID (if specified) of the layout are displayed separately.



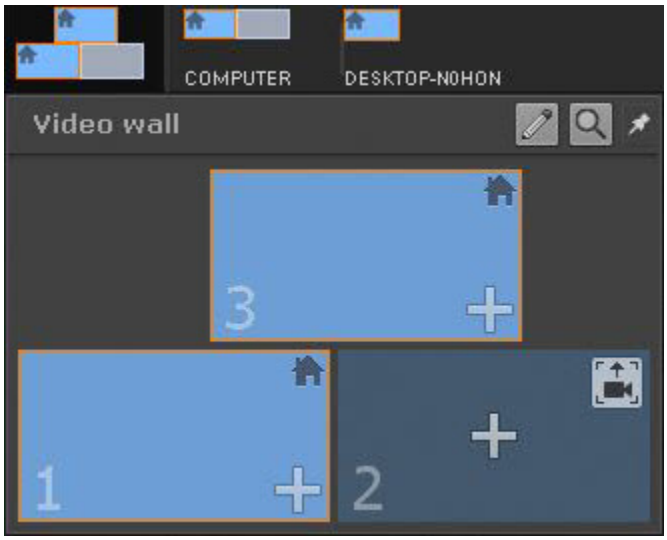
Configuring Video wall

A video wall is a set of monitors that are physically and logically connected into a single screen.

A video wall can include any monitors of all Clients of the domain. Except for cases when the user doesn't have permissions to the Servers to which some monitors in the video wall are connected (see Creating and configuring roles). In such cases, the user won't see the monitors to which they don't have access.

By default, the video wall is displayed with the initial configuration from the monitors of a local Client. However, after you make changes and save the configuration of the video wall, these changes are applied to all users in the domain.

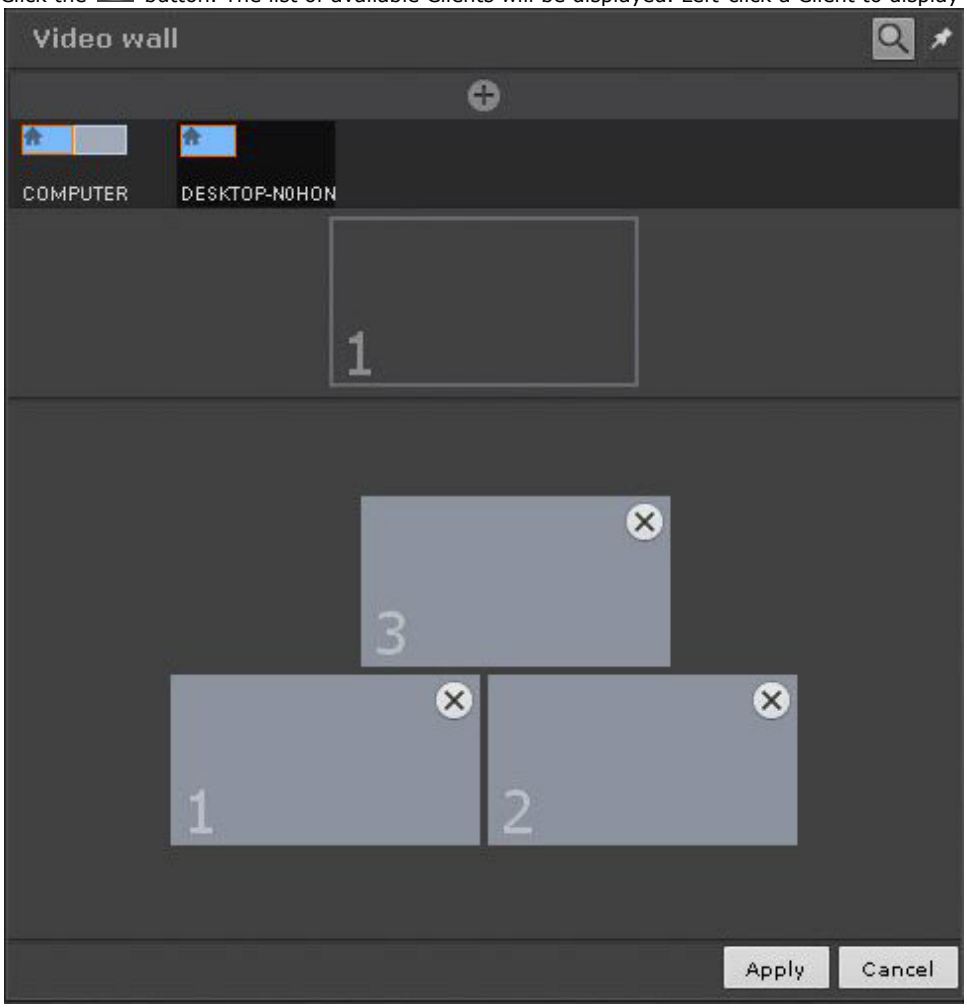
You can configure a video wall on the corresponding panel (see Video wall panel).



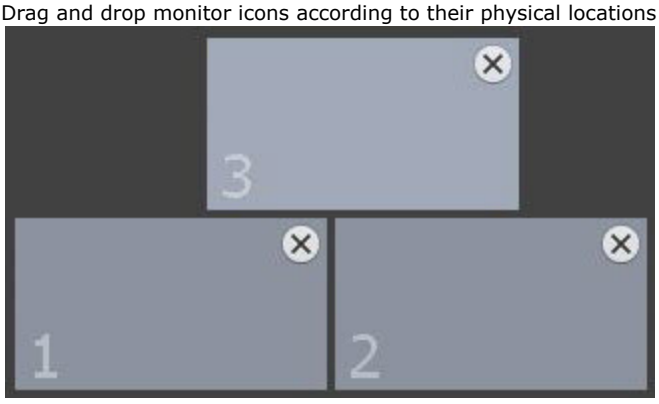
To configure a video wall, do the following:

1. Click the  button.

2. Click the button. The list of available Clients will be displayed. Left-click a Client to display its active monitors.



3. Drag and drop monitor icons according to their physical locations on the video wall.



> **Note**
>
> An ID number is assigned to each monitor added to the video wall. To display the ID number of a monitor, click the button.

4. Click the **Apply** button.

The video wall is configured.

> **Note**

You can manage the monitors of the video wall similarly to the Client monitors (see Managing monitors on a local Client, Managing monitors on remote Clients within the Axxon-domain).

Configuring the interactive map

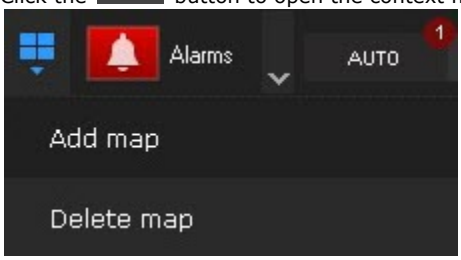
Configuration of the interactive map is performed in layout editing mode (see the sections Interactive Map, Switching to layout editing mode).

> **Note**
>
> Creation, editing, and deletion of interactive maps are available to users with roles for which the **Change maps** component is activated (see the section Configuring user permissions).

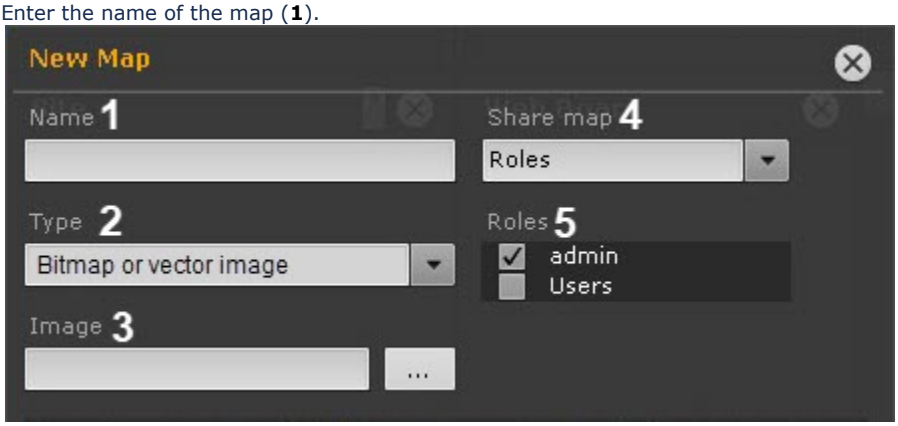
Adding a new map

Vector maps in Axxon One

To add a new map, do the following:

1. Do one of the following four actions:
   a. In the lower-left part of the screen, click the  button.
   b. Click the  button to open the context menu of the layouts panel and select the **Add map** item.


   c. Right-click the empty background of the map, from the map context menu, select the **Add new map** item.


   d. Select a camera from the list on the cameras panel with a mouse cursor and, while holding down the mouse button, move the cursor to the empty map background and then release the mouse button. The action is available, if no maps have been created in the system.
2. Enter the name of the map (**1**).


3. Select what will be used as a map (**2**, see Vector maps in Axxon One):
   a. **Bitmap or vector image**.
   b. **Google**:
      i. **Google Hybrid**;
      ii. **Google Map**;
      iii. **Google Satellite**.
   c. **OpenStreetMap.**
4. If you select the **Bitmap or vector image** type of the map, click the 

button and select the image (**3**) that will be used as a graphic plan of the protected territory.

> **Note**
>
> - The maximum image size is 4 million pixels (the number of pixels at 2000x2000 resolution). If a larger image is selected, the map won't be created.
> - If the image isn't selected, a map with a white background will be created.

Supported formats:

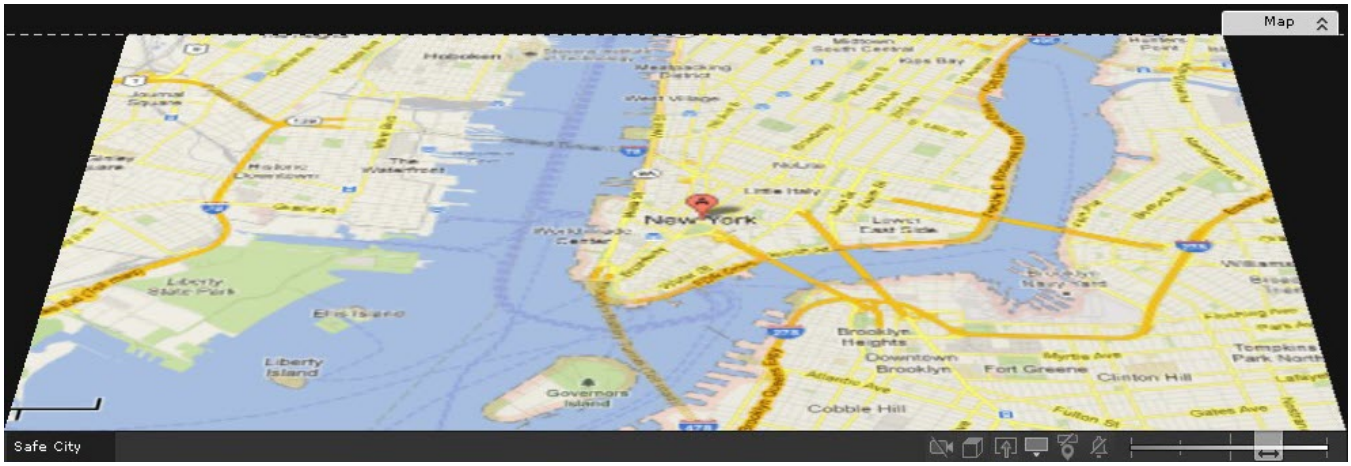
a. Bitmap: PNG, JPG, JPEG, JPE, GIF, BMP.
b. Vector image: SVG.

5. If you use a geomap, in the **Address** field (**6**), enter the address, or zip code, or geographical coordinates of the required territory on the **Google** map or **OpenStreetMap** and click the ... button. You can scale the map with the scale slider or the mouse wheel, you can move on the map in the common way.



6. Select the users for whom the map will be available (**4**):
   a. **Any user**.
   b. **Not shared**—only for the current user.
   c. **Roles**—for the users of the selected roles (**5**).
7. Click the Apply button. To cancel adding a map, click the Cancel button.

Adding a map is complete.



Adding system objects to the map

You can add these types of objects to your map:

- video cameras,
- outputs (relays),
- inputs (sensors),
- macros,
- counters,
- switches to another map.

Adding video cameras

On this page:

- General information
- Adding a video camera using the drag-and-drop method
- Adding a video camera through the menu
    - Changing the size of video camera icons

General information

You can add a video camera to the map via:

- drag-and-drop method;
- camera menu or object panel.

Adding a video camera using the drag-and-drop method

You can add a video camera to the map using the drag-and-drop method:

- from the Camera Search Panel (see Camera Search Panel);
- from the Object Panel (see Objects Panel).

When using this method:

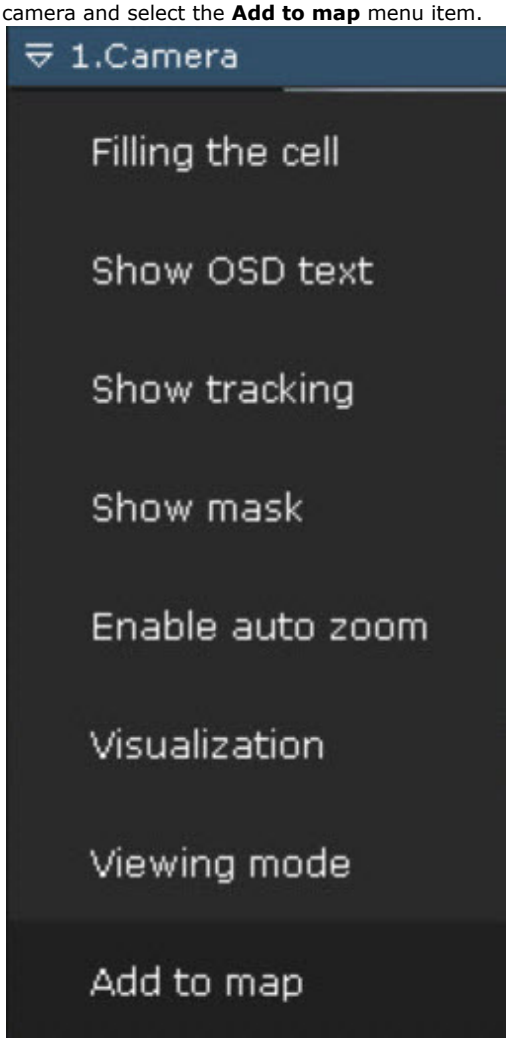
- if you add a group of video cameras, all video cameras in this group will be added to the map (see Configuring video camera groups);
- the position of the video camera is pinned at the current location on the map. When you move existing video cameras on the map, their position is also pinned.

Adding a video camera through the menu

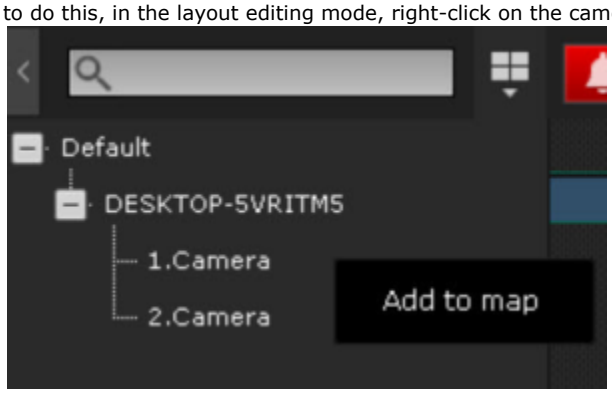
You can add a video camera to the map through the menu:

- of the video camera:

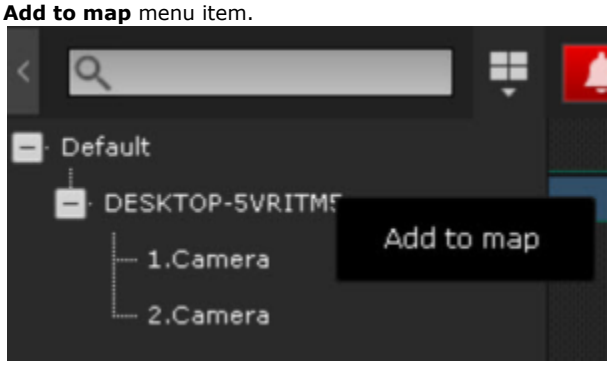
- to do this, in the layout editing mode (see Switching to layout editing mode), left-click on the short name of the video camera and select the **Add to map** menu item.



- of the object panel:
  - to do this, in the layout editing mode, right-click on the camera and select the **Add to map** menu item.



- if it is necessary to add all cameras of a group or Server, right-click on the name of the group or Server and select the **Add to map** menu item.



If the **Geo location latitude**, **Geo location longitude** and **Geo location azimuth** are specified for the camera (see The Camera object), then the video camera icon will be automatically positioned on the map in accordance with the specified coordinates.

If coordinates are not specified, the video camera icon will automatically be positioned at the center of the visible map area.

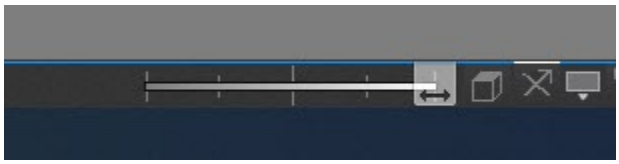
Attention!

- If the video camera's longitude and latitude values are **0**, the azimuth value will not be taken into account when adding the video camera to the map.
- **Geo location azimuth** is measured in degrees from north clockwise, where:
  - **0** degrees indicates that the camera field of view is north (up);
  - 90 degrees—east (right).
- If a video camera has a built-in GPS tracker, its location on the geomap changes automatically according to the received data (see Configuring cameras with a built-in GPS tracker).

If the camera coordinate settings are changed, it is necessary to remove the camera from the map and add it again to apply the new coordinate values.

Changing the size of video camera icons

To change the size of the video camera icons, you must use the Change icon size slider in the lower right corner of the screen in the layout editing mode.



Adding inputs and outputs

Only Input and Output objects that have been activated can be added to the map.

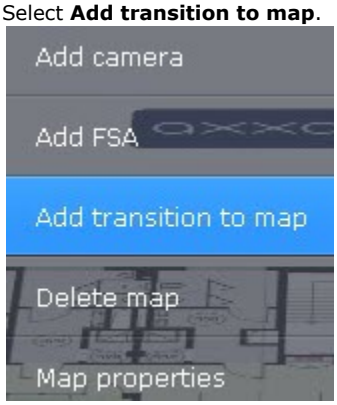
To add inputs/outputs to the Map, do the following:

1. Open **Objects Panel** (see Objects Panel).
2. Drag and drop the inputs/outputs to the map.

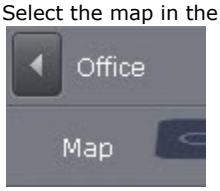
Adding switches to another map

You can add a "switch" to another map in one of two ways:

1. Select the tab of the map to which you want the switch to point and, without releasing the mouse button, drag it to the map and release the mouse button.
2. By using the map context menu.
    a. Select **Add transition to map**.



    b. Select the map in the system to which the new switch will point.



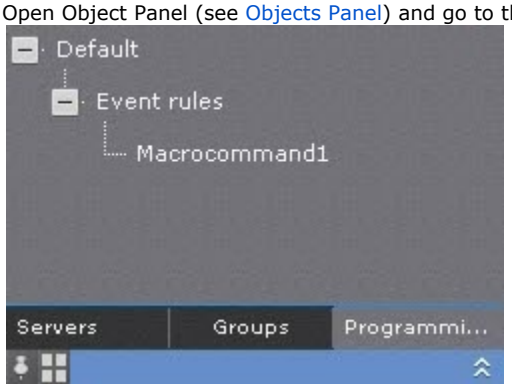
Addition of the switch is now complete.

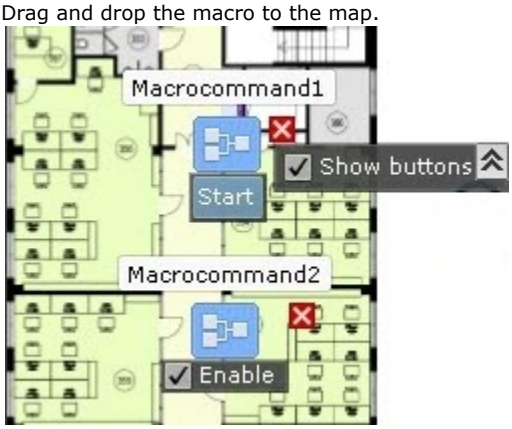


Then drag the switch icon to the necessary place on the map.

Adding macros

To add macros (see General information about the macros) to the map, do as follows:

1. Open Object Panel (see Objects Panel) and go to the **Programming** tab.


2. Drag and drop the macro to the map.


3. By default, for event-driven macros you will see the Start button, and the on/off checkbox for cyclic macros. To hide them, deselect the **Show buttons** checkbox. In this case, you can manage the macros only through the context menu.|

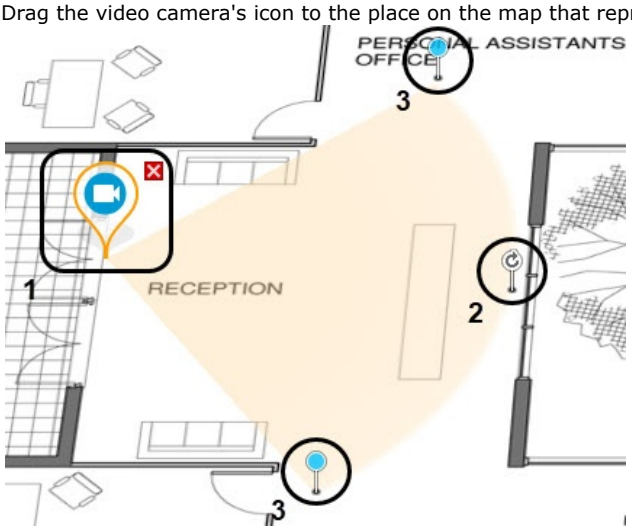
> **Note**
>
> To remove a macro from the map, click .

Configuring cameras on the map

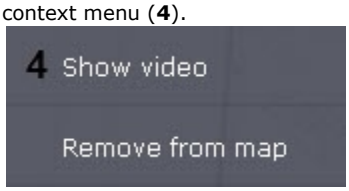
Configuring a camera in standard map viewing mode

After you add a camera to the map (see Adding video cameras), perform the following actions:

1. Drag the video camera's icon to the place on the map that represents the camera's actual location at the site (**1**).

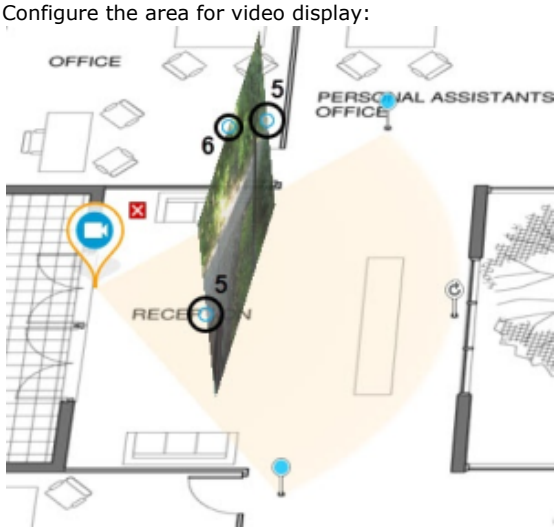


2. Set the video camera's field of view in the same direction as at the real site (**2**).
3. On the map, use the nodal points to adjust the video camera's field of view to match the actual situation at the site (**3**).
4. To display the video image, right-click on the area of the video camera's field of view and select the **Show video** item from the context menu (**4**).



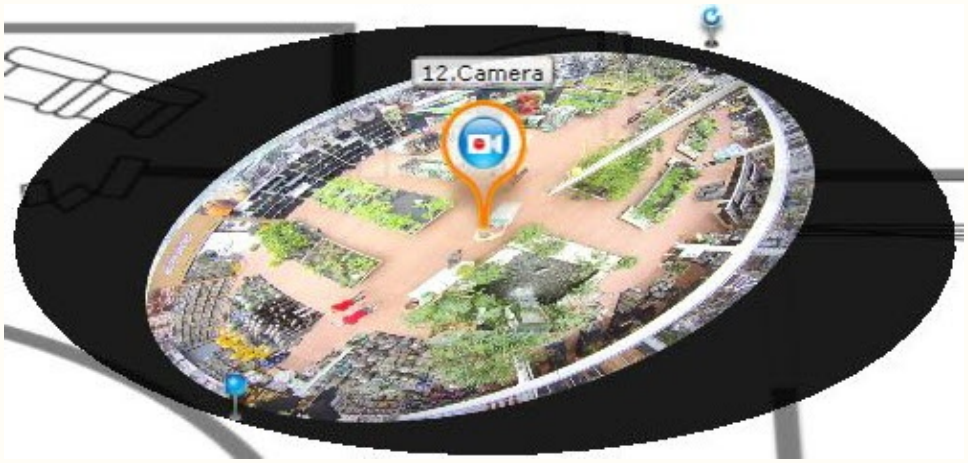
> **Note**
>
> This option (**Show video** or **Hide video**) can be configured separately from the layout editing mode. In this case, the parameter setting will be saved until the client is restarted.

5. Configure the area for video display:



Important!

To display the video image when using ceiling-mounted fish-eye cameras (see Configuring fisheye cameras), it is necessary to set the area of the camera's field of view (**3**) in the form of a circle (360° field of view). In this case, the video image from the video camera will be displayed directly in the specified area:



To enable this feature on cameras with Immervision lenses, it is necessary to select the **PTZ** display mode (see Configuring fisheye cameras).

If the camera's fish-eye field of view is different from the ceiling position, the video image display area is not available.

a. Using dots (**5**), adjust the size of the video image area – left-click the dot, hold and drag the cursor.
b. Using a dot (**6**), change the tilt angle of the area.

Note

You can switch map display to "flat" while working with the Map (see Customizing an interactive map).

c. Using the slider in the lower right corner of the screen, adjust the transparency of the video image display area.



Configuration of the camera in standard map viewing mode is complete.

Configuring cameras with an embedded GPS tracker

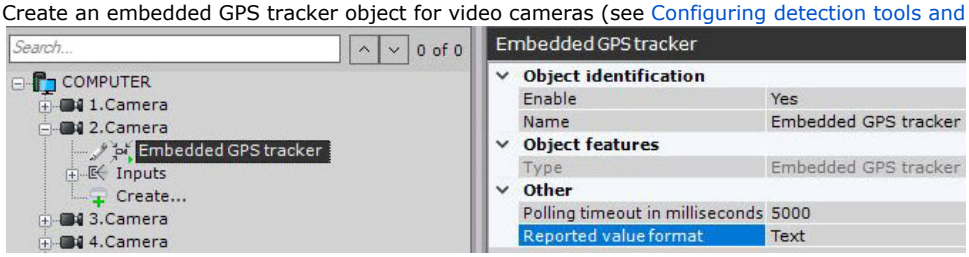
Some devices contain an embedded GPS tracker that transmits the current coordinates of the device to *Axxon One* VMS.

Location of these devices/cameras and their feeds are automatically geotagged when displayed on a geo map.

> **Note**
>
> This feature is widely used when cameras are installed, for example, in ambulances or public transport.

To enable this feature, do as follows:

1. Create an embedded GPS tracker object for video cameras (see Configuring detection tools and their sub-tools).



2. Create a geomap (see Adding a new map).
3. Add video cameras to the geomap (see Adding video cameras).

Configuring cameras in immersion mode

You can link video to the objects shown on a map. This allows making video surveillance more visual and informative.

The feature is available through immersion mode (see Immersion mode).

To link video to a map, use the four attachment points. Objects in the video need to be linked to their depiction on the site map.

To link objects with symbols on the map:

1. Click an object in the video. A point is added.

   Important!

   When specifying points on an image, follow the rules:

   1. All 4 points should belong to the same horizontal plane. Place points on the floor or on the ground.

   2. Do not place 3 points on one line.

   3. Points should show the perspective of the plane.

2. Click on the depiction of the object on the map. A second point is added, connected by a line to the first point.

Important!

When a fourth link is made, it is possible that the second point cannot be placed in some areas. This occurs when the system cannot find a valid angle for displaying the video and map for the given links. Most likely, the links have been set incorrectly.



After a fourth link is added, an angle is chosen so that the surveillance objects in the video and on the map coincide.

To remove a link, place the cursor above the first point in the link and click the button. After all links are added, it is possible to change the location of previously set points by dragging them while holding the left mouse button.

To save links between video and the map, exit layout editing mode and save changes. The links you make are discarded if any of the following occur before you exit and save changes:

- The position of the video camera icon on the map is changed.

- The angle of display of the video display area for the camera on the map is changed.
- The field of view of the camera on the map is changed in any way.

Attaching a map to a layout

You can attach a map to a layout. This means that when you switch to the layout, the attached map opens automatically.

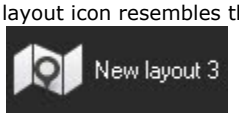
To attach a map to a layout:

1. Select the layout with which you want to associate the map in the layouts ribbon or create a new layout (see Creating and deleting layouts and Selecting a layout for editing).
2. Go to map editing mode (see the section Opening and closing the map)
3. Go to an existing map with which you want to associate the layout or create a new map (see the sections Switching between maps and Adding a new map).
4. Save changes and exit layout editing mode (see Exiting Layout Editing mode).

After you save the layout, its icon resembles than shown in picture below.



If a map is open in 2D mode when you save a layout, when you switch to that layout, the map will always open in 2D mode. The layout icon resembles that shown in picture below.



The map is now attached to the layout.

Configuring the floors

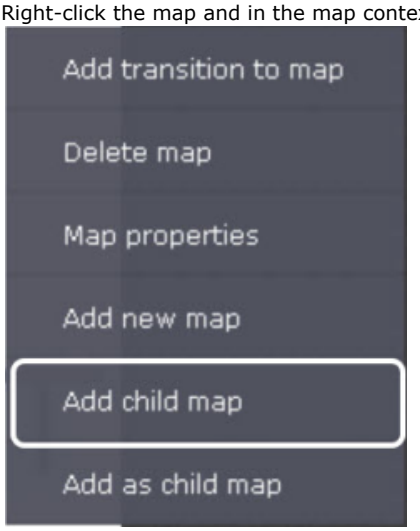
Creating a new floor

You can create a new floor in two ways: by adding child map or by adding a map as a child.

Adding child map

To add child map, do the following:

1. Right-click the map and in the map context menu, select the **Add child map** item.



> **Note**
>
> You can add a floor to an existing map (see Adding a new map).

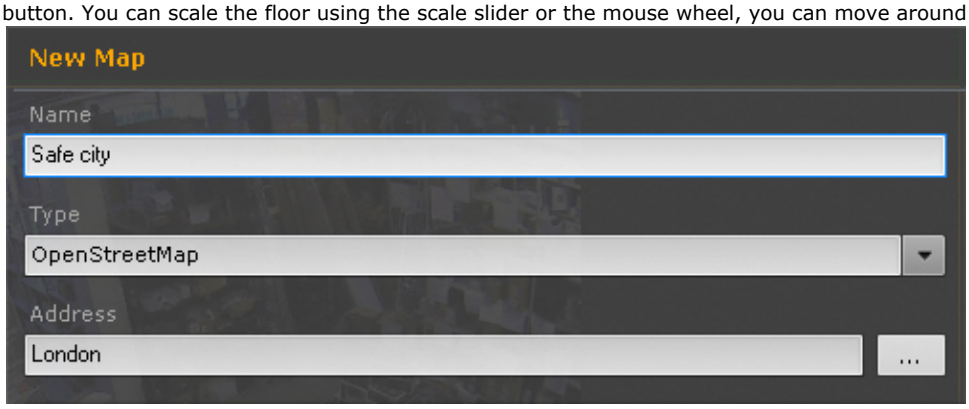
2. Enter the name of the floor (**1**).



3. Select the item that will be used as a floor map (**2**, see Vector maps in Axxon One).
4. Click the ... button and select the image (**3**), which will be used as a graphic plan of the protected area (if the **Bitmap or vector image** type is selected). The supported formats: png, jpg, jpeg, jpe, gif and bmp. If no image is selected, a floor with a white background will be created.

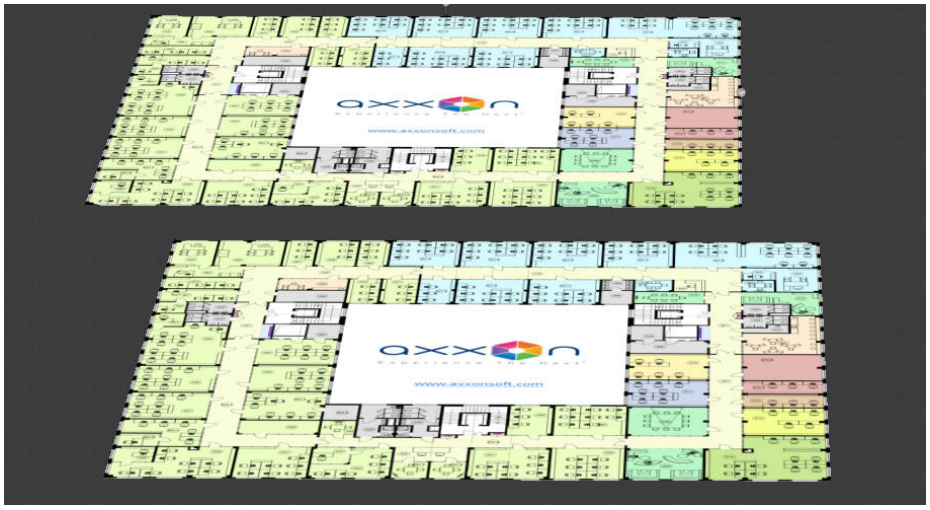
> **Note**
>
> The maximum image size is 4 million pixels (the number of pixels in the resolution 2000x2000). If you select a larger image, the floor will not be created.

5. If a geo map is used, in the **Address** field, enter either the address, or the zip code, or the geographical coordinates of the required area on the **OpenStreetMap** map (for details, see the provider's website) or **Google** map and click the ... button. You can scale the floor using the scale slider or the mouse wheel, you can move around the floor in a standard way.



6. Select the users for whom the floor will be available (**4**): for everyone, only for the current user (**Nobody** option), for users of the selected roles (**5**).
7. Click the **Apply** button.
8. If necessary, repeat steps 1–7, adding a new floor to the last created floor.

The floor is created.



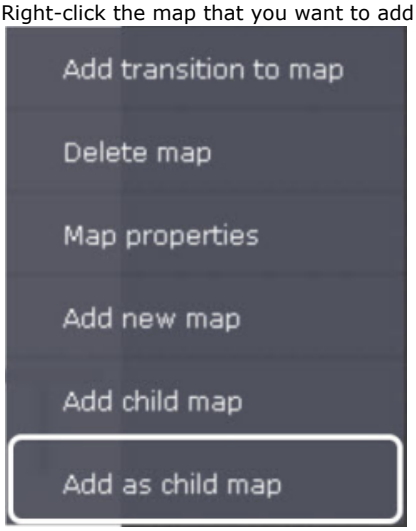
Adding as child map

Attention!

- You can only add a map as child if it does not have lower floors. At the same time, the parent map should not have upper floors.
- If a map, which is added as a child, and a parent map both are a part of map hierarchies, then these map hierarchies must be independent.
- If one of the conditions described above is not met, the **Add as child map** item will not be displayed.
- Geomaps cannot be added as top or bottom floors in a map hierarchy

To add a map as a child map, do the following:

1. Right-click the map that you want to add as a child and in the map context menu, select the **Add as child map** item.

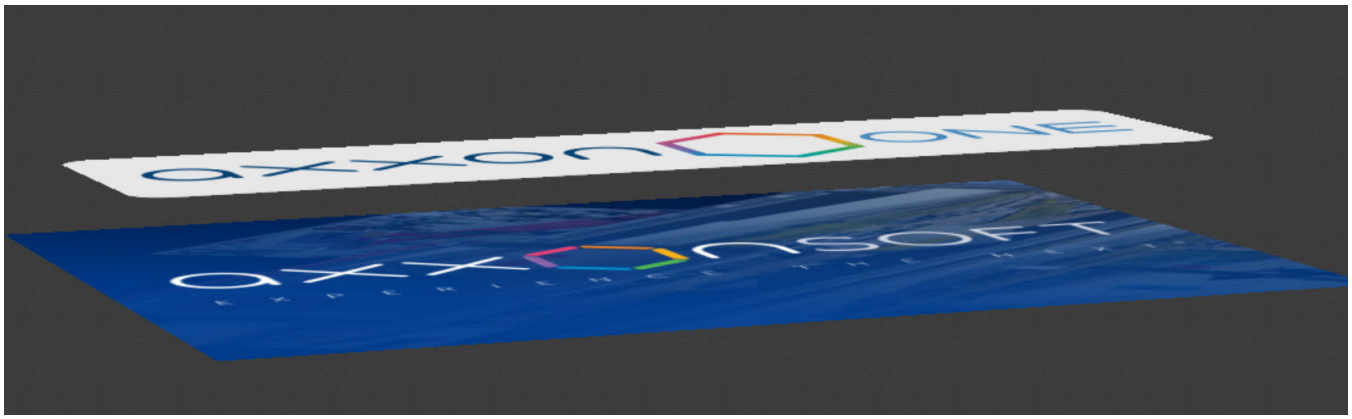


2. Select the map to which you want to add a map as a child map.



3. Click the **Apply** button.

Creating a map as a child map is complete.

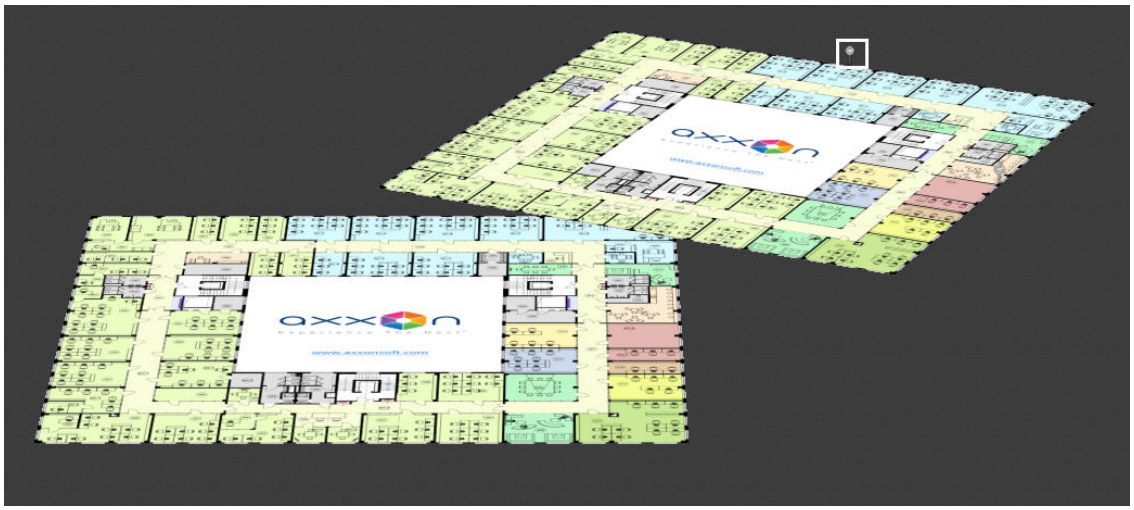


Configuring floor location on the map

To shift a floor in an arbitrary direction, click on the floor image and, while holding down the left mouse button, move the image to the required location.

> **Note**
>
> Both the selected floor and the floors created on its basis will move.

To rotate or resize the floor image, click and hold the  button, and rotate or enlarge the floor image.



Editing a floor

When you create a floor, each new floor is created as a separate map. To edit a floor, go to the tab with its map:



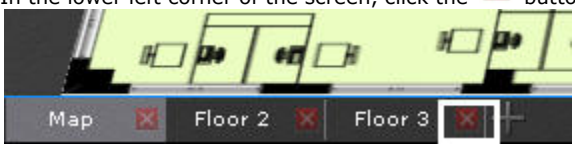
The same functions are available for editing a floor as for a map:

1. Adding objects to the floor — see Adding system objects to the map.
2. Configuring the display of added video cameras — see Configuring cameras on the map.
3. Removing objects from a floor — see Removing objects from the map.
4. Changing the type and display — see Changing map type and display.
5. Changing the name of the floor — see Renaming the map.

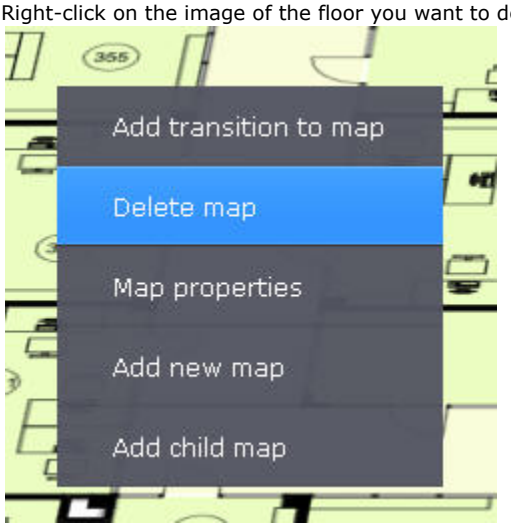
Removing a floor

You can delete a floor in two ways:

1. In the lower left corner of the screen, click the button on the tab corresponding to the floor you want to delete:



2. Right-click on the image of the floor you want to delete and select the **Delete map** item from the context menu:



Removing objects from the map

To remove an object from the map, click the button that is next to the object icon, or in the context menu, select **Remove from map**.



Note

To delete a map switch, you must click the button.

Setting keywords for geomap search

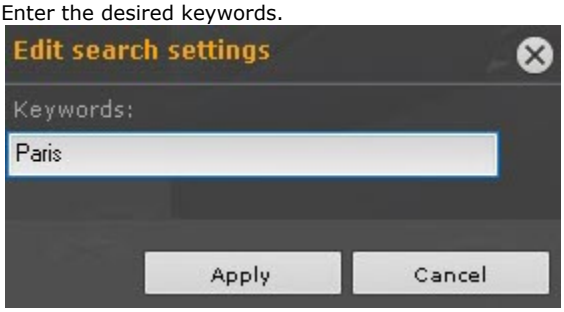
The keywords are needed to locate a site or a street on OpenStreetMap.

For example, if you are searching for a site or a street in a particular city/town, the name of the town has to be entered as a keyword.

The default keyword is the address set during the map creation process (see Adding a new map).

To set new keywords, you need to:

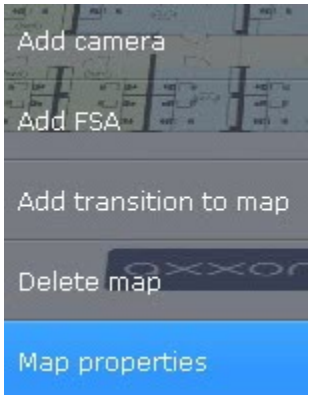
1. Click  in the lower panel.
2. Enter the desired keywords.



3. Click **Apply**.

Changing map type and display

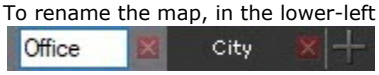
You can change the type and display of a map that has been created previously. To do so, open the map context menu and select **Map properties**.



A map properties configuration window opens, which is similar to the map creation window (see Adding a new map).

Renaming the map

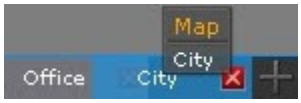
To rename the map, in the lower-left corner of the screen, left-click a tab and specify a new name.



Sorting of map lists

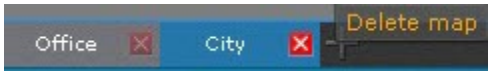
You can change the order of tabs for previously created maps. By default, tabs with maps are ordered by creation date.

To change the order, drag and drop tabs as necessary. Left-click a tab and drag it to the desired location.



Deleting a map

To delete a map, in the lower-left corner of the screen, select the button on the corresponding tab. Alternatively, in the context menu, you can select **Delete map**.





System preferences

Server settings

Configuring Forensic Search MomentQuest in Archive

On the page:

- Turning on the video stream metadata recording
- Configuring user permissions for Forensic Search in archive

To make it possible to perform Forensic Search MomentQuest of the archives of a video camera, the following conditions must be met:

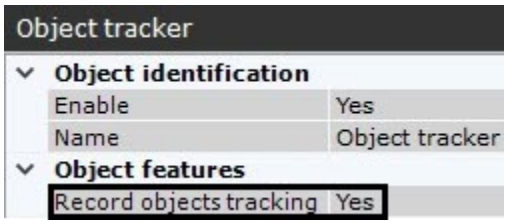
1. Video meets the requirements (see Video suitability for Forensic Search of recorded video (requirements)).
2. There are video stream recordings from the desired video camera in the archive (see Configuring recording to an archive).
3. There are metadata recordings from this video stream in the object trajectory database. Metadata can be generated by *Axxon One* (see General information on the standard detection sub-tools, Category: Face) or received from a video camera (see General information about embedded detection tools).
4. The user has the appropriate permissions.

This section contains information on how to configure the *Axxon One* software package to satisfy these conditions.

Turning on the video stream metadata recording

To enable metadata recording, select **Yes** in the **Record objects tracking** list for the corresponding detection tool (object tracker, facial recognition, base motion detection, onboard video analytics).

> **Note**
>
> The metadata recording is enabled by default.



In video motion detection (VMD) settings, you have to activate the **Object tracking** parameter (see Setting up VMD-based Scene Analytics detection tools).

> **Note**
>
> Information on configuring storage of metadata is provided in the section titled Configuring storage of the archive, system log, and metadata.

Configuring user permissions for Forensic Search in archive

You need **Live/Archive**, **Live/Archive/Control** or **Live/Archive/Control/Configure** permissions for a video camera to perform a smart search (see Configuring user permissions).


TEST
Custom
1.Camera
No access
2.Camera
No access
3.Camera
Archive only
4.Camera
Live in armed mode
5.Camera
Live
8.Camera
Live/Archive
9.Camera (-)
Live/Archive/Control
Archive Aqua
Live/Archive/Control/Configure

Video suitability for Forensic Search of recorded video (requirements)

For Forensic Search of recorded video to be possible, video must meet the same requirements as those applied to video for detection tools (see Video requirements for scene analytics detection tools).

In addition, the minimum and maximum detectable object speeds in video are related to the camera's frame rate.

1. The maximum detectable speed depends on the size of the object. The following table shows the relationship between the maximum detectable speed and the frame rate for typical objects (people and cars):

Frame rate	Maximum detectable speed for people	Maximum detectable speed for cars
6 fps	5 km/hr	40 km/hr
12 fps	10 km/hr	85 km/hr
25 fps	20 km/hr	170 km/hr

   So if it is necessary, for example, to detect people moving at speeds of up to 10 km/hr, it is sufficient to record at 12 fps.
2. The minimum object speed should be such that the object moves at a rate of at least 1 pixel per frame.

Setting up privacy masking

Masking faces

You can mask recognized faces of a designated users' group (role).

The face(s) will be masked:

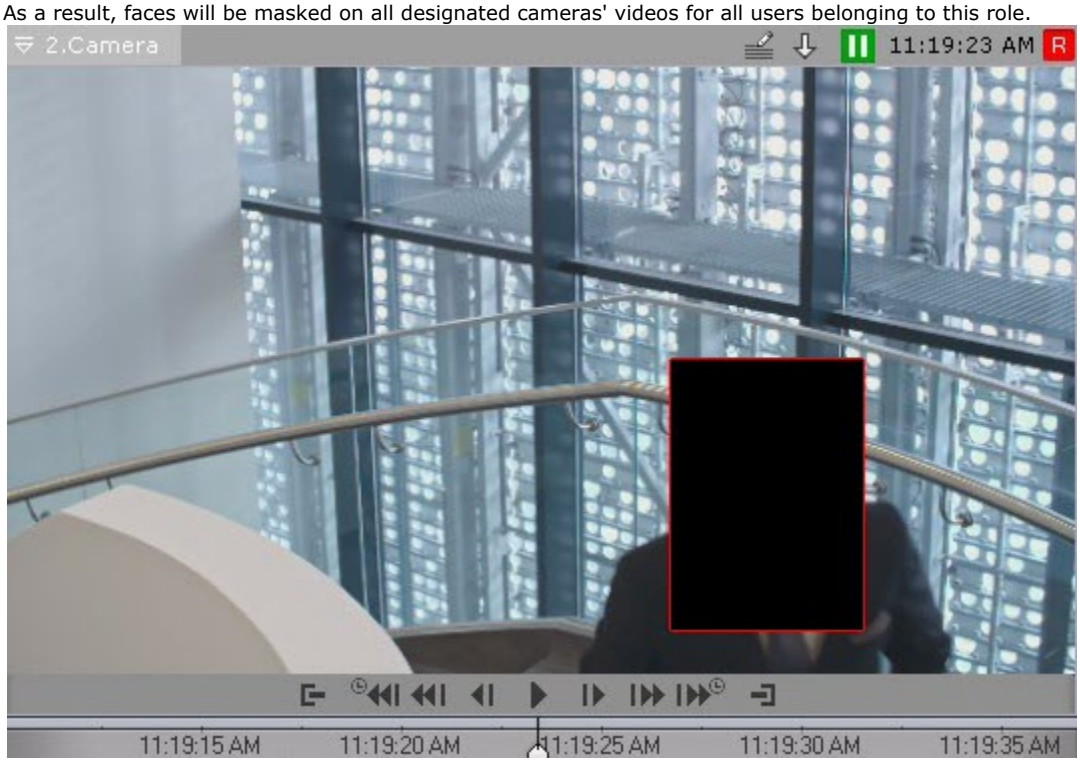
- during Live or Video Footage viewing;
- during Video Footage search.

> **Attention!**
>
> Privacy masks are displayed in the standalone Client software only. You cannot use masks with both Web and Mobile Clients.

To do it, follow the steps below:

1. Create and configure Face Detection Tools for cameras where face masking is necessary (see Category: Face).
2. Set **No** for the **Show faces** parameter in the Role Settings panel (see Creating and configuring roles).

As a result, faces will be masked on all designated cameras' videos for all users belonging to this role.



Setting up privacy masking in Video Footage

You can mask any objects from Video Footage viewing by any particular user.

The objects will be masked:

- during Video Footage viewing;
- during Video Footage search;
- on exported videos.

> **Attention!**
>
> Privacy masks are displayed in the standalone Client software only. You cannot use masks with both web and mobile Clients.

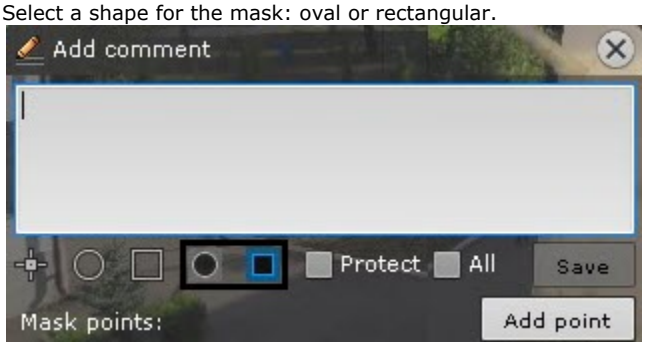
To do this, set **No** for the **View masked video** option in Role Settings (see Creating and configuring roles). The objects will be masked for all users belonging to this role.

To mask an object from Video Footage viewing, do the following:

1. Proceed to Archive Mode and find the object to be masked (see Switching to Archive Mode).
2. Locate the frame where the object first appears in the camera's FoV (see Navigating in the Archive).

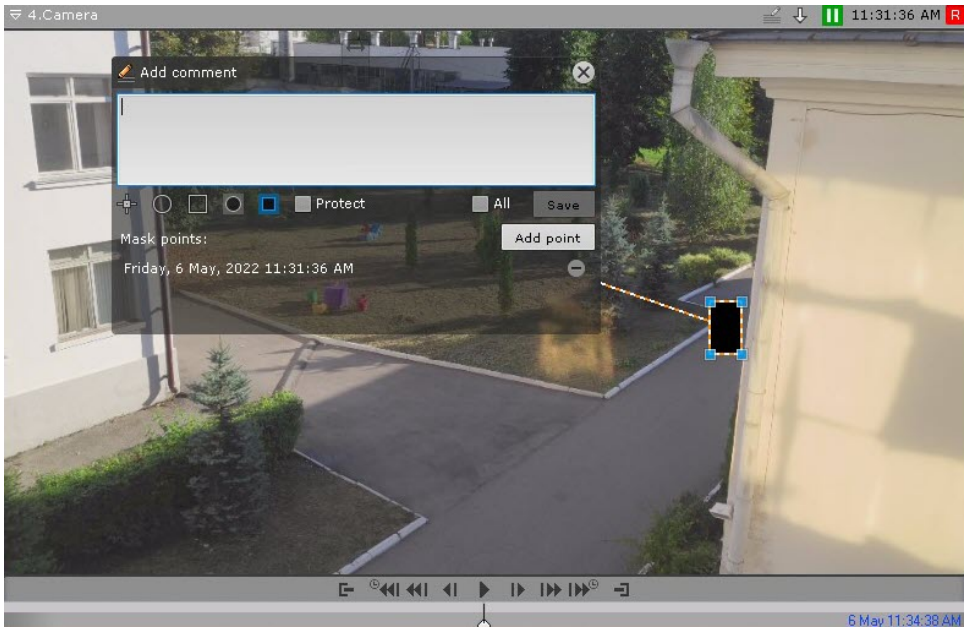


3. Click the  button.
4. Select a shape for the mask: oval or rectangular.

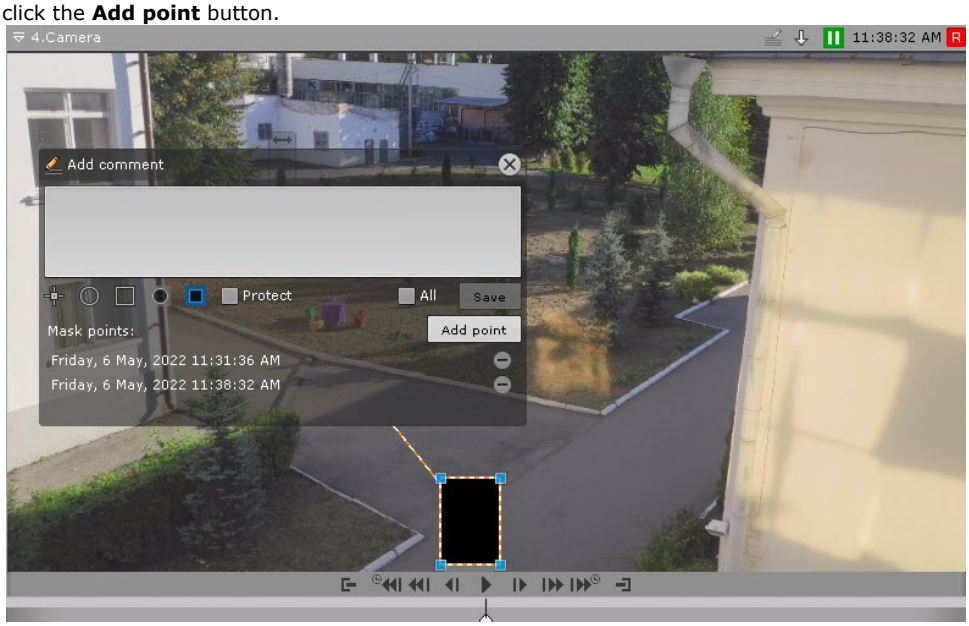


5. Apply the mask over the object.

> **Note**
>
> The procedure of setting up a mask is similar to adding a comment (see Adding a comment).

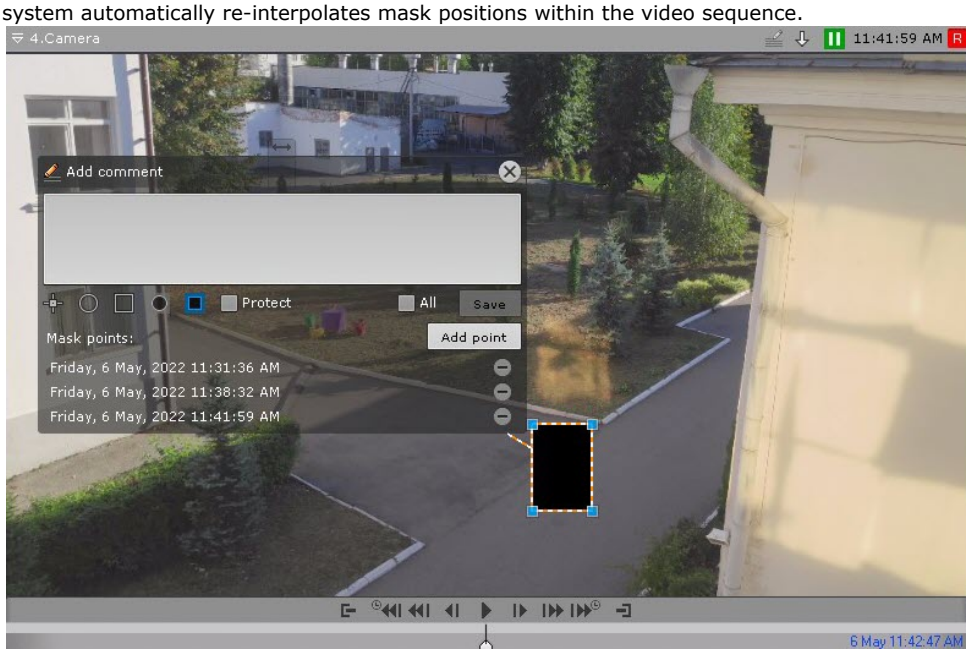


6. Locate the last frame before the object disappears from the camera's FoV and place the mask over it. To save mask position, click the **Add point** button.



7. The system automatically interpolates the mask position on intermediate frames, assuming the object's motion is uniform and rectilinear.

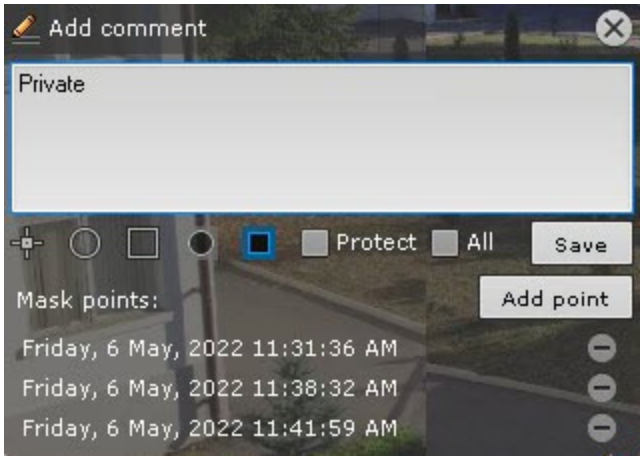
8. Check the video. If necessary, you can specify additional mask positions on intermediate frames for better masking. The system automatically re-interpolates mask positions within the video sequence.



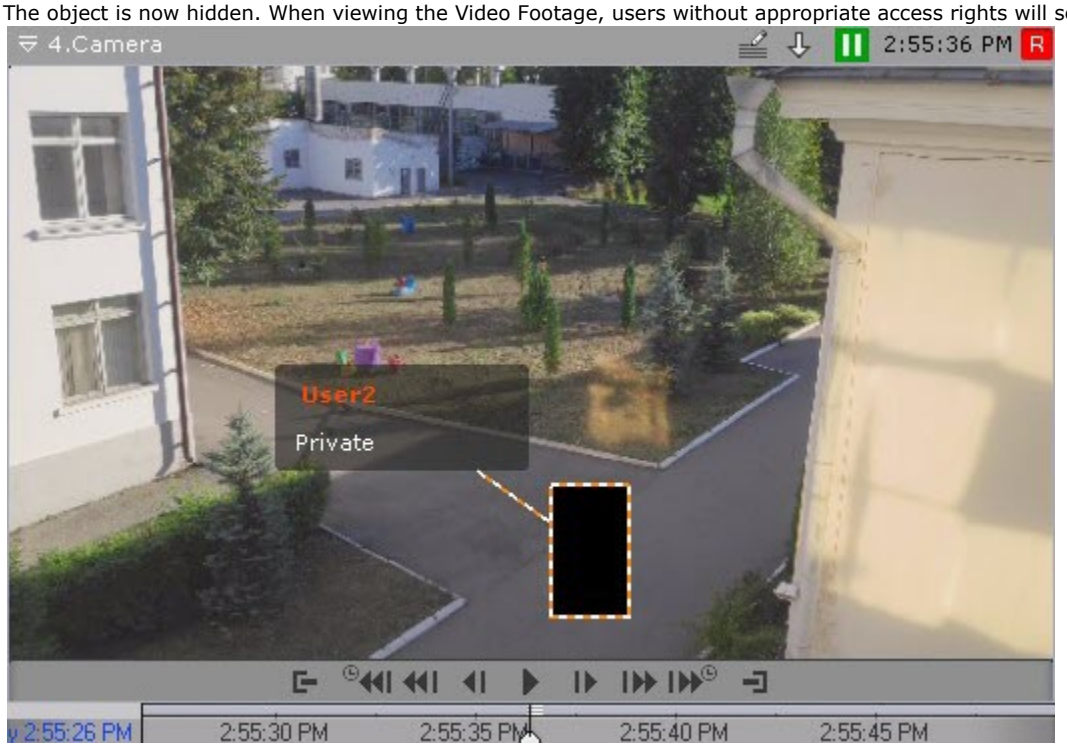
> **Note**
>
> To remove a mask position, click the button.

9. After setting all necessary mask positions, enter your text notes and click **Save**.

> **Attention!**
>
> After the mask is saved, you can not delete it. Only the users having roles where **View masked video** parameter is set to **Yes** may bypass the masking (see Creating and configuring roles).



The object is now hidden. When viewing the Video Footage, users without appropriate access rights will see the object masked.



Configuring hardware video decoding for display on the Client

In the *Axxon One* Client, there are two ways for hardware video decoding:

1. Using the Intel Quick Sync Video technology (see Hardware-based decoding with Intel Quick Sync Video).
2. Using the NVDEC chip on NVIDIA graphics cards (see Hardware-based decoding with NVIDIA NVDEC chips).

In addition, decoding with both Intel QSV and NVDEC is possible (see Simultaneous decoding with Intel Quick Sync Video and NVIDIA NVDEC chips).

> ⚠ **Attention!**
>
> Hardware decoding is not supported for the videos that were created using the YUV422 format. If hardware decoding is enabled, such video will be decoded by the software on the CPU.

Hardware-based decoding with Intel Quick Sync Video

Intel Quick Sync Video is a technology available on some Intel processors, that provides hardware acceleration for video encoding and decoding. This technology provides faster and more energy efficient processing of video content.

Attention!

Axxon One applies Intel Quick Sync Video for decoding:

1. Video in the formats: H.264, H.265 and H.265+.
2. Live mode, Archive mode (forward playback only) and TimeCompressor mode.

Attention!

If the Client shares the same computer with the Server, which applies a detection tool to a video stream, Intel Quick Sync Video will not be used for displaying this stream.

Note

Maximum pixel resolution depends on your particular version of the Intel Quick Sync. For details, refer to https://www.intel.com/content/www/us/en/homepage.html.

To use Intel Quick Sync Video, make sure your system meets the following requirements:

1. The CPU has an integrated graphics core with Intel Quick Sync Video support.

   Note

   You can check if the CPU supports Intel Quick Sync Video here.

   Attention!

   For H.265 and H.265+ video formats, Intel Quick Sync Video technology is supported only on Intel processors with microarchitecture: Braswell (only decoding), Cherry Trail (only decoding), Skylake, Apollo Lake, Kaby Lake, Gemini, Coffee Lake and newer microarchitecture.

2. The mainboard supports the GPU core (includes Flexible Display Interface).
3. The graphics driver supports Intel Quick Sync Video. We recommend using the latest version of the Intel HD Graphics Driver.

   Note

   You can also update the driver automatically using the Intel Driver Update Utility.

To enable Intel Quick Sync Video in *Axxon One*, do the following:

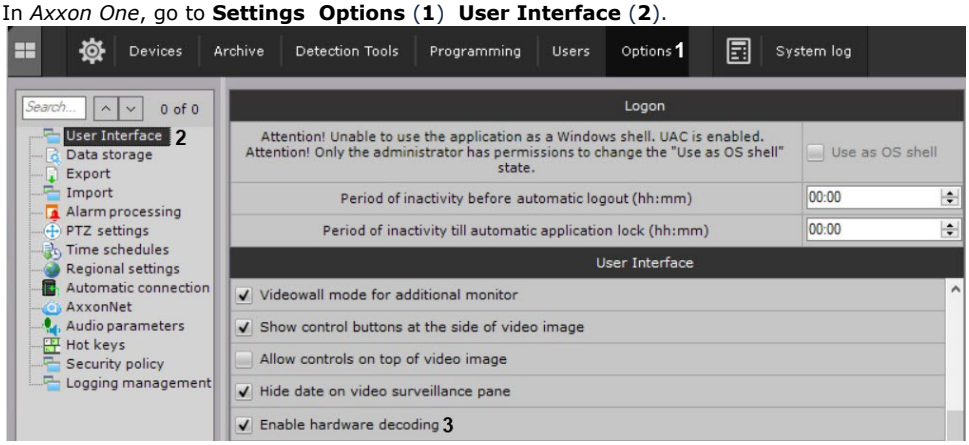
1. Enable using the integrated graphics core in the BIOS settings.

   Note

   Depending on the BIOS version, the option may be named differently (**iGPU**, **Internal Graphics**, **Integrated Graphics Adapter** – **PEG**).

2. It is not allowed to use an integrated graphics core and an external graphics card at the same time. In this case, to use Intel Quick Sync Video, do the following:
   a. Enable **Multi-Monitor** in the BIOS settings.
   b. In Windows OS connect a virtual monitor to the integrated graphics core and extend the desktop to it.

3. In *Axxon One*, go to **Settings** **Options** (**1**) **User Interface** (**2**).



4. Set the **Enable hardware decoding** checkbox (**3**).
5. Click the **Apply** button.

Intel Quick Sync Video in *Axxon One* is enabled.

Hardware-based decoding with NVIDIA NVDEC chips

NVDEC chips on NVIDIA GPUs provide accelerated hardware-based video decoding. This helps to reduce the load on the CPU and/or increase the number of the video cameras displayed on the Client.

Attention!

In *Axxon One*, the NVDEC chips are used to decode:

1. Video in the H.264, H.265 and MPEG-2 formats.
2. Live mode, Archive mode (forward playback only) and TimeCompressor mode.

Attention!

Before you start, make sure to install the latest driver for your NVIDIA GPU.

Note

A list of the devices that support decoding with NVDEC chips, see on the NVIDIA official website.

Note

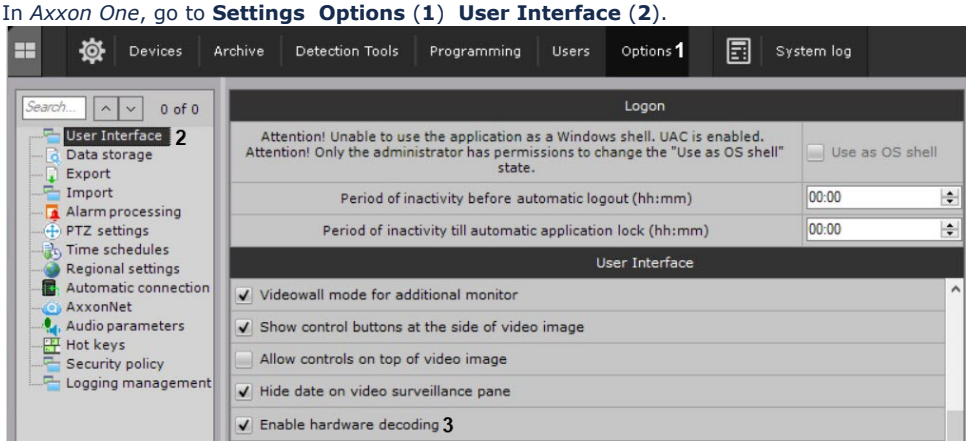
When decoding with NVIDIA NVDEC chips on portable computers due to the specifics of the devices interaction, the resources of the built-in graphics card will also be used.

When decoding with NVDEC chips, the following limitations apply:

1. Maximum video resolution for the H.264 format is 4096x4096.
2. Maximum video resolution for the H.265 format is 8192x8192.
3. The maximum total frame rate per second for the H.264 format is 648 FPS.

To enable decoding with NVDEC chips, do the following:

1. In *Axxon One*, go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. Set the **Enable hardware decoding** checkbox (**3**).
3. Click the **Apply** button.

Decoding with NVDEC chips is enabled.

Simultaneous decoding with Intel Quick Sync Video and NVIDIA NVDEC chips

Axxon One allows simultaneous decoding with Intel Quick Sync Video and NVIDIA NVDEC chips.

In this case, NVIDIA devices will be used first for decoding. When their resources end, Intel Quick Sync Video technology will be used.

For the simultaneous decoding, it is necessary to configure the decoding with Intel Quick Sync Video (see Hardware-based decoding with Intel Quick Sync Video) and with NVIDIA NVDEC chips (see Hardware-based decoding with NVIDIA NVDEC chips).

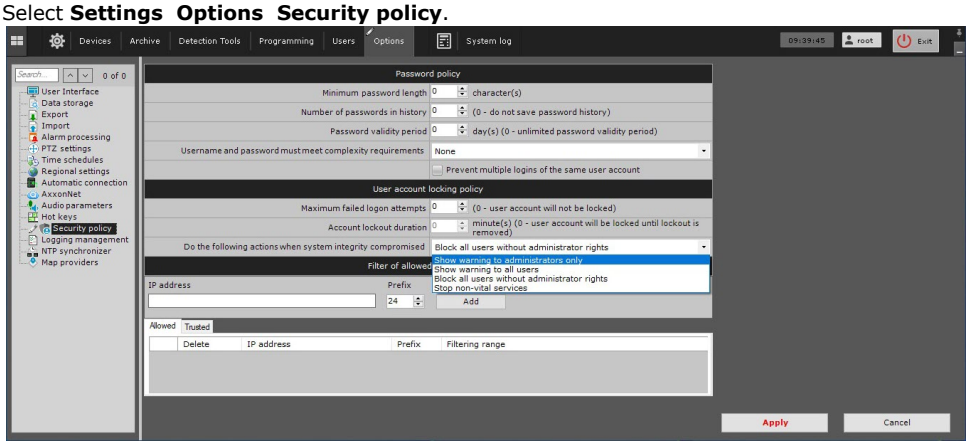
Configuring automatic response when Axxon One integrity check fails

When you start each Servers and Clients, *Axxon One* automatically checks the digital signature for all executable files (exe, dll, so).

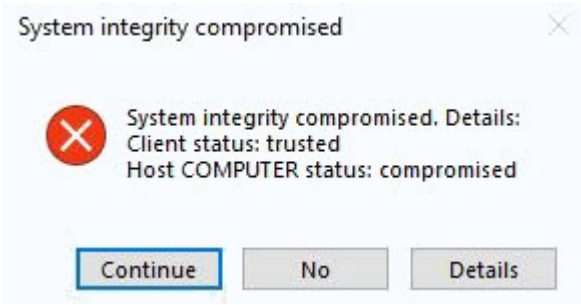
If all files are in place and match their signatures, the **System integrity check passed successfully** record appears in the system log (see The System Log).

If the integrity of system files and directories is compromised, altered by malware, or someone has attempted to hack into the system, *Axxon One* will automatically perform one of the pre-configured actions. To select the system response when integrity is compromised, do the following:

1. Select **Settings Options Security policy**.



2. From the **Do the following actions when system integrity compromised** drop-down list, select the necessary response:

Response	Description
Show warning to administrators only	Users of the **admin** role will see a warning when the Client starts. To continue launching the Client, click **Continue**. To quit, click **No**. To open a text file containing the list of compromised files, click **D etails**. 
Show warning to all users	All users will see a warning
Block all users without administrator rights	The Client will shut down and the warning will be displayed for all users, except for the users of the **admin** role. They also won't be able to connect to the Server
Stop non-vital services	Operation of all objects that are subject to licensing (cameras, detection tool, and so on) will be stopped. A warning will be displayed for all users when starting the Client

3. Click the **Apply** button.

Configuring storage of the system log and metadata

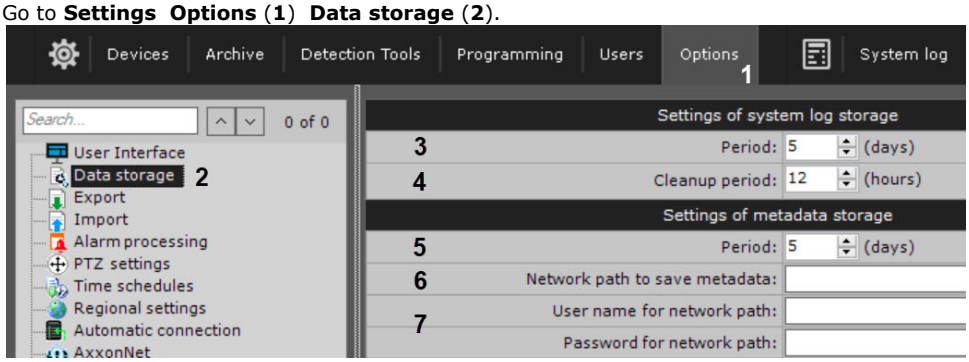
The system log is a log containing system information on events, including system error entries.

The system log is stored in a local database for each server. You can set access to the system log for a user group in the **Users** tab under **Settings** (see the section titled Configuring user permissions).

By default, metadata files are stored in Server's metadata database. The metadata storage path is set during the *Axxon One* installation (see Installation). If necessary, you can place metadata on any available network storage.

To configure storage of the system log and metadata:

1. Go to **Settings** **Options** (**1**) **Data storage** (**2**).



2. In the **Settings of system log storage** parameters group, in the **Period** field, enter the amount of days to store the system log in the Server's database (**3**). The maximum time is 1000 days.

> **Attention!**
>
> If you enter **zero** value, system Log events will be stored 0 days.

3. In the **Cleanup period** field, enter the amount of hours after which outdated events will be purged from the system log (**4**). Outdated events are events that have been stored in the system log for a period greater than that indicated in the previous step.
4. In the **Settings of metadata storage** parameters group, in the **Period** field, enter the amount of days to store metadata in the database (**5**). The maximum time is 1000 days.

> **Attention!**
>
> - If you enter **zero** value, metadata retention time becomes unlimited.
> - If you have less than 15 GB of free disk space, the metadata DB is overwritten, that is, the new data is recorded over the oldest data records (see General information about the self-diagnostics service).

> **Note**
>
> The metadata database is purged of video recordings that have been stored for more than the specified storage period:
>
> a. Every 12 hours after *Axxon One* is started.
> b. Every time you start the MomentQuest forensic search tool (see Forensic Search for Fragments (MomentQuest)).
>
> If the camera is not recording when DB is cleaned up, then its recordings are preserved irrespective of their timestamp.

5. The metadata database can be stored on NAS if necessary (by default, it is located locally as set during Installation). Do the following:

   a. Enter a path to the network destination for metadata database (**6**).
   b. Enter the user name and password (**7**). The user must have permissions to access the NAS.

> **Note**
>
> If you clear the path to NAS, metadata will be stored in the local database again

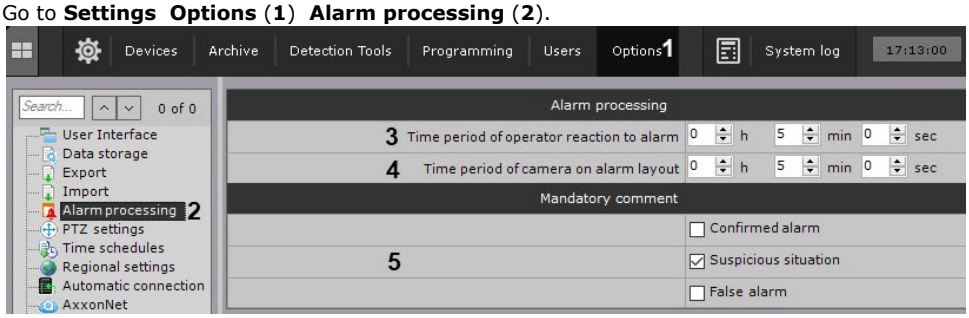
6. Click the **Apply** button.

Configuration of the system log is now complete.

Configuring Alarm processing

To configure alarm processing in the system, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **Alarm processing** (**2**).



2. In the **Time period of operator reaction to alarm** field, enter the time during which the alarm should be taken into processing, otherwise it will be assigned the **Skipped** status (**3**). The minimum value is 2 minutes.

> **Note**
>
> To take an alarm into processing, it is necessary to switch to the alarm management mode.

> **Note**
>
> After an alarm is taken into processing, the time for handling it is not limited.

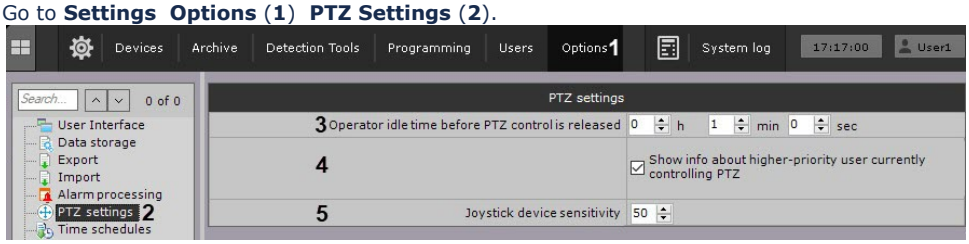
3. Set the maximum time for an alarm to stay on a special layout (**4**, see Working with Special layouts). After the specified time has elapsed, the alarm will be removed from the layout and its place will be taken by the next one, which has not yet been displayed on the layout.
4. Select the alarm assessment, after accepting which the operator is required to enter a comment (**5**).
5. Click the **Apply** button.

Configuration of alarm processing is now complete.

Configuring PTZ control

To configure PTZ control, do as follows:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **PTZ Settings** (**2**).



2. Set the operator idle time in hours, minutes and seconds (**3**). When the time runs out, the PTZ control is unlocked automatically if the operator did not perform any actions.
3. By default, if the higher priority user controls the PTZ camera, then the PTZ control panel displays the name of the user. To disable the display of this information, clear the corresponding checkbox (**4**).
4. Set the **Joystick device sensitivity** (**5**, see Joystick Configuration). The sensitivity range depends on the value specified in the device model repository for a particular device.

> **Note**
>
> For example, the following is specified in the Axis T8311 device model repository:
>
> ```
> <property id="deviceSensitivity" xsi:type="PropertyIntRangeType">
> <value>
> <min>5</min>
> <max>100</max>
> <default>50</default>
> </value>
> </property>
> ```
>
> This means that the sensitivity for this device can be set in the range from 5 to 100.

5. Click the **Apply** button.

PTZ control is now configured.

Controlling a PTZ Camera

Creating and configuring roles

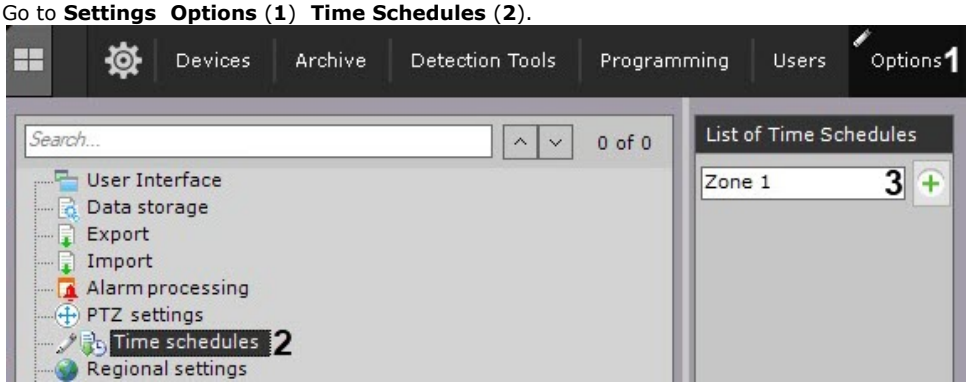
Configuring schedules

A schedule consists of all the time intervals for which video streams from video cameras will be recorded to archive.

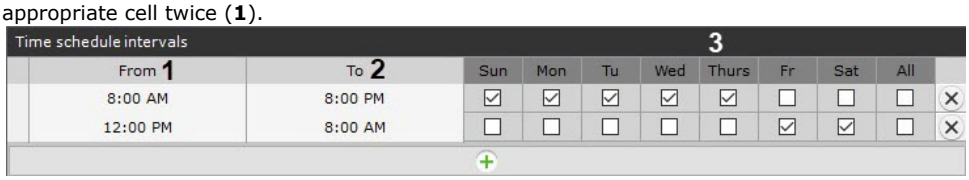
Creating schedules

To create a schedule, complete the following steps:

1. Go to **Settings** **Options** (**1**) **Time Schedules** (**2**).



2. In the **List of Time Schedules**, enter the name of the required schedule (**3**) and click  .
3. Set the time intervals for the schedule:
   a. Enter the interval's start time in the **From** column with the help of the buttons accessible by left-clicking the appropriate cell twice (**1**).

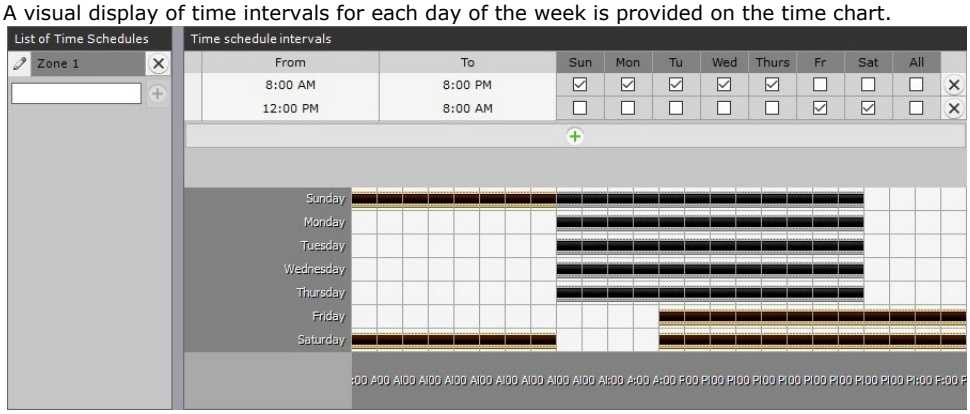


Button	Action
	Shift the interval start back by 1 hour
	Shift the interval start back by 5 minutes
	Shift the interval start ahead by 5 minutes
	Shift the interval start ahead by 1 hour

   b. Enter the interval's end time in the **To** column with the help of the buttons accessible by left-clicking the appropriate cell twice (**2**).
   c. Select the days of the week to be included in the interval by selecting the appropriate check boxes (**3**).
   d. Create the necessary number of intervals to be included in the schedule.

> **Note**
>
> To delete a time interval, click  in the corresponding row.

A visual display of time intervals for each day of the week is provided on the time chart.



4. Click the **Apply** button.

Creation of a schedule is now complete.

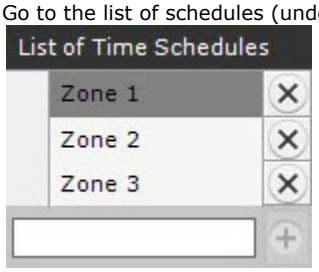
Configuring recording to an archive

Create Macros

Deleting a schedule

To delete a schedule, complete the following steps:

1. Go to the list of schedules (under **Settings Options Time Schedules**).



2. Click  beside the schedule that you want to delete.
3. Click the **Apply** button.

Deletion of a schedule is now complete.

Configuring the Server ports

On this page:

- Changing the gRPC API port
- Changing the port range of the Server

After *Axxon One* is installed, you can change the port range for Servers, the gRPC API port number (see Ports used by the Axxon One Software Package).

Changing the gRPC API port

To change the gRPC API port number, create an NGP_NATIVE_BL_PORT system variable, and set its value to the required port number (see Appendix 9. Creating system variable).

Changing the port range of the Server

To change the port range for a Server, use the Network settings utility (see Network settings utility).

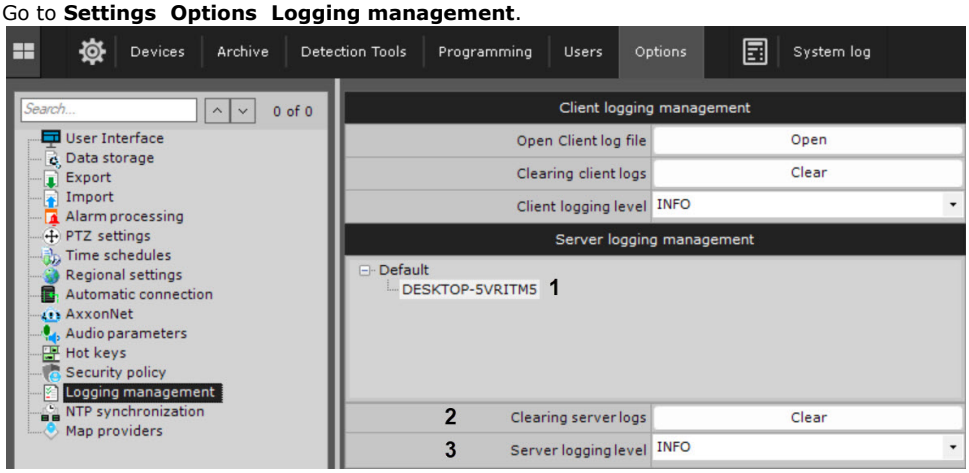
Configuring the Server logging level

By default, the Server logging level is determined by the settings specified in a special utility (see Log Management Utility). But you can temporarily change the Server logging level for operational analysis of current logs.

Changes made to the logging level will remain in effect until the Server is turned off. The next time you start the Server, the logging level will correspond to the one specified in the Log management utility.

To temporarily change the Server logging level, do as follows:

1. Go to **Settings Options Logging management**.



2. Select the Server of Axxon-domain for which you want to change the logging level (**1**).
3. Select the required level from the **Server logging level** list (**3**). Levels are described in Configuring the logging levels.
4. Click the **Apply** button 

.

The Server logging level is temporarily changed.

You can also delete all Server logs. To do this:

1. Next to the **Clearing server logs** area (**2**), click the **Clear** button.
2. Click **Apply**.

All Server logs are deleted.

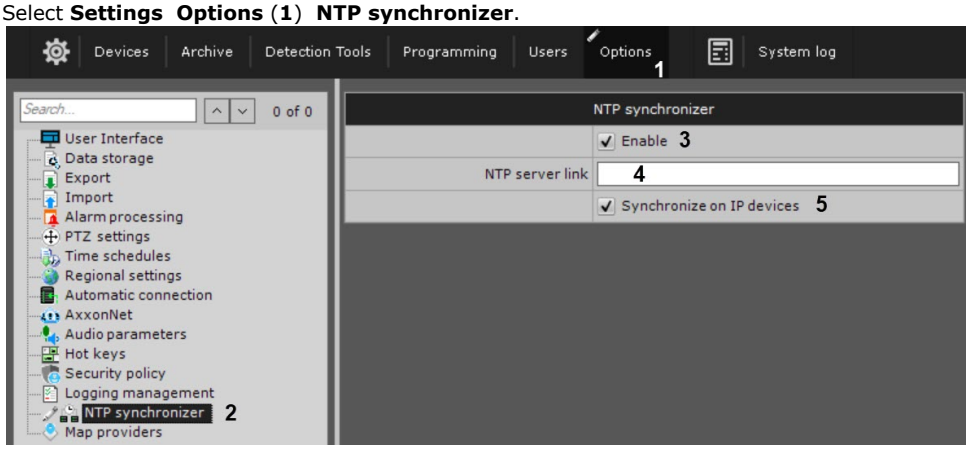
Configuring NTP synchronization

By default, the server time is synchronized with the OS time. It is possible to synchronize the server time with the NTP Server. For this, the following conditions should be met:

1. *Axxon One* is installed in Windows OS.
2. In Windows OS, the **Set time zone automatically** option is enabled. To enable it, in Windows 10, go to **Settings Time & Language**.

To configure NTP synchronization, do the following:

1. Select **Settings Options** (**1**) **NTP synchronizer**.



2. Set the **Enable** checkbox (**3**) to enable NTP synchronizer.
3. In the **NTP server link** field (**4**), specify the address of the required NTP Server.
4. Set the **Synchronize on IP devices** checkbox (**5**) to enable time synchronization for the IP devices connected to the Server.

> **Note**
>
> NTP time synchronization on IP devices works only for devices that support this feature.

5. Click the **Apply** button.

NTP synchronization will be performed automatically once every 24 hours, and when the settings are changed.

Vector maps in Axxon One

On the page:

- Adding vector maps
- Bitmap or vector image
- Google
- OpenStreetMap

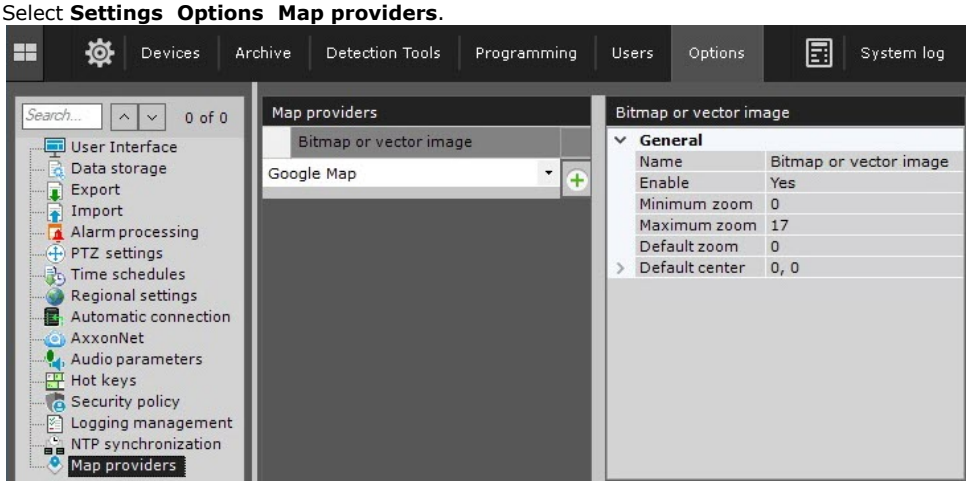
You can use vector maps in *Axxon One*: Bitmap or vector image, Google Map, and OpenStreetMap.

Adding vector maps

In *Axxon One*, a **Bitmap or vector image** map is added by default. You cannot delete it.

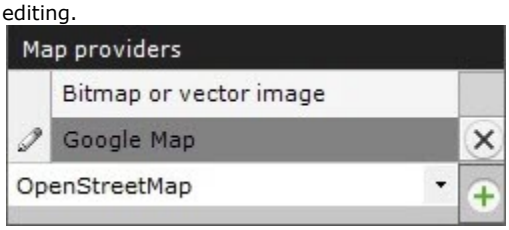
To add vector maps as an interactive map to *Axxon One*, do the following:

1. Select **Settings** **Options** **Map providers**.



2. In the **Map providers** table, click the button. From the list, select the necessary map provider and click the button.

Adding a vector map to *Axxon One* is complete. The map of the selected provider will be displayed in the table and will be available for editing.



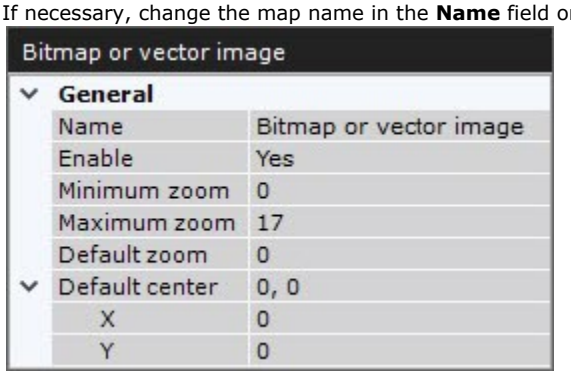
To cancel adding a vector map or to delete a map, click the button.

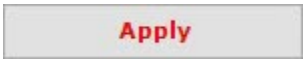
Bitmap or vector image

Bitmap or vector image is an image that will be used as a graphic plan of the protected territory.

To configure the map display as a bitmap or vector image in *Axxon One*, do the following:

1. If necessary, change the map name in the **Name** field or leave the default name.



2. In the **Enable** field, select the **Yes** value to enable **Bitmap or vector image**.
3. Set the **Minimum zoom** and **Maximum zoom** of the map. The values must be in the range [0; 19].
4. In the **Default zoom** filed, set the scale of the map that will be displayed by default. The value must be in the range [0; 19].
5. In the **Default center** field, set the coordinates of the map center that will be displayed by default:
    a. **X**—latitude;
    b. **Y**—longitude.
6. Click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.
7. Restart the *Axxon One* Client (see Shutting down an Axxon One Client, Starting the Axxon One Client).
8. Configure the map display (see Adding a new map).

Configuring the display of the **Bitmap or vector image** map in *Axxon One* is complete.

Google

You can use **Google Map** in *Axxon One*. To use **Google Map** as an interactive map in *Axxon One*, do the following:

1. Sign up with Google Maps and purchase a license:
    a. Sign up with Google Cloud. To do this you need to contact one of Google Cloud partners: https://cloud.withgoogle.com/partners/, which will give you access to the Google Cloud console (user account) after signing up.

    > **Note**
    >
    > Individuals can sign up with Google Cloud on their own. In this case, the Credit Card will be used for payment.

    b. Subscribe and, in the account, find a link to Api Key that you will need to use for each *Axxon One* Client. Charging will be done by subscription, the company will receive invoices for payment. You can see the prices here: https://developers.google.com/maps/billing-and-pricing/pricing?hl=en.
    c. Configure Google Maps using 2D Tiles.
2. Configure **Google Map** display in *Axxon One:*
    a. In the **General** section:

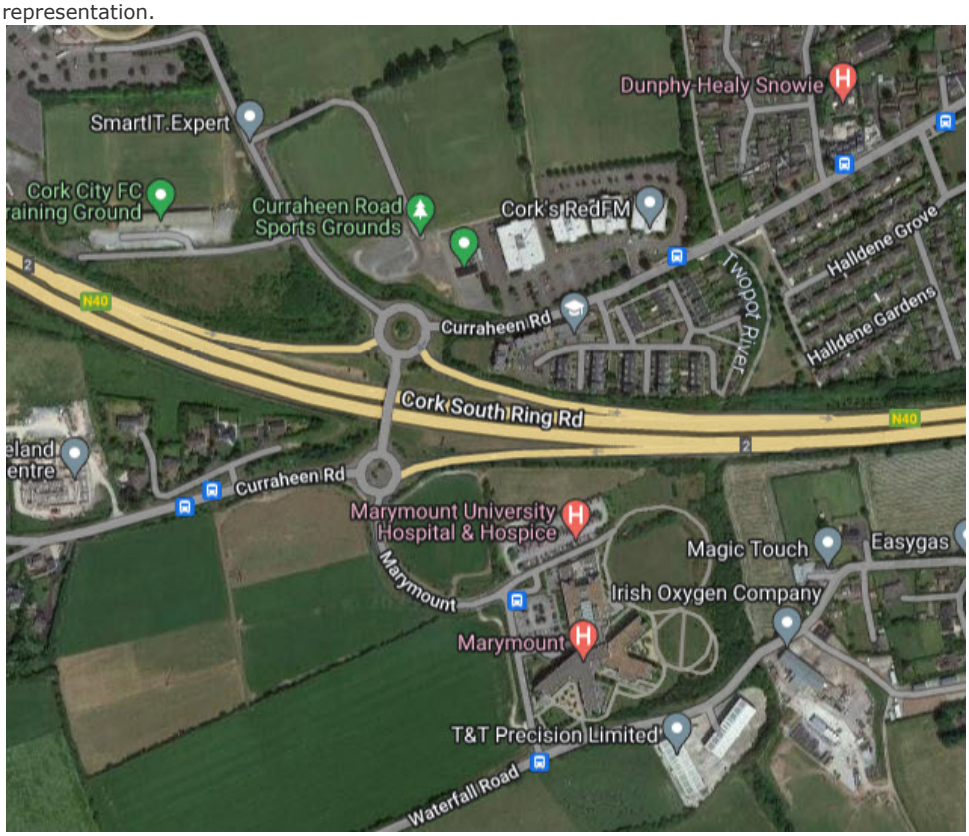
i. If necessary, change the provider name in the **Name** field or leave the default name.

Google Map	
General	
Name	Google Map
Api key	
Google Map	
Name	Google Map
Enable	Yes
Minimum zoom	3
Maximum zoom	19
Default zoom	9
Default center	0, 0
X	0
Y	0
Google Hybrid	
Name	Google Hybrid
Enable	No
Minimum zoom	3
Maximum zoom	17
Default zoom	9
Default center	0, 0
X	0
Y	0
Google Satellite	
Name	Google Satellite
Enable	No
Minimum zoom	3
Maximum zoom	17
Default zoom	9
Default center	0, 0
X	0
Y	0

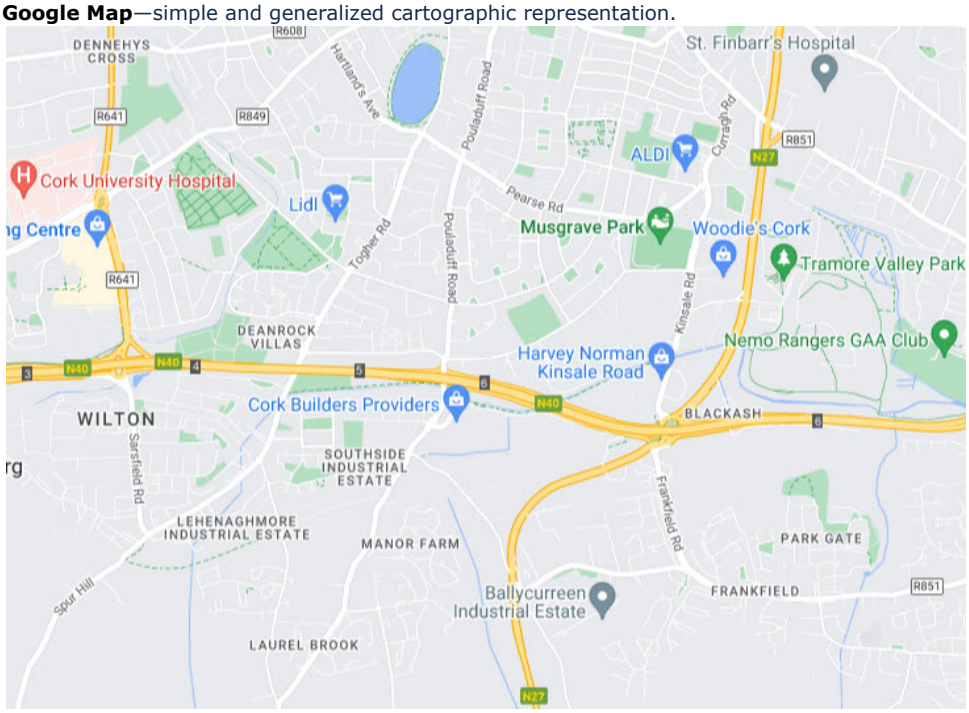
ii. Enter the received **ApiKey**.

b. Select the type of the map display:

i. **Google Hybrid**—satellite cartographic representation combined with a simple and generalized cartographic representation.



ii. **Google Map**—simple and generalized cartographic representation.



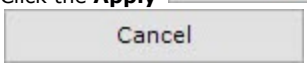
iii. **Google Satellite**—satellite cartographic representation.



> **Note**
>
> In *Axxon One*, you can use all three types of **Google** maps to display on the layout (see Adding a new map).

c. Configure the settings of the selected type of the map display:
   i. If necessary, change the map name in the **Name** field or leave the default name.
   ii. In the **Enable** field, select the **Yes** value to enable **Google Hybrid**/**Google Map**/**Google Satellite**
   iii. Set the **Minimum zoom** and **Maximum zoom** of the map. The values must be in the range [0; 19].
   iv. In the **Default zoom** filed, set the scale of the map that will be displayed by default. The value must be in the range [0; 19].
   v. In the **Default center** field, set the coordinates of the map center that will be displayed by default:
      1. **X**—latitude (**8**);
      2. **Y**—longitude (**9**).

d. Click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

e. Restart the *Axxon One* Client (see Shutting down an Axxon One Client, Starting the Axxon One Client).

f. Configure the map display (see Adding a new map).

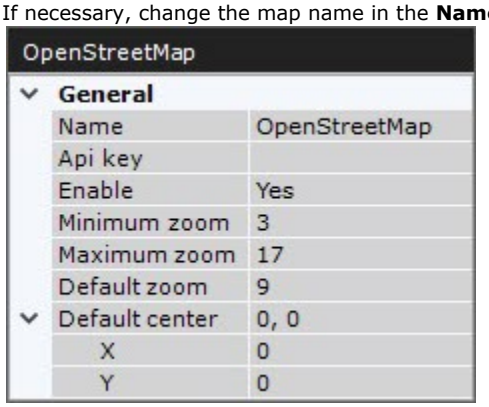
Configuring the display of **Google Map** in *Axxon One* is complete.

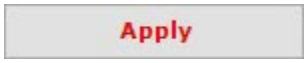
OpenStreetMap

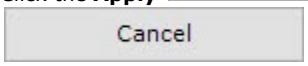
Axxon One uses geodata from the **OpenStreetMap** provider via the Mapbox service. To use **OpenStreetMap** as an interactive map in *Axxon One*, do the following:

1. Purchase a license for Tilequery API from the Mapbox provider: https://www.mapbox.com/pricing/#gltile and get an **ApiKey**.
2. Configure the display of **OpenStreetMap** in *Axxon One*:

a. If necessary, change the map name in the **Name** field or leave the default name.



b. Enter the received **ApiKey**.
c. In the **Enable** field, select the **Yes** value to enable **OpenStreetMap**.
d. Set the **Minimum zoom** and **Maximum zoom** of the map. The values must be in the range [0; 19].
e. In the **Default zoom** filed, set the scale of the map that will be displayed by default. The value must be in the range [0; 19].
f. In the **Default center** field, set the coordinates of the map center that will be displayed by default:
    i. **X**—latitude;
    ii. **Y**—longitude.
g. Click the **Apply** 

button. To cancel the changes, click the **Cancel** 

button.

3. Restart the *Axxon One* Client (see Shutting down an Axxon One Client, Starting the Axxon One Client).
4. Configure the map display (see Adding a new map).

Configuring the display of **OpenStreetMap** in *Axxon One* is complete.

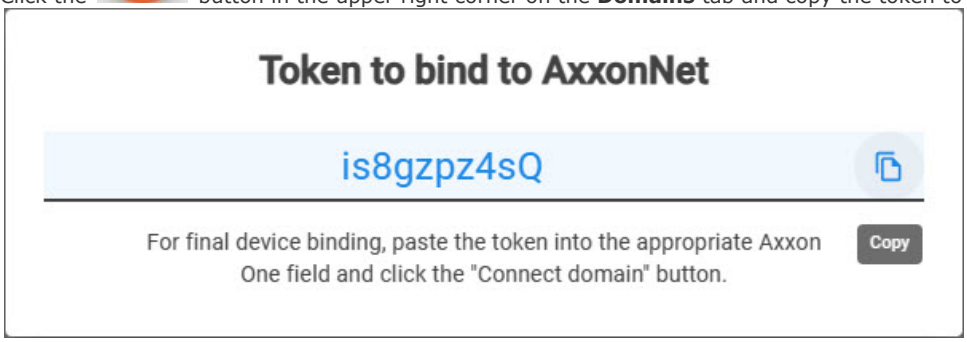
Connecting the Axxon One domain to AxxonNet

AxxonNet documentation

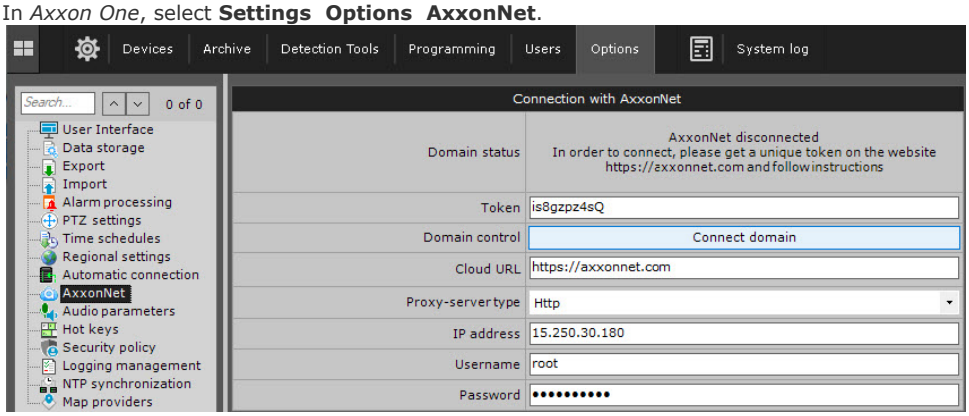
Configuring domains

To connect the *Axxon One* domain to *AxxonNet*, you must:

1. Have access to the internet.
2. Open ports 80 and 443.
3. Allow access of incoming and outgoing traffic to the https://axxonnet.com/ website if the Server has limited internet access.
4. Log in to *AxxonNet* https://axxonnet.com/ (see Registration, authorization, password recovery and change in AxxonNet).
5. Click the  button in the upper right corner on the **Domains** tab and copy the token to bind to the *Axxon One* domain.

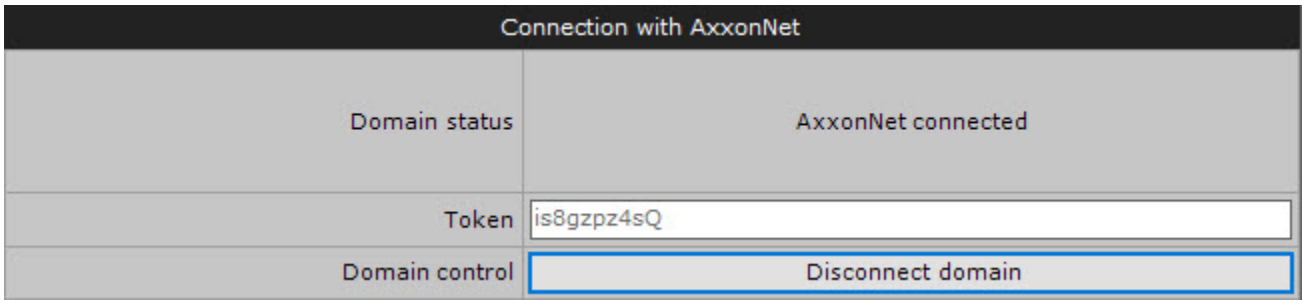


6. In *Axxon One*, select **Settings** **Options** **AxxonNet**.

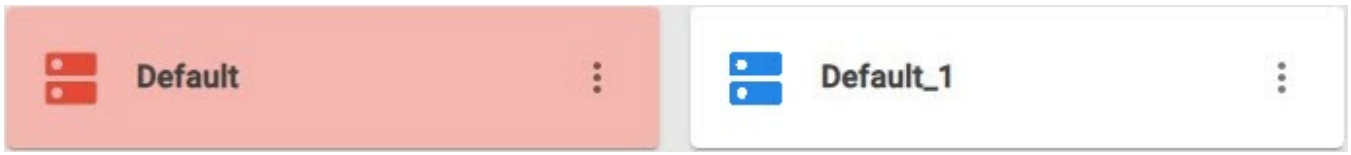


7. Paste the copied key to bind to *AxxonNet* into the **Token** field.
8. Enter the **Cloud URL** to which you want to connect.
9. If you connect through a proxy-server:
    a. From the drop-down list, select the **Proxy-server type**:
        i. **None**
        ii. **Http**
        iii. **Https**
        iv. **Socks5**
    b. Enter the **IP address** of the cloud service to which you want to connect.
    c. Enter the **Username** and **Password** to connect to the proxy-server.
10. Click the **Connect domain** button.

If the connection is successful, the status in the *Axxon One* will change to **AxxonNet connected**. To disconnect the domain from *Axxo nNet*, click the **Disconnect domain** button.



If several domains with identical names are connected to *AxxonNet*, a sequential number will be added to each of the names listed on the **Domains** tab. If there is no connection with the Server, the domain is highlighted in red color.



Client settings

Configuring the user interface

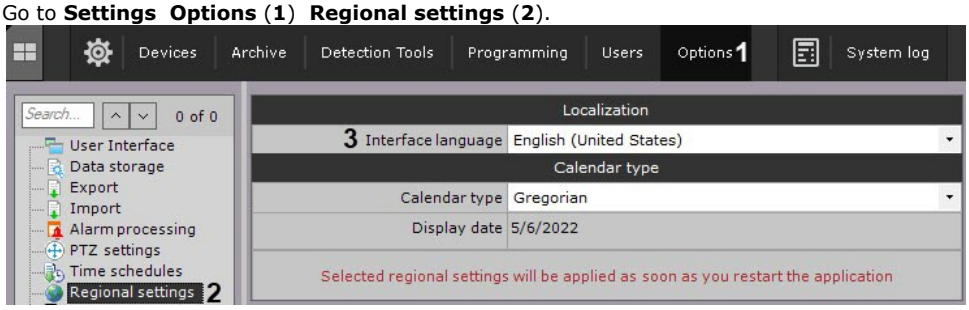
Selecting the interface language

When working with *Axxon One*, the user can choose the Client interface language.

> **Attention!**
>
> The language of the events in the system log is determined by the settings of the OS on the Server.

To select the Client interface language, do the following:

1. Go to **Settings** → **Options** (**1**) → **Regional settings** (**2**).



2. Select *Axxon One* interface language from the **Interface language** drop-down list (**3**).
3. Click the **Apply** button to save the changes.
4. Restart *Axxon One* (see Shutting down an Axxon One Client, Starting the Axxon One Client).

When *Axxon One* is restarted, the selected interface language will be applied.

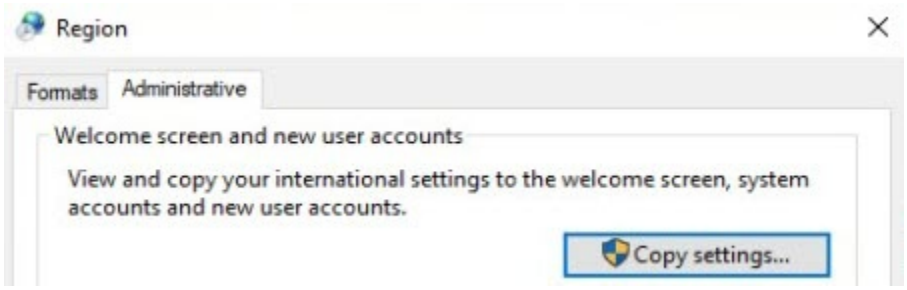
To change the language of the events in the system log, do the following:

1. On the Server, go to **Control Panel** → **Region**.

> **Note**
>
> The configuration is given for Windows 10 OS.



2. From the **Format** drop-down list, select the required language.
3. Go to the **Administrative** tab.



4. Click the **Copy settings** button.

5. Set the **Welcome screen and system accounts** checkbox.



6. Click the **OK** button in both windows.
7. Restart the Server (see Shutting down a Server, Starting a Server).

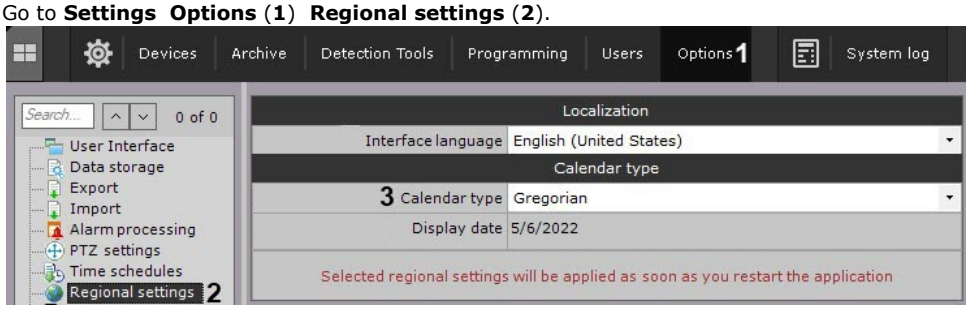
The language of the events in the system log is changed.

Selecting the calendar type

When working with *Axxon One*, the user can choose the calendar type (Gregorian or Persian).

To select the calendar type, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **Regional settings** (**2**).



2. Select the calendar type that is used in *Axxon One* from the **Calendar type** drop-down list (**3**).
3. Click the **Apply** button to save the changes.
4. Restart *Axxon One* (see Shutting down an Axxon One Client, Starting the Axxon One Client).

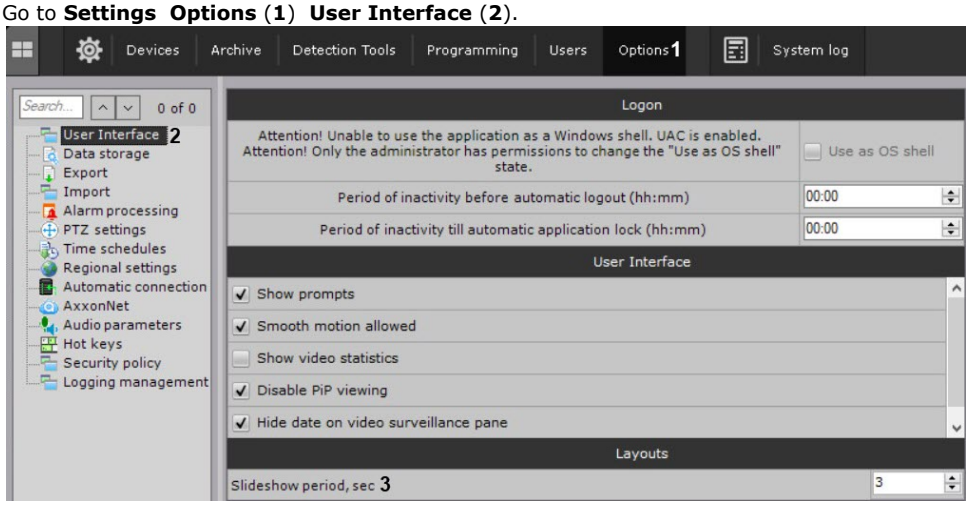
When *Axxon One* is restarted, the selected calendar type will be applied.

Configuring the slideshow parameters

The slideshow mode is a cyclic switching of the layouts within the specified period. The slideshow is launched using the context menu of the layouts panel.

To configure the slideshow period, do the following:

1. Go to **Settings** → **Options** (**1**) → **User Interface** (**2**).



2. Set the slideshow period in seconds (**3**).
3. Click the **Apply** button.

The slideshow period is configured. The layouts will be switched within the specified period.

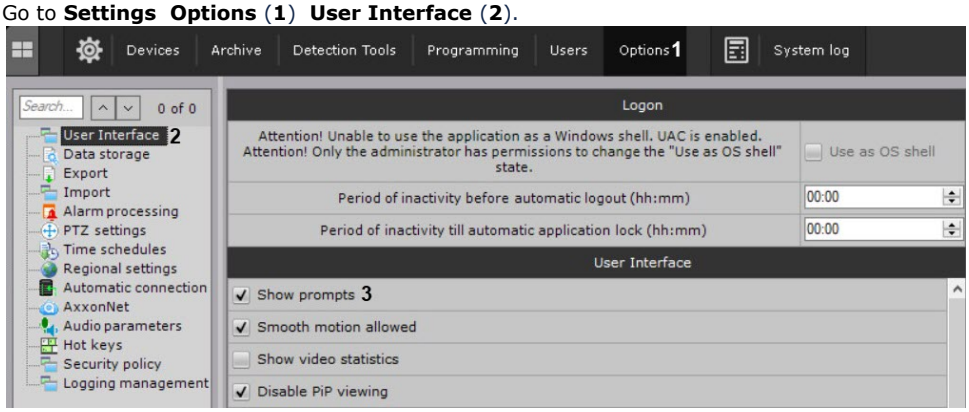
> **Note**
>
> Only the users with the **Layout editing** permission can switch the modes (see Creating and configuring roles).

Hiding prompts

In *Axxon One*, prompts are displayed when the cursor is hovered over a control element. By default, the prompts are enabled.

To disable the prompts, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).



2. Clear the **Show prompts** checkbox (**3**).
3. Click the **Apply** button.

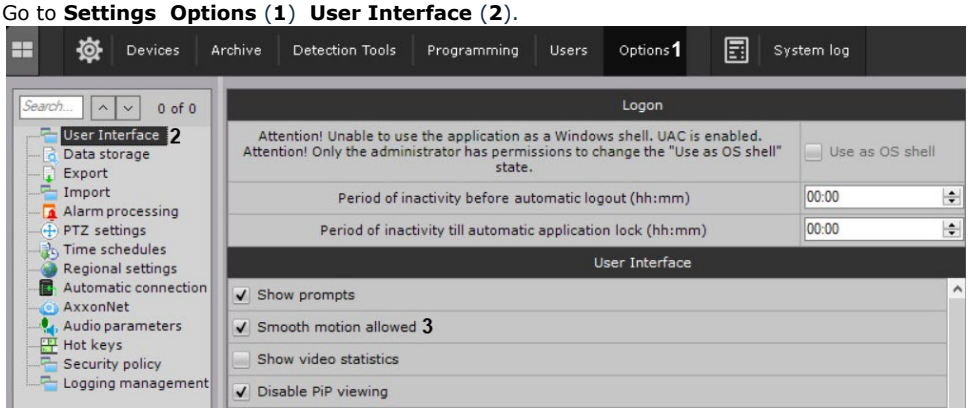
Prompts are now disabled. You can re-enabled prompts by setting the **Show prompts** checkbox.

Configuring smooth motion

Smooth motion allows smoothly changing the position of the surveillance windows, as well as smoothly switching between the tabs. By default, smooth motion is enabled.

To disable smooth motion, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).



2. Clear the **Smooth motion allowed** checkbox (**3**).
3. Click the **Apply** button.

Smooth motion of the surveillance windows is disabled.

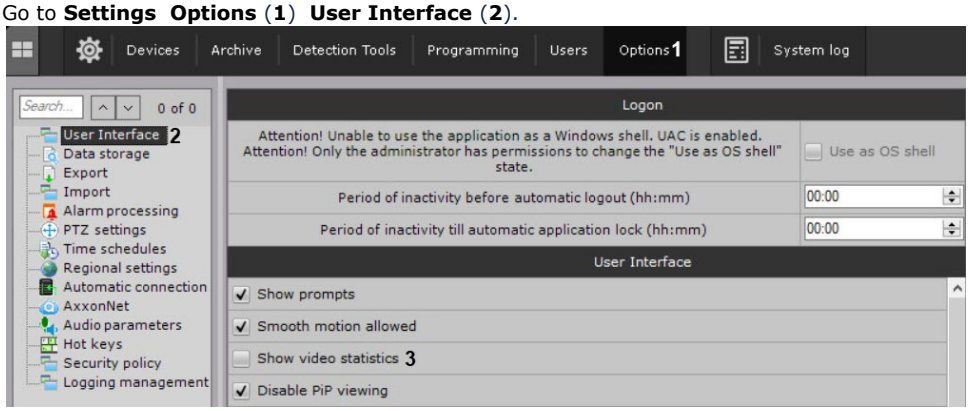
Configuring display of video statistics

You can display the following video statistics in the surveillance window:

1. Frame rate of the displayed video stream.
2. Frame rate of the video stream received from a video camera or an archive.
3. Bitrate of a compressed video stream.
4. Resolution of the displayed video stream.

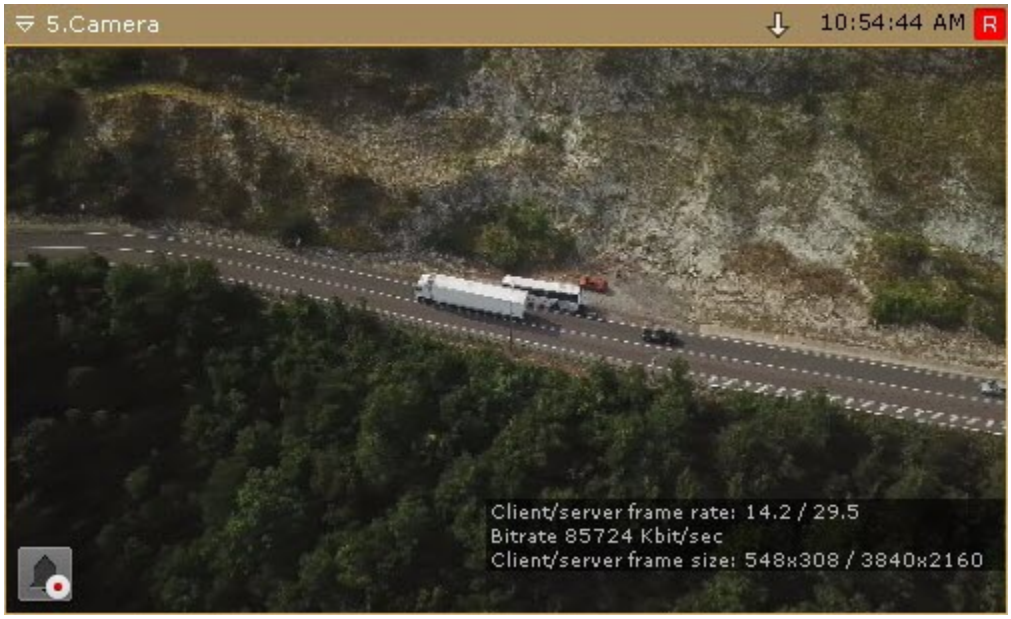
To display video statistics, do the following:

1. Go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. Set the **Show video statistics** checkbox (**3**).
3. Click the **Apply** button.

The video statistics will now be displayed in the surveillance window for the following modes: Live Video, Archive, Alarm, and Archive Search.

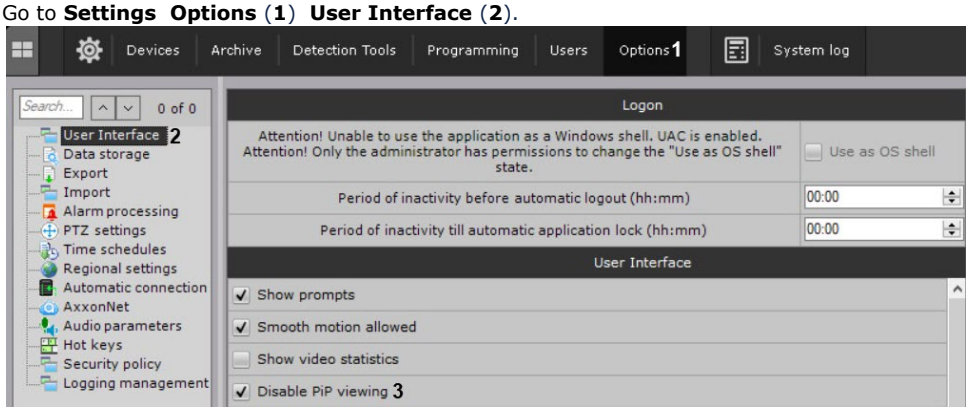


Configuring preview of alarm events

You can disable the preview of alarm events in the surveillance window.

To do this, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).



2. Set the **Disable PiP viewing** checkbox (**3**).
3. Click the **Apply** button.

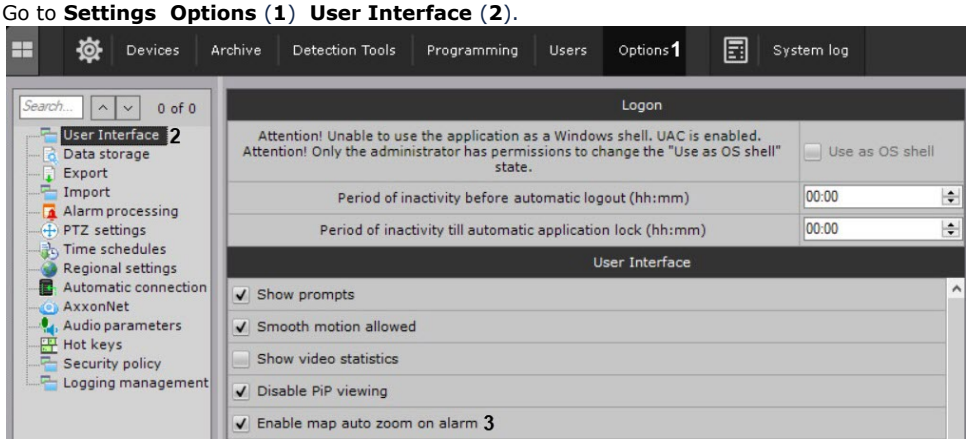
Preview of alarm events is disabled.

Configuring map auto zoom

It is possible to zoom the map automatically and place the icon of the alarm camera at the center of the map.

To do this, do the following:

1. Go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. Set the **Enable map auto zoom on alarm** (**3**) checkbox.
3. Click the **Apply** button.

Map auto zoom on alarm is configured. When an alarm occurs, the icon of the alarm camera will be placed at the center of the zoomed map.

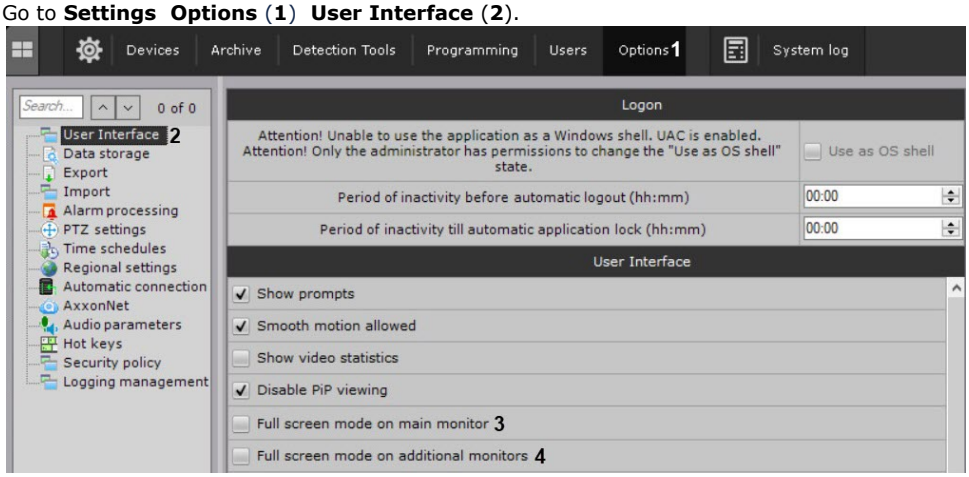
Configuring the Client screen mode (full screen or window)

By default, the Client (main monitor and all additional monitors) is displayed in full screen mode.

It is possible to use window mode both on the main monitor and on the additional monitors.

To do this, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).



2. To use window mode on the main monitor, clear the **Full screen on main monitor** checkbox (**3**).
3. To use window mode on the additional monitors, clear the **Full screen on additional monitors** checkbox (**4**).
4. Click the **Apply** button.
5. Restart *Axxon One* (see Shutting down an Axxon One Client, Starting the Axxon One Client).

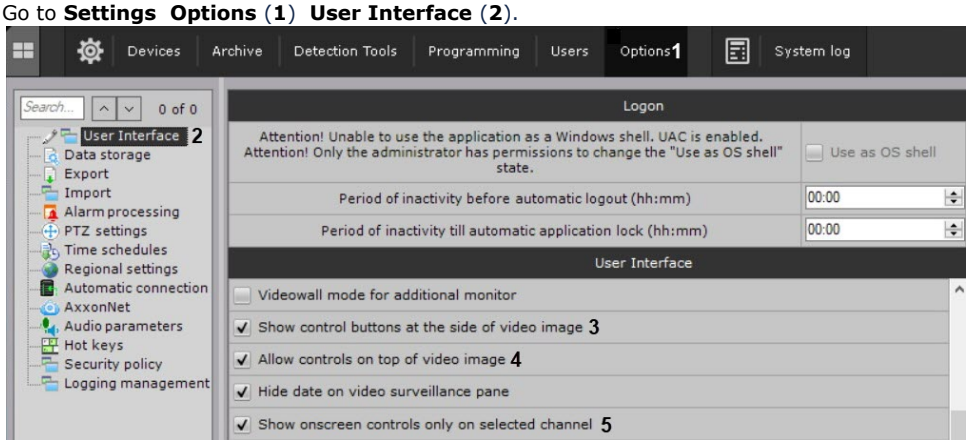
The window mode is configured. The *Axxon One* Client will be displayed in window mode on new start.

Configuring the display of the surveillance window

Surveillance window

To configuring the display of the surveillance window, do the following:

1. Go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. By default, the surveillance mode selection buttons are located at the side of the surveillance window. To move the buttons inside of the surveillance window, clear the **Show control buttons at the side of video image** checkbox (**3**).

> **Attention!**
>
> With this display of the surveillance window, the following won't be available: the zoom function (in real-time and archive modes, see Scaling the surveillance window) and the immersive mode button (see Immersive mode).

3. By default, the surveillance window elements (context menus, export buttons, PTZ mode selection buttons, etc.) are displayed outside of the video image. To move the control buttons on the video image, clear the **Allow controls on top of video image** checkbox (**4**).
4. If it is necessary to display the surveillance window elements only for the active window on the layout, set the **Show onscreen controls only on selected channel** checkbox (**5**). This parameter is valid only if the **Allow controls on top of video image** checkbox is set (**4**).
5. Click the **Apply** button.
6. Reopen the layout or create a new one (see The Layouts panel).

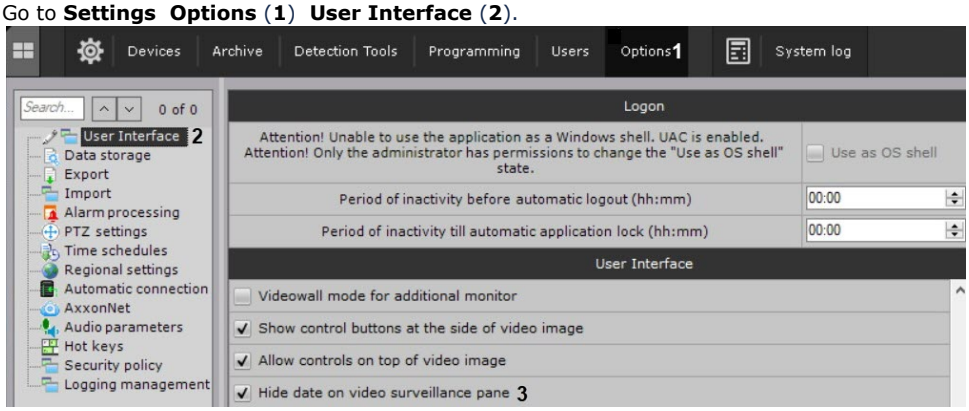
Configuring the display of the surveillance window is complete.

Configuring time display

By default, the time indicator (see Time Display) in the surveillance window does not display the date.

To display the date, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).



2. Clear the **Hide date on video surveillance pane** checkbox (**3**).
3. Click the **Apply** button.
4. Reopen the layout or create a new one (see Layouts management).

The time indicator is configured. The date will be displayed to the left of the time.



You can also hide the time indicator in the surveillance window. To do it, do the following:

1. Go to the role settings (see Creating and configuring roles).
2. In the **Access to Functions** group, set **No** for the **Unlock camera menu button** parameter.
3. Set the camera access level — **Live**.

As a result, the time indicator of the specified cameras will be disabled for all users of this role.

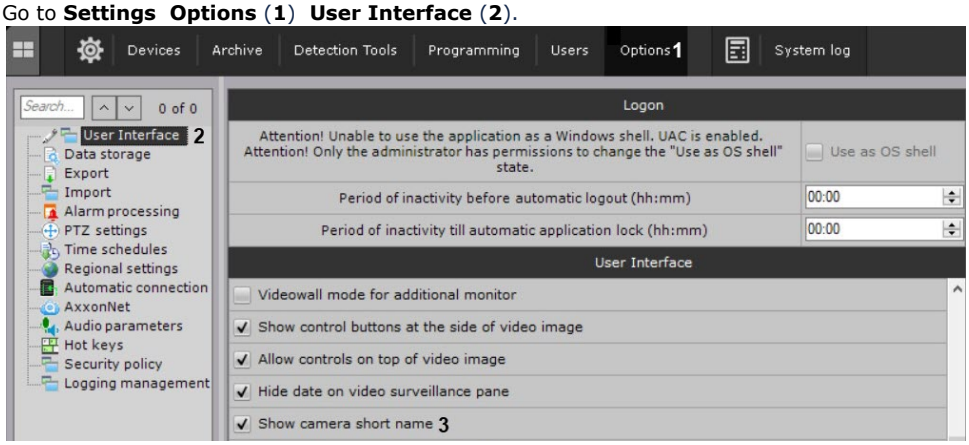
Configuring the display of the camera short name

By default, the camera short name is displayed in the surveillance window (see The Camera object).



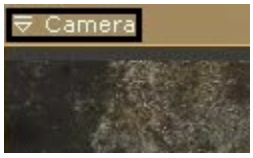
To disable displaying the short name, do as follows:

1. Go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. Clear the **Show camera short name** checkbox (**3**).
3. Click the **Apply** button.
4. Reopen the layout (see Layouts management).

The camera short name display is disabled.



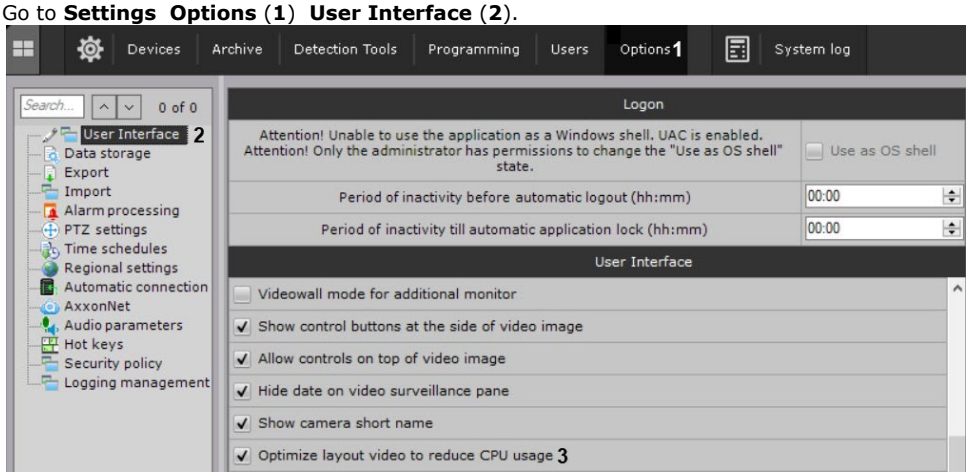
Optimizing video image on the layout

It is possible to automatically reduce the number of the displayed pixels in the layout if the screen resolution is lower than the stream resolution from the video camera. This allows reducing the CPU load.

Video image optimization is enabled by default. To disable it, do the following:

> **Note**
>
> If video image optimization is enabled, the definition of the image in the layout may decrease.

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).

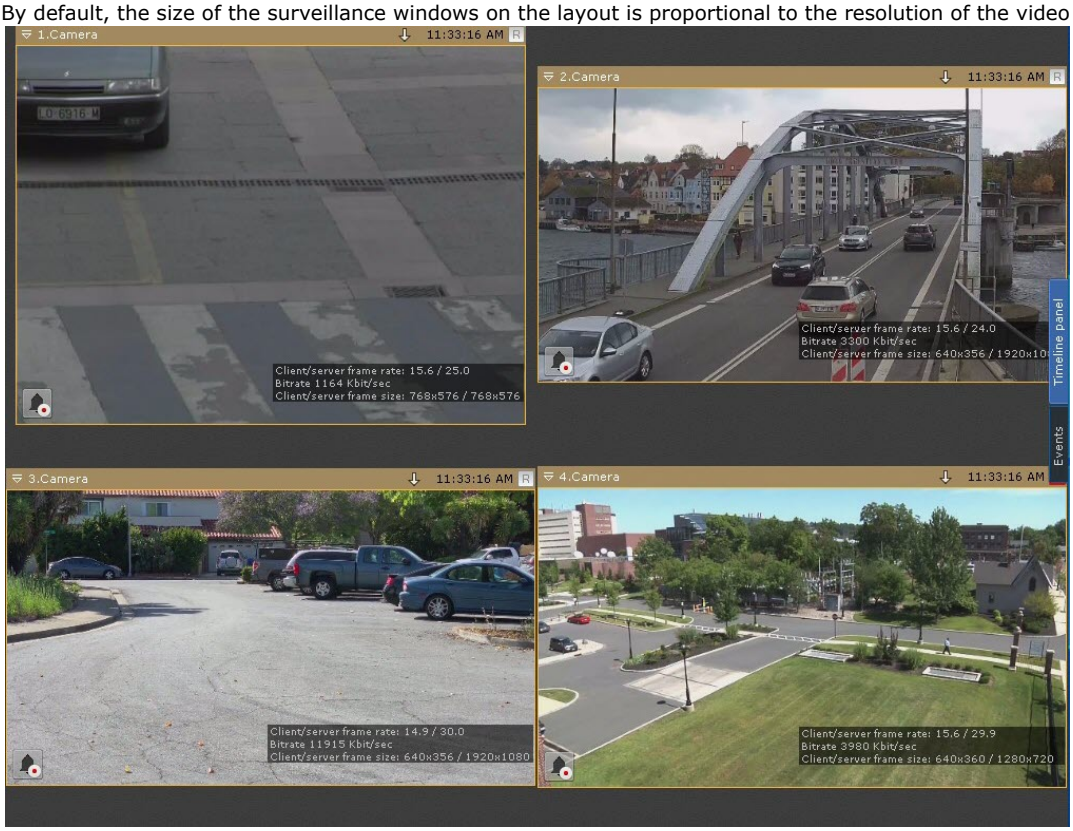


2. Clear the **Optimize layout video to reduce CPU usage** checkbox (**3**).
3. Click the **Apply** button.

Video image optimization is disabled.

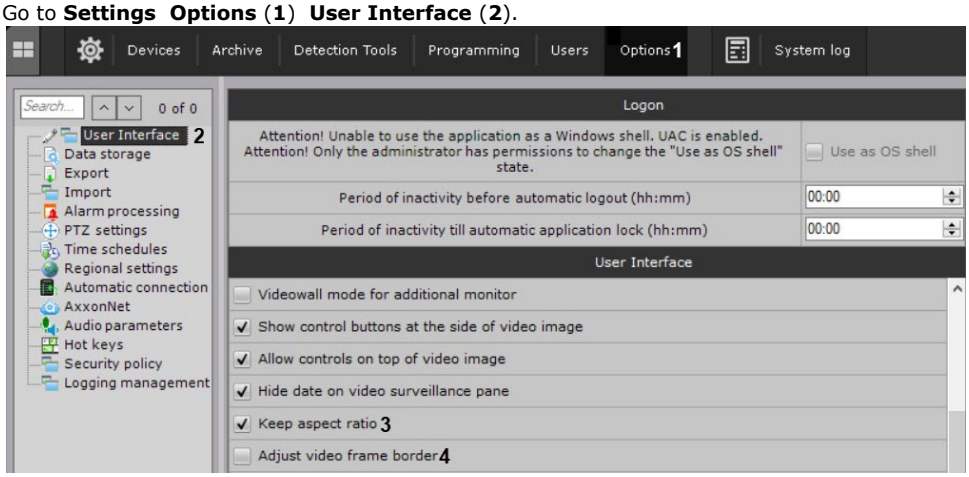
Configuring video display on the layout

By default, the size of the surveillance windows on the layout is proportional to the resolution of the video image.



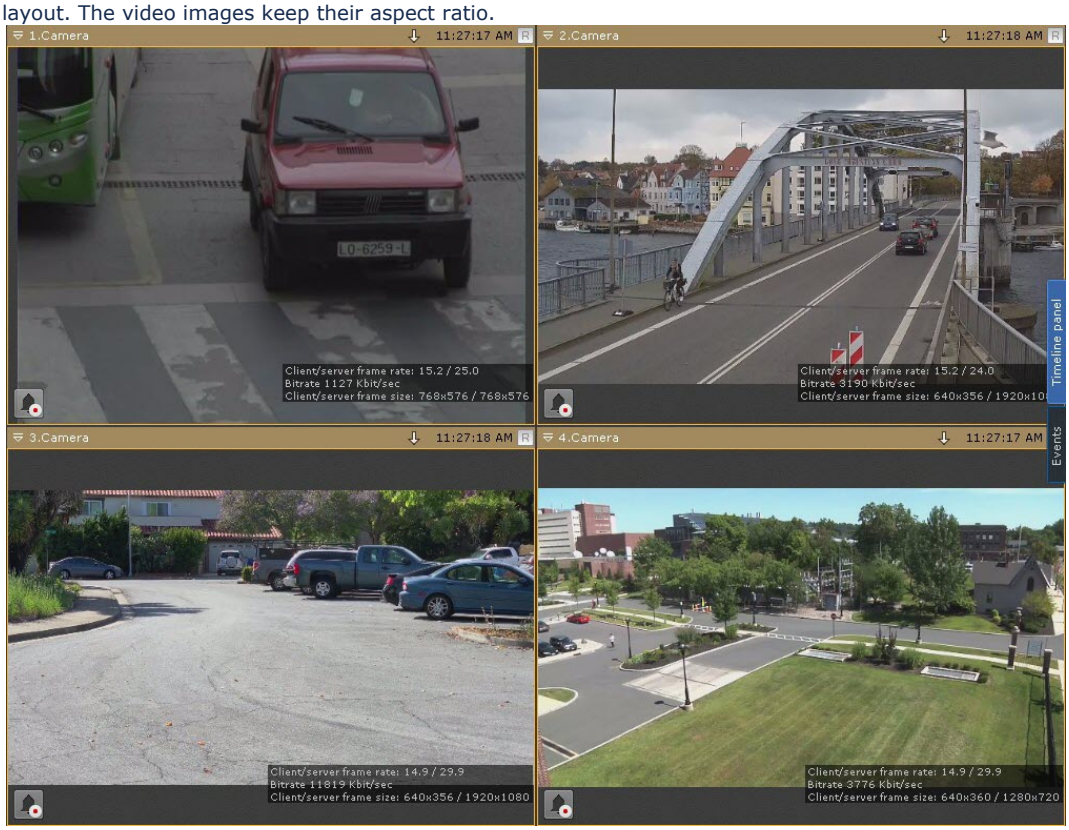
For the surveillance windows to be of a fixed size and occupy the entire area of the layout, do the following:

1. Go to **Settings** ▸ **Options** (**1**) ▸ **User Interface** (**2**).



2. Clear the **Adjust video frame border** checkbox (**4**).
3. Click the **Apply** button.
4. Reopen the layout (see Layouts management).

Configuring the surveillance windows is complete. The surveillance windows are of a fixed size and occupy the entire area of the layout. The video images keep their aspect ratio.



To expand the video image to the entire surveillance window, do the following:

1. Clear the **Keep aspect ratio** checkbox (**3**).
2. Click the **Apply** button.
3. Reopen the layout (see Layouts management).

Configuring the surveillance windows is complete. The video image is expanded to the entire surveillance window.



Configuring layouts

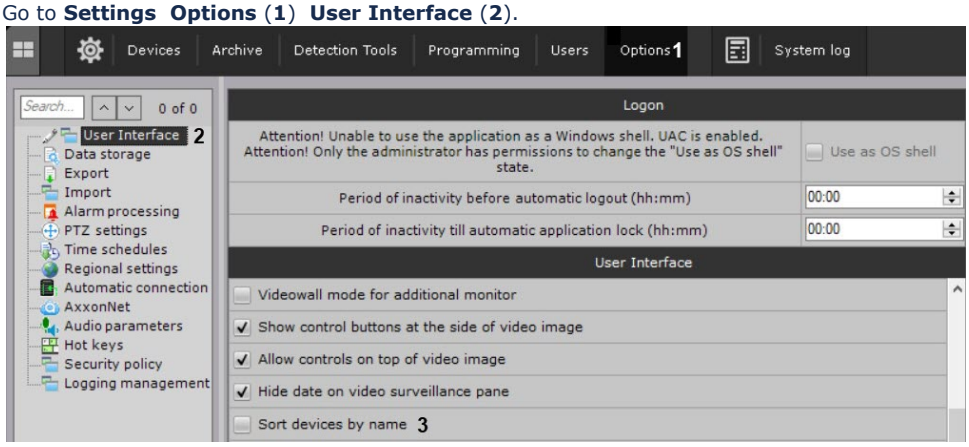
Configuring viewing tiles

Configuring camera sorting on Objects Panel

By default, the cameras on the Objects Panel (see Objects Panel) are sorted by the short name (see The Camera object).

To enable the sorting by the name, do the following:

1. Go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. Set the **Sort devices by name** checkbox (**3**).
3. Click the **Apply** button.

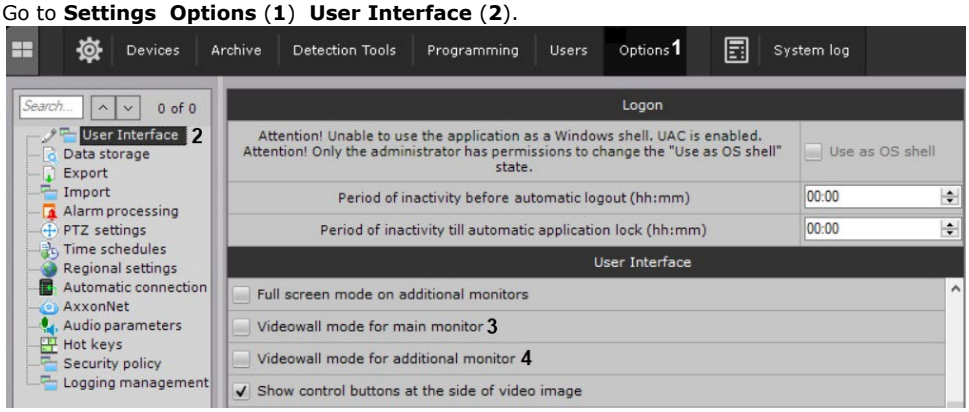
Sorting the cameras by the name on the Objects Panel is enabled.

Configuring the videowall mode

Configuring Video wall

To configure the videowall mode, do the following:

1. Go to **Settings Options** (**1**) **User Interface** (**2**).



2. To use the videowall mode on the main monitor, set the **Videowall mode for main monitor** checkbox (**3**).
3. To use the videowall mode on the additional monitor, set the **Videowall mode for additional monitor** checkbox (**4**).
4. Click the **Apply** button.
5. Restart *Axxon One* (see Shutting down an Axxon One Client, Starting the Axxon One Client).

The videowall mode is configured.

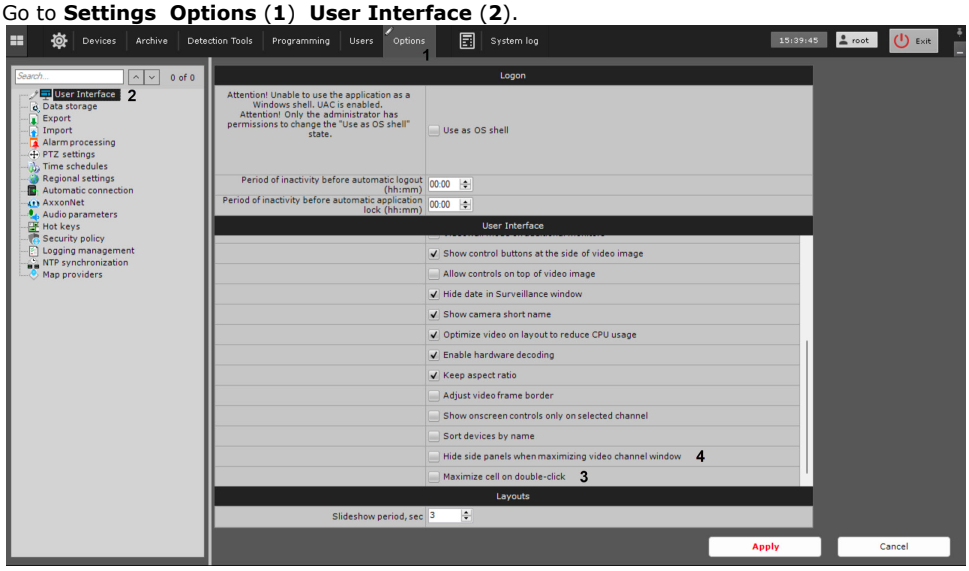
At a new start of the *Axxon One* Client:

1. On the main monitor, the panel pin button won't be active (see Interface of the Axxon One Software Package). The Archive navigation panel and the Event Board (see The Archive Navigation Panel), the Layouts panel (see The Layouts panel), messages about system errors that occurred (see Control in Live Video mode), the Alert panel (see Alert panel) won't be displayed.
2. The additional monitor won't display the Objects panel (see Objects Panel), the Archive navigation panel and the Event Board (see The Archive Navigation Panel), the Alert panel (see Alert panel).
3. The map (see Working with the interactive map) will be available on the main monitor and on the additional monitor.

Configuring cell maximization on double click

To maximize the cell on double click, do the following:

1. Go to **Settings** **Options** (**1**) **User Interface** (**2**).



2. Set the **Maximize cell on double-click** checkbox (**3**).
3. Click the **Apply** button.

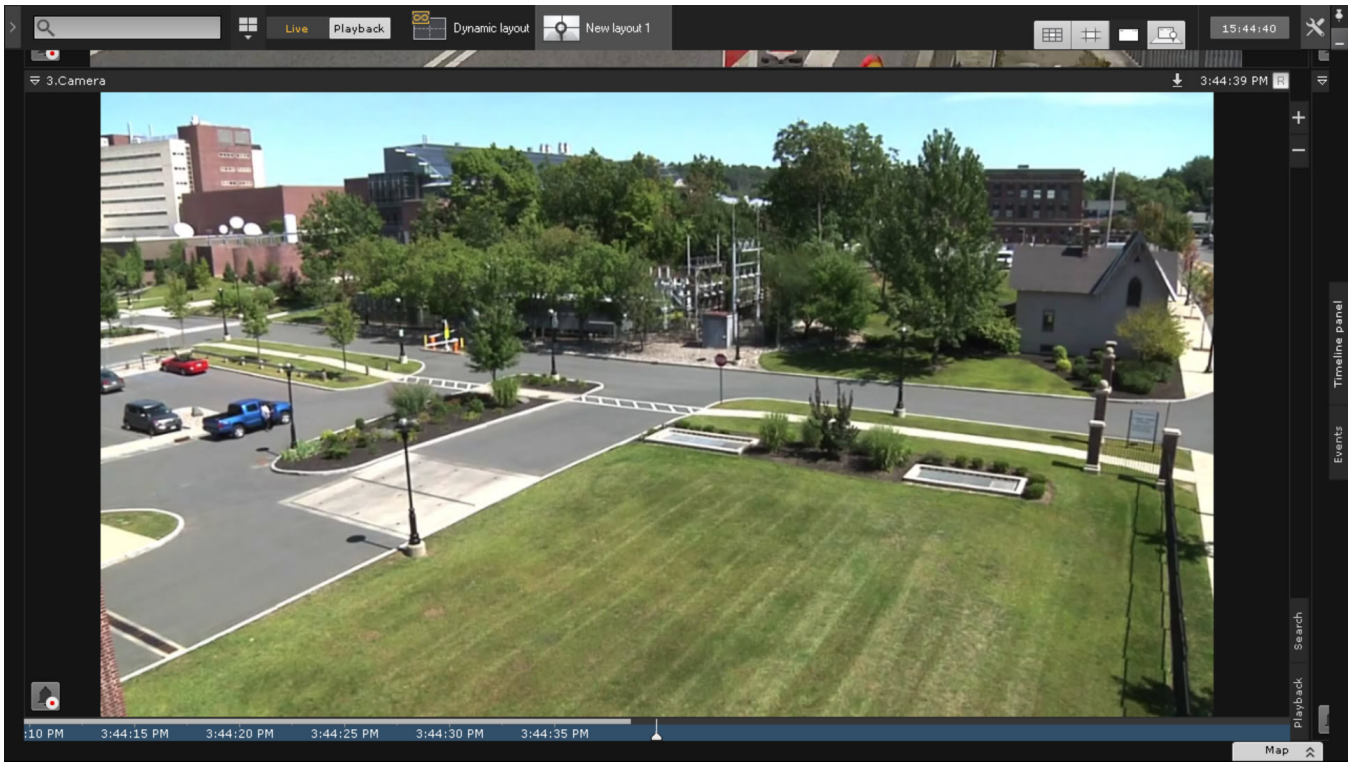
Configuring the cell maximization on double click is complete.

When you double-click on the video window, the top panel will be hidden on the main and additional monitors. The side panels and map will not be hidden; the side panel buttons will always be visible.



To hide the side panels and the map when the video window is maximized, set the **Hide side panels when maximizing video channel window** checkbox (**4**).

In this case, when you double-click on the video window, the top panel will be visible, but the side panels and the map will be hidden on the main and additional monitors. The side panel buttons will always be visible.



You can exit the full-screen mode in the same way. The top and side panels, as well as the map, will be displayed again.



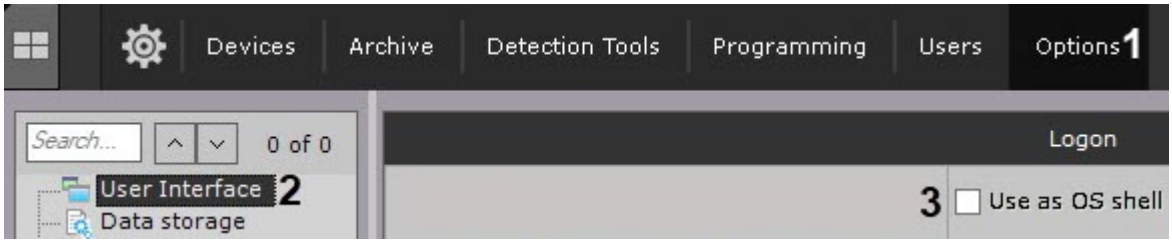
Configuring how Axxon One starts

Configuring Axxon One startup instead of the standard Windows OS shell

Autorun of *Axxon One*, instead of the standard Windows OS shell, is used in cases where you need to restrict access to computers running the digital video surveillance system, including preventing the launch of various applications, file copying and deletion, various Windows operations, and other non-standard use of the computers.

If you configure *Axxon One* to autorun instead of the standard Windows shell, *Axxon One* will launch instead of Windows Explorer immediately after Windows loads. This makes it impossible for the user to launch certain applications installed on the computer or to work with certain program dialog boxes.

To activate autorun of the *Axxon One* software package instead of the standard Windows shell, select the **Use as OS shell** (**3**) check box in **Settings Options User Interface** (**1-2)** and click **Apply**.



Axxon One will now launch instead of the standard Windows shell the next time you start Windows.

> **Note**
>
> If User Accounts Control is enabled in the Windows OS, *Axxon One* VMS cannot automatically start in place of OS shell (the appropriate check box is grayed out). Disable UAC.
>
> In Windows 10 OS, you also need to make changes to the registry and reboot your PC.

Automatic connection

On the page:

- General information about configuring Automatic connection
- Configuring Automatic connection
- Configuration of automatic connection of the Client to Servers located in different domains
- Configuration of automatic connection of the Client to the nodes of the FailOver system
- Changing the Server port
- Exporting and importing the configuration of automatic connection

General information about configuring Automatic connection

This setting is used to automatically connect:

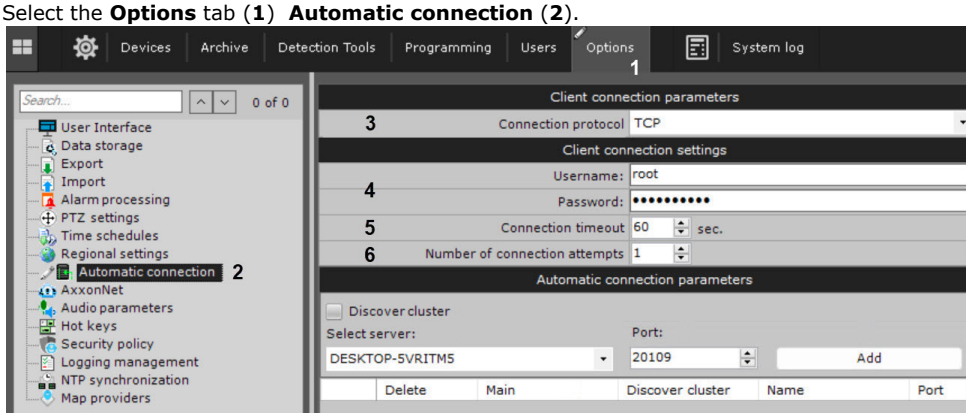
- the Client to the Server without having to re-enter the Server name, username and password when starting the app;
- the Client to Servers belonging to different domains (see Cross-System Client);
- the Client to the nodes of the FailOver system (see Configuring Failover VMS).

If you connect automatically, the Servers specified in the **Automatic connection parameters** group will be used first. If these Servers are unavailable, the system will try to connect to the Servers from the **Preferred servers parameters** group following the set order (see Selecting Preferred Servers).

Configuring Automatic connection

To configure automatic connection, do the following:

1. Select the **Options** tab (**1**) **Automatic connection** (**2**).



2. From the drop-down list (**3**), select the connection protocol.
   Description of the protocol and recommendations for selection are given in the table.

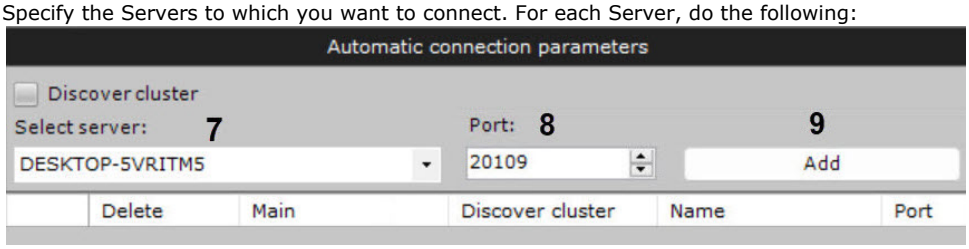
Protocol	Description
TCP	This protocol is more reliable, but has a busy connection. We recommend selecting it for Servers with a small number of cameras
UDP unicast	UDP protocol has a higher data transmission speed, but it is less reliable. The unicast scheme is used to transmit data to a single recipient. You must select this protocol for a Server with a large number of cameras and which has several Clients working with it
UDP multicast	The multicast scheme is used to transmit data to a group of recipients. This protocol is best suited for a Server with a large number of cameras and which has many Clients working with it. **Attention!** This protocol must be supported by all network elements, including switches

The connection protocol of the Clients to the Server determines the choice either in favor of connection reliability or in favor of data transmission speed. You must select the connection protocol for each Sever of the domain. All Clients connected to the Server will receive video streams via this protocol.

3. For automatic authorization when connecting to Servers, enter the username and password (**4**). If you leave these fields blank, authorization will be performed manually when you start the Client.

> **Attention!**
>
> Cross-System Client connects to all Servers using a single username-password pair that must be created in each domain (see Cross-System Client).

4. In the **Connection timeout** field (**5**), specify the wait period for a successful connection before considering the attempt unsuccessful. The default value is 60 seconds, the maximum value is 300 seconds (5 minutes). If you use this setting, an automatic connection attempt will occur immediately. If connection fails, the Server will wait for the period of time specified by the user (timeout) and repeat the connection attempt.
5. Specify the maximum number of automatic connection attempts after the specified timeout (**6**).
6. Specify the Servers to which you want to connect. For each Server, do the following:



   a. Select a Server from the list or enter the Server IP address (**7**).
   b. Specify the port for connecting to the Server (**8**).

> **Note**
>
> If you leave the **Port** field blank, the standard port 20109 will be used for connection.

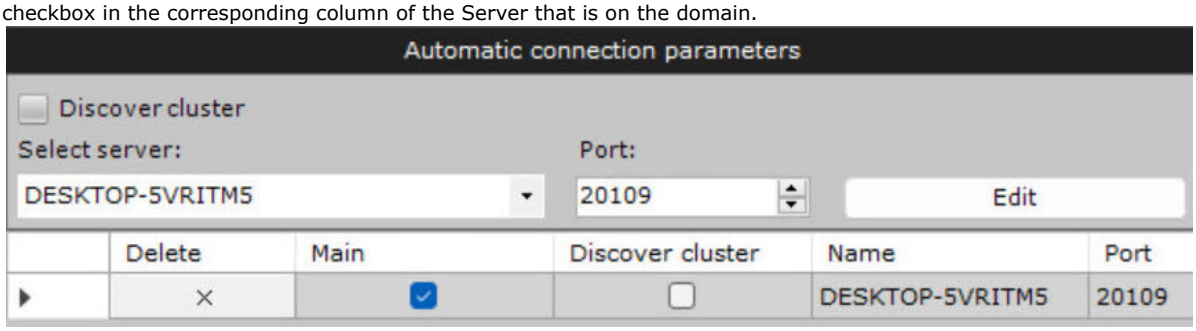
   c. Click the **Add** button (**9**).

> **Note**
>
> - If you use Cross-System Client, you can connect to only one Server of each domain (see Cross-System Client). That is why when you add a Server to the list, all other Servers in that domain become unavailable for selection.
> - To remove a Server from the list, click the ✕ button.

Configuration of automatic connection of the Client to Servers is complete. The next time you start *Axxon One*, it will connect to the selected Servers.

Configuration of automatic connection of the Client to Servers located in different domains

When you use Cross-System Client, select the main domain after adding all Servers to the list. To select the main domain, set the **Main** checkbox in the corresponding column of the Server that is on the domain.

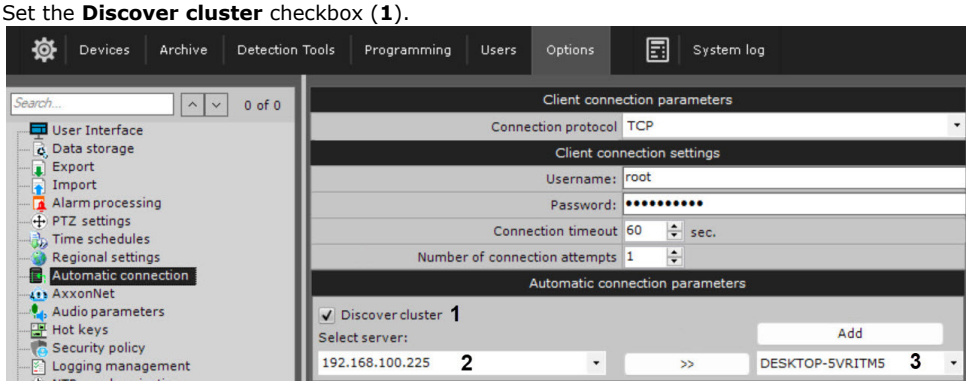


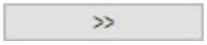
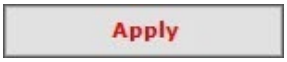
When connecting, the Client will use the parameters (maps, layouts, user permissions) of the main domain.

Configuration of automatic connection of the Client to the nodes of the FailOver system

If you want to configure automatic connection to a node of the FailOver system, do the following:

1. Set the **Discover cluster** checkbox (**1**).



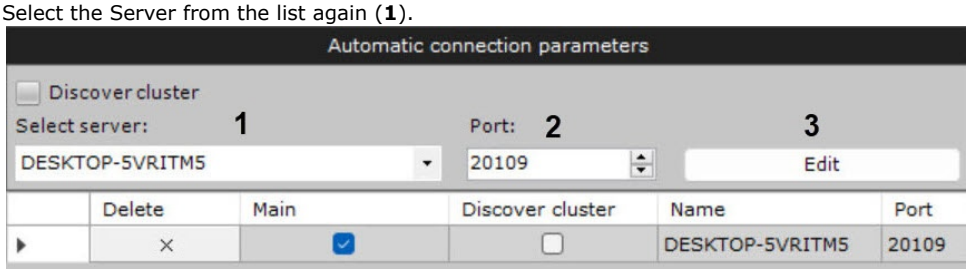
2. Enter the IP address of any Server of the cluster (**2**) and click the  button.
3. From the drop-down list (**3**), select a node that you want to add to autoloading.
4. Click the **Add** button.
5. Click the **Apply**  button.

Configuration of automatic connection of the Client to the node of the FailOver system is complete.

Changing the Server port

To change the port of an already added Server, do the following:

1. Select the Server from the list again (**1**).

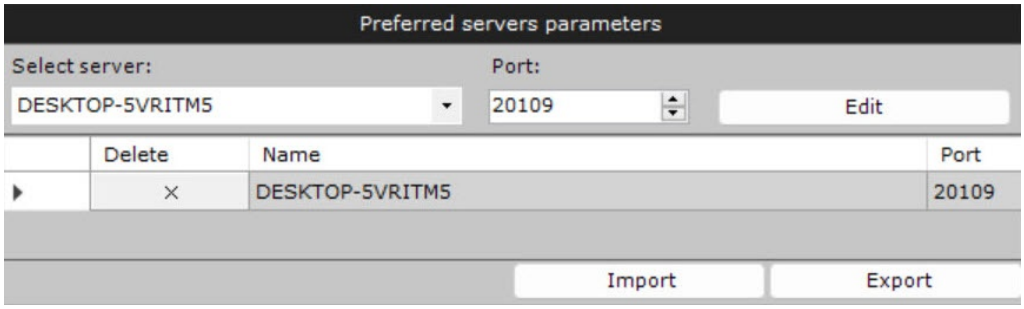


2. In the **Port** field (**2**), specify a new number.
3. Click the **Edit** button (**3**).

Changing the port of the added Server is complete.

Exporting and importing the configuration of automatic connection

To save the configuration of automatic connection to Servers and preferred Servers (see Selecting Preferred Servers) to a JSON file, click the **Export** button.



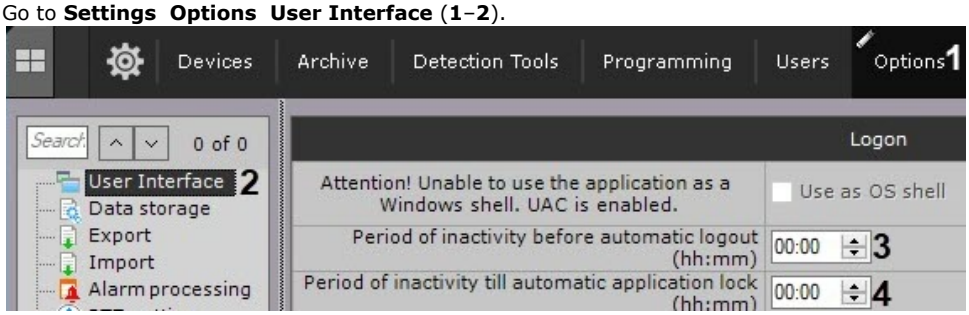
To load the configuration on the Clients, do the following:

1. Click the **Import** button.
2. Click the **Apply**  button.

Configuring automatic exiting and locking of the Client

You can set the system to automatically exit and/or lock the Client if the user stays idle for a pre-determined time, i.e. no signals come from HID devices (keyboard, mouse, joystick, etc.).

To do so:

1. Go to **Settings Options User Interface** (**1**–**2**).


2. In the **Period of inactivity before automatic logout (hh:mm)** field, enter the duration of user inactivity after which the Client should be quit (**3**).
   If the field is blank or equals 00:00, the Client will not be quit.
3. Enter a value in the **Period of inactivity till automatic application lock (hh:mm)** field to set the time interval (**4**). To unlock the Client, the user has to re-login.

   If the field is left blank or the value is set to 00:00, no locking will occur.

   > **Note**
   >
   > - If a viewing layout is open, no automatic blocking occurs.
   > - You can lock the Client at any time using hotkeys (see Assigning hot keys, Appendix 6. Hotkeys in Axxon One).

4. Click the **Apply** button.

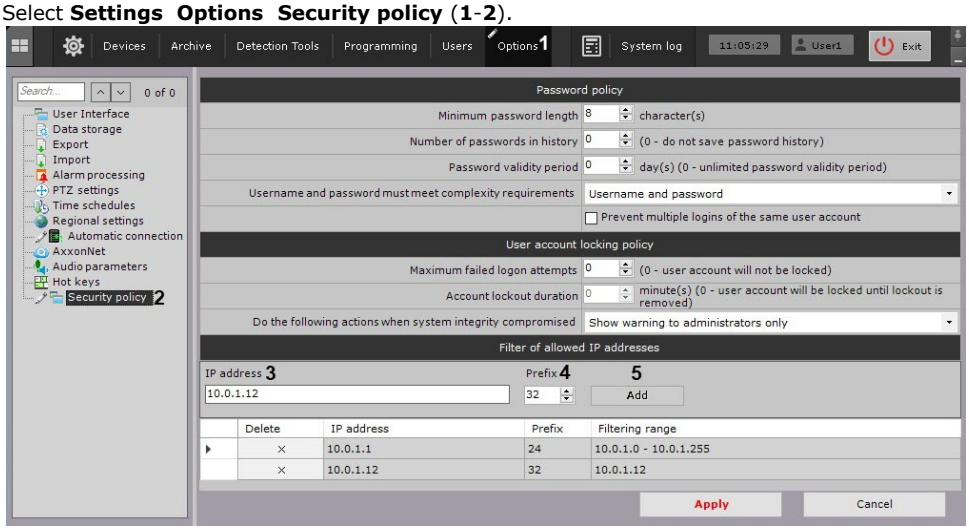
Configuration of automatic quit of the Client is now complete.

IP address filtering configuration

You can restrict remote clients' access to the server to a range of IP addresses.

To do this:

1. Select **Settings Options Security policy** (**1**-**2**).



2. In the **Filter of allowed IP addresses** group, enter the IP address (**3**) and subnet mask (**4**) to set the range of addresses from which a connection will be permitted.
3. Click the **Add** button (**5**).
4. Click **Apply**.

The range is now added to the list. No connection will be possible from addresses not in the list.

To remove an address or a range from the list, do the following:

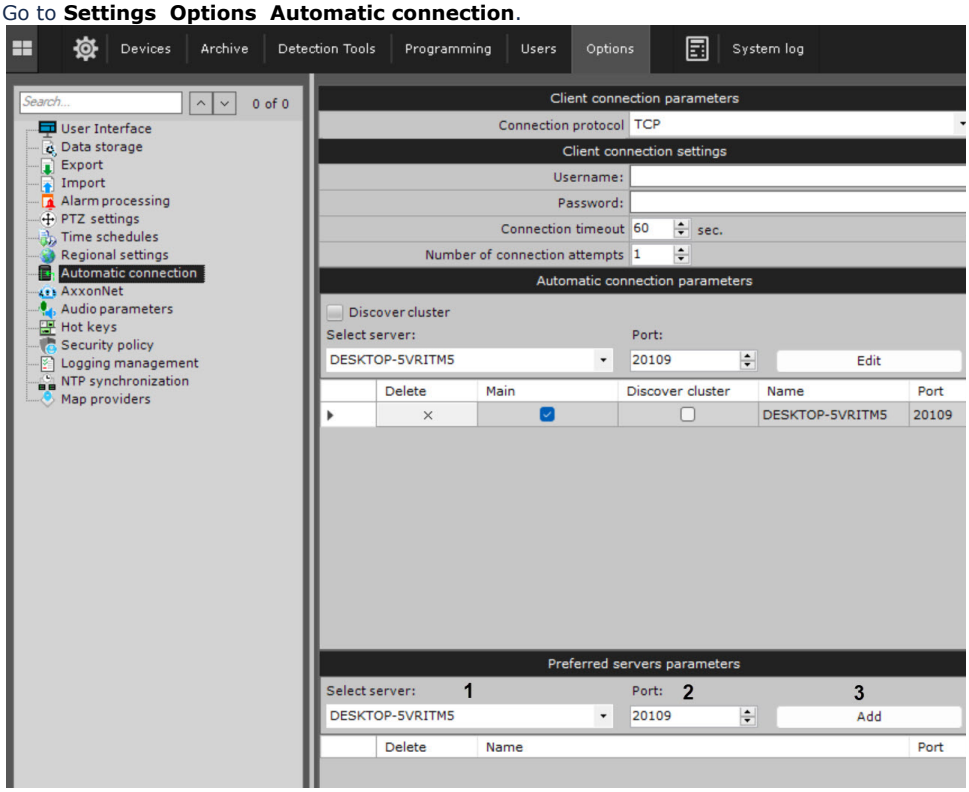
1. Click the ✕ button.
2. Click **Apply**.

Selecting Preferred Servers

You can set Preferred Servers, which will be displayed at the top of the list when you launch Client (see Starting the Axxon One Client). Also, preferred Servers are used for automatic connection: it primarily uses the Servers specified in the **Automatic connection parameters** group (see Automatic connection), and if these Servers are unavailable, then the system will try to connect to Servers from the **Preferred servers parameters** group in the set order.

To set Preferred Servers, follow the steps below:

1. Go to **Settings Options Automatic connection**.



2. In the **Preferred servers parameters** group, select the Server from the list (**1**).
3. Change the default port if necessary (**2**).
4. Click **Add** (**3**).
5. Repeat the steps for all required Servers.
6. Click **Apply** 

.

> **Note**
>
> You can save the Preferred Servers list to a JSON file and load it to another Client (see Automatic connection).

Configuring export

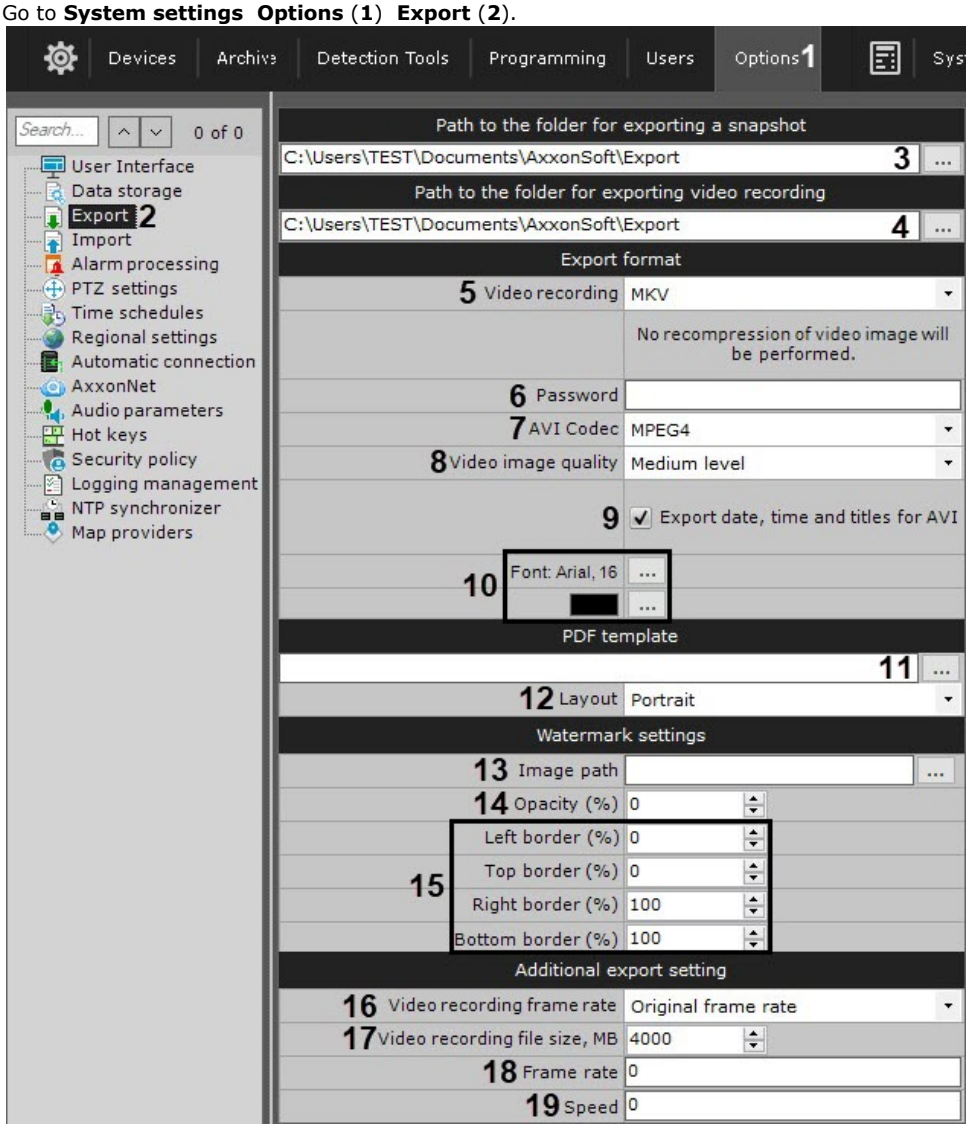
Configuring export options

Configuring export includes:

- setting the default destination folders for exported files,
- setting the default formats for the export of video and snapshots,
- configuring export of video in AVI format,
- configuring the template for the export of snapshots in PDF format,
- other export settings.

Configure export as follows:

1. Go to **System settings** ▸ **Options** (**1**) ▸ **Export** (**2**).



2. In the **Path to the folder for exporting a snapshot** (**3**) and **Path to the folder for exporting video recording** (**4**), enter the full path to the folders in which the exported files should be saved. To do this, click the ... button.

Attention!

During export you can specify any path. These fields also allow you to specify the name template for the exported files, as follows:



- {0}—camera short name;
- {1}—camera name;
- {2}—date;
- {3}—time;
- {4}—recording duration (for video export only).

3. Select the default formats for export of video and snapshots (**5**). You can select any available format during export. Snapshots can be exported in two formats: JPG and PDF. Videos can be exported into the following four formats: MP4, MKV, EXE and AVI.

Note

- Video is exported to MKV format without recompression.
- Video is exported to AVI format with recompression in the selected codec (**7**).
- When video is exported to EXE format, a self-contained executable file is generated, containing video, playback tools, and necessary codecs.

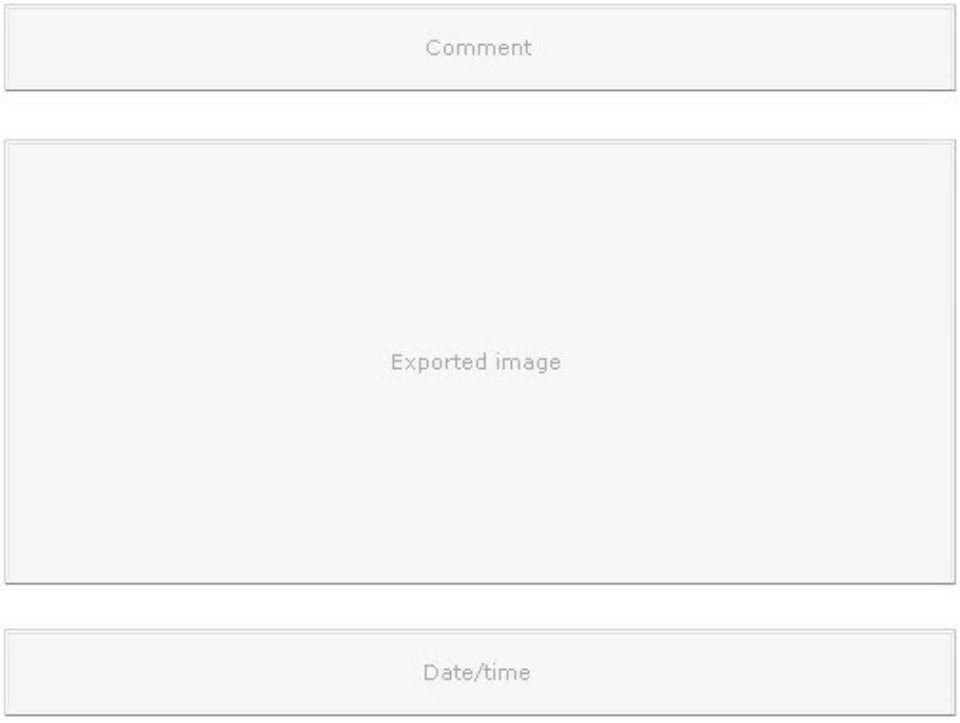
4. If you want to export to an encrypted ZIP archive, set an archive password (**6**). If you export to EXE format, you will need to enter a password when you open the file.
5. Specify settings for video export to AVI format:
   a. Select a codec (**7**):
      i. MPEG4,
      ii. MGPEG,
      iii. h264.
   b. Select video image quality (**8**):
      i. Minimum level,
      ii. Low level,
      iii. Medium/Low,
      iv. Medium level,
      v. Medium/High,
      vi. High level,
      vii. Maximum level.
6. If you want to superimpose captions in the exported video, set the **Export date, time and titles for AVI** checkbox (**9**). When exporting to MKV format, captions are always added, you can disable them when playing back.
7. Configure the template to export snapshots to PDF format:
   When exporting, a PDF document consists of three sections: a comment specified during export; exported image; date and time of the snapshot.
   a. Select the font and set its color (**10**).
   b. If necessary, select a PNG image that will be used as a background of the PDF document (**11**).

Note

The size of the image must not exceed 1 MB.

   c. Select document layout (**12**):
      i. Portrait,
      ii. Landscape.

d. Configure the size of the sections and their position on the page.



> **Note**
>
> You can change the size and position of a section in the same way as working with windows in Windows OS.

8. You can watermark the exported files as follows:

> **Attention!**
>
> The watermark settings are applied to the entire Axxon-domain.

   a. Select a file with a watermark (**13**). PNG, JPEG, BMP images are allowed.
   b. Set the opacity of the watermark: 100%—opaque, 0%—transparent (**14**).
   c. Set the location of the watermark (**15**). To do this, specify the border of the watermarked area on each side of the frame as percentage of the frame size. The top left corner should be taken as the origin point.
   For example, with the default values (Left **0**, Top **0**, Right **100**, Bottom **100**), the specified area will take the entire frame, and the watermark will be located in the center of the image. To place the watermark in a corner, specify the following values:
      i. for the top-left corner—Left **0**, Top **0**, Right **watermark width as percentage of the frame width**, Bottom **watermark height as percentage of the frame height**;
      ii. for the bottom-left corner—Left **0**, Top **100 minus watermark height as percentage of the frame height**, Right **watermark width as percentage of the frame width**, Bottom **100**;
      iii. for the top-right corner—Left **100 minus watermark width as percentage of the frame width**, Top **0**, Right **100,** Bottom **watermark height as percentage of the frame height**;
      iv. for the bottom-right corner—Left **100 minus watermark width as percentage of the frame width**, Top **100 minus watermark height as percentage of the frame height**, Right **100**, Bottom **100**.
9. Select a frame rate for the exported video on one of the following ways:

   a. From the **Video recording frame rate** drop-down list (**16**), select the value:

      i. Original frame rate,
      ii. **1/2**—the frame rate in the exported video recording will be two times lower than the original frame rate,
      iii. **1/4**—the frame rate in the exported video recording will be four times lower than the original frame rate,
      iv. **1/8**—the frame rate in the exported video recording will be eight times lower than the original frame rate.
   b. Set the frame rate per second manually (**18**). The value must be in the range [1; 300].

> **Note**
>
> The minimum frame rate in the exported video is 1 FPS.

10. Set the maximum size of the exported video recording in MB (**17**). When the specified size is reached, a new file will be created.

    > **Attention!**
    >
    > - If you set the **0** value, the export will always be to a single file.
    > - The minimum value is 5 MB.
    > - Due to Windows OS limitations, you cannot export files of more than 4 Gb to EXE format.

11. If it is necessary to change the speed of the exported video recording, in the **Speed** field (**19**), set the speed-up factor from 0 to 128. You can enter fractional values. For example, if you set 10 for the original 10-minute video recording, it will be exported to a 1-minute recording.
12. Click the **Apply** button.

Export configuration is now complete.

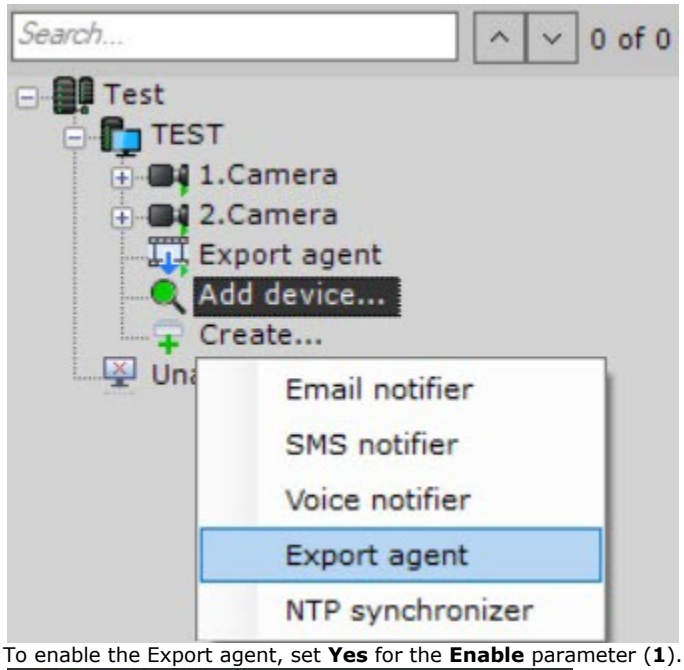
Configuring Export agent

Export agent is a service that allows automatically exporting frames and video recordings to a particular Server when an event occurs in the system.

To start automatic export of frames and video recordings, you need to create a macro in the Cycle rules (see Configuring macros).

To create and configure the Export agent, do the following:

1. In the device list, click **Create** and select **Export agent**.



2. To enable the Export agent, set **Yes** for the **Enable** parameter (**1**).

1.Export agent		
	Object identification	
1	Enable	No
2	Name	
	Object features	
3	Folder for frames	D:/
	Folder for video	D:/
	Frame frequency	Original frame frequency
	Image file format	JPEG
	Maximum file size	4096
	Video codec	Default
	Video file format	MKV
	Video quality	Medium level
	Authorization	
4	Username	
	Password	
	Watermark	
5	Border-bottom	1
	Border-left	0
	Border-right	1
	Border-top	0
	Opacity (%)	100
	Watermark image	

3. In the relevant field, set the object name (**2**).
4. Specify the full paths to the folders that will store the exported frames and video recordings (**3**). For the network folders, enter the username and password of the user who has the access to the NAS (**4**).
5. Specify other export options (**5**). See their description in Configuring export options.

6. Click the **Apply** button.

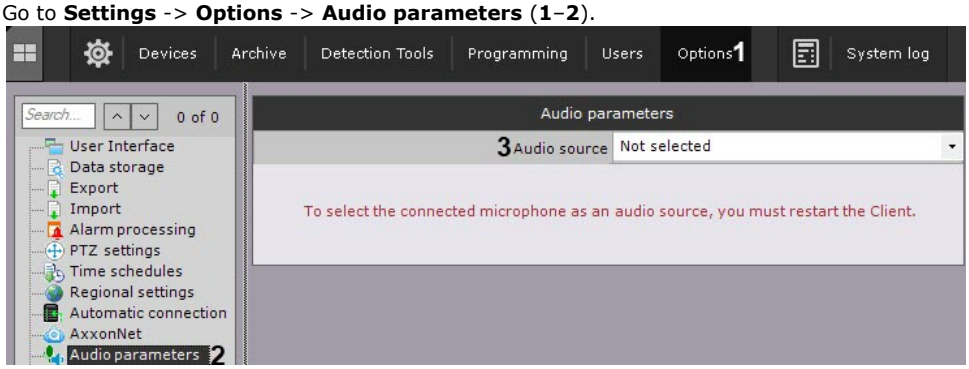
Creating and configuring the Export agent is now complete.

Configuring audio on the Client

To broadcast audio from the Client microphone on a camera speaker, you must configure audio on the Client.

Do the following:

1. Go to **Settings** -> **Options** -> **Audio parameters** (**1**–**2**).



2. In the **Audio source** field, select the system device that will be used as the audio source for playback on the camera speaker (**3**).

> **Note**
>
> The default device is shown in the list in bold.

3. Click the **Apply** button.

Configuration of audio on the Client is now complete.

Configuring hot keys

Introduction to hot keys in Axxon One

In *Axxon One*, hot keys for standard keyboards and joysticks can be set to perform certain actions.

The operator's work with hotkeys is divided into 6 modes:

1. Global mode, in which a hot key is always available.
2. Live Video mode.
3. Archive viewing and search in archive mode.
4. Time Compressor mode.
5. Alarm Processing mode.
6. Programming – running macros.

When setting hot keys, keep the following rules in mind:

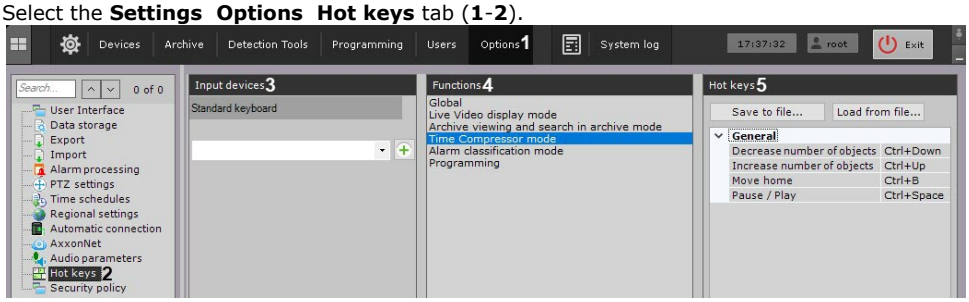
- the same shortcut can be used for different actions in different modes;
- a shortcut in any particular mode can be associated with only one action;
- shortcuts set in Global mode cannot be redefined in other modes;
- hot keys are available only when the Client is active;
- on standard keyboards, alphanumeric keys must be preceded by modifier keys (CTRL, ALT, SHIFT);
- during system configuration (when the Settings tab is open), only one action with hot keys is available: go to layouts (the Activate panel of configuration command).

> **Note**
>
> Please refer to the list of hotkeys in Appendix 6 to this guide.

Assigning hot keys

To assign hot keys:

1. Select the **Settings** ▸ **Options** ▸ **Hot keys** tab (**1**-**2**).



2. In the list, select the device for which you want to configure hot keys (**3**).
3. Select the mode for which you want to configure hot keys (**4**, see Introduction to hot keys in Axxon One).
4. To assign a shortcut to a specific action:
    a. Double-click the current shortcut assigned to the action (**5**). The field is now cleared.

> **Note**
>
> For some actions in Global mode, you cannot change the default hot keys.

    b. Press the key/key combination/joystick button to assign to the action.

> **Note**
>
> If the field is left empty, no hot key will be assigned to the action.

5. Assign hot keys for all actions of interest.
6. Click the **Apply** button.

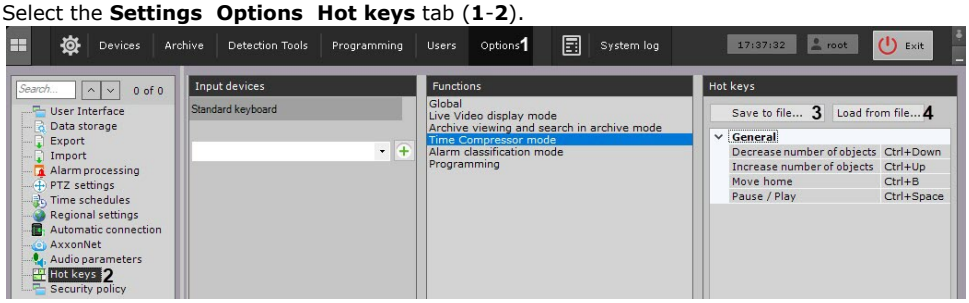
Assignment of hot keys is now complete.

Exporting and importing hot keys

You can export and import hot key configuration files from and to the Client. Export and import of hot keys is performed via files in XML format.

To export hot keys:

1. Select the **Settings Options Hot keys** tab (**1**-**2**).



2. Click the **Save to file...** button (**3**).
3. Select where to save the file and give it a name.

Export of hot keys is now complete.

To import hot keys:

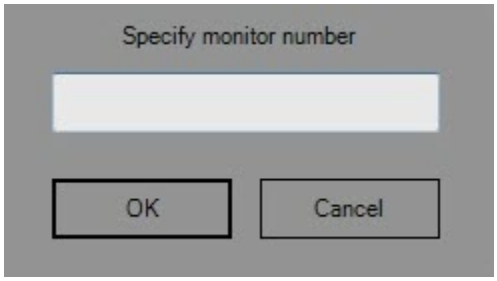
1. Select the **Settings Options Hot keys** tab (**1**-**2**).
2. Click the **Load from file...** button (**4**).
3. Select a file that contains a hot key configuration. Click the **Open** button.
   The hot key combinations are imported into the Client, so long as a valid file is selected.
4. Click the **Apply** button.

Import of hot keys is now complete.

Notes regarding hot key actions

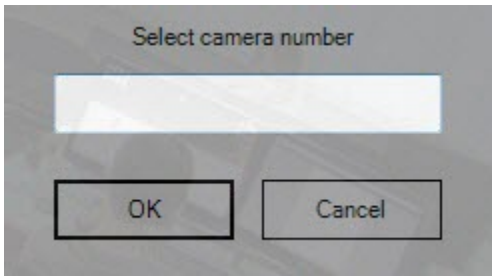
To select an active monitor in a multi-monitor configuration (see Managing monitors on a local Client), click **Select Monitor by number** (Global mode).

When you click the button or press the hotkeys, a window opens, where you can enter the monitor ID.



Enter the monitor ID and click **OK**. This monitor becomes active.

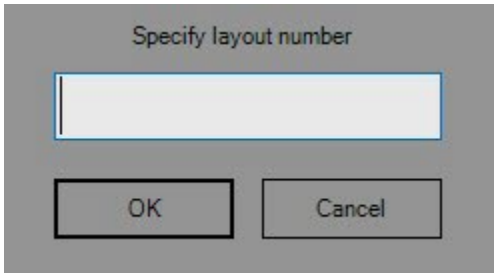
When a key or key combination assigned to the **Camera selection in current layout** action (Global mode) is pressed, the go to camera by number window opens.



Enter the destination camera's user- friendly short name (number) (see The Camera object), then click **OK**.

If the current layout contains a camera with the specified number (short name), the relevant viewing tile becomes active. If the current layout does not contain a camera with the specified number (short name), a minimum layout containing the camera is opened.

If you press hotkeys for **Select layout by number** (Global mode), a window opens requesting you to enter the layout number. The layouts are sorted left to right, starting from 1.



Enter the number of a desired layout, then click **OK**.

If you press hotkeys for **Select layout by ID** (Global mode), a window opens requesting you to enter the layout ID (see Setting a layout ID).

In all other cases, no system actions occur.

Descriptions of other non-trivial actions performed via hot keys are given in the table.

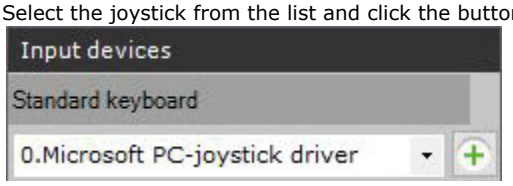
Mode	Action	Description
Global (general)	Navigation (up, left, down, right)	Navigate or move within the selected interface element. These keys are active only when a navigable menu or panel/ribbon is open.
	Activate layout ribbon	When this key is pressed, the layout ribbon expands, allowing to navigate between and select layouts. When the ribbon is minimized or a layout is selected, the relevant viewing tile becomes active.

	Activate panel of video walls	When this key is pressed, the panel of video walls expands, allowing to navigate between available monitors. When the panel is minimized, the viewing tile becomes active.
	Activate camera panel	When this key is pressed, the camera panel expands, allowing to navigate between and select cameras. When the panel is minimized or a camera is selected, a viewing tile becomes active.
	Activate panel of configuration	Pressing this key a second time opens the tools panel, on the **Layouts** ribbon.
	Open alarm panel	Pressing this key again minimizes the panel.
	Open panel with hardware list (left)	Pressing this key again minimizes the panel.
Global (map)	Switch to 3D mode	If the map is in 2D mode, clicking this button switches to 3D mode. If the map is in 3D mode, clicking this button hides the map.
Live Video mode	Open the menu of the selected camera and select a menu item.	Pressing this key again closes the menu.
	Switch to Archive mode	If a viewing tile in a layout is active, the archive is opened only for that particular camera. Pressing this key again switches to Live Video mode. If there are no active viewing tiles in the layout, the archive is opened for all cameras in the layout.
Archive viewing and search in Archive mode	Go to Search in Archive mode.	Pressing this key again switches to Archive mode.
	Go to the next /previous frame	Holding this key moves forward/backward frame by frame until the key is released.
	Go to the next /previous video clip	Holding this key moves forward/backward between video clips until the key is released.
	Go to TimeCompressor mode	Pressing this key again switches to standard Archive mode.
	Open list of timeline events	Pressing this key again closes the list.
	Move to next hour Move to next month Move to next timestamp Move to previous hour Move to previous month Move to previous timestamp	Listed are the actions available while operating the Calendar (see Navigating Using the Timeline).

Joystick Configuration

To configure the joystick, do as follows:

1. Connect the joystick to a computer.
2. Calibrate the joystick.
3. Select the joystick from the list and click the button .



4. Set keyboard shortcuts, and click **Apply**.
5. Configure the sensitivity for PTZ controls:
   a. Start a text processor (i.e. Notepad) and open the file <Joystick_Name>.xml, which is located in C:\Users\<User_Name>\AppData\Local\AxxonSoft\Axxon One\HotKeysXmlConfigurationFiles.
   b. Set the sensitivity for commands in **<Sensitivity>0.2</Sensitivity>**.

```
<HotKeysSchemaDeviceCommands>
<CommandName>DiscreteZoomOut</CommandName>
<HotKey>A2-</HotKey>
<Sensitivity>0.2</Sensitivity>
</HotKeysSchemaDeviceCommands>
```

The sensitivity values range from 0.0 (low sensitivity) to 1.0 (high sensitivity). Please see the commands that have sensitivity settings in the table.

Command	Command description
DiscreteMoveXAxisRight	Pan right (Move right)
DiscreteMoveXAxisLeft	Pan left (Move left)
DiscreteMoveYAxisUp	Tilt up (Move up)
DiscreteMoveYAxisDown	Tilt down (Move down)
DiscreteZoomIn	Zoom in
DiscreteZoomOut	Zoom out
DiscreteFocusNear	Reduce the focal length
DiscreteFocusFar	Increase the focal length
DiscreteIrisOpen	Open the iris
DiscreteIrisClose	Close the iris

Attention!

Do not set values outside the range and edit other parameters in the file.

   c. Save the changes to the file.

Joystick configuration is now complete.

If the joystick is already configured and the specified file does not have the **Sensitivity** parameter, do as follows:

1. Remove/Delete the joystick from the *Axxon One VMS*.



2. Click the **Apply** button.

3. Add and configure the joystick again.

Configuring video capturing on operator monitor

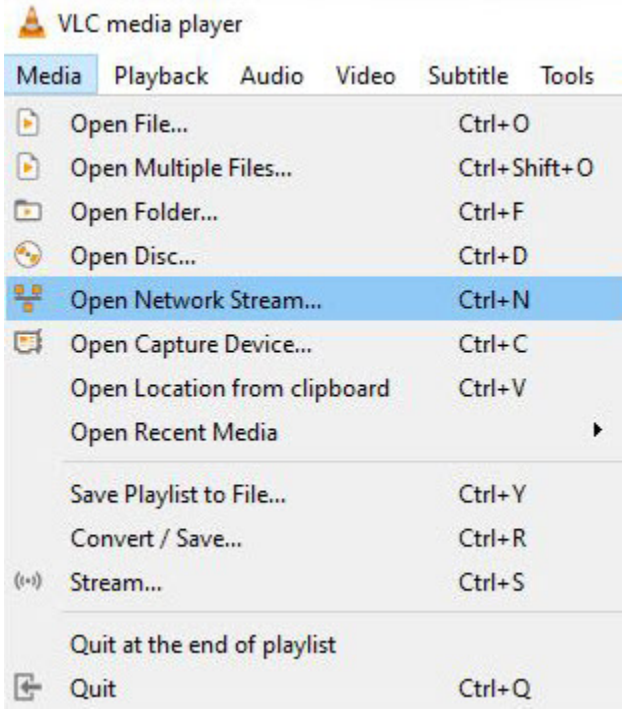
Video recording from the computer monitor is used to control the operator's actions. You can broadcast video from the computer monitor to *Axxon One* via the common protocols using the third-party software, for example:

1. Via the RTSP protocol using the VLC Media Player.
2. Via the ONVIF protocol using the ScreenOnvif software, which can be purchased on the website http://screenonvif.com/en.

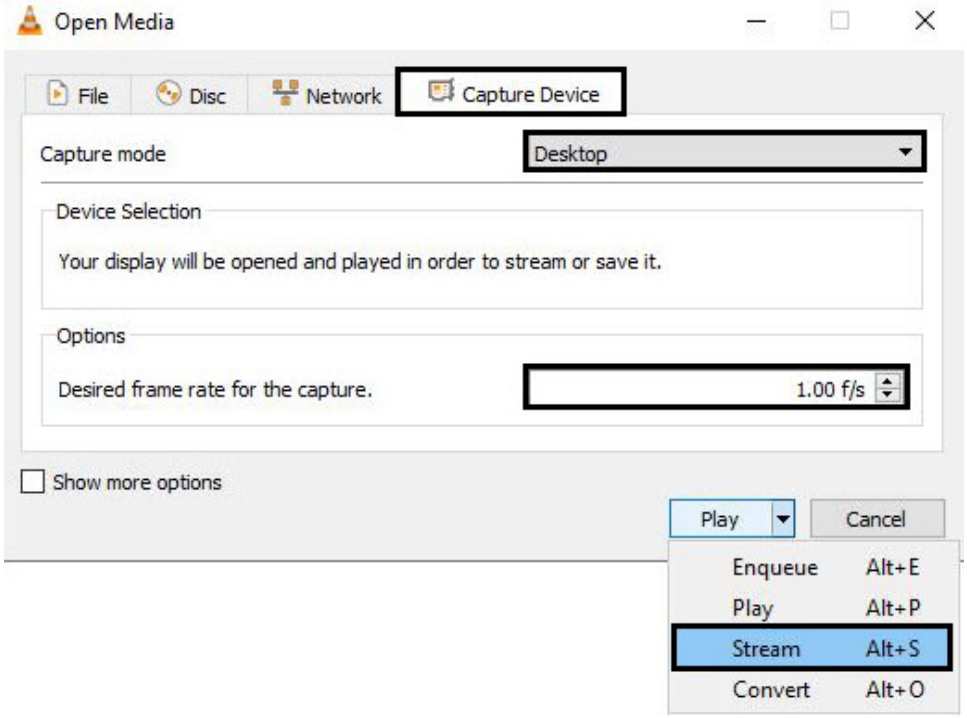
This section describes how to configure VLC Media Player to broadcast video from the computer monitor to *Axxon One* via the RTSP protocol. Configuring *Axxon One* to receive and record such a video stream is performed in a standard way as described in Configuring an RTSP Server and Configuring recording to an archive.

Configuring VLC Media Player to broadcast video from the computer monitor to *Axxon One* via the RTSP protocol is performed in the following way:

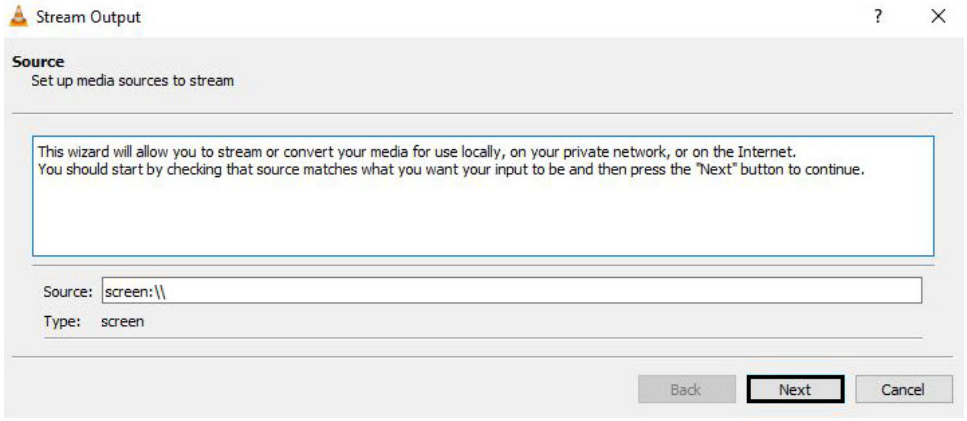
1. Run VLC Media Player.
2. Select the **Open Network Stream...** item in the **Media** menu.



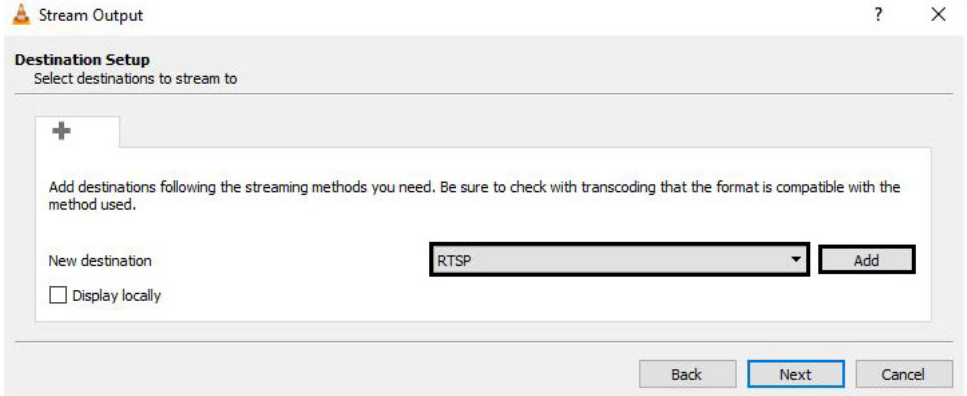
3. In the appeared window go to the **Capture Device** tab.



4. From the **Capture mode** drop-down list, select the **Desktop** value.
5. Set the required frame rate value for the capture in the corresponding field.
6. In the **Play** drop-down list, select the **Stream** value. As a result, the **Stream Output** window will appear.

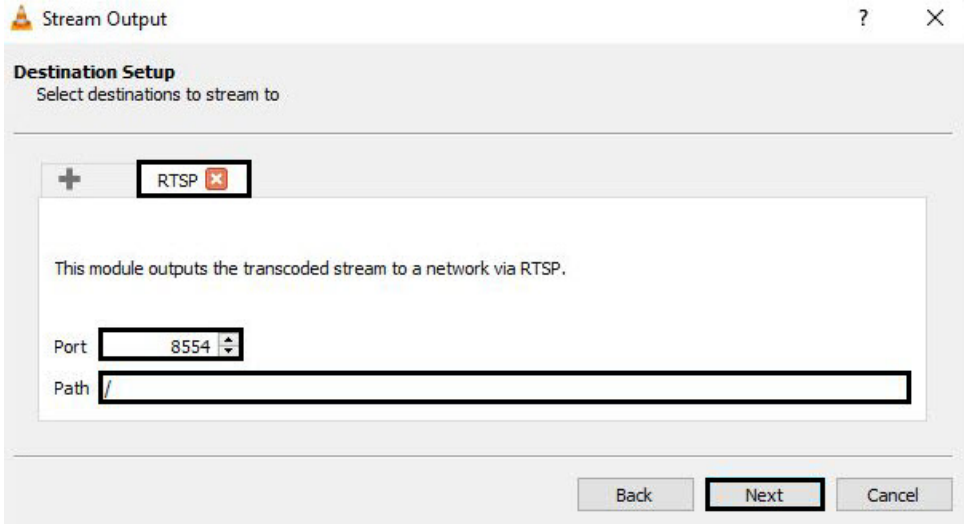


7. Click the **Next** button.
8. In the appeared window, select the **RTSP** value from the **New destination** drop-down list and click the **Add** button.

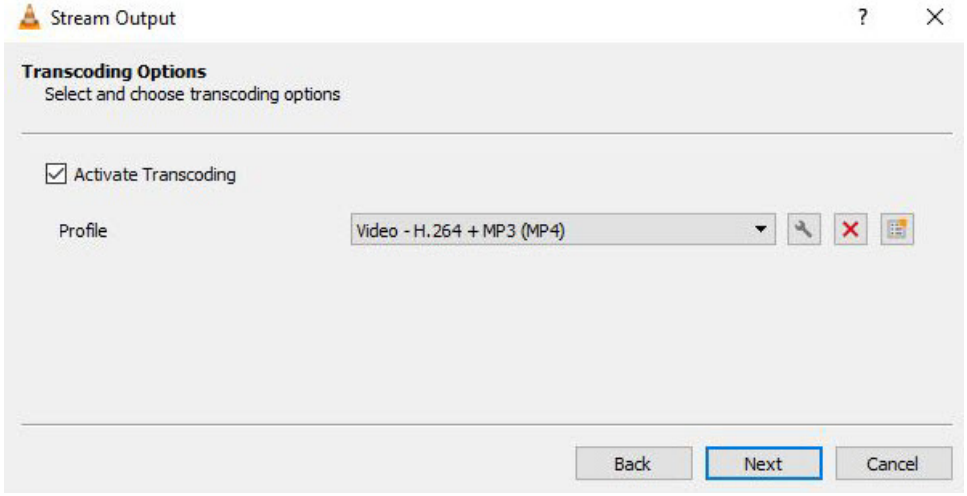


9. Go to the **RTSP** tab.

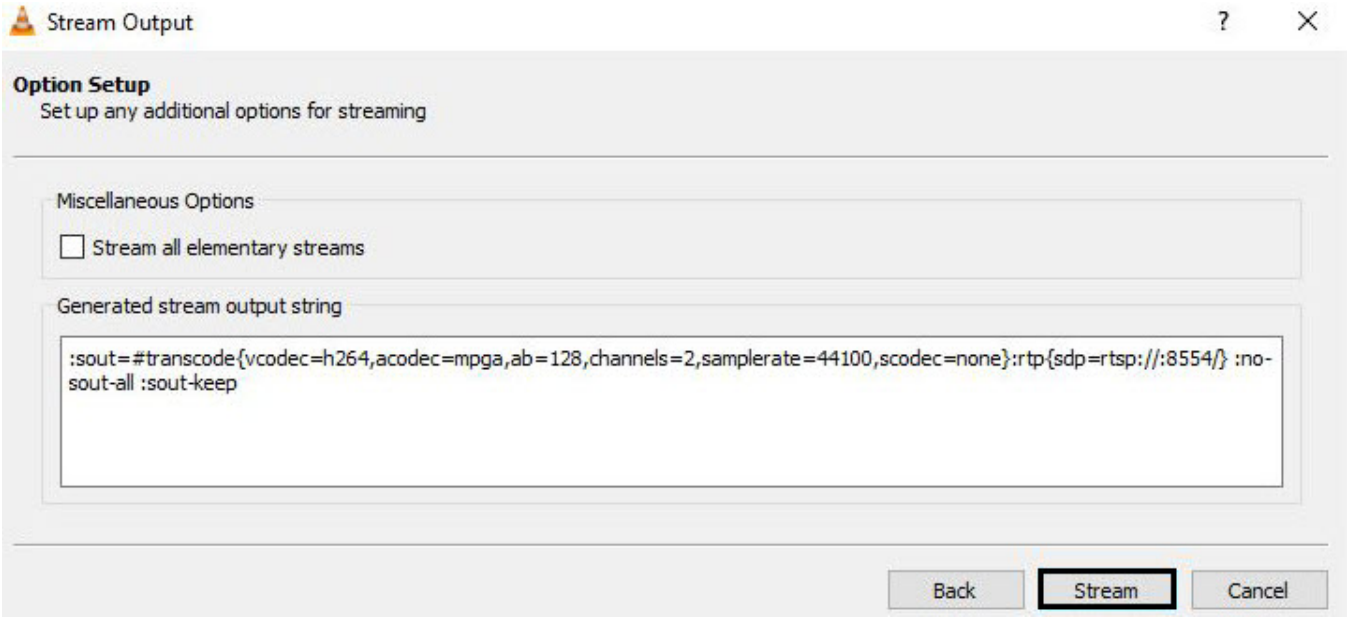
10. Specify the port and the path to the stream, if necessary.



11. Click the **Next** button.
12. Specify the parameters of video transcoding and click the **Next** button.



13. Click the **Stream** button in the appeared window.



After that, you can configure *Axxon One* to receive the RTSP stream and record it to the archive (see Configuring connection of devices via RTSP and Configuring recording to an archive).

Configuring VLC Media Player to broadcast video from the computer monitor to *Axxon One* via the RTSP protocol is completed.

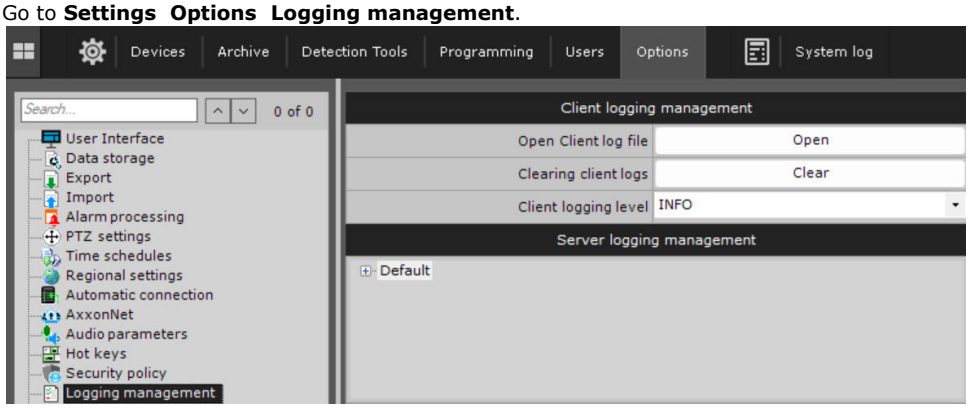
Configuring the Client logging level

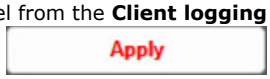
By default, the Client logging level is determined by the settings specified in a special utility (see Log Management Utility). But you can temporarily change the Client logging level for operational analysis of current logs.

Changes made to the logging level will remain in effect until the Client is turned off. The next time you start the Client, the logging level will correspond to the one specified in the Log management utility.

To temporarily change the Client logging level, do as follows:

1. Go to **Settings Options Logging management**.



2. Select the required level from the **Client logging level** list. Levels are described in Configuring the logging levels.
3. Click the **Apply** button 

.

The Client logging level is temporarily changed.

You can also delete all Client logs. To do this:

1. Next to the **Clearing client logs** area, click the **Clear** button.
2. Click the **Apply** button.

All Client logs are deleted.

Configuring Failover VMS

General information about a failover system

A failover system automatically prevents data loss when one of the Servers in the system fails.

In a failover system, the Servers are combined into a logical structure—the cluster.

The *Axxon One* Failover system has two types of configuration.

1. The basic configuration allows system supervisors to permit launching *Axxon One* servers (nodes) on any Servers within the system.

   > **Note**
   >
   > When selecting a Server to transfer a node to, the supervisor tries to keep in balance the whole cluster's performance. If all Servers deliver more or less the same performance, the selection is performed randomly.
   >
   > If Servers significantly differ in their performance, the supervisor may launch several nodes on a more capable Server, and no nodes on a less capable one.

2. In the configuration with the specified backup Server, a node from the primary Server can be migrated only to the backup Server. After the primary Server is back online, the node is returned.

Node migration is automatic and takes no more than one minute.

> **Note**
>
> In a system counting 100 cameras, the node is transferred in less than one minute in both Failover System configuration types. All Servers within the system have identical specifications: Intel i5-7400 3GHz 4-core CPU, 16Gb RAM.

This section contains the following terms:

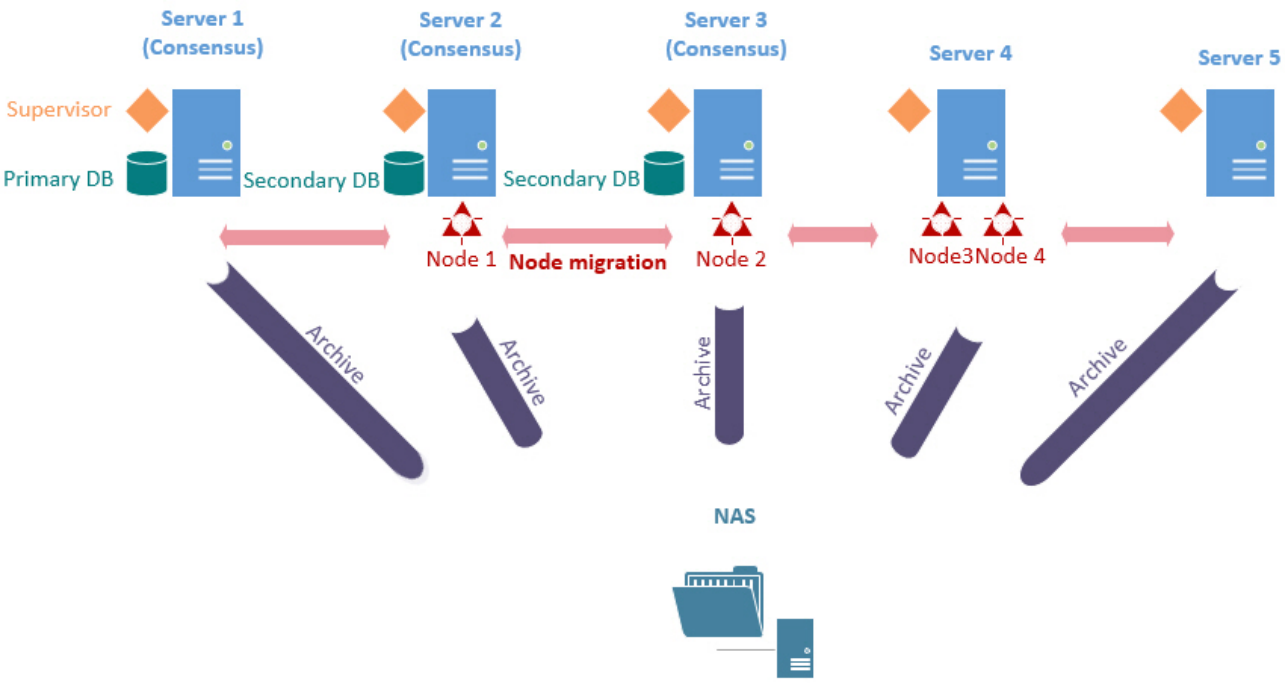
- **Server**—a computer with **Failover Server and Client** configuration of *Axxon One* installed;
- **Node**—an instance of the Server services. A Server can have multiple nodes running;
- **Cluster**—logical grouping of Servers that allows migration of nodes between them. A cluster may encompass nodes from different Axxon-domains;
- **Supervisor**—the service that monitors the status of nodes and their migration.

To implement Failover in your system, we strongly recommend that:

- the system administrator should have full control over all communication channels and hardware that provides fault tolerance at all times;
- you should build a cluster from servers in the same LAN;
- use only the network archives, that are available from all servers in the cluster.

Example of a Failover system:

CLUSTER



Note

You can install *Axxon One* Server in the Failover mode in Linux OS (see Installing from repository, Manual installation).

Ports used by the failover system

Each failover system Server uses the following ports:

- 4000 (Supervisor Web-Interface, only TCP),
- 4646 (Nomad HTTP API, only TCP),
- 4647 (Nomad RPC, only TCP),
- 4648 (Nomad LAN/WAN Serf (Gossip), TCP and UDP),
- 8300 (Consul Server RPC, only TCP),
- 8301 (Consul LAN Serf (Gossip), TCP and UDP),
- 8302 (Consul WAN Serf (Gossip), TCP and UDP),
- 8500 (Consul HTTP API, only TCP),
- 8600 (Consul DNS, TCP and UDP).

Moreover, each node of the cluster has its pre-defined unique port range (see Installation).
For best results, use port numbers from 20111 to 32000.



Changing ports in the nodes of the failover system

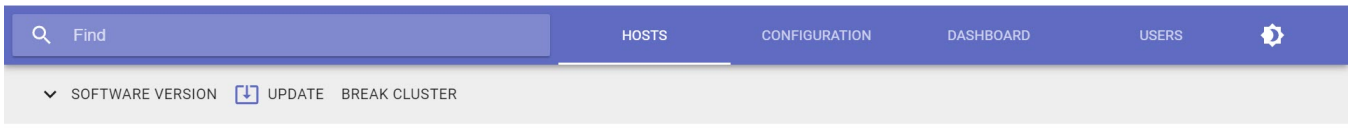
Supervisor Web-Interface

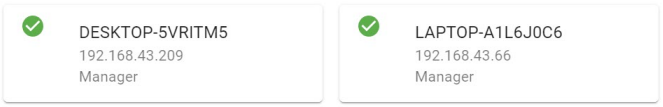
You can configure a failover system in the Supervisor Web-Interface at http://localhost:4000.

> **Note**
>
> After installation, a shortcut is added to your desktop.
>
> 
>
>
> On Linux OS, no additional shortcuts are created after installation. To access the Supervisor Web-Interface, go to http://localhost:4000.

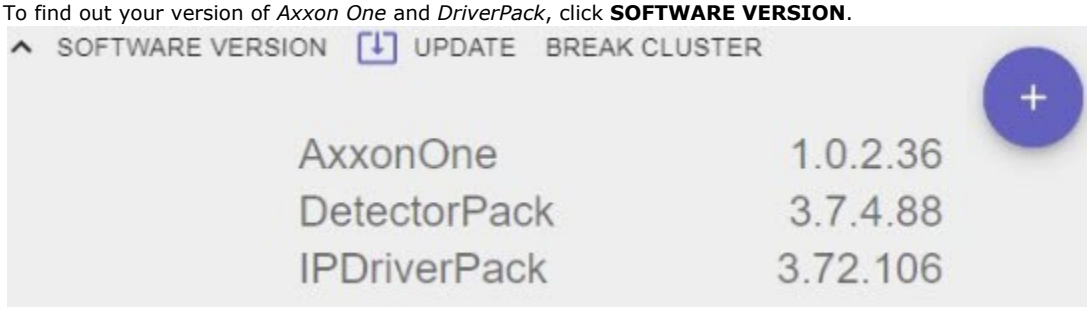
The Supervisor Web-Interface has four tabs:

1. **HOSTS**—Creating a cluster.
2. **CONFIGURATION**—Failover Database, Configure a Failover System Cluster.
3. **DASHBOARD**—Monitoring the status of a cluster.
4. **USERS**—Set up access to a supervisor.





To find out your version of *Axxon One* and *DriverPack*, click **SOFTWARE VERSION**.



To search hosts and servers, enter their names in the search bar in the **HOSTS** or **DASHBOARD** tabs in the top left part of the interface.

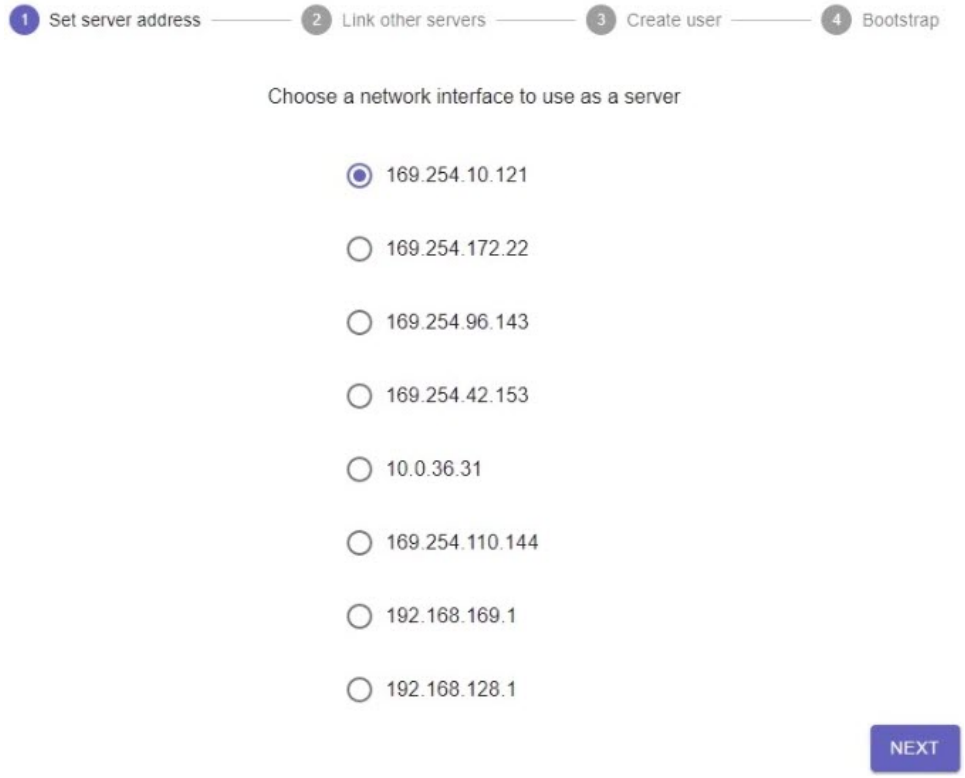


You can choose the Supervisor theme in the Web-Interface: dark or light. To enable the dark theme of the Supervisor Web-Interface, click the  button in the top right part of the interface. To enable the light theme of the Supervisor Web-Interface, click the  button.

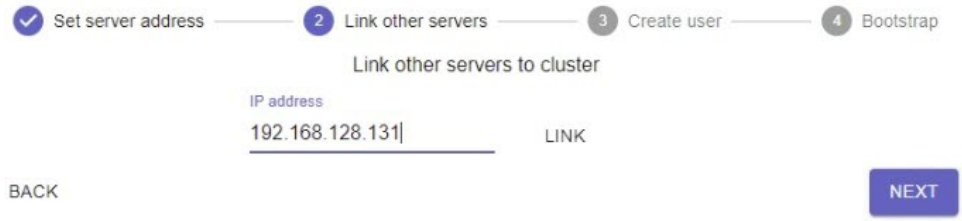
Creating a cluster

The first time you launch the Supervisor, you should initialize the cluster. To do this, do the following:

1. Select the Server's IP address from the list and click **NEXT**.



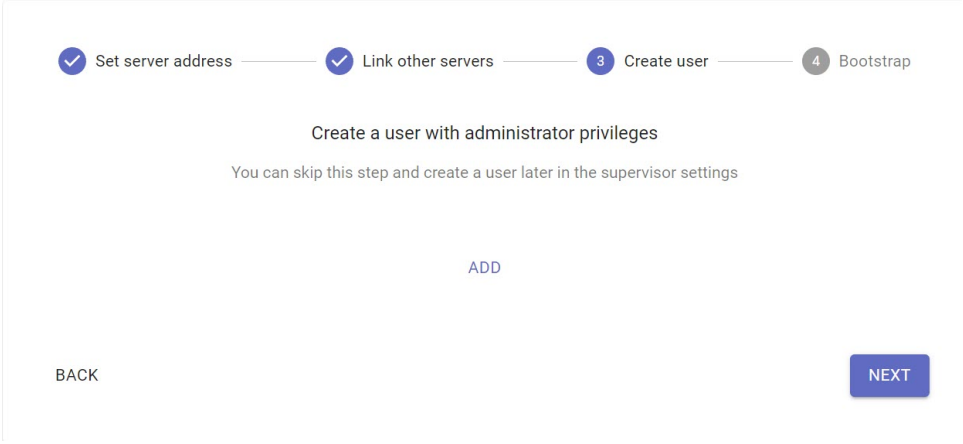
2. Add the required Servers to the cluster. To do this, enter the IP address and click **LINK**.



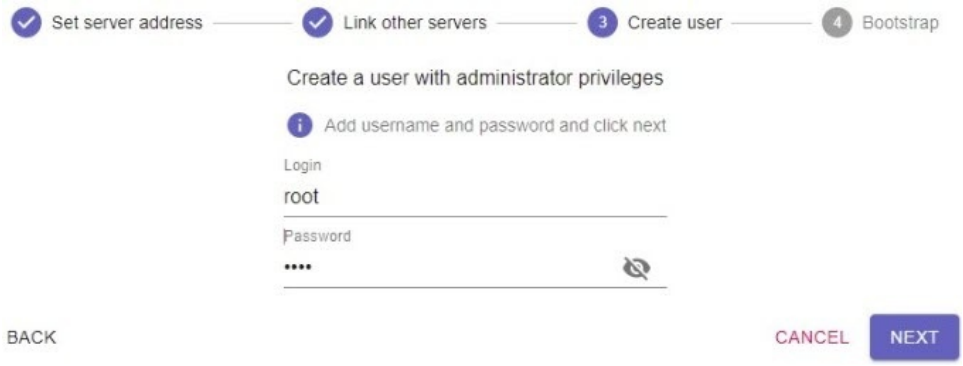
> **Attention!**
>
> - All cluster Servers must be available to each other.
> - It is necessary to use Servers with the same architecture (x64), OS type and PostgreSQL version.
> - The first three Servers added become the master Servers.
> - The operation of the cluster is coordinated by its master Servers, which, in particular, take decisions to migrate nodes from one Server to another.
> - The number of the master Servers in the cluster must be either 3 or 5.
> - The role of the master Server does not affect the configuration and implementation of fault tolerance. Thus, the master server can be used as a fault-tolerant one (for example, to implement a **2+1** configuration).
> - If only two Servers are added, they can be configured as **1+1**—master + backup Server (see 1+1 cluster configuration).

3. If required, you can add a user with administrator rights (see Set up access to a supervisor). After the cluster is created, only this user will have access to the supervisor. Do the following:

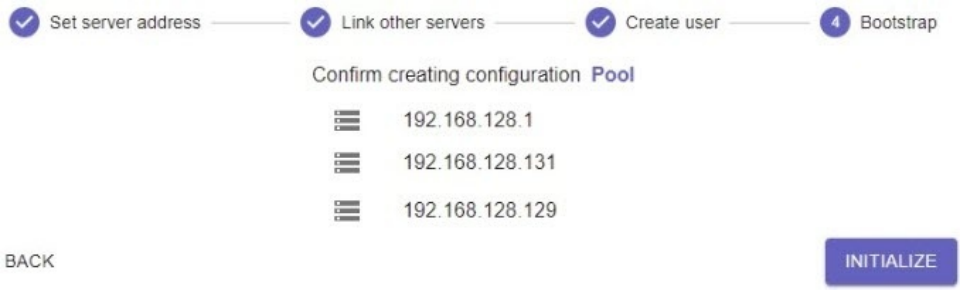
a. Click the **ADD** button.



b. Enter access credentials and click the **NEXT** button.



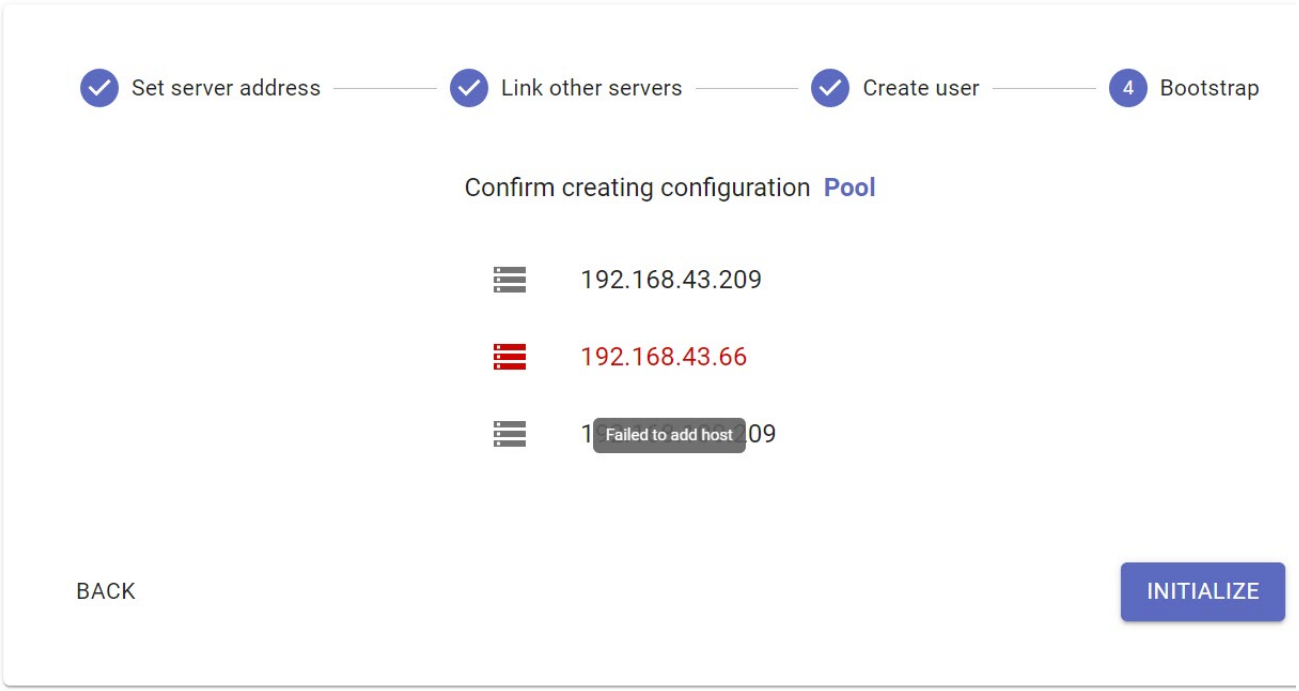
4. After you added all Servers, click the **INITIALIZE** button.



This will initialize the cluster based on the selected Servers.

Note

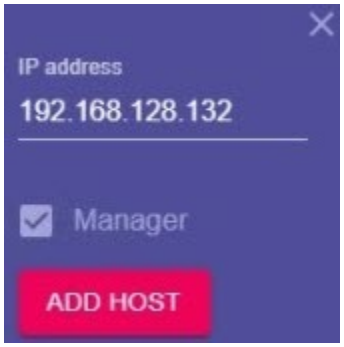
If during the process of cluster creation, you added the Server that were already added to another cluster, they will be unavailable. If you try to initialize the cluster with unavailable Servers, they will be marked red, and the cluster won't be initialized.



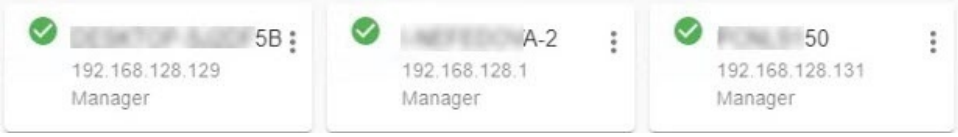
In this case you need to go back to the step of adding the Servers and add the available Servers.

To add other Servers to the cluster, do the following:

1. On the **HOSTS** tab, click  .
2. Enter the IP address of the Server.

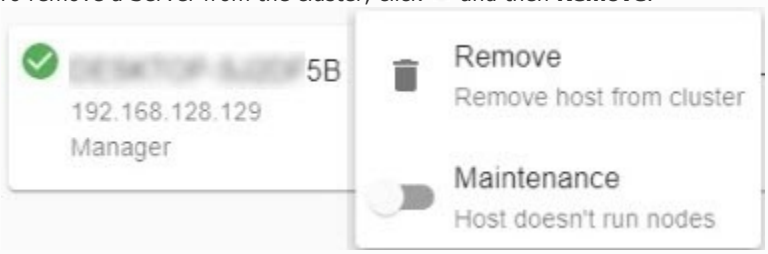


3. If the Server you are adding is master, set the **Manager** checkbox.
4. Click **ADD HOST**.
5. Add all required Servers.



Note

To remove a Server from the cluster, click ⋮ and then **Remove**.



Attention!

To change the IP addresses of the Server in the cluster, do the following:

1. Remove the Server from the cluster.
2. Change the IP address of the Server.
3. Add the Server with a new IP address.

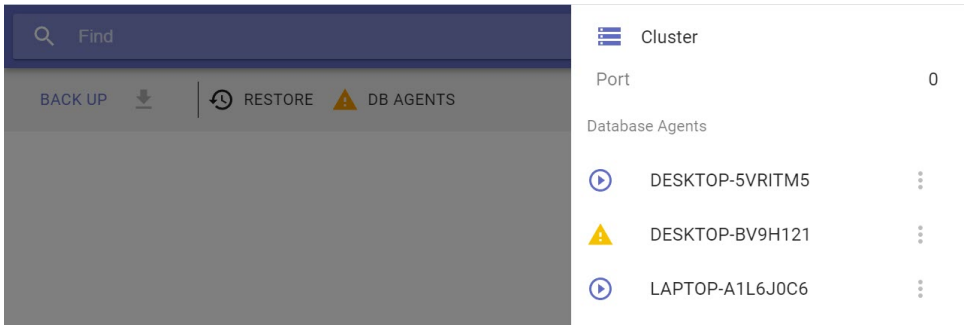
Failover Database

By default, the database is created automatically when the cluster is initialized, and its agents are launched on the master Servers.

> **Attention!**
>
> For the database to work correctly, its agents must be running on the Servers with the same type of operating system.

To manage database agents, do the following:

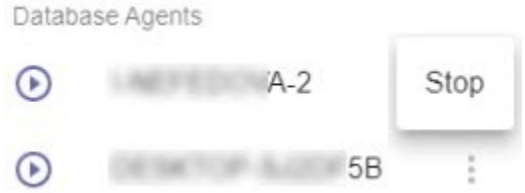
1. Go to the **CONFIGURATION** tab.
2. Click **DB AGENTS**.



3. The **Port** field specifies the value of the port that the database agents use. If the value is 0, the database agents use dynamic ports.
4. The icon next to the Server indicates the current status of the agent.

Icon	Status
	Launch expected
	Launched
	Stopped
	Unavailable

5. Click ⋮ to stop or launch the agent, and select the required action.



Configure a Failover System Cluster

A failover system can be configured in two ways:

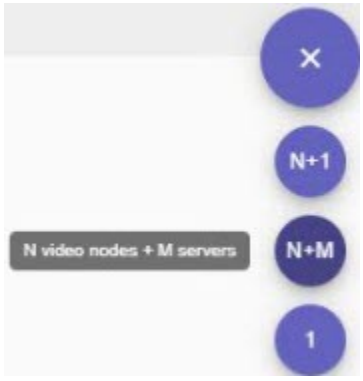
1. Basic configuration. There are no pre-assigned backup Servers in this configuration. The supervisor independently decides where to host a particular node. Only network archives can be used in this configuration.
2. Configuration with the specified backup Server. In this configuration, a backup server is assigned to host a node which for some reason cannot operate on its primary server. Along with network archives, local archives can be used in this configuration.

In addition, you can create independent nodes.

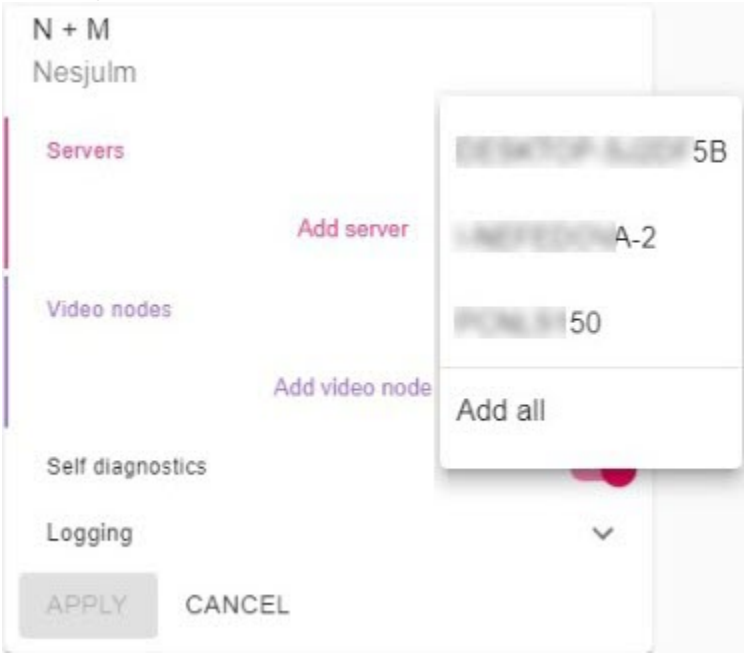
Setting up basic configuration

To set up a basic configuration of a Failover system, do the following:

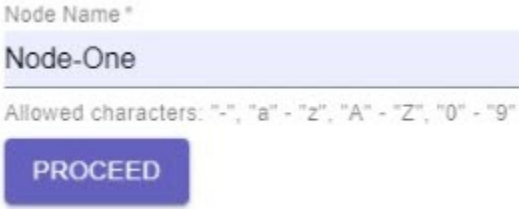
1. Go to the **CONFIGURATION** tab.
2. Hover the mouse cursor over the  button and click the **N+M** button.



3. Add Servers to the configuration.
   a. Click  .
   b. Select a specific Server, or add all Servers at once.



4. Create nodes:
   a. Click  .
   b. Enter the node name and click the **PROCEED** button.

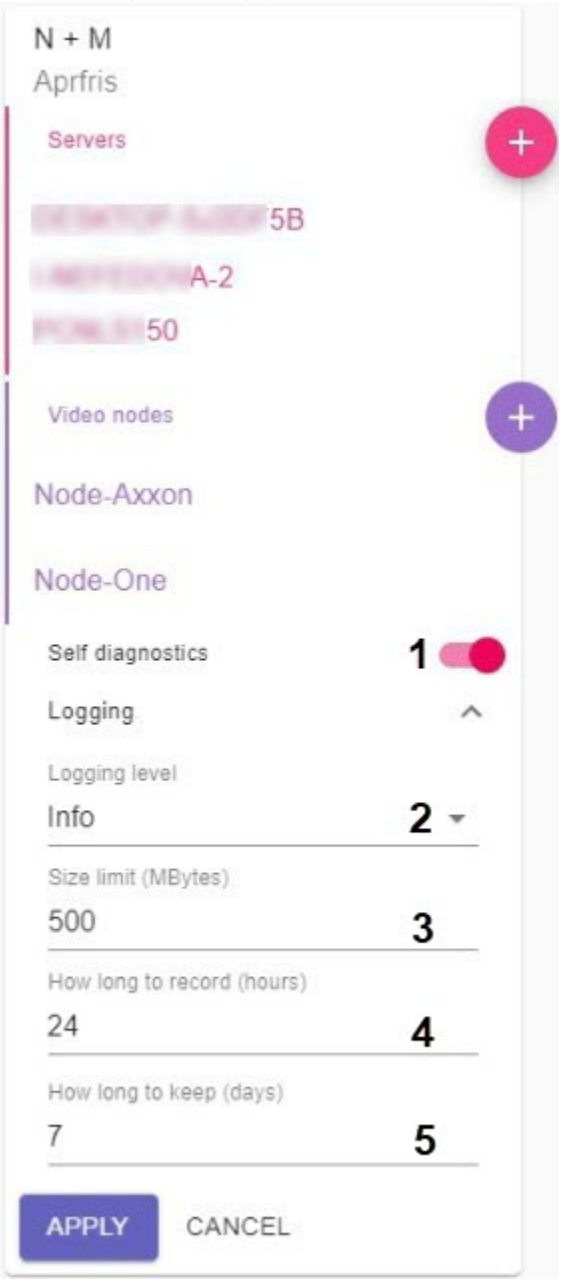


> **Attention!**
>
> A node name may contain Latin and numerical characters, and the "-" symbol.

c. Create the required number of nodes.

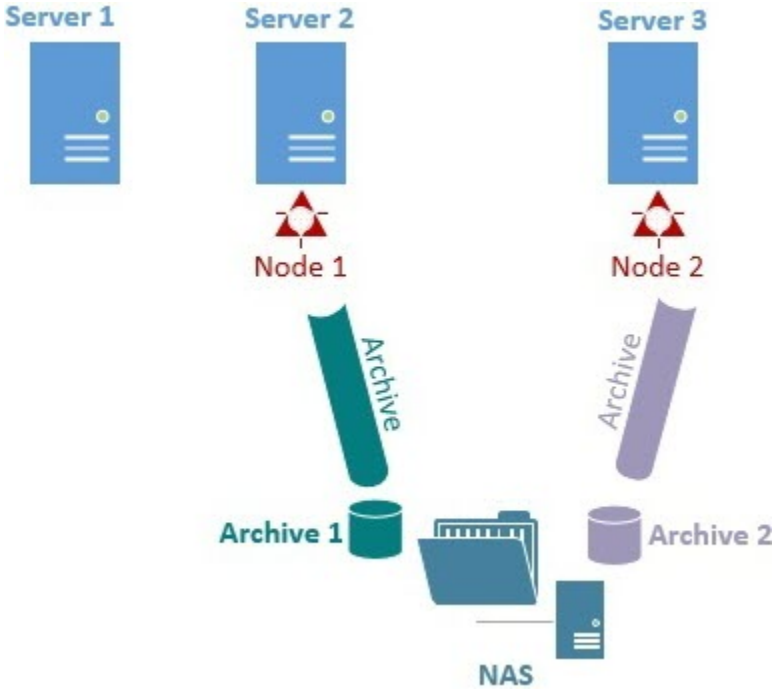
> **Attention!**
>
> - The number of nodes must be less than the number of Servers.
> - No more than 10 nodes must be connected to a single event cluster database.

5. By default, the self-diagnostics service is running on all nodes (see Self-diagnostics service). To stop it, de-activate the **Self diagnostics** parameter (**1**).

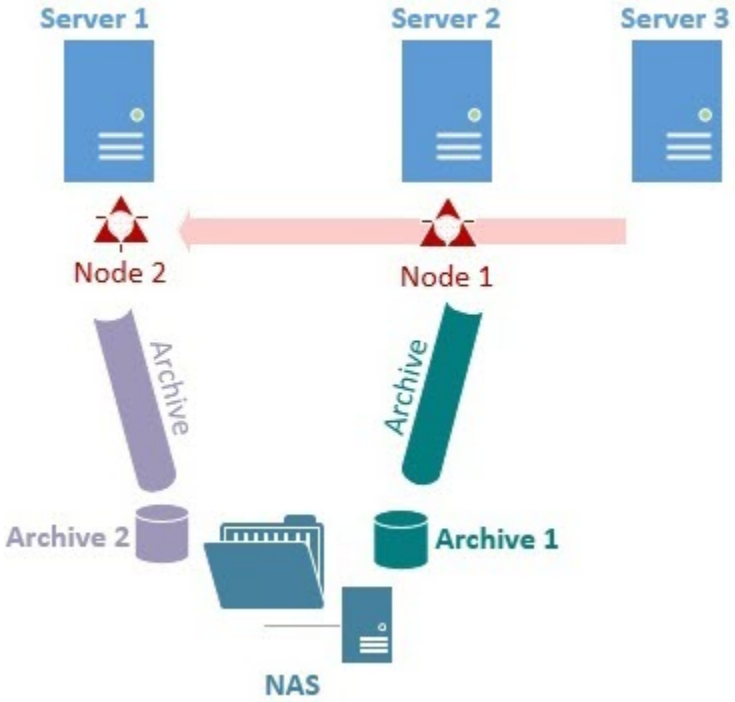


6. Click the **Logging** button to set the logging options:
   a. Select Logging level (**2**, see Configuring the logging levels).
   b. Set the settings for the archive of logs (**3**-**5**, see Configuring the Server log storage and archiving options).
7. Click the **APPLY** button.
   The configuration is now created, and the nodes are now automatically started.

8. Merge all nodes into a single domain (see Connecting to a Node and Configuring of an Axxon domain).
9. Set up the archive of the Failover system.
   In a Failover system, we recommend you to physically locate the archive on a separate NAS remote storage that all servers in the cluster have access to.
   For each node, create a separate archive in the remote storage (see Creating a remote archive).



If the node is moved to a different server, it will continue to write to the specified archive.



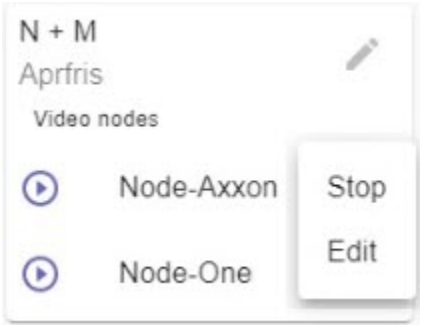
The basic configuration of the Failover system is now complete.

If necessary, you can further edit the configuration. To do so, click . You can perform the following actions:

- add/remove Servers;
- add/delete nodes;
- activate/de-activate the self-diagnostics service;
- change logging parameters;

- completely remove the configuration.

To manually stop or launch a node, click ⋮ and select the required action.

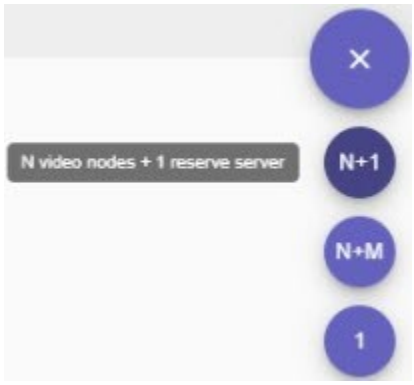


Setting up a configuration with the backup Server

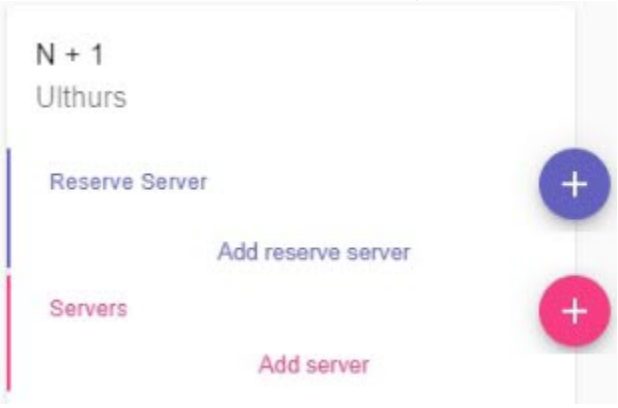
A configuration with the backup Server can include two or more Servers.

To set up the configuration, do the following:

1. Hover the mouse cursor over the  button and click the **N+1** button.

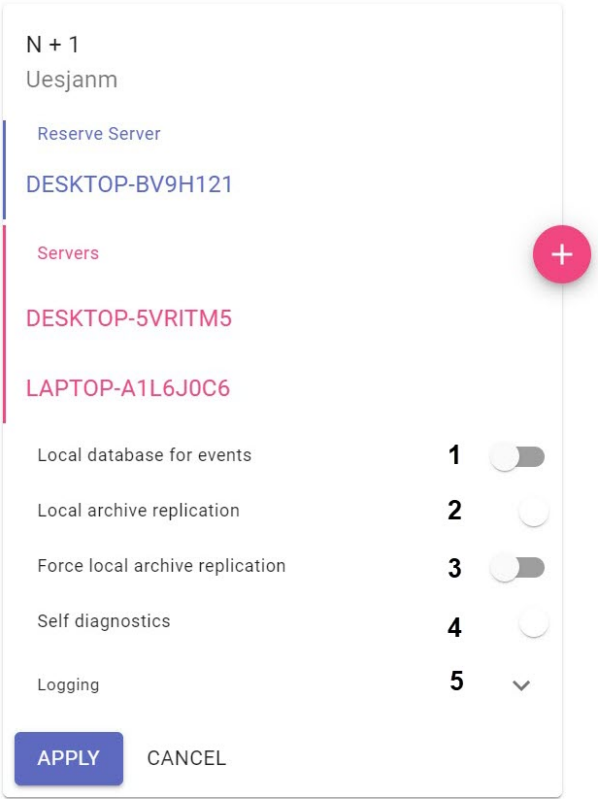


2. Click the  button and add a backup Server.



3. Click the  button and add primary Servers.

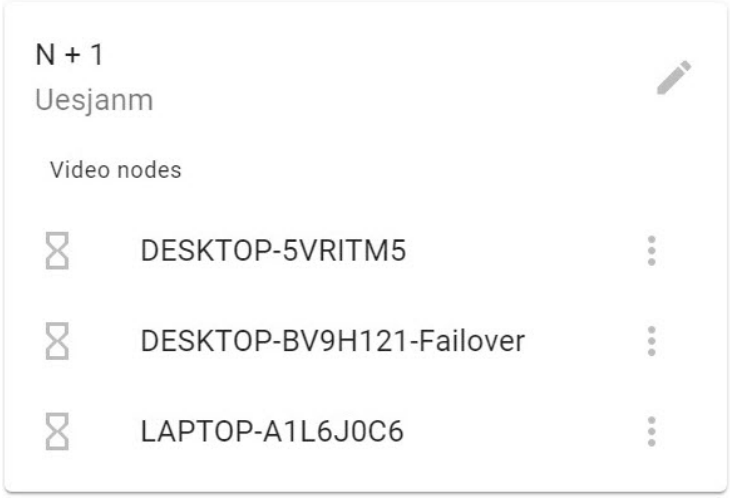
4. If you need to maintain a local event database on Servers, activate the corresponding switch (**1**).



5. If you want to replicate the local archive when the master node is on the backup Server, activate the corresponding switch (**2**).

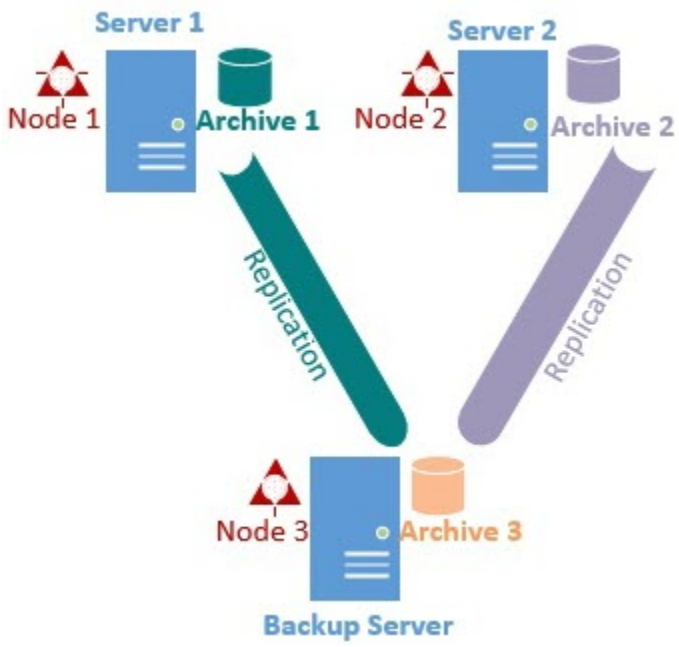
> **Attention!**
>
> The local archive must be created on the master node (see Creating a local archive).

6. If you need to replicate local archives to the backup Server on permanent basis, activate the corresponding switch (**3**). Otherwise, the replication will be performed only when the corresponding node is migrated to the backup Server.
7. By default, the self-diagnostics service is running on all nodes (see Self-diagnostics service). To stop it, deactivate the **Self diagnostics** parameter (**4**).
8. Click the **Logging** button to set the logging parameters (**5**):
   a. Select the logging level (see Configuring the logging levels).
   b. Set the log archive parameters (see Configuring the Server log storage and archiving options).
9. Click the **APPLY** button.
   The configuration is now created, and the nodes are now automatically started. "Failover" string will be automatically added to the name of the backup node.



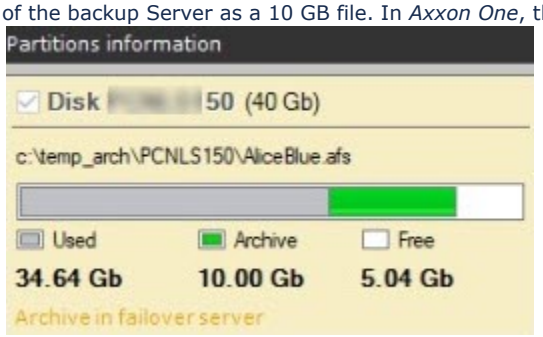
10. Merge all nodes into a single Axxon-domain (see Connecting to a Node and Configuring of an Axxon domain).
11. Configure the archives operation:

a. On the backup node, create an archive for replication (see Creating archives).
b. On the master nodes, configure the replication from the master Servers' archives to the backup node's archive (see Configuring data replication). The replication period should be set to **Always** regardless of the value of the **Force archive replication** parameter (see item **6**).



Setting up a configuration with the backup Server is now complete.

When a master node is migrated to the Failover Server, a temporary archive will be automatically created in the C:/temp_arch folder of the backup Server as a 10 GB file. In *Axxon One*, the temporary archive will be marked as **Archive in failover server**.

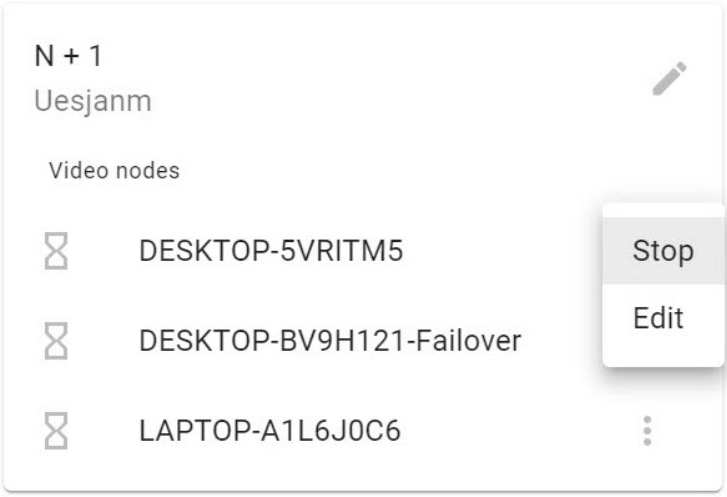


The records from the temporary archive will be replicated to the archive for replication (see **Archive 3** on the figure above) of the backup Server.

If necessary, you can further edit the configuration. To do so, click the button. You can do the following

- add/remove Servers;
- add/delete nodes;
- activate/deactivate the self-diagnostics service;
- change logging parameters;
- completely remove the configuration.

To manually stop or start a node, click ⋮ and select the required action.

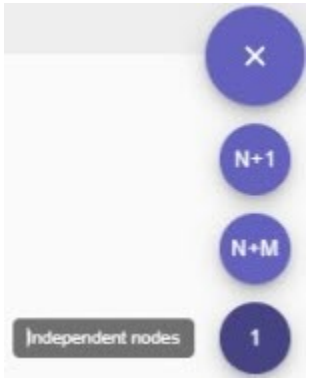


Creating and configuring independent nodes

You can host separate nodes on cluster's Servers which are not used by any configuration.

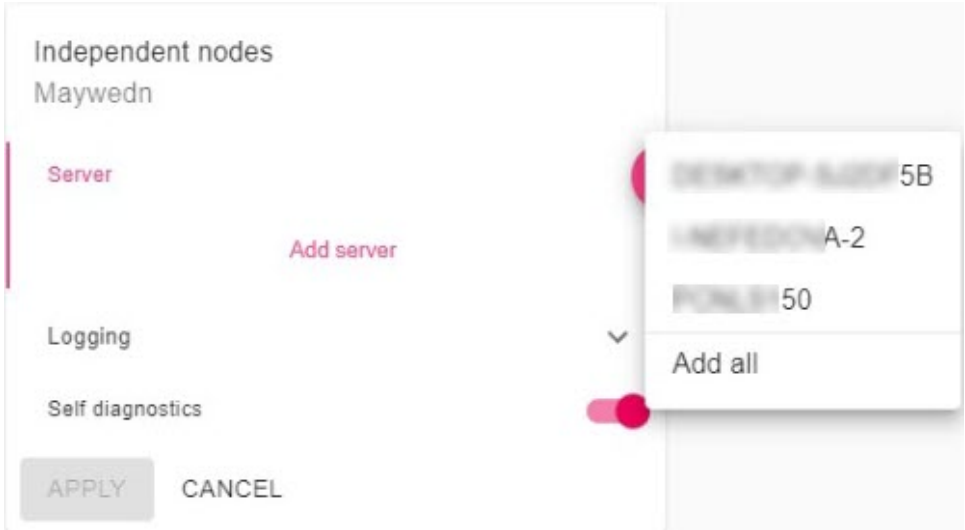
Failover doesn't cover these nodes since they rely on local databases. If the host Server fails, the nodes can not be migrated.

To create an independent node, do as follows:

1. Go to the **CONFIGURATION** tab.
2. Point the cursor at  and click **1**.


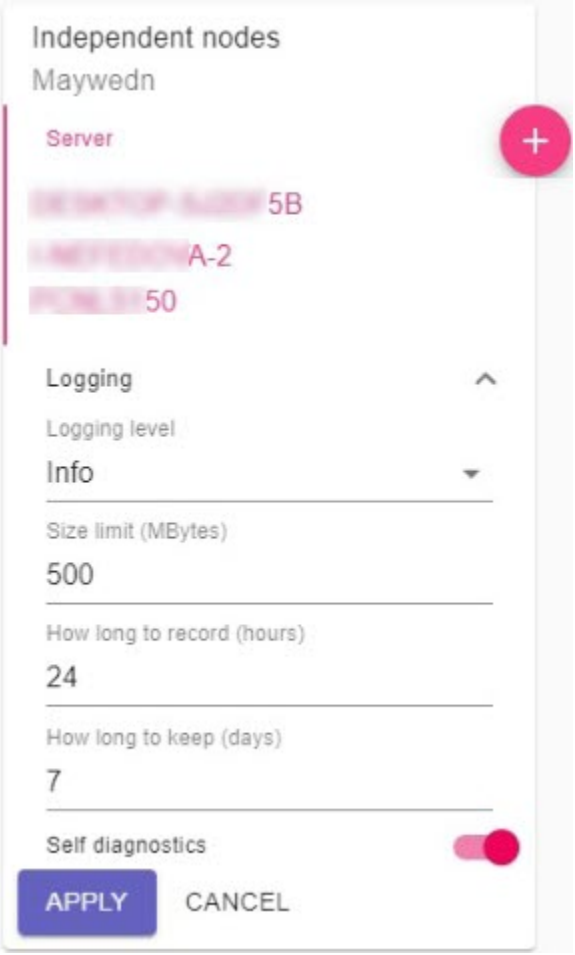
3. Click  and select Servers where independent nodes should be launched.

   > **Attention!**
   >
   > You can create only one independent node on each Server.



4. By default, the self-diagnostics service is running (see Self-diagnostics service). To stop it, de-activate the **Self diagnostics** parameter.

5. Click the **Logging** button to set the logging options.



6. Click the **APPLY** button.

The nodes are now created; they should start automatically.



1+1 cluster configuration

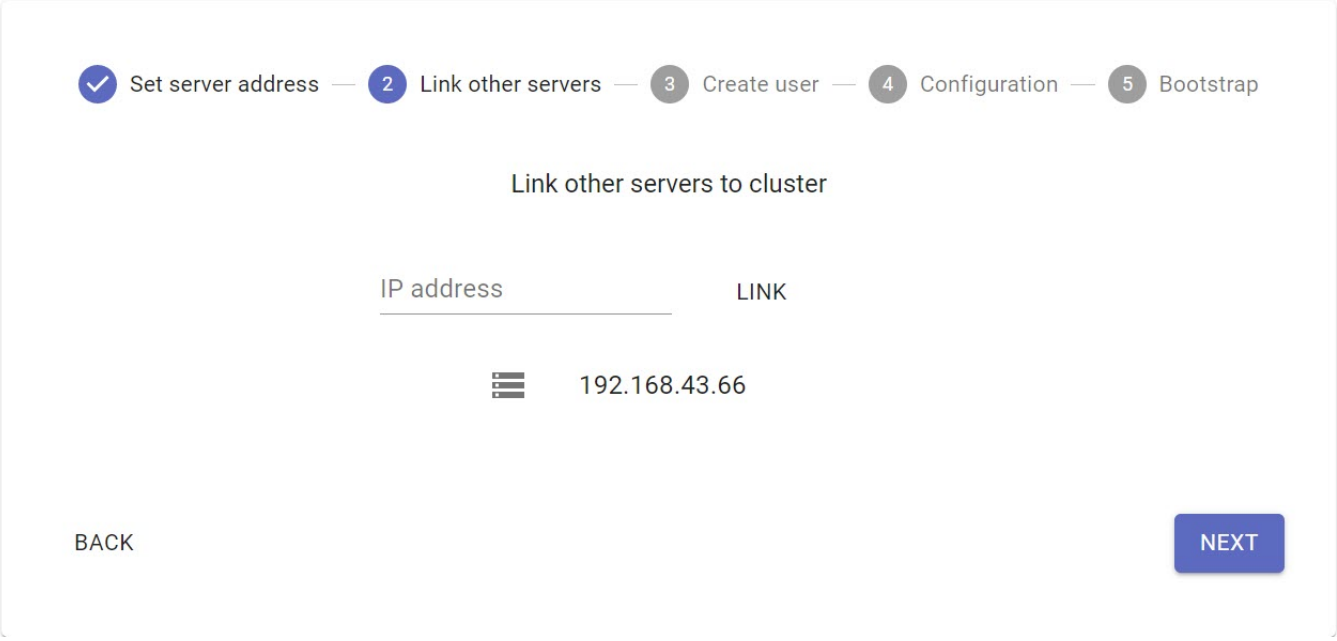
On this page:

- Setting up 1+1 configuration
- Converting to 1+1 configuration
- Editing the configuration
- Setting up archive replication
- How replication will run

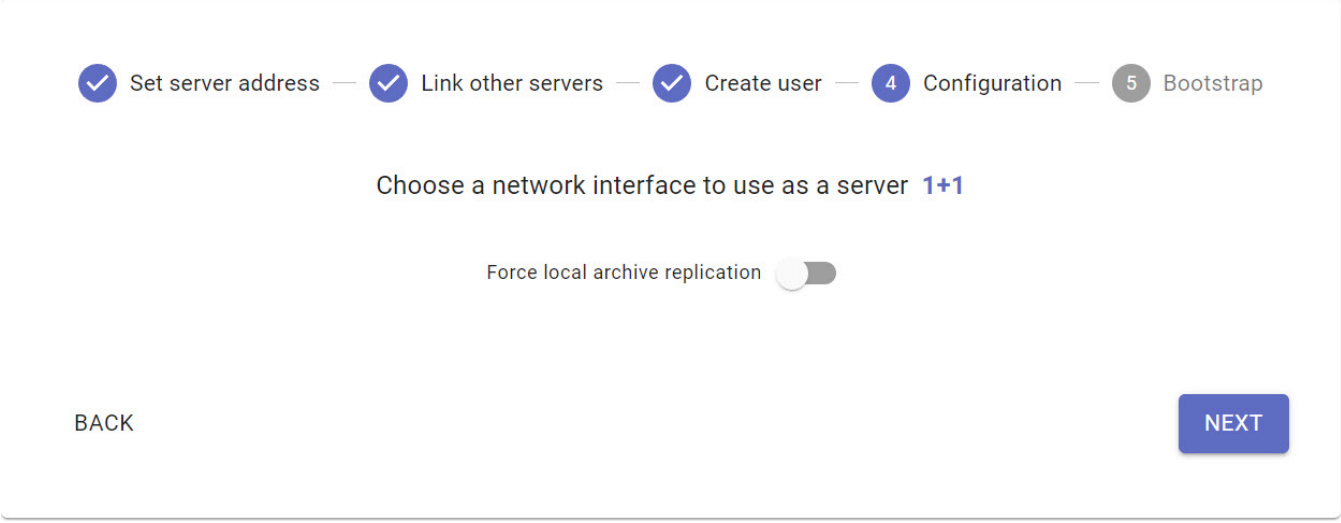
Only two Servers can be added into 1+1 configuration.

Setting up 1+1 configuration

To initialize 1+1 configuration, add a second Server to the configuration. To do this, enter the IP address and click **LINK**.



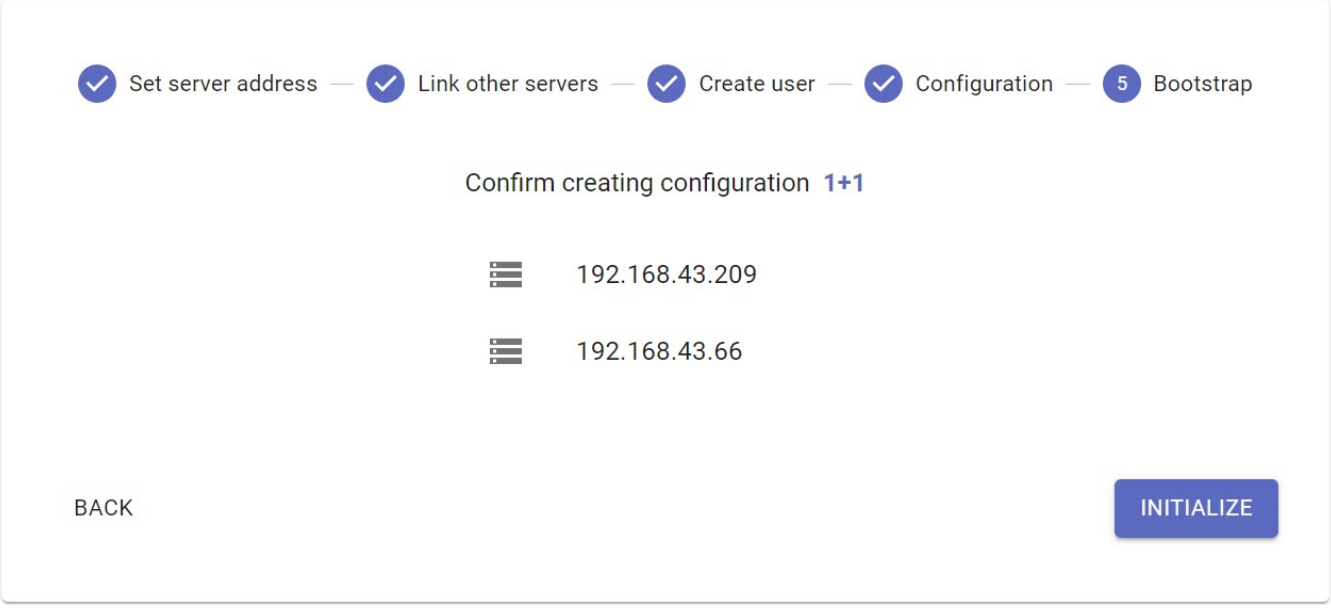
Next, activate the **Force local archive replication** parameter if you want the replication to the backup archive to be continuous regardless of the location of the master node.



Note

You can activate this parameter only at the 1+1 configuration setting stage or at the conversion to 1+1 configuration stage. Then you can activate this parameter only if you recreate the cluster.

To set up a cluster in this configuration, you must initialize the cluster after adding two Servers.



In this case, the master node will be located on the Server from which the cluster was initialized.

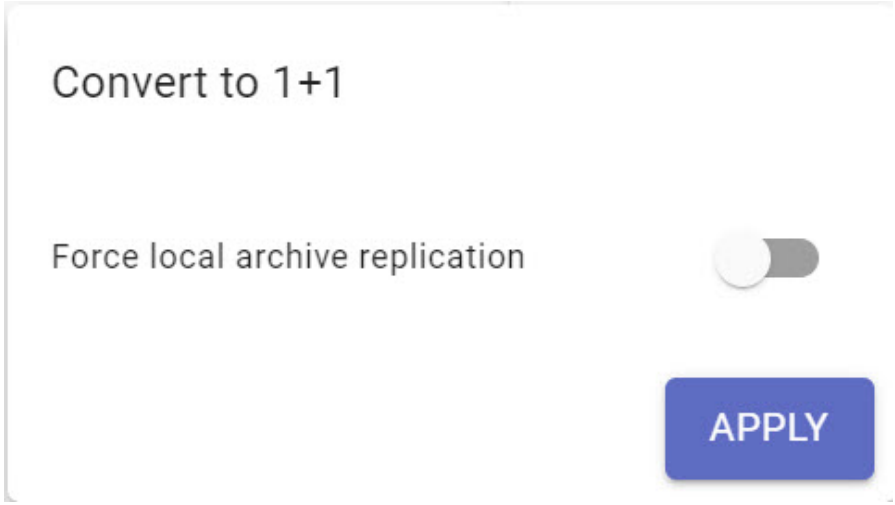
Converting to 1+1 configuration

If a cluster was initialized on one Server, do the following:

1. Add a second Server to the configuration (see Creating a cluster).
2. On the **Configuration** page, click **CONVERT TO 1+1**.



3. Activate the **Force local archive replication** parameter if you want the replication to the backup archive to be continuous regardless of the location of the master node.

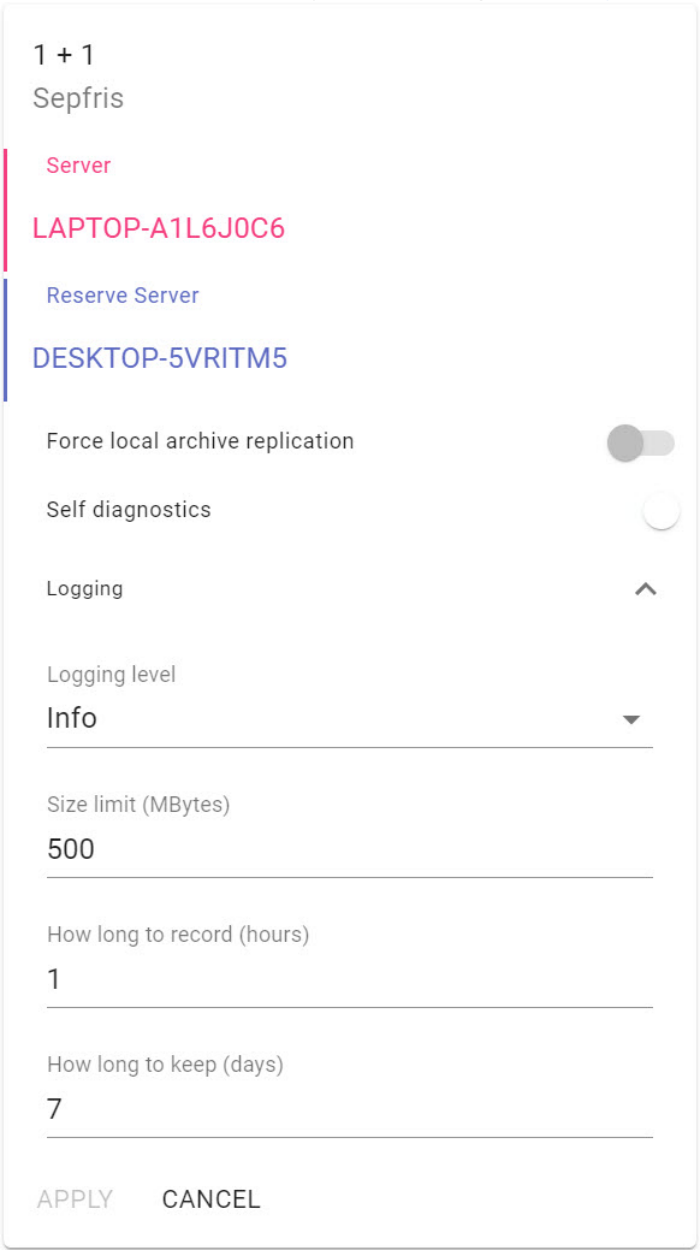


4. Click the **APPLY** button to convert to 1+1 configuration.

Editing the configuration

You can edit the configuration. To do so, click the button. You can do the following:

- activate/deactivate the self-diagnostics service (see Self-diagnostics service);



- change the logging level (see Configuring the logging levels);
- change the log archive parameters (see Configuring the Server log storage and archiving options).

Setting up archive replication

To set up archive replication, do the following:

1. Combine the master and the backup nodes into one domain (see Adding a Server to an existing domain).
2. Create a local archive on the master node (see Creating archive).
3. Add video cameras on the master node (see Searching, adding, configuring and removing IP devices).
4. Set up video camera recording to the local archive (see Configuring recording to an archive).
5. Create an archive for replication on the backup node.
6. Set up the replication from the local archive to the archive for replication (see Configuring data replication). The replication period should be set to **Always**.

> ⚠ **Attention!**
>
> Archive replication is available only with the *Axxon One* Enterprise or Unified license (see Axxon One license types).

How replication will run

When the master node is migrated to the backup Server:

- a temporary archive will be automatically created in the C:/temp_arch folder of the backup Server as a 10 GB file;
- video cameras will record into the temporary archive;
- replication from the temporary archive to the archive for replication will be simultaneous.

If the master node is migrated bask to the master Server, the recording will be made to the local archive.

You need to use different archives to view camera recordings:

- to view the recordings when the master node was on the master Server, use the local archive;
- to view the recordings when the master node was on the backup Server, use the archive for replication (see Selecting an Archive).

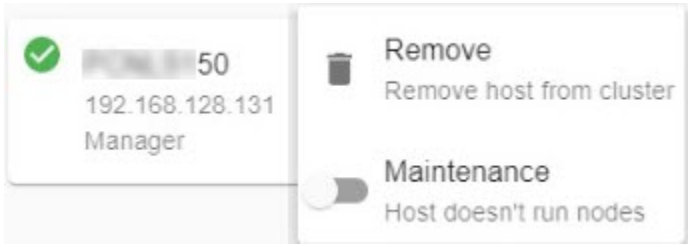
Attention!

- If the backup Server fails when the system is running, you cannot stop the master node.
- If the backup Server is unavailable, you cannot restart the master node.
- If the main node is located on the backup Server, then face recognition and license plate recognition by lists using detection tools will not be available until the main node is moved back to the master Server.

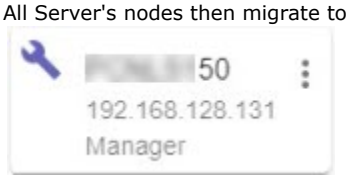
Suspending a Server within a cluster

In some cases, you may need to temporarily suspend the operation of a Server within a cluster. To do this:

1. Open the Server menu on the **Configuration** page.
2. Activate the **Maintenance** switch.



All Server's nodes then migrate to other Servers, and the status of the Server is updated.

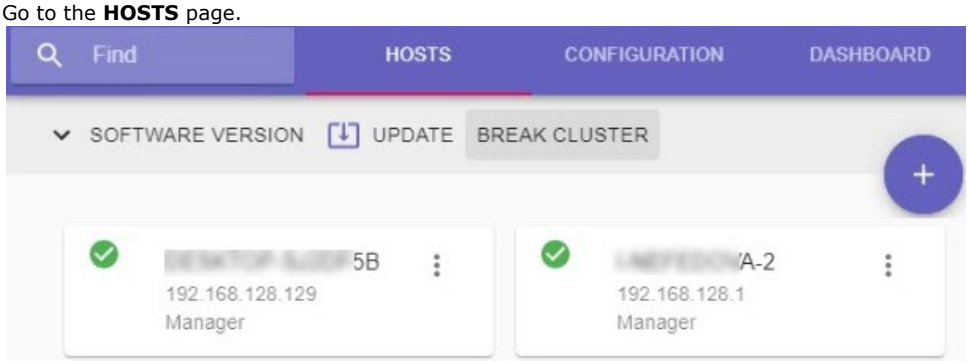


To resume the Server's operation within the cluster, toggle the Service switch to its initial position.

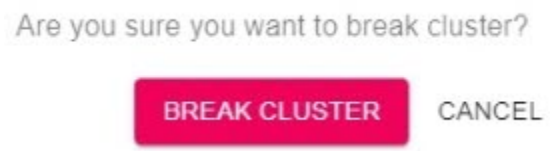
Disbanding a cluster

To disband a cluster, do the following:

1. Go to the **HOSTS** page.



2. Click the **BREAK CLUSTER** button.
3. Confirm the action.



The cluster is now disbanded.

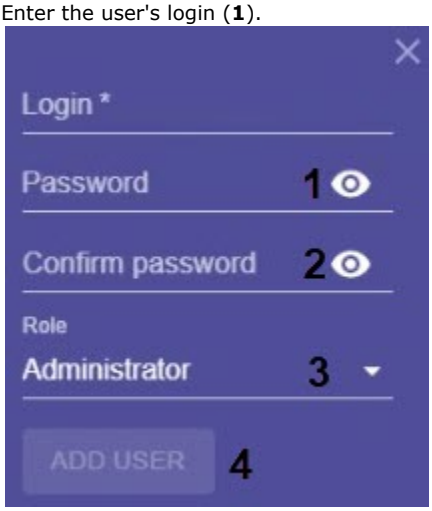
Set up access to a supervisor

When you launch the supervisor for the first time and create the cluster, you can create a user with the Administrator role (see Creating a cluster).

In the future, you can create users with two roles: Administrator or Operator. Administrators have full access to the cluster configuration while operators can only view the configuration and monitor the state of the system.

Users can created in the **USERS** tab. To create a user:

1. Click the  button.
2. Enter the user's login (**1**).

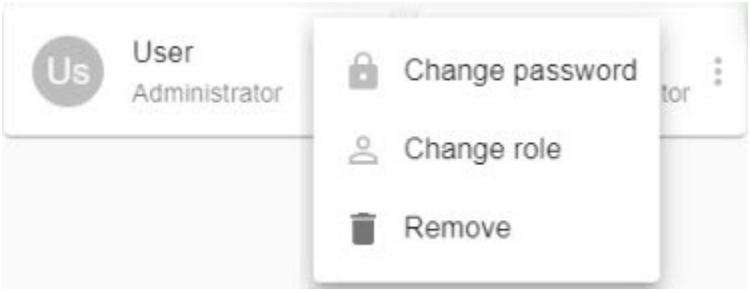


3. Enter the user's password (**2**).
4. Select the role to which the user will be added (**3**).

> **Note**
>
> The first user you create will be automatically added to the Administrator role.

5. Click the **ADD USER** button (**4**).

User creation is complete. Click to edit the user.



The following operations are allowed:

- change password,
- change role,
- delete user.

If at least one user was created, then the authentication is required when connecting to the Supervisor web interface.


Sign in
http://127.0.0.1:4000
Username
Password
Sign in
Cancel

Configuration backup and restore for failover VMS

You can back up your cluster, database, and nodes configuration and restore it.

By default, backup copies of the cluster configuration are created each 24 hours on each Manager Server. If a backup copy was created by operator's command, the next automatic backup will be performed not earlier than after 24 hours.

> **Attention!**
>
> The object trajectory DB cannot be backed up. In the event of server hardware failure, all metadata stored in the database will be lost irretrievably.

To create a backup:

1. Go to the **CONFIGURATION** tab.
2. Click the **BACK UP** button (**1**) and download the backup by clicking the button.



To restore a configuration from a backup:

Create a cluster first.

1. Go to the **CONFIGURATION** tab.
2. Click the **RESTORE** button (**2**) and select the file with the configuration backup.



3. Click the **RESTORE** button.

> **Attention!**
>
> Restoring configuration will stop all active tasks.

Configuration restore is completed.

Transferring the configuration from a common security server to a failover system

Attention!

- If you transfer the configuration, old events from the database will be lost.
- VMDA metadata will be saved as long as it is stored on a network drive.
- A failover system must have the **Enterprise** or **Unified** license type (see Types of licenses).

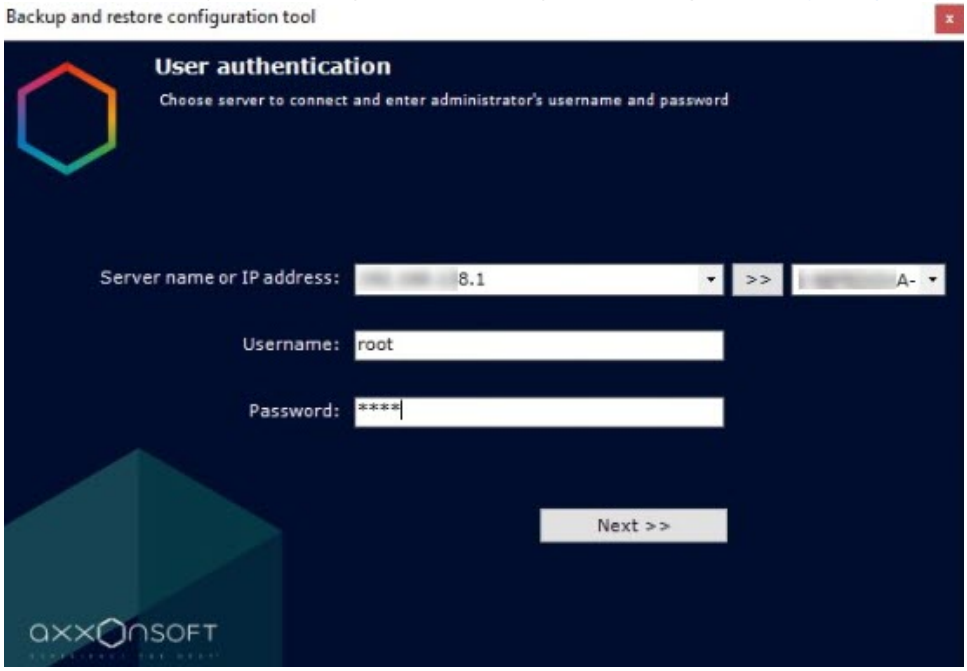
To transfer the configuration from a common security server to a failover system, do the following:

1. Create a copy of the configuration on the server (see Configuration backup).
2. Remove *Axxon One* from all Servers of the domain but keep the configuration (see Removal).
3. Install *Axxon One* on all Servers using the **Failover server and client** installation type (see Installation).
4. Initialize a cluster (see Creating a cluster) using the supervisor Web-interface (see Supervisor Web-Interface).
5. Add Servers that were used in the domain to the cluster.
6. Add nodes to the cluster.

   Note

   The names of the nodes in the cluster must match the names of the Servers that were used in the common *Axxon One* security system.

7. Connect the Client to one of the cluster nodes (see Connecting to a Node and Configuring of an Axxon domain).
8. Add nodes to the domain.
9. Connect to the configuration backup and restore utility on the node (see Starting and quitting BackupTool.exe).

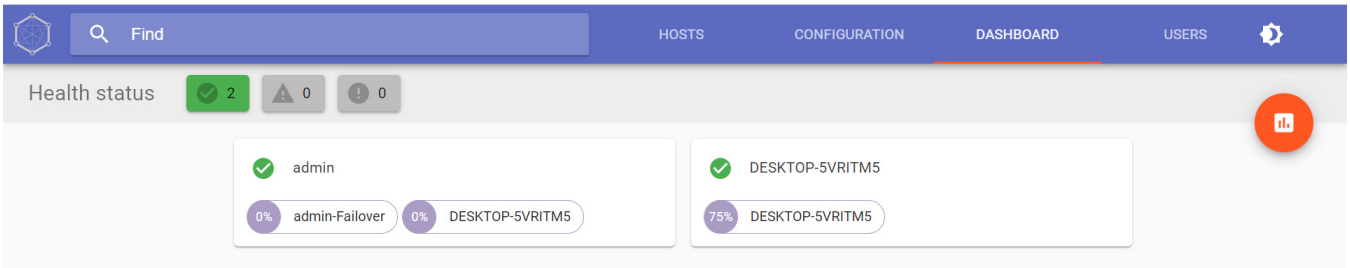


10. Restore the saved configuration (see Configuration restore).

As a result, the configuration will be transferred from a common security system to a failover system.

Monitoring the status of a cluster

You can monitor the status of a cluster on the **DASHBOARD** tab.



The following information is available:

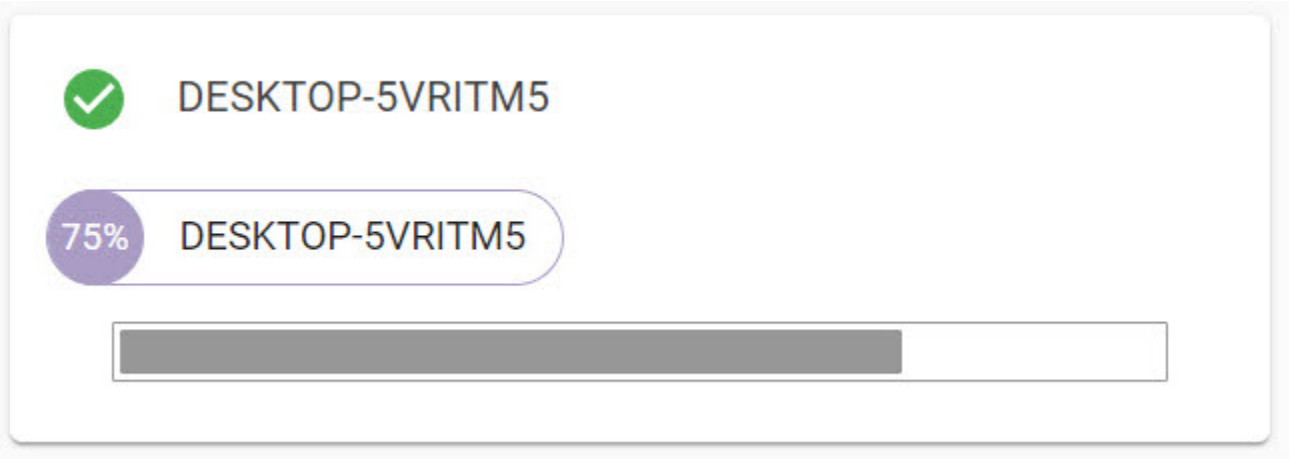
1. The status of all Servers of a cluster. All Servers of a cluster are cross-checked against a number of criteria. The status info of a server reflects the cross-check results.

Status	Description
	The server successfully passed all checks
	The server didn't pass some checks. The red stripe around the icon reflects the percentage of failed checks

2. Running nodes and the percentage of CPU resources allocated to them of the total CPU resources of the Server. For example, if a node has been allocated 9300 CPU units and the total number of CPU resources of the Server on which it is running is 12400 CPU units, the following value is displayed: (9300/12400)*100%=75%.

> **Attention!**
>
> This parameter doesn't reflect the actual CPU load of the Server by the node. The amount of the node related load can be either higher or lower than the displayed value.

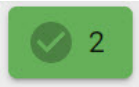
To open the diagram of allocated CPU resources, click the  button.



You can filter the Servers by their status using the **Health status** panel.

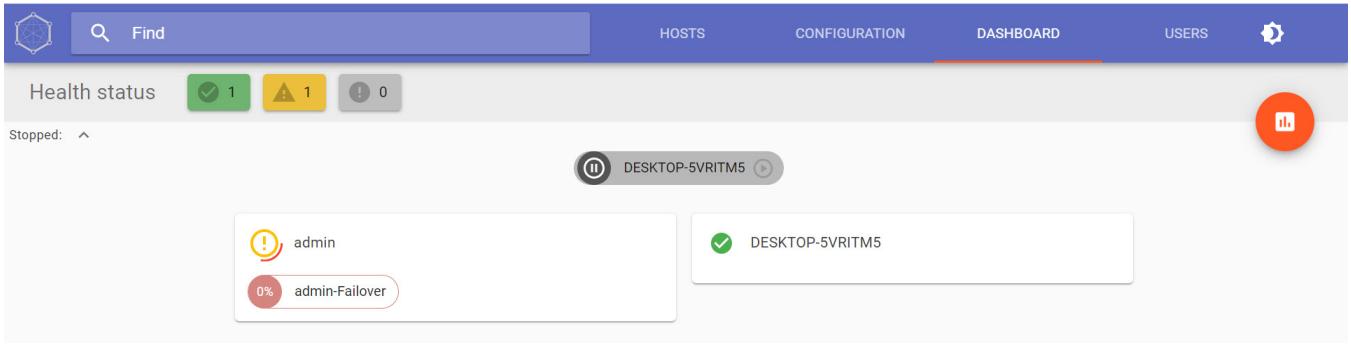


Status	Description

	Servers that passed all checks
	Servers that didn't pass some checks
	Servers that failed all checks

> **Note**
>
> The icon indicates the number of Servers of a cluster in this status.

If some nodes of the cluster have been stopped, they will be displayed on the **Stopped** tab.



To

- minimize the tab and hide the stopped nodes, click the  button;
- open the tab, click the  button.

You can start the stopped nodes by clicking the  button.

Connecting to a Node and Configuring of an Axxon domain

When the cluster is configured, it is necessary to connect the client to the node. To do this:

1. Start the Client (see Starting the Axxon One Client).



2. Enter the IP address of any cluster server (**1**) and click the >> button.
3. Select from the list the node you want to connect to (**2**). Enter the first characters of the node name into this field, and the fast search starts.
4. Enter the username and password (**3**) and click the **Connect** button (**4**).

During the first connection to the node, you will be prompted to create an Axxon domain (see Creating a new domain).

You can then merge nodes into a unified logical structure following standard procedures of Axxon domain configuration (see Configuring domains).

Attention!

An Axxon domain cannot include nodes from different clusters.

If necessary, you can switch the domain operating mode to a cluster domain. To do this, create a system variable NGP_ENABLE_CLUSTER_DOMAIN (see Appendix 9. Creating system variable) and specify the value: 1—enable the cluster domain mode, 0—disable it.

Attention!

- This variable must be created on each Server in the cluster where domain nodes will be running.
- When the NGP_ENABLE_CLUSTER_DOMAIN variable is enabled, the nodes will belong to the domain in which they were created.

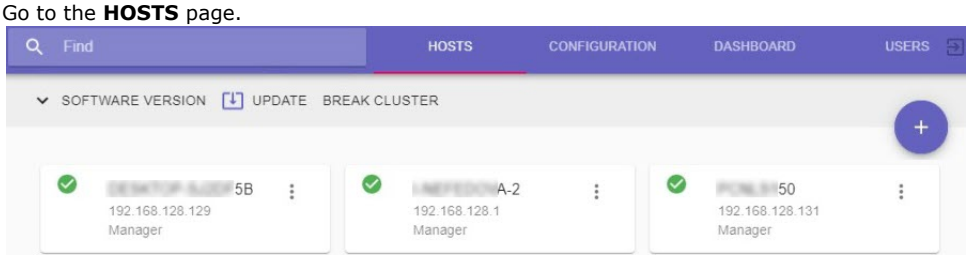
Configuring automatic connection to nodes

You can configure the connection to a node of the FailOver system through any Server of the FailOver system cluster. You can add a node to autoloading similarly to adding a regular Server (see Automatic connection).

Updating Servers within a cluster

To update all Servers within a cluster, do the following:

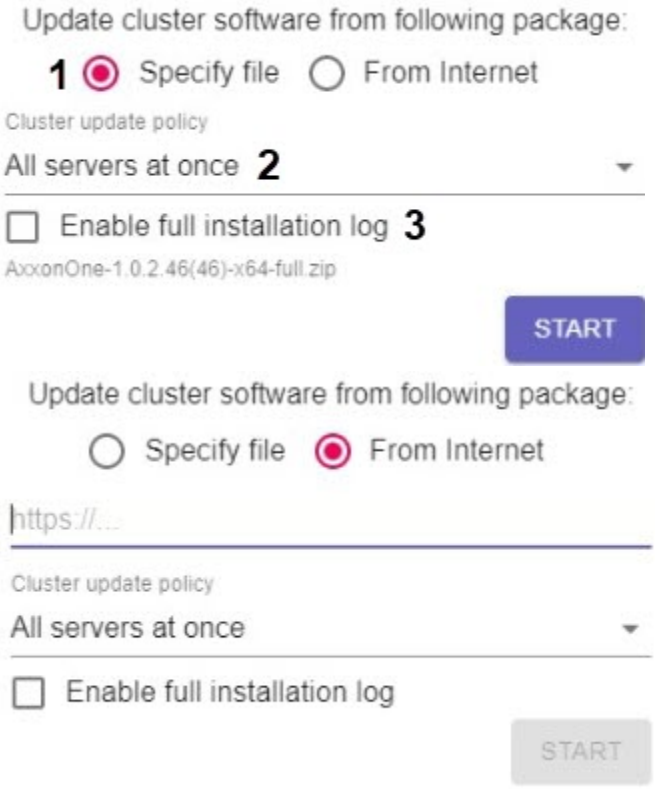
1. Back up the configuration (see Configuration backup and restore for failover VMS).
2. Go to the **HOSTS** page.



3. Click **UPDATE**.

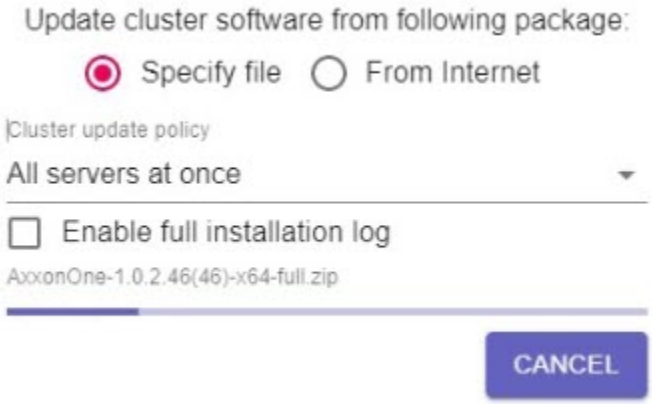
> **Attention!**
>
> You can bulk update the entire cluster only if all of its servers are accessible.

4. On your computer, select the required distribution in zip archive, or specify a web link (**1**).

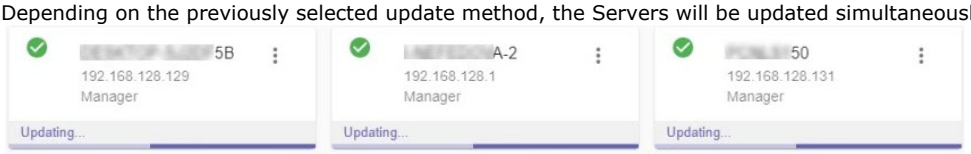


5. Select the update method: all Servers simultaneously, or one after another (**2**). In the former case, all nodes operation will be halted until the update is finished, in the latter case the nodes will operate without interruption.
6. To record all installation-related events to a log file (**3**), select the **Enable full installation log** checkbox.
7. Click **START**.

The installation package download starts. You can cancel the update unless the download is complete.



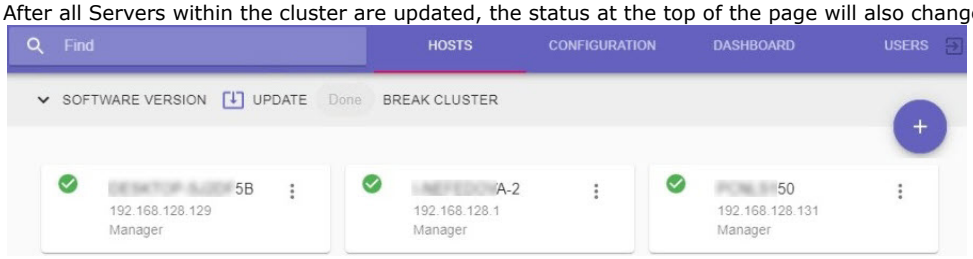
8. After the installation package is downloaded, *Axxon One* will be updated in quiet mode on all Servers within the cluster. Depending on the previously selected update method, the Servers will be updated simultaneously or one after another.



After the update is completed on a Server, its status will change to **Done**.

> **Note**
>
> If the update fails, you will see the **Error** message in the status bar.

After all Servers within the cluster are updated, the status at the top of the page will also change.



Setting network interfaces for system nodes operation

By default, the Failover system nodes use all available network interfaces.

To limit the number of the used network interfaces, do the following:

1. Add the following parameter to the C:\Program Files\AxxonSoft\Axxon One\bin\raft\raft-settings.xml file:

   ```
   <item key="NGP_IFACE_WHITELIST">172.17.0.0/16</item>
   ```

   Use the following interfaces setting format: "IP-address1/number of unit bits in the mask, IP-address2/number of unit bits in the mask".

By default, the stale mode is activated to reduce the network traffic and the load on the CPU. In this mode, any Server in the Failover system can process queries, regardless of whether it is the master Server.

To disable the stale mode, do the following:

1. Change the value of the following parameter to 0 in the C:\Program Files\AxxonSoft\Axxon One\bin\raft\raft-settings.xml file:

   ```
   <item key="SVISOR_CONSUL_STALE_MODE_THRESHOLD_MS">0</item>
   ```

To activate the stale mode, change the value of the parameter to 200 in the file.

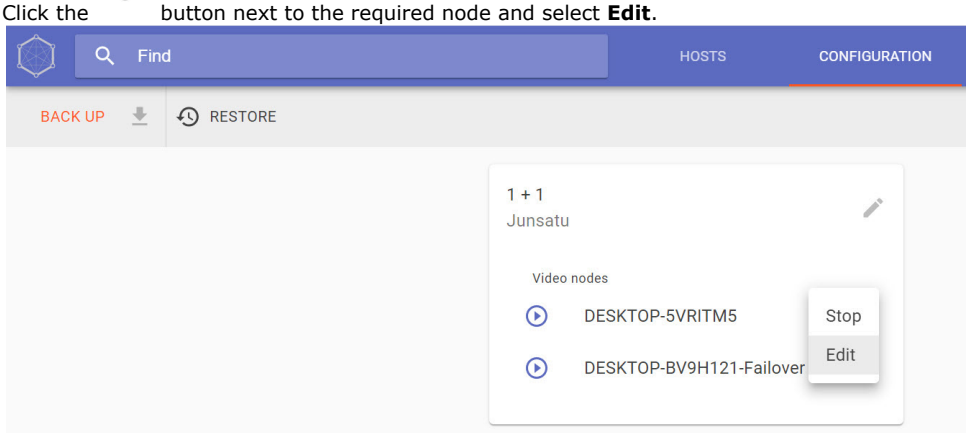
> **Note**
>
> Effective work in the stale mode is performed in the clusters with a large number of added Servers.

Changing ports in the nodes of the failover system

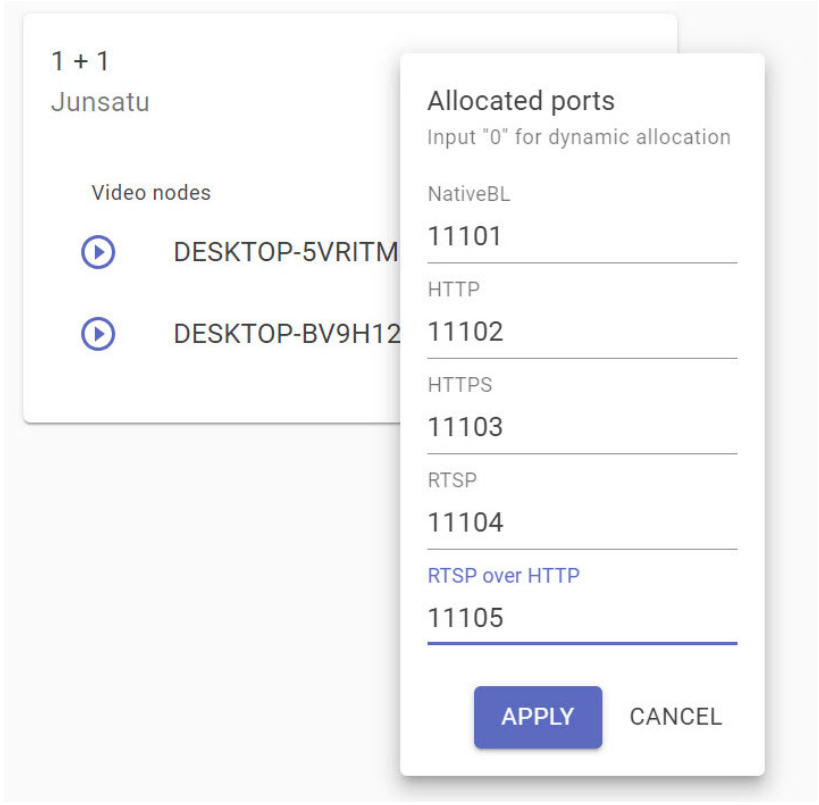
By default, nodes in the cluster are assigned dynamic ports. If necessary, you can explicitly specify ports for NativeBL, Web-Server, and so on. You can configure ports individually for each node in the cluster.

To change the ports in a node, do the following:

1. Go to the **CONFIGURATION** tab.
2. Click the button next to the required node and select **Edit**.



3. In the **Allocated ports** window, specify an unused port. You can change all ports, a few ports, or any specific port.



4. Click the **APPLY** button.

As a result, the node will automatically restart and operate on the specified ports.

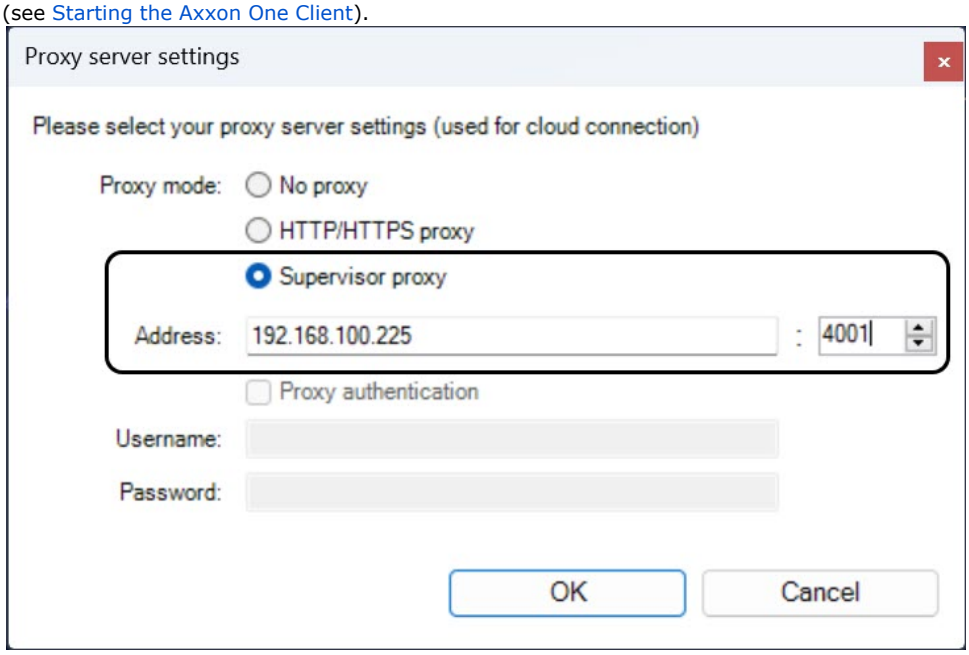
The allocated ports in the node must not be the same as the ports specified in Ports used by the failover system.

If you want to return the dynamic port allocation, enter the **0** value.

Connecting the Client to the Failover Server behind NAT

To connect the Client to the Failover Server behind NAT, do the following:

1. Create a cluster and add Servers to it (see Creating a cluster).
2. On one of the cluster Servers, via which the Client will connect to the Failover Server behind NAT, in the C:\Program Files\AxxonSoft\Axxon One\bin\raft-settings.xml file, specify the port value for the SVISOR_GRPC_PROXY_PORT parameter. For example, specify port 4001 (see Ports used by the Axxon One Software Package).
3. Forward ports 4000 and 4001 to the internal IP address of the Server specified in step 2.
4. Start the Client and in the proxy server settings, specify the Server external IP address and the forwarded port from step 2 (see Starting the Axxon One Client).



5. Enter the external IP address of the cluster Server (**1**) and click the >> button.



6. From the list (**2**), select the node you want to connect to. To quickly find the node, you can enter the first characters of its name in this field.
7. Enter the username and password (**3**) and click the **Connect** button (**4**).

Attention!

If the connection to the Server to which the ports are forwarded fails, the connection to the cluster nodes behind NAT becomes unavailable. If necessary, configure the network infrastructure so that a proxy server is configured for multiple cluster Servers. This will provide fault tolerance and the ability to connect to the cluster even if one of the Servers becomes unavailable.

Changing logging levels for the Consul and Nomad processes in a failover system

On the page:

- Changing the logging level for Consul
- Changing the logging level for Nomad

By default, the logging level for the Consul and Nomad processes is set as Info (see Configuring the logging levels). If you want to log debugging events, you must change the logging level for the Consul and Nomad processes to Debug.

Changing the logging level for Consul

To change the logging level for the Consul process, do the following:

1. Open the file in a text editor:
   - **Windows OS**: C:/ProgramData/AxxonSoft/Axxon One/RaFT/cluster/consul/config/main.json.
   - **Linux OS**: /opt/AxxonSoft/RaFT/data/cluster/consul/config/main.json.
2. Change the value of the log_level parameter to DEBUG.

   ```
   "log_level": "DEBUG"
   ```

3. Save the file:
   - **Windows OS**: C:/ProgramData/AxxonSoft/Axxon One/RaFT/cluster/consul/config/main.json.
   - **Linux OS**: /opt/AxxonSoft/RaFT/data/cluster/consul/config/main.json.
4. Run command prompt as administrator and go to the folder:
   - **Windows OS**: C:/Program Files/RaftLauncher/current/.
   - **Linux OS**: /opt/AxxonSoft/RaFT/bin/.
5. Execute the command to restart the process and change the logging level:
   - **Windows OS**:

     ```
     consul.exe reload
     ```

   - **Linux OS**:

     ```
     consul reload
     ```

Changing the logging level for Nomad

To change the logging level for the Nomad process, do the following:

1. Open the file in a text editor:
   - **Windows OS**: C:/ProgramData/AxxonSoft/Axxon One/RaFT/cluster/nomad/config/misc.json.
   - **Linux OS**: /opt/AxxonSoft/RaFT/data/cluster/nomad/config/misc.json.
2. Change the value of the log_level parameter to DEBUG.

   ```
   "log_level": "DEBUG"
   ```

3. Save the file:
   - **Windows OS**: C:/ProgramData/AxxonSoft/Axxon One/RaFT/cluster/nomad/config/misc.json.
   - **Linux OS**: /opt/AxxonSoft/RaFT/data/cluster/nomad/config/misc.json.
4. Run command prompt as administrator and go to the folder:
   - **Windows OS**: C:/Program Files/RaftLauncher/current/.
   - **Linux OS**: /opt/AxxonSoft/RaFT/bin/.
5. Execute the command to restart the process and change the logging level:
   - **Windows OS**:

```
nomad.exe reload
```

- **Linux OS**:

```
nomad reload
```

As a result, the process will restart and from the moment it restarts, the detailing in the logs will increase because the logging level will change to Debug.

Self-diagnostics service

General information about the self-diagnostics service

The self-diagnostics service collects the information about the system metrics and checks the operation of all *Axxon One* components. The data obtained are compared with the indicators of the normal operation of the system. When deviations occur, system health alerts are generated, which can be tracked in the web interface (see Viewing metrics in the self-diagnostics service).

Examples of errors that are tracked:

- Out of RAM.
- Camera is connected but does not send data.
- No events from a detection tool.
- Archive doesn't work.
- The frame rate is 0 when recording to the archive.
- No video is recorded on detection.
- Any internal errors of *Axxon One*.
- Out of system disk space.

The self-diagnostics service has the following rules for cleaning the system disk:

Free memory remaining	Cleanup mechanism
< 20 GB	All server logs, including the archived logs, are deleted from the system disk
< 15 GB	All events older than one week are deleted
< 10 GB	All events older than one day are deleted
< 5 GB	All events older than one hour are deleted
< 3 GB	All events are deleted

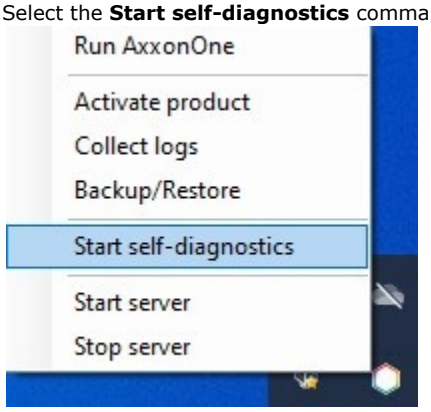
Starting and stopping the self-diagnostics service

Note

The *Axxon One* self-diagnostics service is running by default.

To launch the self-diagnostics service, complete one of the following two actions:

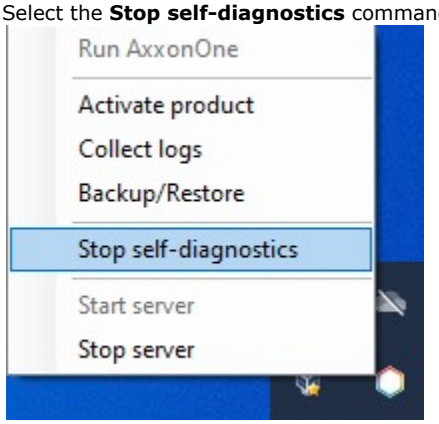
1. Select the **Start self-diagnostics** command in the Axxon One Tray Tool utility.



2. Launch the NGP_Self_Diagnostics.

To stop the self-diagnostics service, complete one of the following actions:

1. Select the **Stop self-diagnostics** command in the Axxon One Tray Tool utility.



2. Stop the NGP_Self_Diagnostics.

Note

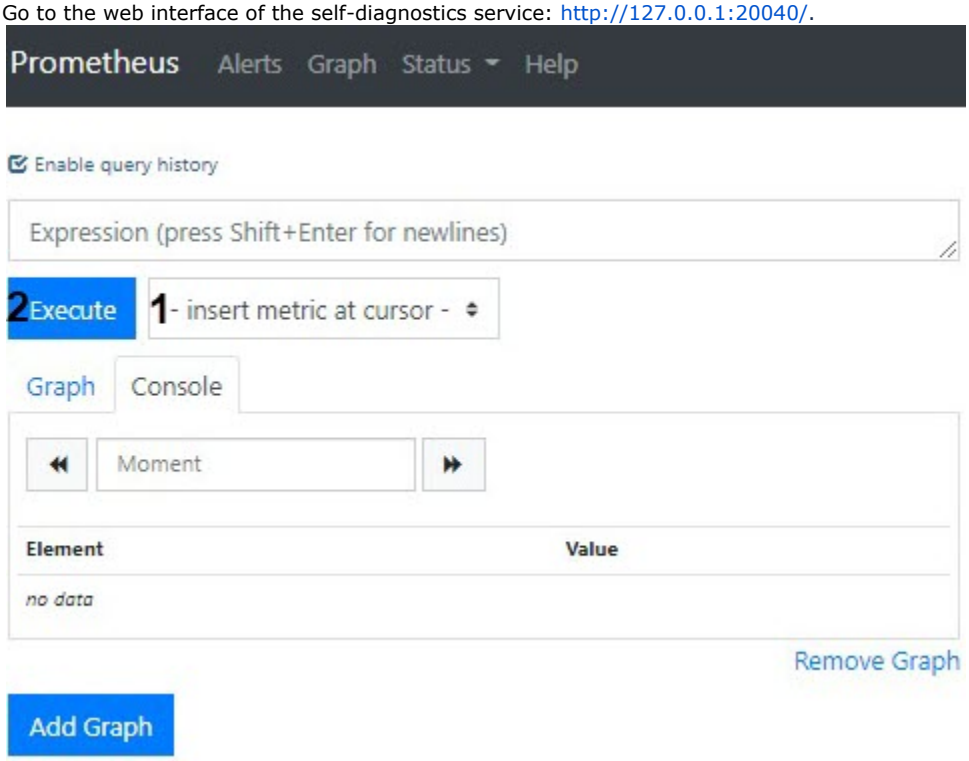
In a failover system, the self-diagnostics service is activated/de-activated in cluster settings (see Configure a Failover System Cluster).

Starting and stopping the Axxon One self-diagnostics service in Linux OS

Viewing metrics in the self-diagnostics service

To view the system status data, do the following:

1. Go to the web interface of the self-diagnostics service: http://127.0.0.1:20040/.



2. Select the required metric in the list (**1**) or enter the query in the **Expression** field.

Metric	Description
ALERTS_FOR_STATE	Troubleshooting by the self-diagnostics service. **Example** `ALERTS_FOR_STATE{alertname="ipint_is_not_activated",ep_name="hosts/Server1/DeviceIpint.99",instance="127.0.0.1:20108",job="ngp_exporter",ngp_alert="true"}` Possible values of the alertname parameter (see General information about the self-diagnostics service): • **low_os_memory** — out of RAM; • **ipint_is_not_activated** — camera is connected but does not send data; • **no_samples_in_detector** — no events from a detection tool; • **restart_services_when_archive_source_not_activated** — the archive is not working; • **restart_services_when_no_samples_in_archive** — recording to archive with 0 FPS; • **restart_services_when_no_ping_from_detector_to_archive** — no recording to the archive on detection tool triggering; • **logs_disk_space_is_low/db_disk_space_is_low** — out of system disk space.
ngp_archive_channel_fps	The frame rate of all video cameras recording to archive.
ngp_cpu_total_usage	The percentage of CPU load on a Server.
ngp_fps	The frame rate of all Server video cameras, all detection tools and their decoders.

The request allows for:

a. Using multiple metrics.
b. Using expressions to find problems. For example, a query like ngp_fps <17 will return all metrics, where FPS was less than 17. For a complete list of logical and arithmetic operators, see the official Prometheus documentation.

c. Filtering by any of the parameters. For example, a query like

```
ngp_fps{ep_name=~"hosts/TEST/DeviceIpint.2/SourceEndpoint.video:0:0"}
```

will return FPS values only for the specified source.

Examples of useful queries for Windows OS:
The CPU loading graph similar to the Windows System monitor:

```
sum by (process_id) (100 / scalar(wmi_cs_logical_processors) * (irate(wmi_process_cpu_time_total
{process="AppHost"}[10m]))) or ngp_cpu_total_usage
```

The graph of RAM usage by the AppHost processes and a total memory space:

```
sum by (process_id) (avg_over_time(wmi_process_working_set{process="AppHost"}[5m])) / 1024 or
avg_over_time(wmi_os_virtual_memory_bytes[5m]) / 1024
```

The percentage of RAM usage:

```
100.0 - 100 * avg_over_time(wmi_os_virtual_memory_free_bytes[5m]) / avg_over_time
(wmi_os_virtual_memory_bytes[5m])
```

Examples of useful queries for Linux OS:
The graph of total RAM usage by the AppHost processes:

```
sum by (groupname) (namedprocess_namegroup_memory_bytes{memtype="resident"})
```

The percentage of RAM usage:

```
100 - node_memory_MemAvailable_bytes * 100 / node_memory_MemTotal_bytes
```

The graph of the CPU load by the AppHost processes as a percentage:

```
sum by (object_id) (rate(namedprocess_namegroup_cpu_seconds_total{groupname="AppHost"}[1m])) * 100
```

The graph of the CPU load as a percentage:

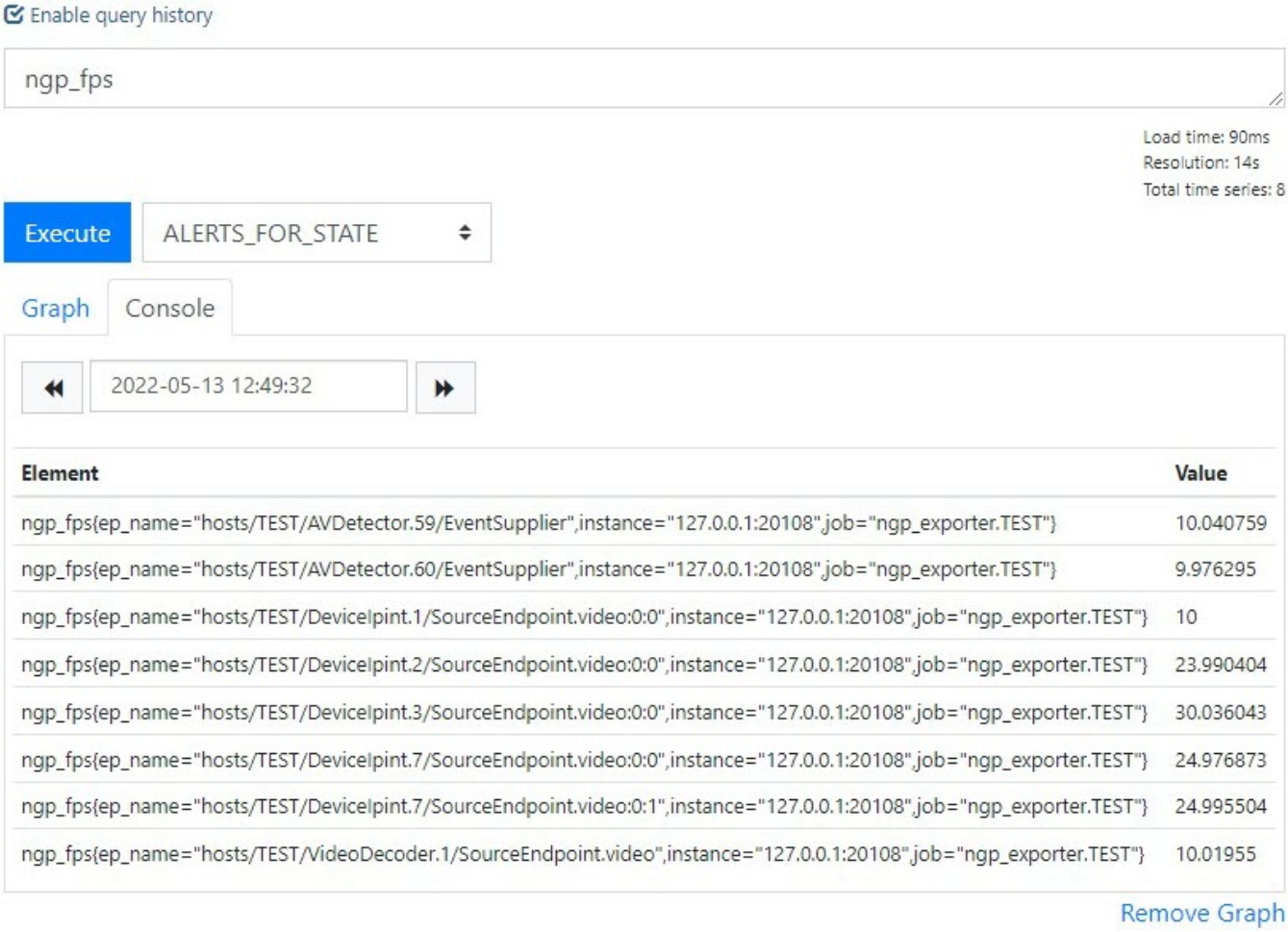
```
100 * avg without (cpu) (1 - rate(node_cpu_seconds_total{mode="idle"}[1m]))
```

The graph of RAM usage by the AppHost processes to determine the memory leak:

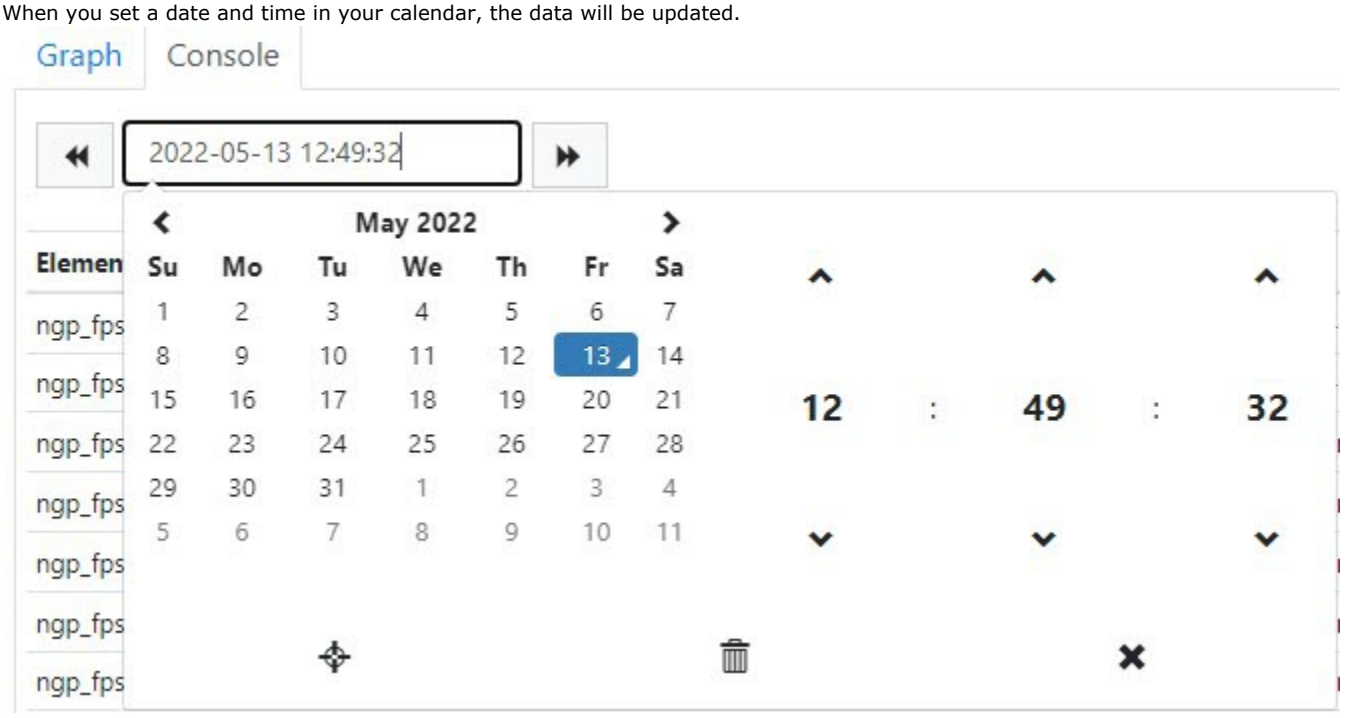
```
namedprocess_namegroup_memory_bytes{object_id=~"APP_HOST.*",memtype="proportionalResident"}
```

3. Click the **Execute** button (**2**).

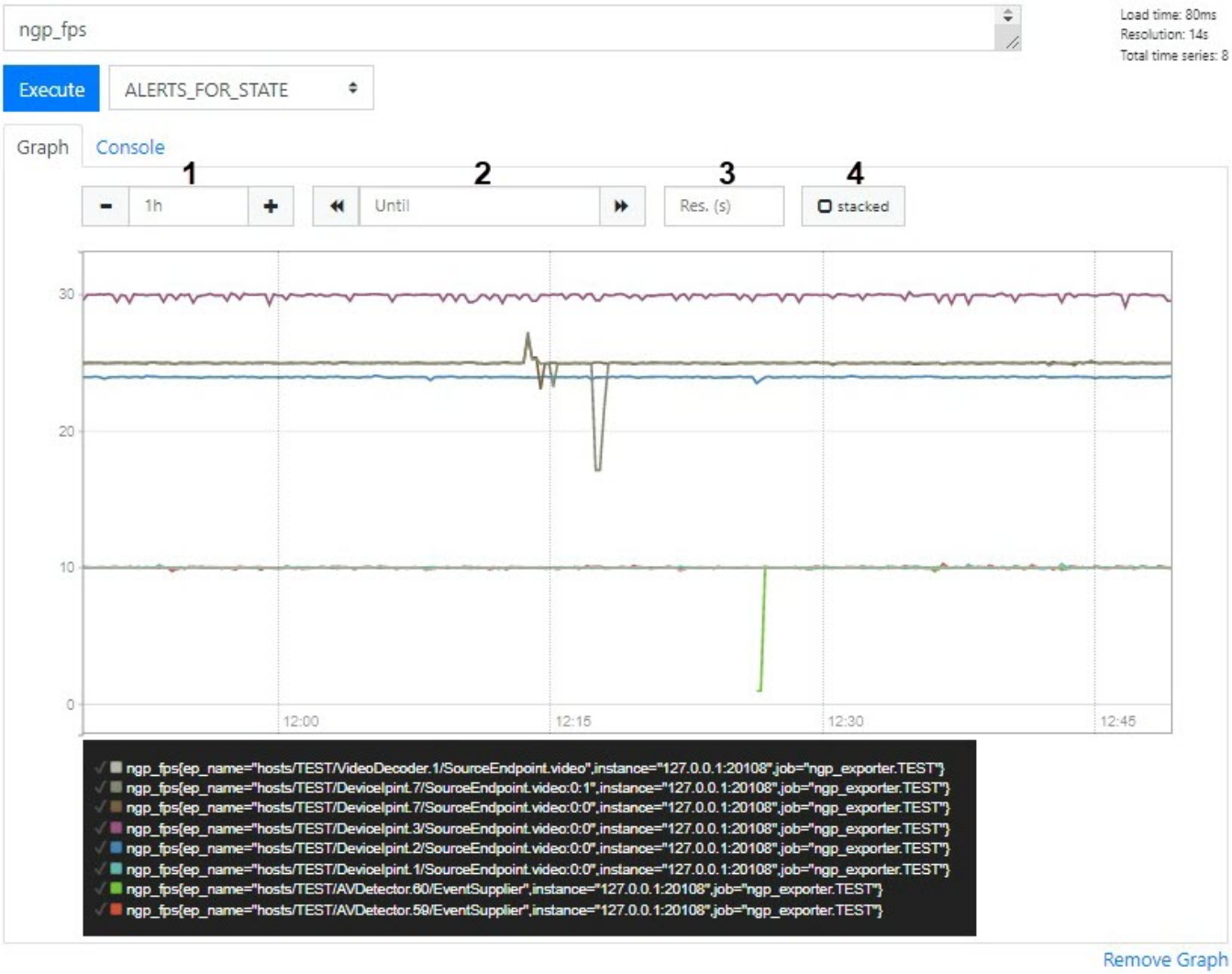
The **Console** tab will display all possible values of all elements at the time the query is completed.



When you set a date and time in your calendar, the data will be updated.



To build a graph, go to the **Graph** tab. In the field **1**, set the time interval of the graph. In the field **2**, set its end point. In the filed **3**, set the interval between the data points. To fill the chart, set the **stacked** (**4**) checkbox.



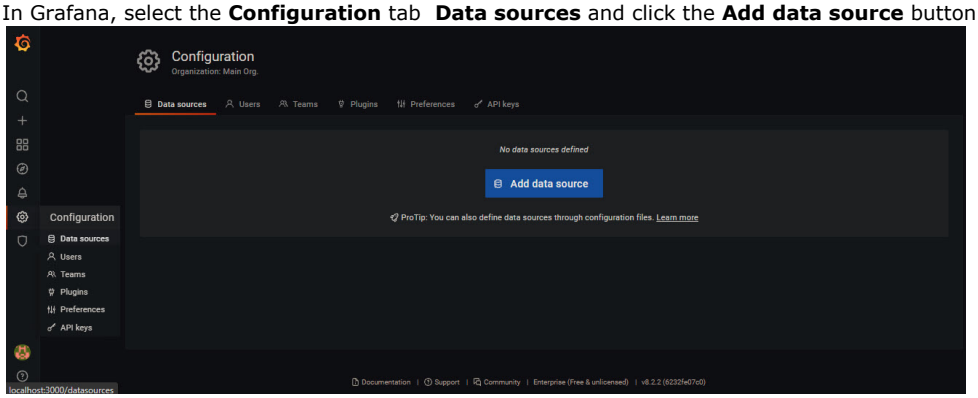
Viewing self-diagnostics metrics using third-party Grafana | Prometheus software

> **Attention!**
>
> AxxonSoft isn’t a developer and doesn’t provide technical support for Grafana | Prometheus software.

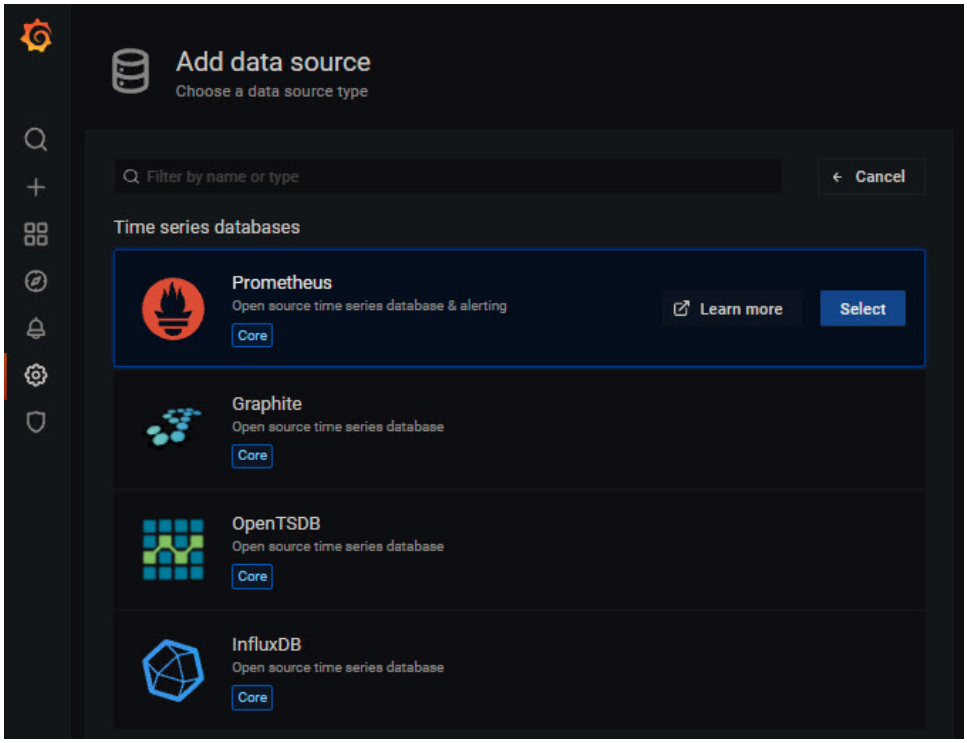
To view the self-diagnostics metrics using third-party Grafana | Prometheus software, do the following:

1. Download and install Grafana.
2. Go to the web interface of Grafana self-diagnostics service: http://localhost:3000.
3. Add Prometheus as a data source in Grafana:

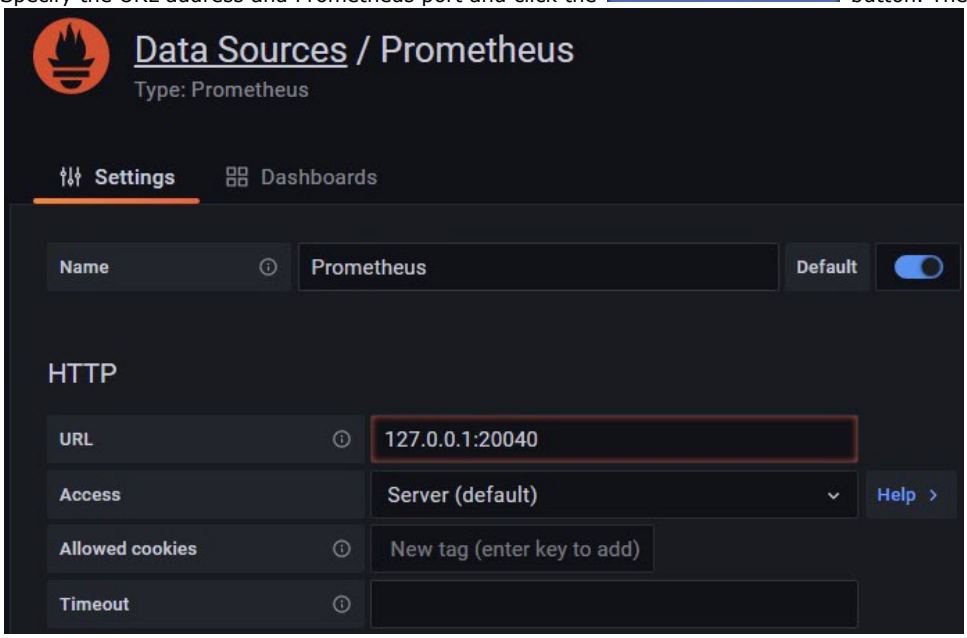
   a. In Grafana, select the **Configuration** tab **Data sources** and click the **Add data source** button.



   b. Select **Prometheus** and click the **Select** button.



c. Specify the URL address and Prometheus port and click the Save & test button. The default is port 20040.

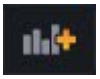


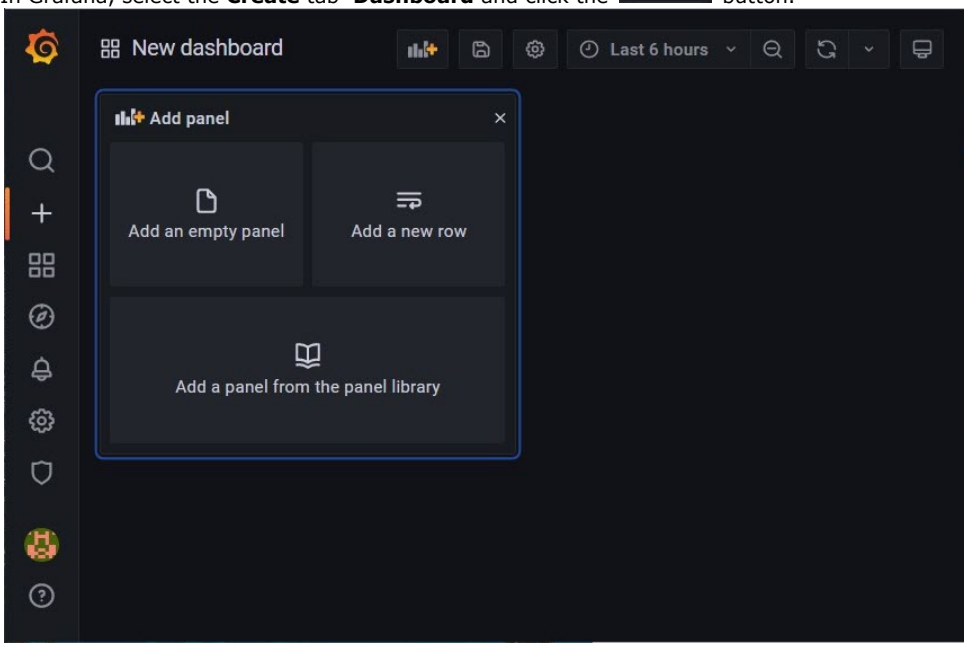
When Prometheus is successfully added to Grafana, the following window will be displayed:



4. Configure the display of dashboards in Grafana.

> Querying Prometheus

a. In Grafana, select the **Create** tab **Dashboard** and click the  button.



b. Configure the dashboards to display the necessary information (see documentation).

After configuring dashboards in Grafana, you will be able to view the self-diagnostics metrics.

Working with Axxon One

Main Elements of the User Interface

Surveillance window

Surveillance window is used to display video stream on the monitor of a computer with specific parameters for the purpose of video surveillance, archive viewing, and forensic search in archives. The surveillance window also has a function which allows the generation and evaluation of alarm events in the process of video monitoring of a guarded location.

The surveillance window has flexible display options (see Configuring the display of the surveillance window):

1. Control buttons over the video image, mode selector buttons inside the window.



2. Control buttons over the video, selector buttons outside.



3. Control buttons outside the video, selector buttons inside.



4. Control buttons and selector buttons outside the video image.



There are two states of a surveillance window within the layout: active or inactive.

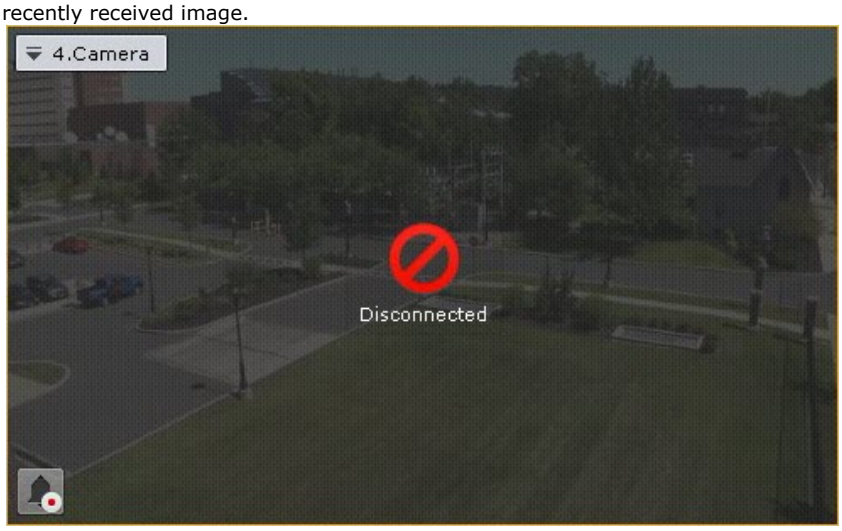
A window in active state includes an additional navigation panel (see Advanced Archive Navigation Panel) and video mode selection tabs (see Video Surveillance Mode Selection Tabs).

To switch a window to active state, click anywhere inside the window; clicking outside de-activates it.



A more detailed description of the functions of the surveillance window can be found in Video Surveillance.

If the connection to the camera is lost, the surveillance window is darkened and you get a corresponding message on the most recently received image.



To copy the camera name to the Clipboard, right-click on it 

.

Color Coding of Frames

Color coding of the frame of a viewing tile is used to indicate the status of the video camera.

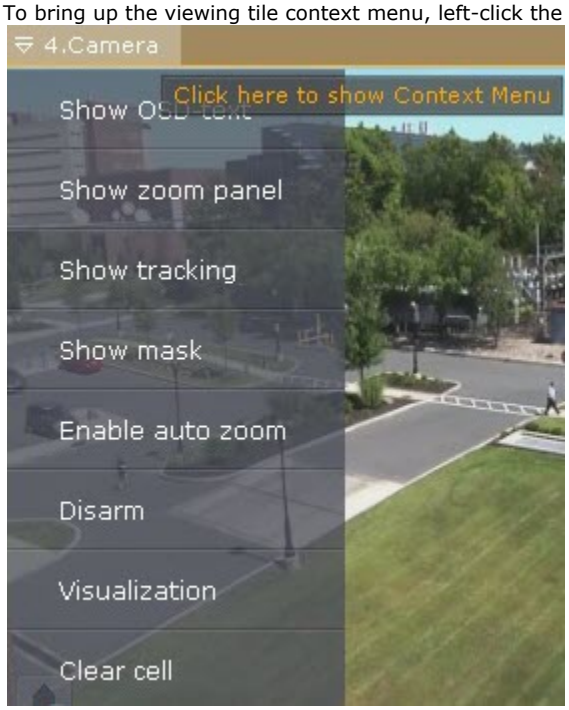
Color of viewing tile frame	Camera status
Red	Active alarm
No active camera alarms	
Green	Camera disarmed
Dark-gray	Camera armed
Blue	Archive mode

Viewing Tile Context Menu

The viewing tile context menu is used to access the following functions (depending on the enabled surveillance mode):

1. Video surveillance.
2. Audio monitoring.
3. Exporting frames and recordings.
4. Object tracking.

To bring up the viewing tile context menu, left-click the video camera icon in the upper left-hand corner of the tile.

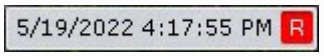


Time Display

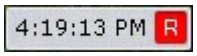
The time display appears in the upper right-hand corner of the viewing tile.



Note

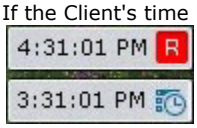
Depending on the settings (see Configuring time display), the indicator may show the date 

.

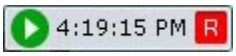
Current time of Client is displayed on the indicator in real-time mode: 

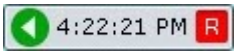
.

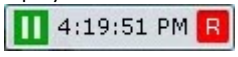
If the Client's time is different from the Server time, the Server time will also be displayed below the indicator.



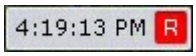
In archive, alarm, and video frame search modes, it shows the time of the fragment being viewed and the playback mode:

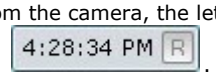
1. Forward playback 

.
2. Reverse playback 

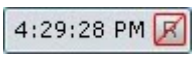
.
3. Pause 

.

If the video is currently being recorded from the camera, the letter **R** is displayed in red to the right of the clock: 

. O therwise, the letter **R** is displayed in gray: 

.

If the camera is not linked to the archive, the letter **R** is crossed out: 

.

Display of Video Statistics

You can display video statistics in the viewing tile (see the section titled Configuring display of video statistics). In real-time mode the video display statistics are shown. In Alarm, Archive, and Clip Search modes, it shows the time of the fragment being viewed and the playback mode:



Video statistic	Parameter description
Client-side FPS	Frame rate of the displayed video stream.
Server-side FPS	Frame rate of the video stream received from a video camera or an archive.
Bitrate	Bitrate of a compressed video stream.
Frame size	Resolution of the displayed video stream.

Note

The video stream parameters are updated every 10 seconds.

Video Surveillance Mode Selection Tabs

To select the video surveillance mode, use the tabs in the lower right-hand part of the viewing tile:



Alarm Management mode is activated when an alarm is triggered (see Initiating an alarm event).

Advanced Archive Navigation Panel

The advanced Archive Navigation Panel is displayed in the lower portion of the screen in **Archive** or **Archive Search** modes.



When you click a live camera tile, the advanced Navigation Panel shows only the timeline and the Archive selection button.



> **Note**
>
> If the camera is not linked to a video Archive, the panel will be unavailable.

In Live Video mode, if you click the timeline, you go to Archive mode.

The advanced Archive Navigation Panel includes the following components:

1. Timeline.
2. Playback control buttons.
3. Archive selection button.
4. Tabs for compressed and standard Archive playback modes.

Tracks are marked in different colors depending on the archive status:



Condition	Track color
Archive absent (**1**)	Black

Archive present (**2**)	White
Archive present, input or detection tool activated (no alarm) (**3**)	Blue
Archive present, alarm active (**4**)	Red

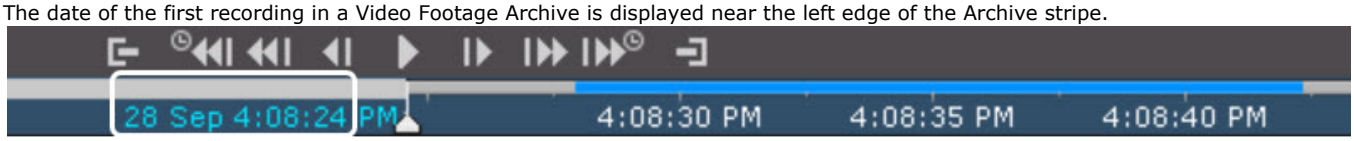
Additionally, the timeline on the advanced Archive Navigation Panel features missing footage tags  . A tag is displayed when footage is missing for over 40% of the currently visible part of the timeline. Depending on the duration of the missing footage, tags may have different thickness:

1.  – less than one hour.
2.  – from 1 to 24 hours.
3.  – more than 24 hours.

The duration of missing footage is indicated near the tag.



The date of the first recording in a Video Footage Archive is displayed near the left edge of the Archive stripe.



Note

In this case, the Archive period to the left of the marker  means that the camera was not linked to the Archive.

The playback control buttons on the advanced Navigation Panel are the same as the buttons on the Playback Panel (see The Playback Panel). The advanced Archive Navigation Panel also has the buttons to jump forward and back by **N** seconds:  and  .

N – is a step value, 30 sec by default. If you press Ctrl +  once, you increase the jump step by 30 sec, if you hit Ctrl +  – you cut the jump step by 30 sec. The maximum step value is – 300 seconds.

The advanced Archive Navigation Panel is used to position the Archive at a specific time, control playback, and switch to compressed Archive playback mode.

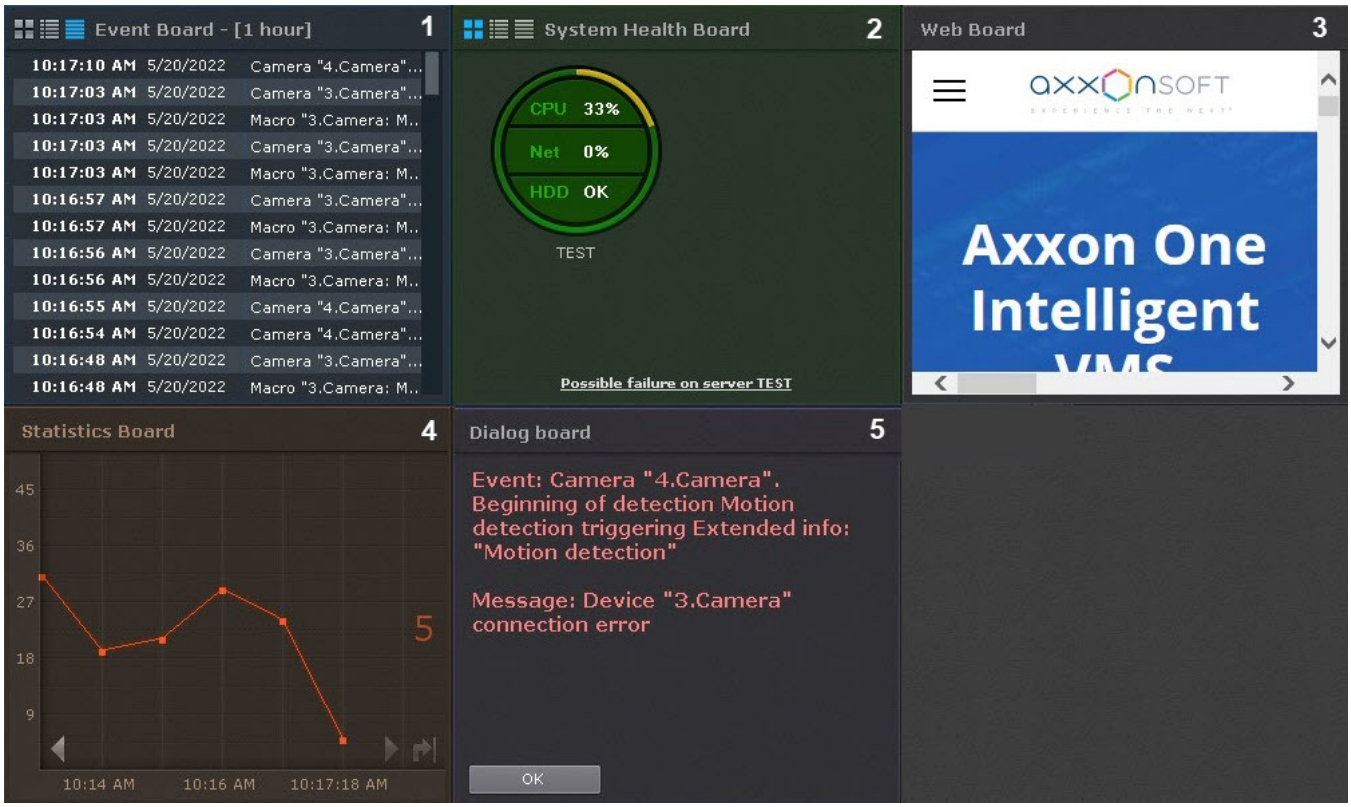
The advanced Archive Navigation Panel works completely in sync with the Playback Panel and the timeline:

1. The playback mode selected on the advanced Navigation Panel is displayed on the Playback Panel.
2. The playback speed that is set on the Playback Panel will be used as the playback speed when playback is restarted on the advanced Navigation Panel, and vice versa.
3. Any movement through the main timeline is duplicated onto the timeline of the advanced Navigation Panel.

Information boards

Information boards offer a quick view of system status and events. There are five kinds of information boards, each displaying a specific type of information:

1. Event Board (**1**).
2. System Health Board (**2**).
3. Web Board (**3**).
4. Statistics Board (**4**).
5. Dialog board (**5**).

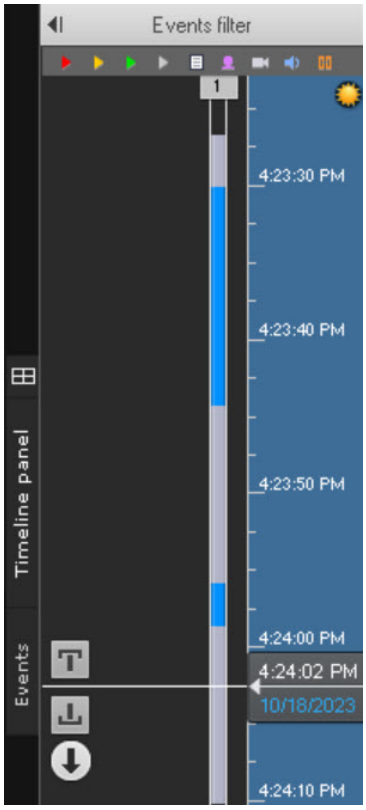


To learn about information boards, consult the relevant section.

The Archive Navigation Panel

Show and Hide the Archive Navigation Panel

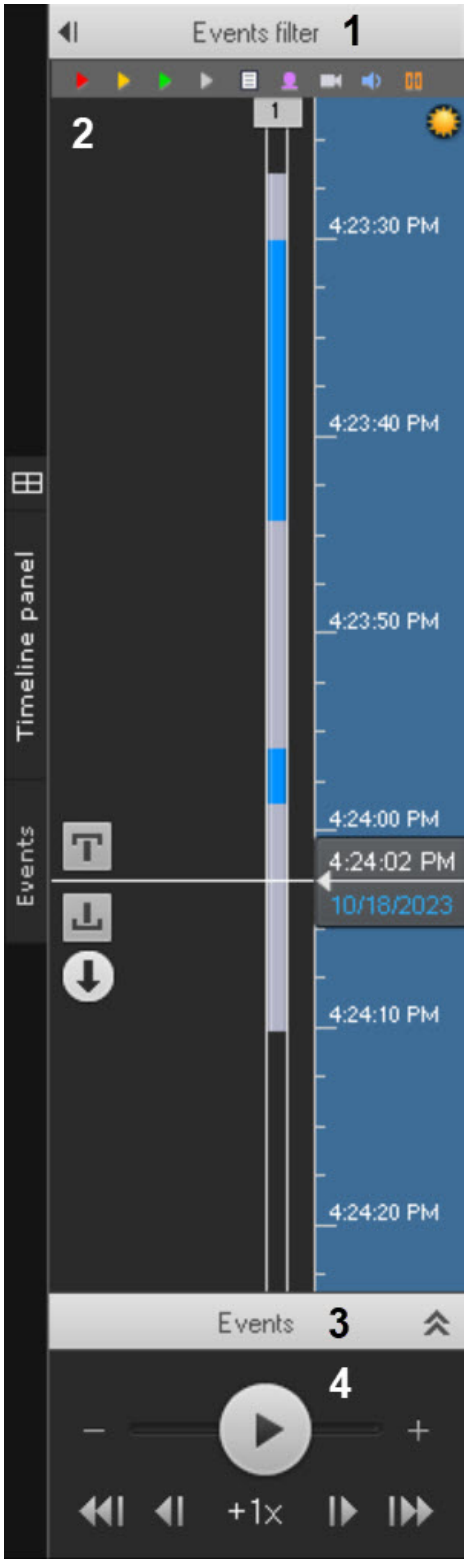
The Archive Navigation Panel is located on the right side of the screen and is automatically displayed when you switch to Archive mode (see Switching to Archive Mode).



To show/hide the panel, press the **Timeline panel** button.

The Structure and Function of the Archive Navigation Panel

The archive navigation panel is automatically displayed in the right-hand part of the screen when you switch the viewing tile to Archive or Search for Clip by Frame mode.



The archive navigation panel includes the following components:

1. The alarm events filter (**1**).
2. Timeline (**2**).
3. Events List (**3**).
4. Playback panel (**4**).

The archive navigation panel is used for the following functions:

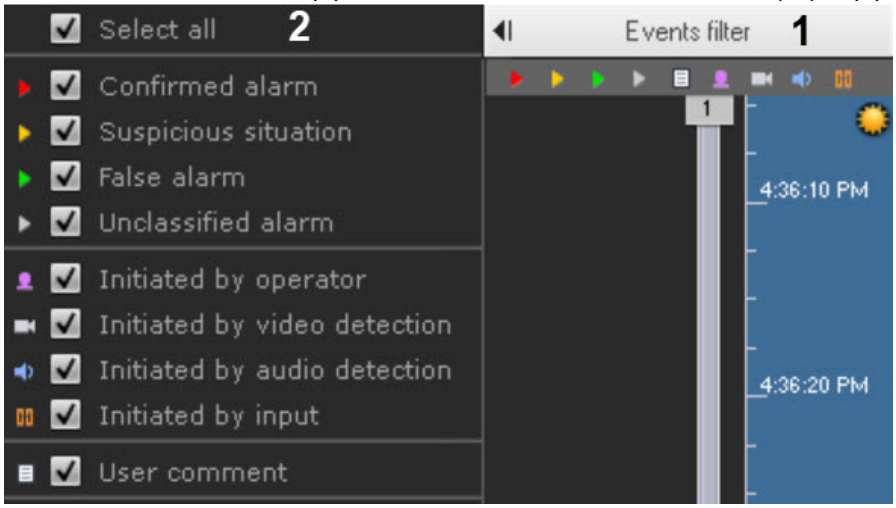
1. Navigating through the archive.
2. Playing back recordings.
3. Selecting playback mode: forward or backward.
4. Setting playback speed.
5. Selecting events for display on the timeline and in the events list.
6. Viewing the list of events of the selected type.

Events filter

The **Events filter** component allows selecting the type of events that are displayed on the Archive Navigation Panel.

To select an event type:

1. Click the **Events filter** button (**1**). The **Events filter** window will then be displayed (**2**).



2. Select the checkboxes for the types of alarms which should be displayed on the Archive Navigation Panel, according to their status:
   a. Confirmed alarm.
   b. Suspicious situation.
   c. False alarm.
   d. Unclassified alarm.

> **Note.**
>
> If you clear the checkbox for a certain type of alarm, this type of alarm and the corresponding track are no longer displayed on the timeline.

3. Select the checkboxes for the types of alarms which should be displayed on the Archive Navigation Panel, according to the cause of their initiation:
   a. Initiated by operator.
   b. Initiated by video detection tool (basic or embedded, including their sub-detection tools).
   c. Initiated by audio detection tool (basic, situation analysis, or embedded).
   d. Initiated by input.

> **Note**
>
> By default, all checkboxes are already selected.

> **Attention**
>
> To display alarms on the timeline, select at least one type of alarm event and one initiator.

4. Select the checkbox to display operator comments.
5. Click the **Apply** button.

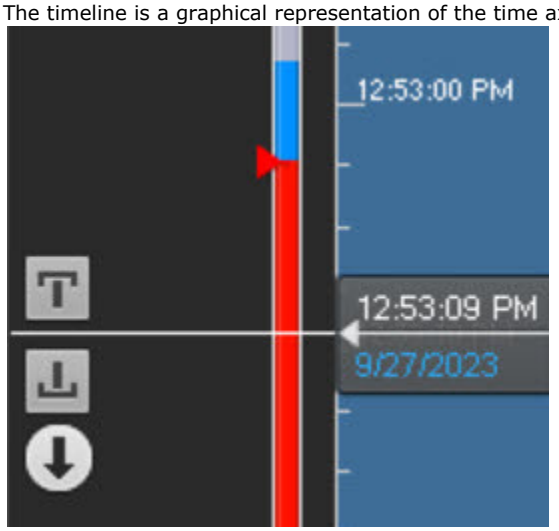
> **Note**
>
> To close **Events filter**, click to same button again.

Selection of events is now complete.

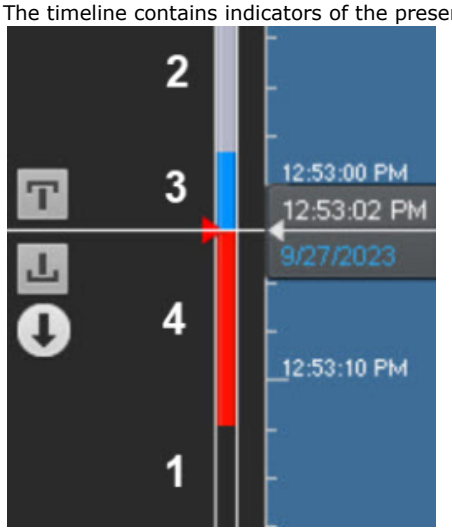
Events of the selected type are now displayed on the timeline (see The Timeline) and in the events list (see Events List).

The Timeline

The timeline is a graphical representation of the time axis of the archive and is located in the middle part of the navigation panel.



The timeline contains indicators of the presence of recordings, or tracks.



Tracks are marked in different colors depending on the archive status:

Condition	Track color
Archive absent (**1**)	Black
Archive present (**2**)	White
Archive present, input or detection tool activated (no alarm) (**3**)	Blue
Archive present, alarm active (**4**)	Red

Note

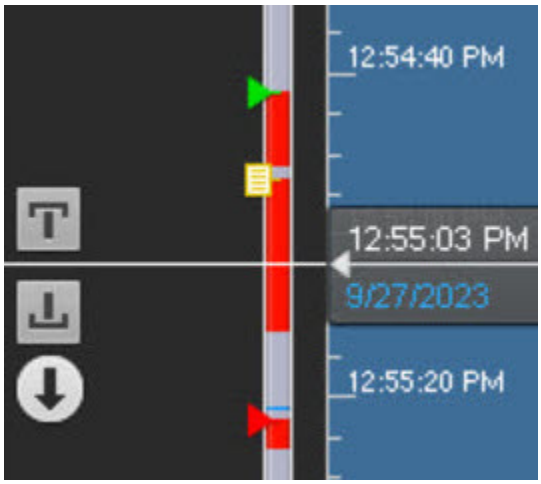
Pre-alarm recordings are white on the timeline, post-alarm footage is blue.

Note

If video recordings overlap or coincide in time, the available footage is prioritized as follows:

1. If there is recorded video, then red colored recordings have the highest priority and white ones have the least priority.
2. Blue footage takes priority over white.

At the moment when an alarm is assigned a status (critical, non-critical, false, or unclassified), a flag is added to the track. A flag is added to the point on the timeline when the alarm began.

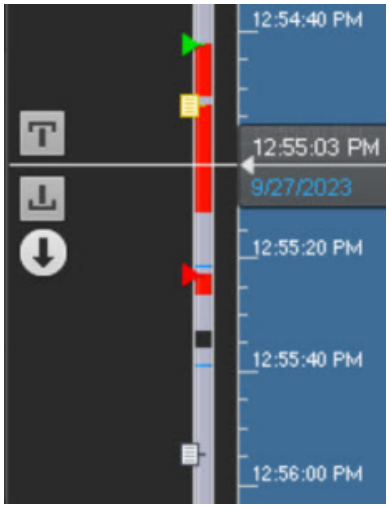


The flag is colored according to the alarm status:

1. Green – false alarm.
2. Yellow – non-critical alarm.
3. Red – critical alarm.
4. Gray – unclassified alarm.

> **Note**
>
> Display of any particular alarm event in the list is determined by filter settings (see the section titled Events filter).

Operator comments are displayed with the corresponding icons on the track. An icon is placed on the timeline at the point corresponding to the commented frame (or to the first frame of the interval, if the comment is for an interval).



If comments were left during alarm classification, the icons are displayed in the appropriate colors.

You can scroll and zoom the timeline using the mouse.

To scroll the timeline, move the cursor on its background vertically while holding down the left mouse button. To change the scale of the timeline, right-click the timeline's background and, while holding down the right mouse button, move the cursor down to zoom out or up to zoom in.

The timeline lets you select at which moment to start playback of a recording in the viewing tile. To choose at which moment to begin playback, you can either left-click the indicator and hold it down while dragging it to the desired position, or just left-click the left portion of the timeline.

If there is no recording in the selected position, the indicator will automatically move to the position corresponding to the nearest recording.

Note

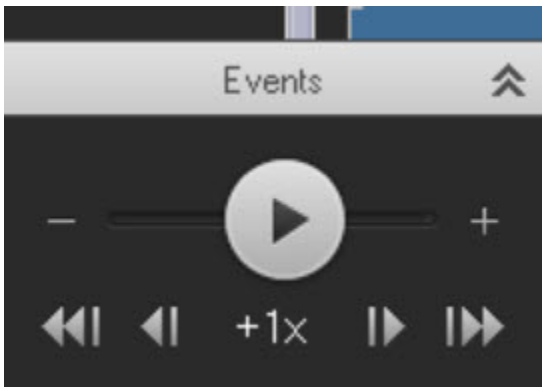
You can also set a timeline indicator in the desired position by indicating the exact date and time (see the section titled Navigating Using the Timeline).

You can also position the timeline indicator with the help of the events list (see the section Events List).

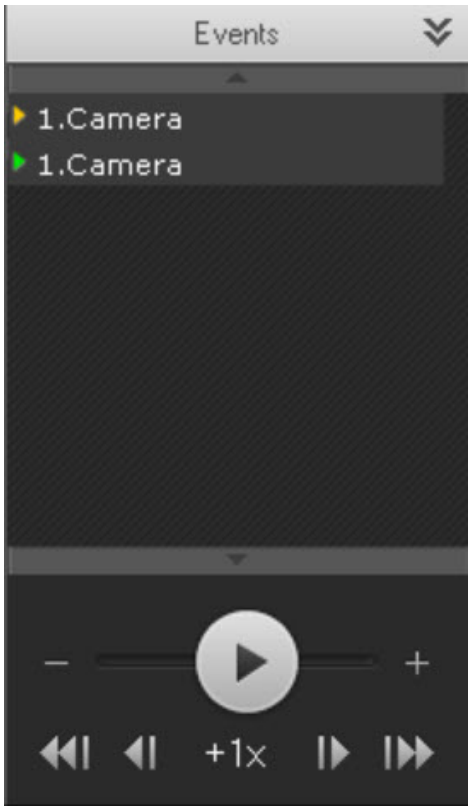
Events List

The Events List displays alarms and operator comments.

To display the events list, click the **Events** button.



The events list is now displayed.



> **Note**
>
> Whether or not a particular event is displayed in the list depends on the filter settings (see the section Events filter).

> **Note**
>
> The list displays only the alarm events that are currently in the visible portion of the timeline.

To hide the events list, click the **Events** button again.
When you place the cursor over an event in the list, detailed event information appears.

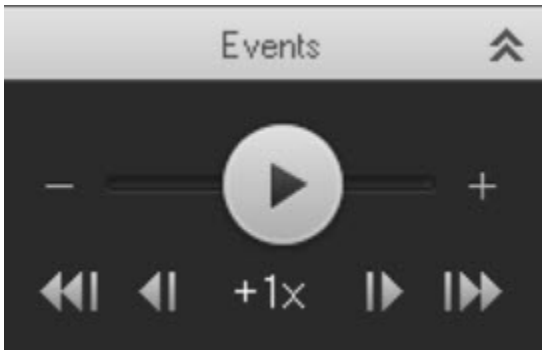


Note

Navigation through the archive by using the events list is described in the section Navigating Using the Events list.

The Playback Panel

The playback panel is located in the lower part of the navigation panel.



The playback panel contains the following buttons:

1. Go to preceding frame .
2. Go to next frame .
3. Switches to the preceding recording .
4. Switches to the next recording .
5. Play / Pause .

The button also acts as a slider which sets the speed and mode (forward/backward) of playback.

> **Note**
>
> Use of the playback panel is described in detail in the section Navigating Using the Playback Panel.

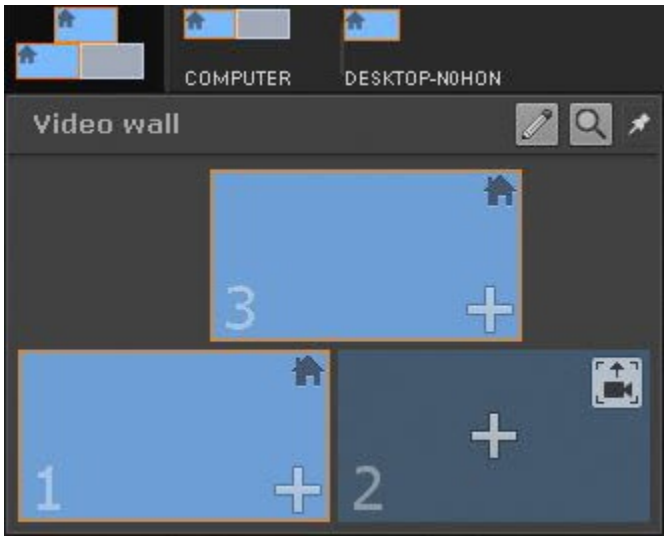
Video wall panel

Configuring Video wall

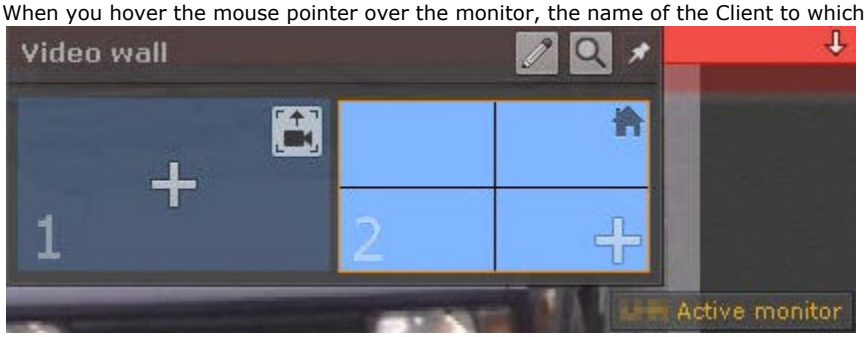
The Video wall panel is automatically displayed at the top of the screen. You can use the panel to configure the video wall from all monitors currently connected the domain Servers which video wall management is available to the current user.

Note

The panel is hidden from users with no permissions for management of video walls of domain Servers (see Creating and configuring roles).



When you hover the mouse pointer over the monitor, the name of the Client to which it belongs and its status will be displayed.



To keep the panel always visible, click the button. To hide the panel, click the button.

Monitor panel

Monitor management

The Monitor panel is automatically displayed at the top of the screen.

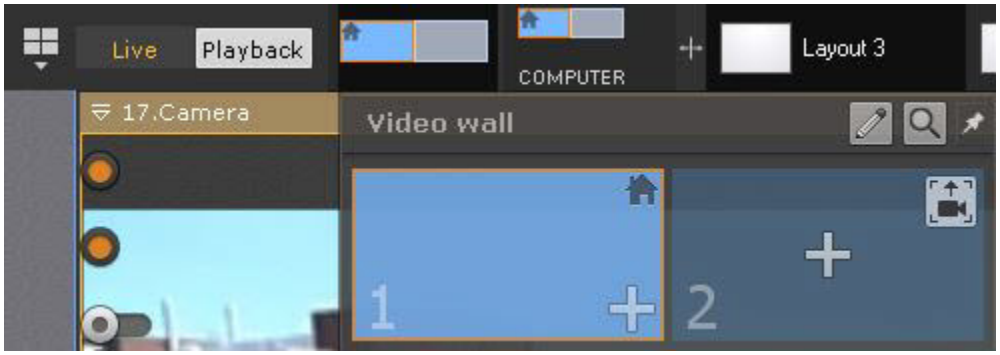
Note

If the user doesn't have permissions to manage the video walls of all domain Servers, only the local monitor management scheme will be displayed (see Creating and configuring roles).



The panel displays the schematic images of the Client monitors currently connected to the domain Servers which video wall management is available to the current user.

To open an expanded monitor images, click their schematic images.



If you want to always display expanded monitor images, click the button.

Note

To disable expanded view, click the bitton.

You can change width of the Monitor panel. To do it, click and drag the panel border .

When you resize the Monitor panel, the size of the Layout panel is automatically changed (see The Layouts panel).

The Layouts panel

The Layouts panel is automatically displayed at the top of the screen.



The panel shows layouts available in the system.

Note

If the client is connected to multiple Axxon domains, only layouts from the main Axxon domain are available.

Layouts management

Interactive Map

The 3D interactive map is used to visualize the secured facility, control cameras and identify cameras' location.

Interactive maps in *Axxon One* can obtain image data from graphics of the site or geospatial data from OpenStreetMap.

> **Note**
>
> To work with OpenStreetMap maps in *Axxon One*, you need to purchase an OpenStreetMap license.

The map can contain icons for cameras, inputs, and outputs. The area in which live video is displayed and field of view are indicated for each camera.



Please refer to the section titled Working with the interactive map for further details on how to work with the 3D map.

Camera Search Panel

The **Camera Search Panel** is used to search for and display video cameras connected to *Axxon One* VMS.

When the object panel is closed (see Objects Panel), after you click on the search bar (**1**), the area (**2**) opens that lists all cameras within your Axxon-domain.



When the object panel is open, the search will be performed inside it. To open the Objects Panel, click the  button.

Note

- You can search for cameras in the object tree on additional monitors.
- If the Client is connected to several Axxon-domains, the cameras of the main domain are displayed by default. To search for cameras from another domain, select the domain from the drop-down list (**3**).

To search for a specific camera, enter its full name or part of it into the search bar.



If you click a camera, a layout opens with the minimum number of cells for displaying the selected camera views.

Note

If the current layout contains the selected camera, the corresponding video surveillance window becomes active.

If there is no layout with the selected video camera, a new layout with a single cell is created.

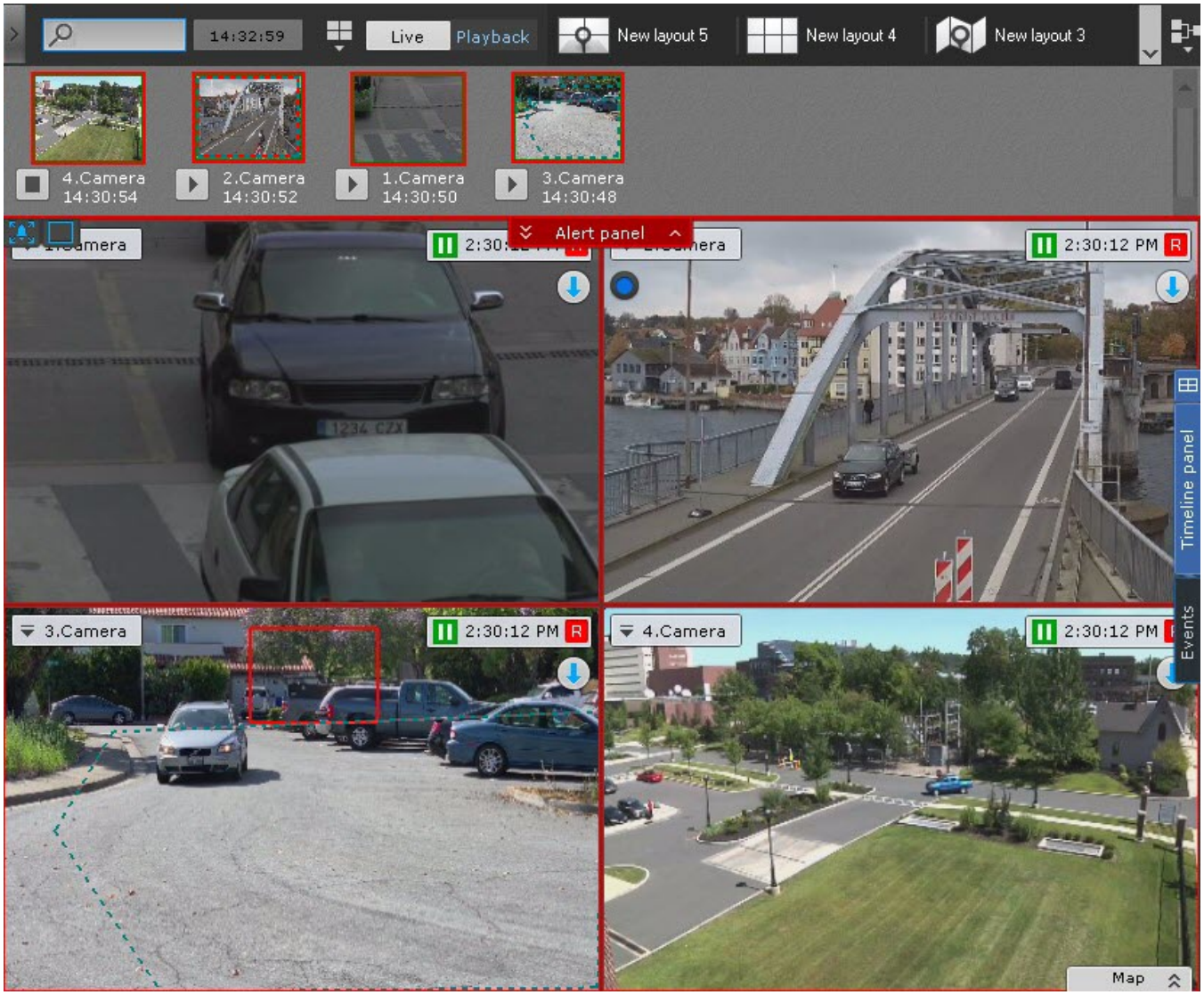
Alert panel

Alert panel is used to display alert events and work with them.

Alert panel displays video segments of all alert events in the system.

Alert panel is located at the top of the screen and is hidden by default. To open the Alert panel, click the 

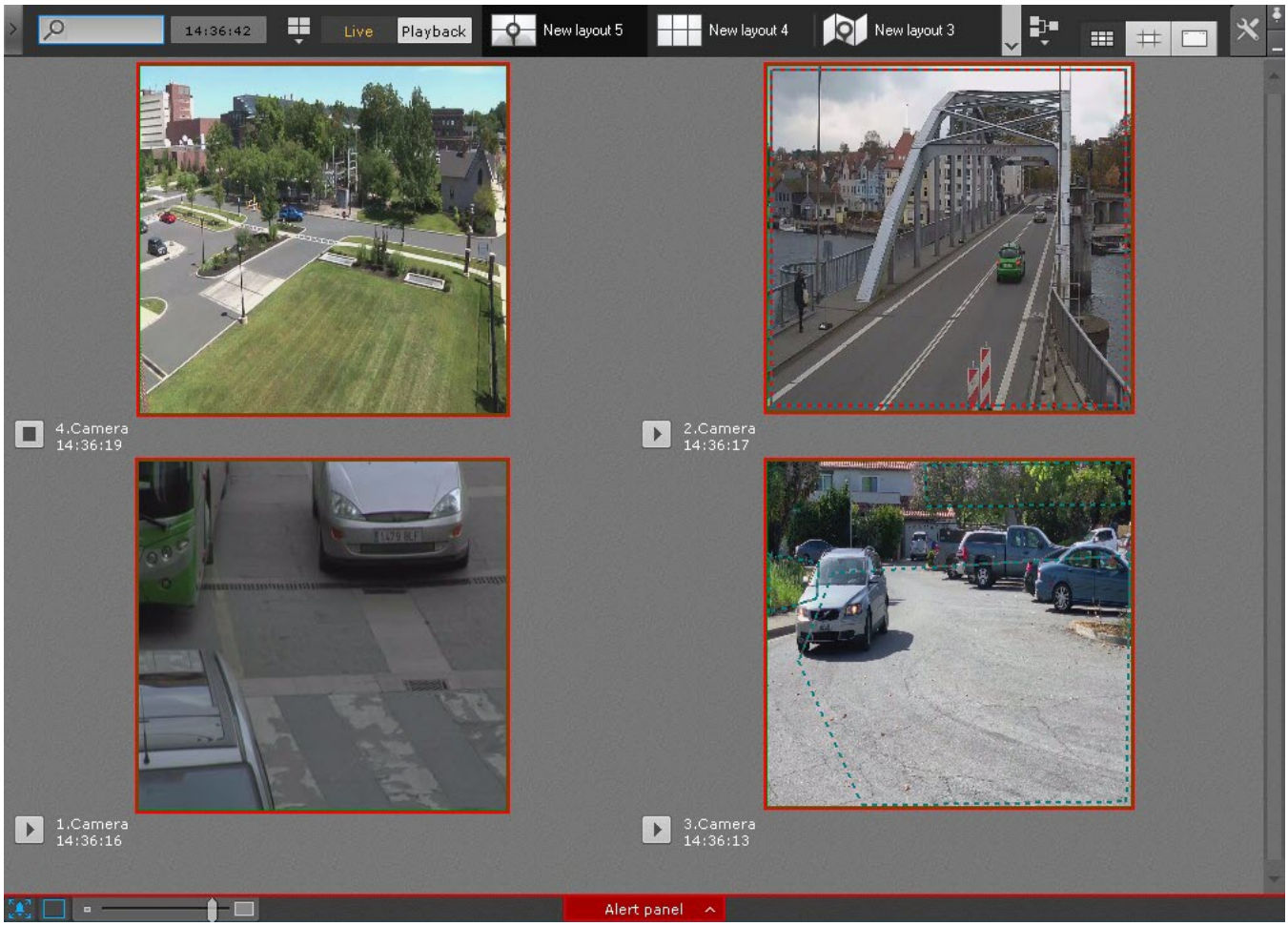
 button.



The size of the Alert panel is adjustable from 10% to 50% of the screen vertically.

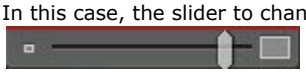
To resize the panel, left-click the **Alert panel** button and, holding it, move the cursor up or down.

You can expand the Alert panel to the full screen. This will hide the layout. To do this, click the  button.



You can resize the video segments displayed on the Alert panel.

You can do this, if the size of the panel exceeds the minimum size (10% of the screen height).

In this case, the slider to change the size of the video segments is displayed in the bottom left corner of the panel—  .

To hide the Alert panel, click the  button.

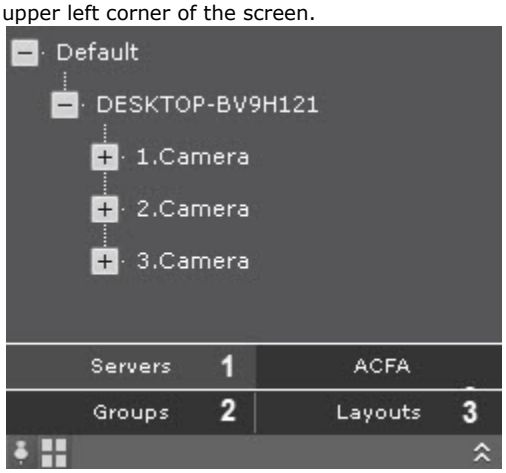
> **Note**
>
> The Alert panel button isn't displayed in the Videowall mode.

Objects Panel

If you have permissions, the Objects Panel displays cameras from all Servers in the Axxon-domain, as well as their sensors and relays.

> **Note**
>
> If the Client is connected to several Axxon-domains, you can see cameras from all Axxon-domains according to your permissions.

The Objects Panel is located on the left side of the monitor and is hidden by default. To open this panel, click the  button in the upper left corner of the screen.



> **Note**
>
> To open the Objects Panel on an additional monitor (see Monitor management), click the **Object tree** button on the left side of the screen.

The objects tree on the Objects Panel can be represented as:

- Servers (**1**): all available Servers of the Axxon-domain with created devices are displayed;
- Groups (**2**): all created camera groups are displayed (see Configuring video camera groups);
- Layouts (**3**): all available layouts with video cameras added to them are displayed (see Creating and deleting layouts).

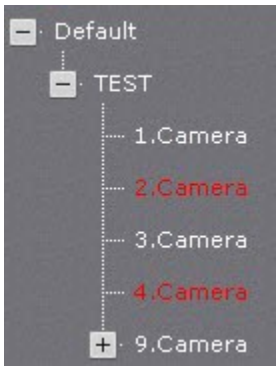
When you click on a layout name in the object tree, the corresponding layout is selected from the list. When you click on the camera name, if it is absent on the current layout, the layout with the selected camera will open.

There are two display modes for the camera selected on the panel:

1. The camera cell is displayed in the existing layout (default mode, to open it click ).
2. A temporary layout with a camera cell is created (to open it click ).

The display mode toggle buttons are located in the lower left corner of the screen. The selected display mode is saved until the client is restarted.

If the camera connection is lost, it will be highlighted in red on the Objects Panel.



If you select a camera on the panel, it will be the same as if you selected a camera on the video camera search panel (see Camera Search Panel).

Note

To search for objects inside the panel, use the search bar, same as the search panel for video cameras (see Camera Search Panel).

If you specify the search query in the search bar, then the Objects Panel will display only those cameras that match the search conditions (see Camera Search Panel).

On the Objects panel, the cameras can be sorted either by name or short name (see Configuring camera sorting on Objects Panel).

To lock the panel, click the button in the lower left corner. Click the button to unlock the panel.

You can resize the Objects Panel. To do this, left-click on the right border of the panel and drag it to the right or left.



To hide the panel, click the button.

The PTZ Control Panel

The PTZ control panel is displayed automatically in the right-hand part of the screen when the viewing tile of a PTZ camera is activated in Live Video mode.

> **Note**
>
> The PTZ control panel is displayed only if the **PTZ** object for the particular video camera is enabled (see the section titled The PTZ Object).



The PTZ control panel is used for the following functions:

1. Controlling PTZ video cameras.
2. Setting and switching to camera presets.
3. Launching/stopping PTZ tours.
4. Launching/stopping patrolling.

The PTZ control panel includes the following interface elements:

1. Presets list.
2. PTZ tours list.
3. Dialer.
4. PTZ controls for iris, focus, and optical zoom.

> **Note**
>
> If a camera does not support a function, the controls for this function cannot be accessed.

5. Virtual 3D joystick.

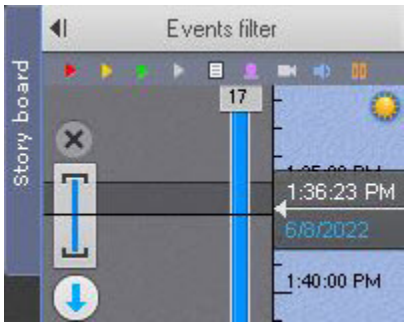
> **Note**
>
> The type of virtual 3D joystick and adjustment scale depend on the type of PTZ cameras: discrete or continuous control of Pan, Tilt, Zoom, Focus, and Iris.
>
> 
>

6. Patrol button.

> **Note**
>
> Use of the dialer, PTZ controls, joystick, and patrol button is described in the section Controlling a PTZ Camera.

Story board

The Story board becomes available after you set a time interval on the timeline (see Standard video recordings export).



To open the board, click the corresponding button.

In the Story board, you can check all videos related to an incident to export them with one click (see Simultaneous export of all event videoss).



To hide the board, click once more the **Story board** button.

Video Surveillance

Video Surveillance Modes

The video image from a video camera is displayed on the computer monitor through the Client’s interface objects, namely the video surveillance monitor and the viewing tile.



There are four modes for working with a viewing tile:

1. Live Video mode.
2. Alarm Management mode.
3. Archive mode.
4. Archive Search mode.

> **Note**
>
> Alarm Management mode is available if an alarm has been initiated in the system.

Functions Available in All Video Surveillance Modes

The following video surveillance functions are available in all video surveillance modes:

1. Selecting a video camera.
2. Scaling the viewing tile.
3. Digitally zooming video images.
4. Processing video images.
5. Rotating video Images.
6. Tracking objects.
7. Operator comments.
8. Viewing titles from POS terminals.
9. Partial decoding of video.

Scaling the surveillance window

The scale of the surveillance window can be adjusted.

This can be done in one of three ways:

1. Using the buttons in the upper right-hand part of the active surveillance window.
2. Using the buttons in the top panel.
3. Using the mouse.

If you click a surveillance window, you can see the size control buttons on the right-hand side.



1.  – increases the size of the surveillance window by one step.
2.  – resets the size of the surveillance window.

When a surveillance window is enlarged, the scale of the entire layout is increased. Some of the cells are moved off the screen.

Surveillance windows are enlarged as follows:

1. If a surveillance window occupies 100% of any of the sides of the layout (maximum surveillance window size), it cannot be enlarged.
2. If a surveillance window occupies 50% or more (but not 100%) of any of the sides of the layout, it is enlarged as much as possible.
3. If a surveillance window occupies less than 50% on both sides of the layout, it is enlarged in two steps: the first step enlarges the surveillance window to 50% on the corresponding side of the layout and the second step enlarges the surveillance window to the maximum size.

> **Note**
>
> The third case applies to layouts that contain nine or more cells.

If a surveillance window is linked to another one or an information board, at the first enlargement step (to 50%), the surveillance window and the other window/information board are displayed together and occupy all of the screen on one side.

> **Note**
>
> In this case, the first step takes into account the total size of the related cells: the related cells must be less than 50% of both sides of the layout.

Also, if you click a surveillance window, you can control its size with the buttons on the top panel:



1.  – esets the size of the surveillance window.
2.  – resizes the window up to 50% on one side of the layout.
3.  – maximizes the size of the surveillance window.

How to resize the surveillance window using a mouse:

1. In full screen mode, click anywhere to minimize the window.
2. Otherwise, double click inside the window to display it in full screen mode.

Digitally Zooming Video Images

Digital zooming in a video image enables a gradual increase in the magnification of a video image without changing the dimensions of the viewing tile.

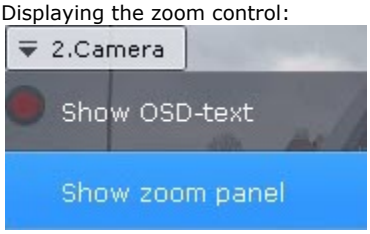
The video image can be enlarged using the following tools:

1. Digital zoom scale.
2. Area selection.
3. Mouse scroll wheel.

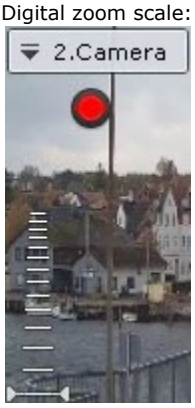
Enlarging a video image using the digital zoom scale

To display the digital zoom scale on the viewing tile screen, select **Show digital zoom** in the context menu of the viewing tile.

Displaying the zoom control:

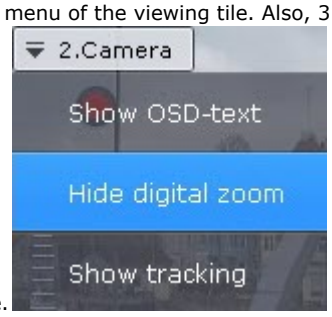


Digital zoom scale:



To enlarge a video image, left-click the slider and hold and drag the digital zoom scale up to the desired value. The maximum zoom is 16x. To return back to the original image, move the slider back to its original position.

To hide the digital zoom scale, select **Hide digital zoom** in the context menu of the viewing tile. Also, 3 seconds after you scale down the video image to the minimum, the zoom scale will automatically hide.



After hiding the digital zoom scale, the selected zoom level of the image will be preserved when switching between image viewing modes.

Enlarging a video image through area selection

To enlarge a video image, select the area of the image that you would like to enlarge.



You can select an area by doing the following:

1. Click and hold down the left mouse button inside the viewing tile.
2. Move the mouse cursor to the desired position.
3. Release the left mouse button.

Once you have completed the above actions, the selected area will be displayed across the entire viewing tile.



Note

If you select an area that requires a zoom of more than 16x to display, it will be marked with a red frame. The video image will not be enlarged.



Enlarging a video image using the mouse scroll wheel

When using the mouse scroll wheel, the video image is enlarged relative to the mouse cursor. A description of this process is provided in the table below.

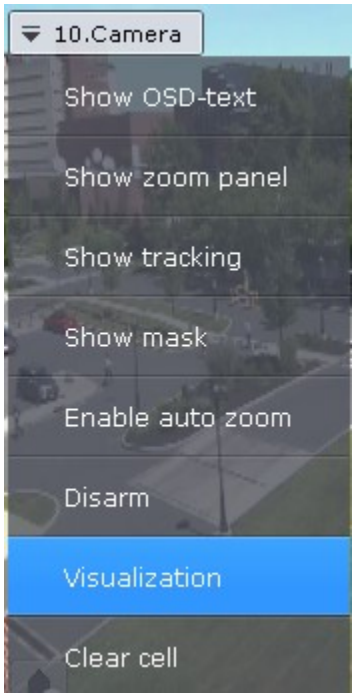
Action	Executed function
Mouse wheel is scrolled forward by one level	The video image is enlarged by 2x
Mouse wheel is scrolled backward by one level	The video image is reduced by 2x

Video image processing

In *Axxon One*, the video image processing functions implemented in the viewing tile enhance the performance and convenience of using the video surveillance system.

The following video image processing functions are available from the viewing tile:

1. Contrast.
2. Sharpness.
3. Deinterlacing.



To enable video image processing functions, use the **Visualization** option in the context menu of the viewing tile. Only one image processing function can be enabled at a time.

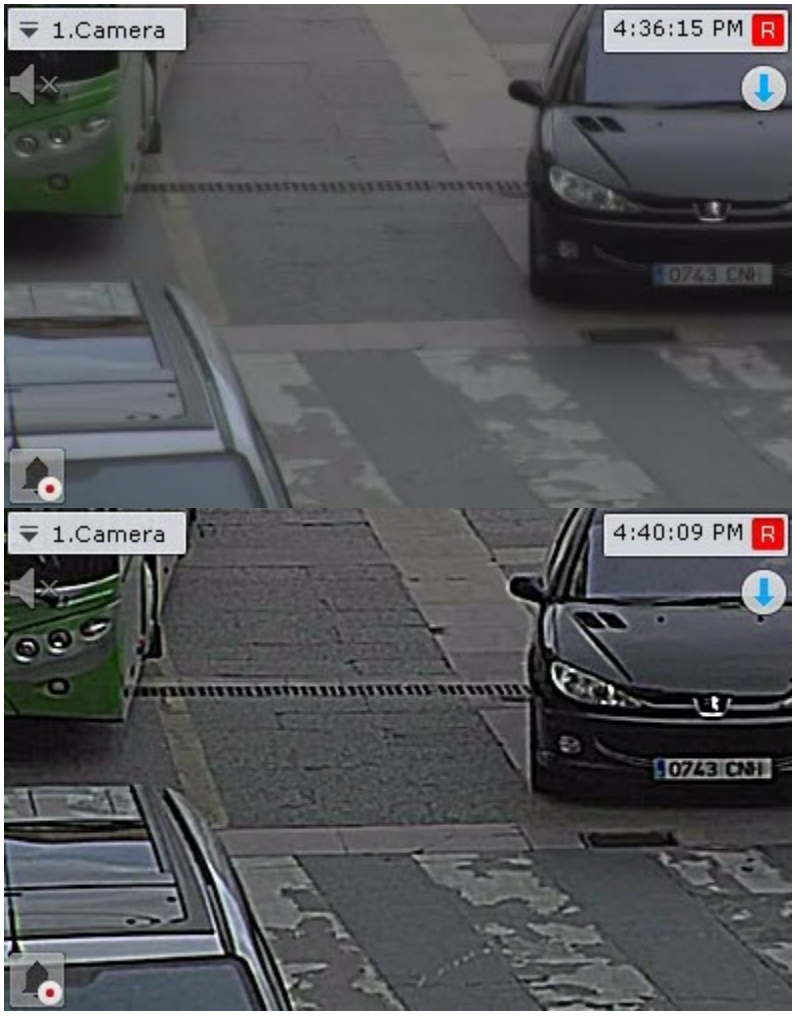
Changing the Contrast Level

An *Axxon One* operator is granted access to adjust the contrast of a video image.

To adjust the contrast, select the **Contrast** option in the **Visualization** context menu.



An example of the **Contrast** function is given in the following image.



To return to the original image, reselect the **Contrast** option in the **Visualization** context menu.

Setting the Sharpness Level

An Axxon One operator is granted access to adjust the sharpness of a video image.

To adjust the sharpness, select the **Sharpness** option in the **Visualization** context menu.



The image in the following picture shows an example of use of the **Sharpness** tool.



To return to the original image, use the **Sharpness** function again.

Using Deinterlacing

The **Deinterlacing** tool is used to correct tooth-type distortions (also called "combing artifacts"), which appear on the borders of video image fragments when objects move quickly relative to the background.

An example of a combing artifact is shown in the picture below.



To utilize this tool, select the **Deinterlace** option in the **Visualization** context menu.



The image in the viewing tile will then be corrected.



To disable **Deinterlacing**, reselect the **Deinterlace** option.

Rotate Video Image

You can rotate a video 90°, 180° or 270° degrees.

Note

If you enable video rotation, only video in Live Video and Archive modes is rotated:

- NA (not applicable) for video display on the map and on the alarms.
- NA to recording for archives.
- NA for export.
- NA for analytics (metadata).

To rotate video, complete the following steps:

1. In the viewing tile context menu, select **Visualization**.



2. Select the angle of rotation (clockwise).



Video rotation is now complete.



To disable video rotation, select **Visualization Disable rotation** in the viewing tile context menu.



Tracking objects

Object tracking allows a user to visually track the movement of objects in a camera's field of view or in a video recording in an archive.

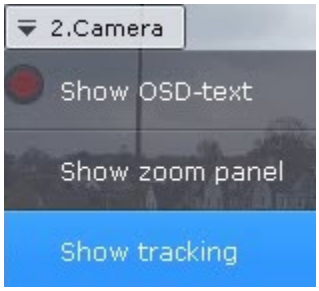
> **Attention!**
>
> Object Tracking is available if:
>
> 1. the object tracker is activated for this camera (see General information on the standard detection sub-tools);
> 2. the Video Motion Detection tool is activated (see Configuring the Motion detection);
> 3. at least one of the Embedded Analytic tools is activated (see General information about embedded detection tools).

Object tracking performs the following functions:

1. Recognizes the presence of a moving object and dynamically marks it with a transparent rectangle on the video image.
2. Displays the trajectory of the object's movement.

Motion is detected based on the time gradient of the video image’s difference between frames.

To enable object tracking, select **Show tracking** in the viewing tile context menu.



Object tracking functions will now be activated.



To disable object tracking, click **Hide tracking** in the viewing tile context menu.

If you have created a Scene Analytics detection tool for this video camera (see Functions of Scene Analytics detection tools), then you can see the detection parameters (areas, lines) in Live Video mode along with object tracking in the camera window.



Note

Areas to be excluded from surveillance are outlined in dotted black and green line while detection areas are outlined in black and gray.

If an ANPR detection tool has been created for a camera, the license plates within the video image will be outlined (see Category: Vehicle).



> **Attention!**
>
> To ensure correct display of the outline, set the camera's **Video Buffering** parameter with the range of 500–1000 (see The Camera object).

If a face detection tool has been created for a camera, all faces within the video image will be outlined.



If a pose detection tool (see Configuring the Pose Detection) has been created for a camera, a human skeleton is highlighted over the video image.



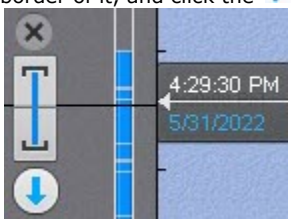
Operator comments

Operator comments on past or ongoing events allow a more complete understanding about the situation at the site.

Comments are displayed during playback (see Viewing recorded video with operator comments) and are marked with tags on the timeline (see The Timeline). Comments can also be searched (see Searching comments).

Adding comments in different surveillance modes

In Archive and Archive Analysis modes, comments can be added both for specific frames and for intervals of time.
To add a comment for an interval, select an interval on the timeline, place the timeline indicator either inside the interval or at one border of it, and click the button.



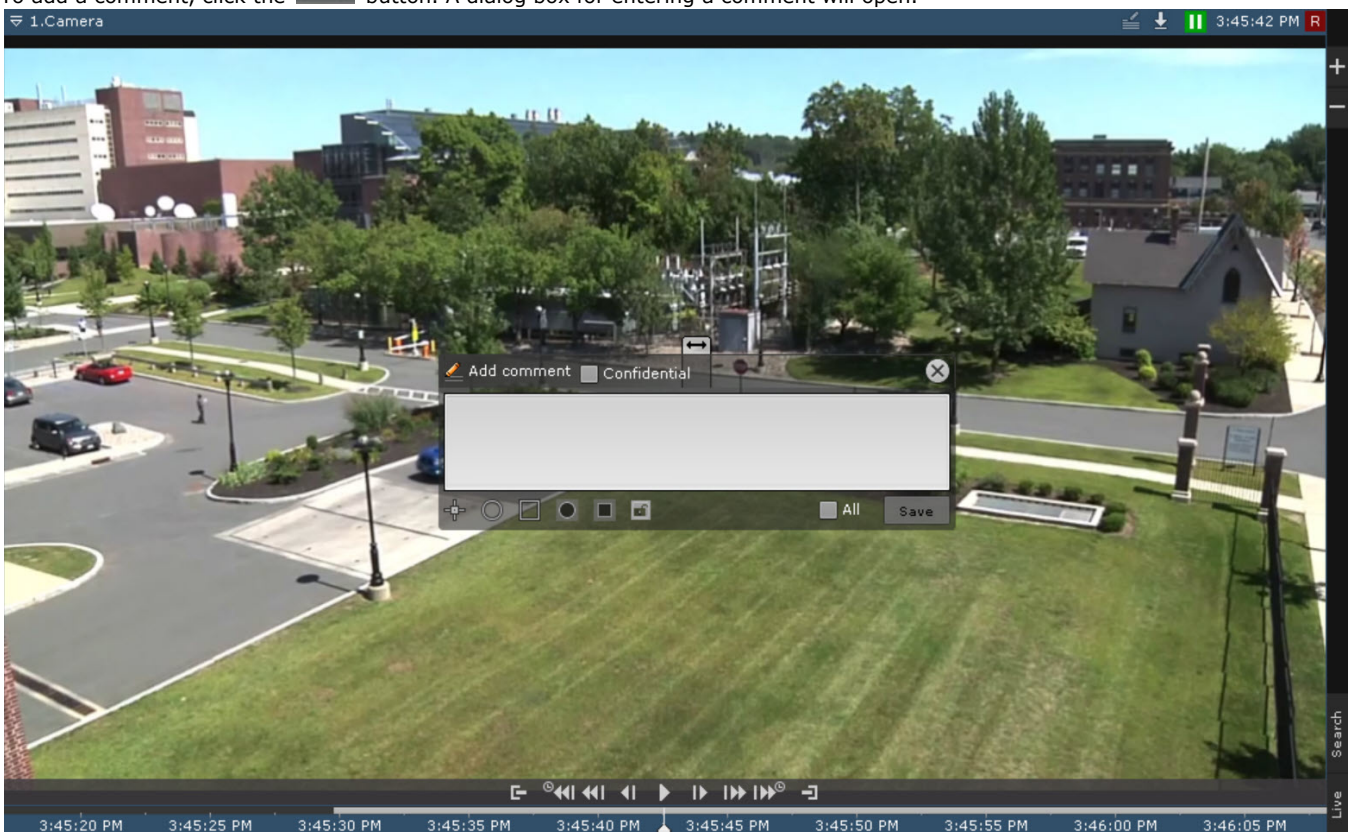
Note

If comments are added during playback in Archive or Archive Analysis mode, playback is paused after the button is clicked.

In Alarm Management mode, operators can be required to give comments after classifying an event (see Configuring Alarm processing) or comments can be left in free form, before event classification, by clicking the button. The comment applies to the entire duration of the alarm. You can add a comment in real time only if archive recording is enabled.

Adding a comment

To add a comment, click the  button. A dialog box for entering a comment will open.

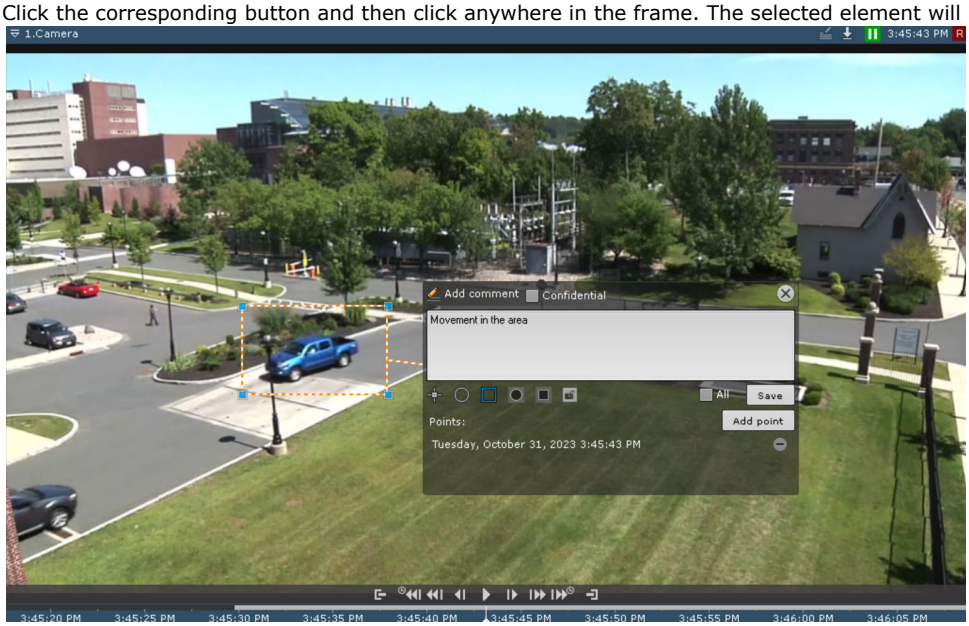


The number of characters in the comment is limited.

The following parameters can be configured:

1. Position of a comment in the frame—you can move the window with the comment when you click the window title and hold it with the left mouse button.
2. Transparency of the comment window is adjusted by moving the  slider from left to right, from opaque to maximum transparency.
3. Marking the area of interest in the frame. You can mark the area with a dot (), an oval (), or a rectangular () area. To do so, do the following:

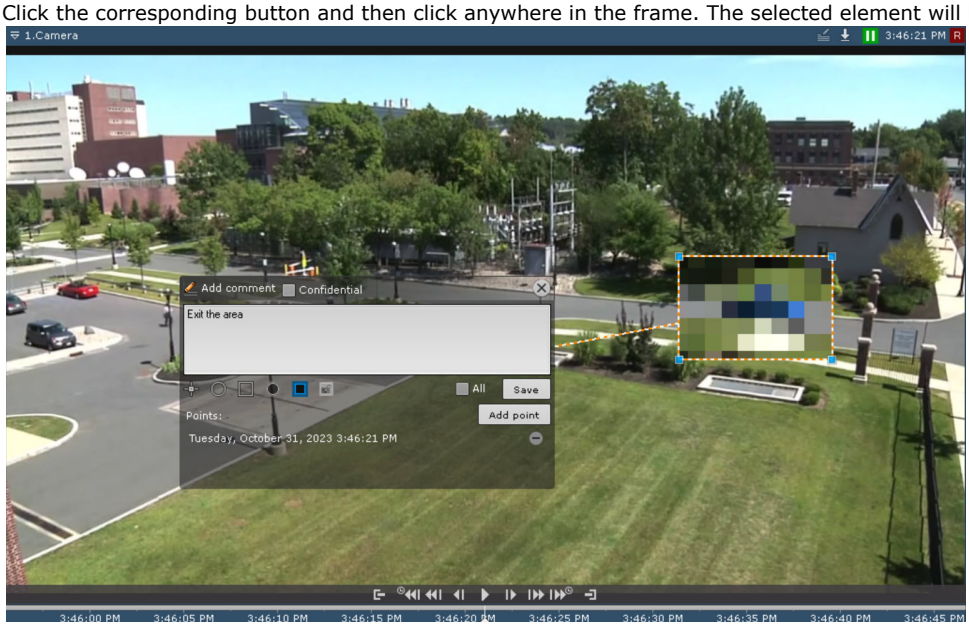
a. Click the corresponding button and then click anywhere in the frame. The selected element will be displayed.



b. Move the element to the required area of the frame. To do this, left-click on the element and move the cursor without releasing it.
c. Set the size of the element by stretching its anchor points.
d. **Points** will be displayed below the comment. You can set several points in different frames. To do this, go to another frame, move the element in it to the required area, and click the **Add point** button. To delete a point, click . As a result, one comment will be displayed for all added points.

> **Note**
>
> You can set points only for an oval and a rectangular area.

4. Marking the privacy zone—the area of the frame that should be hidden. You can mark it with an oval ( ) or a rectangular ( ) area. To do so, do the following:
a. Click the corresponding button and then click anywhere in the frame. The selected element will be displayed.



b. Move the element to the required area of the frame. To do this, left-click on the element and move the cursor without releasing it.
c. Set the size of the element by stretching its anchor points.
d. The **Mask position** will be displayed below the comment. You can set several positions in different frames. To do this, go to another frame, move the element in it to the required area, and click the **Add** button. To delete a position, click . As a result, one comment will be displayed for all added positions.

> **Note**
>
> The privacy zone cannot be set in real time.

> **Note**
>
> For one comment, you can specify either the area of interest, or the privacy zone.

5. Protection of an archive interval with a comment from overwriting. To protect archive records with a comment from being deleted, click the button. To cancel protection, click the button (see Setting up record protection).
6. Adding a comment to all cameras on the layout—set the **All** checkbox.
7. To make a comment confidential, set the **Confidential** checkbox. Such comments are visible to users who have rights to access confidential comments (see Creating and configuring roles).

To save the comment, click the **Save** button. Otherwise, click to cancel.

After being saved, a comment is displayed in the frame as specified. To delete the comment, before you perform any other command in the system, click the button.



Switching to other camera via a link in the Camera window

The Camera window may contain links to other cameras (see Adding links to other cameras to the Camera Window).



When you click a link, the corresponding camera is selected, and the Camera window expands.

If a linked camera is not present on the currently selected layout, a layout containing the required camera is selected. If there are multiple layouts containing the required camera, the layout with the least number of windows is selected.

If a linked camera is not present on any layouts, a temporary layout is selected that will be automatically deleted after you proceed to another layout.

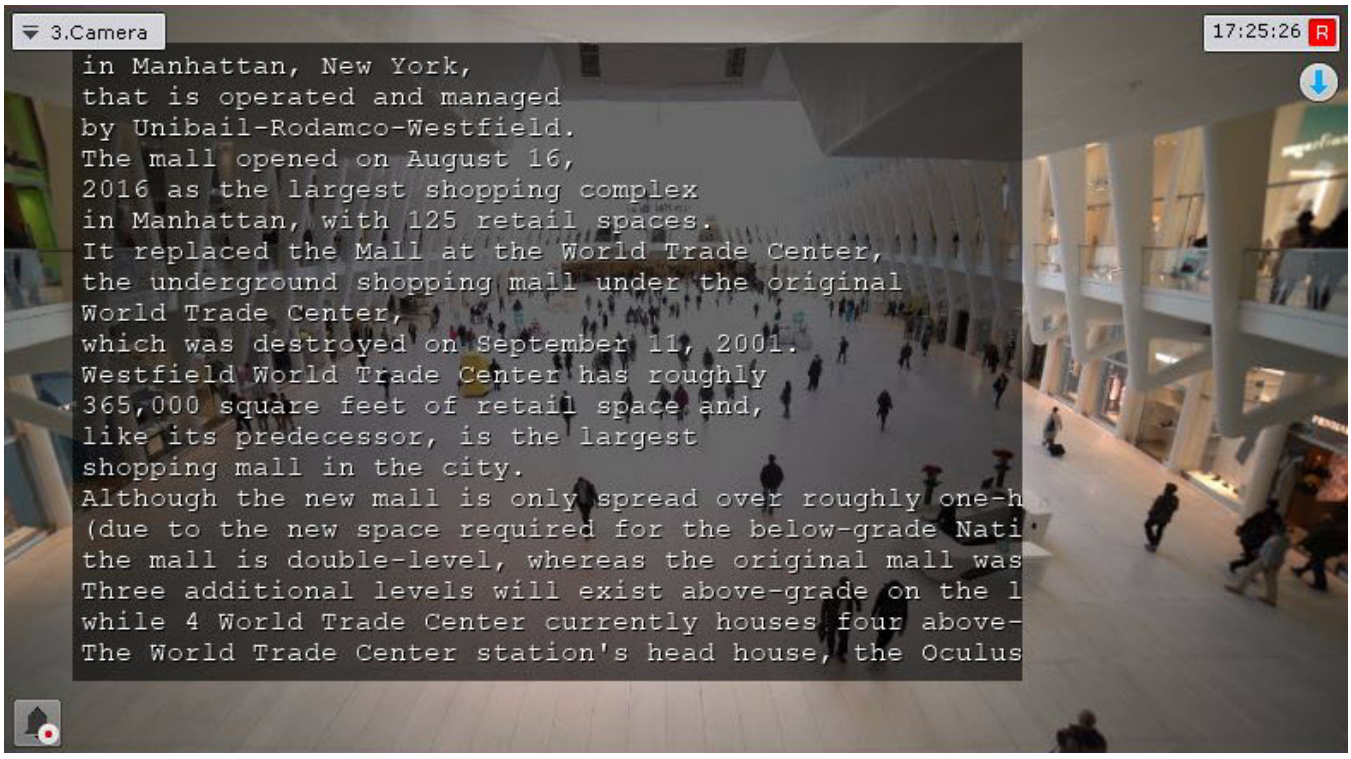
If one or more cameras are in Archive or Archive Search modes, after you click the link, you will see it | them also in Archive or Archive Search modes respectively.

Viewing titles from POS terminals

If you have configured the titles overlay, the video tiles show titles superimposed on video (see Configuring titles view).

You can have titles from several POS terminals in the same camera window.

> **Attention!**
>
> Captions/titles are displayed only if the camera is located on the current layout.
>
> If you collapse the Client, then captions are not received.

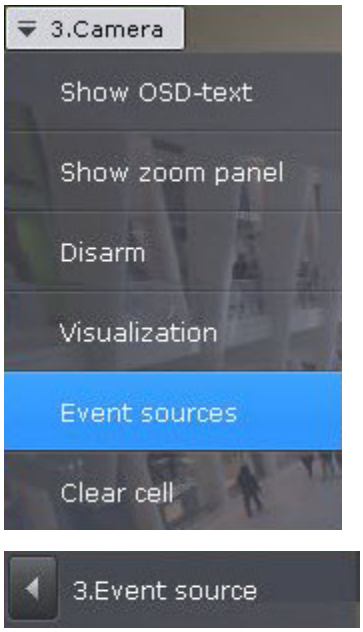


> **Note**
>
> Keywords or lines can be highlighted according to the settings (see Configuring keywords).

If you view recorded video, titles are synced by time.

> **Note**
>
> With certain captions' output settings (the **Display duration** parameter = 0, see Configuring titles view) and low-intensity events at the checkout, you may have a time lag between the captions displayed and the video time stamp.

To disable titles overlay, select **Event sources** in the context menu of the viewing tile and a POS terminal that you want to hide.


3.Camera
Show OSD-text
Show zoom panel
Disarm
Visualization
Event sources
Clear cell

3.Event source

Partial decoding of video

Video encoding/compression is a digital video processing technique aimed at reducing the bit rate of streamed video and bandwidth consumption. Video is compressed according to a specific software algorithm – codec.

To compress video signals from IP-devices, standard codecs such as MPEG-4 or vendor's proprietary codecs are used.

Before displaying the compressed video signal on screen, it is automatically decompressed.

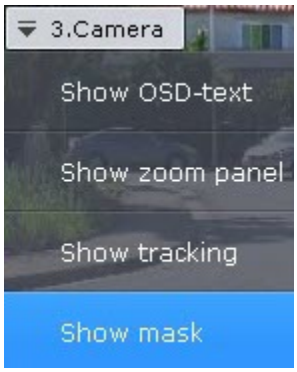
If the resolution of a viewing tile is lower than that of compressed video, only part of the video stream is decoded. This reduces CPU load on *Axxon One* Clients. Partial decoding does not affect bandwidth requirements. Partial decoding works with MPEG-2, MJPEG and MxPEG.

Displaying information from a detection tool (mask)

Some detection tools can superimpose different information on the video image:

1. Motion detection (VMD)—motion mask.
2. Equipment detection (PPE) and Person-based Privacy Masking—segments of the human body.
3. Object Presence Detection, Fire Detection and Smoke Detection—the sensitivity scale of the detection tool.
4. Neurocounter—highlighting of the recognized objects.
5. Water Level Detection—the water level indicator.
6. Queue Detection—highlighting of the queue.
7. People masking detection tool—masking people.
8. Privacy Masking—hides moving objects.

To enable displaying information from a detection tool, select the **Show mask** item in the context menu of the Surveillance window.



Note

This item is available only if you have created one of the above mentioned detection tools for this camera.

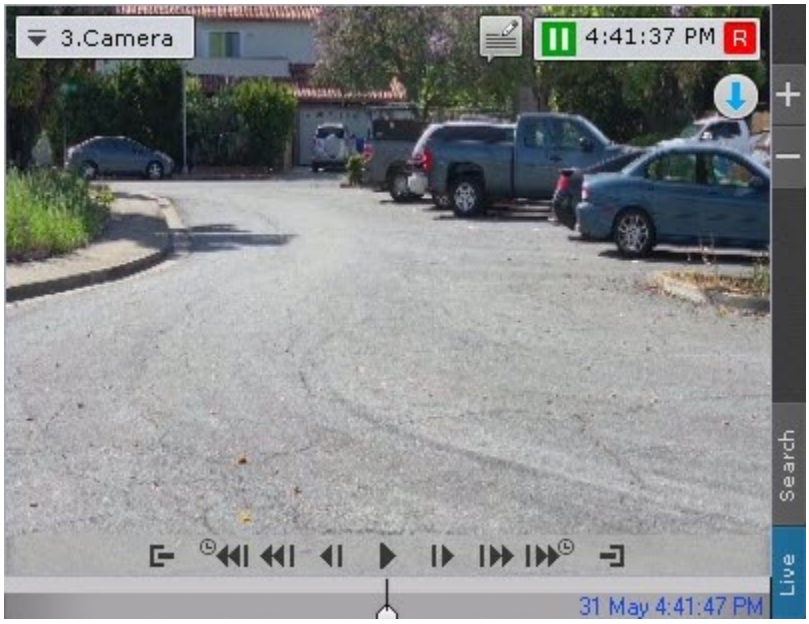
As a result, the necessary information will be displayed in the Surveillance window. To disable this function, select the **Hide mask** item in the context menu of the Surveillance window.



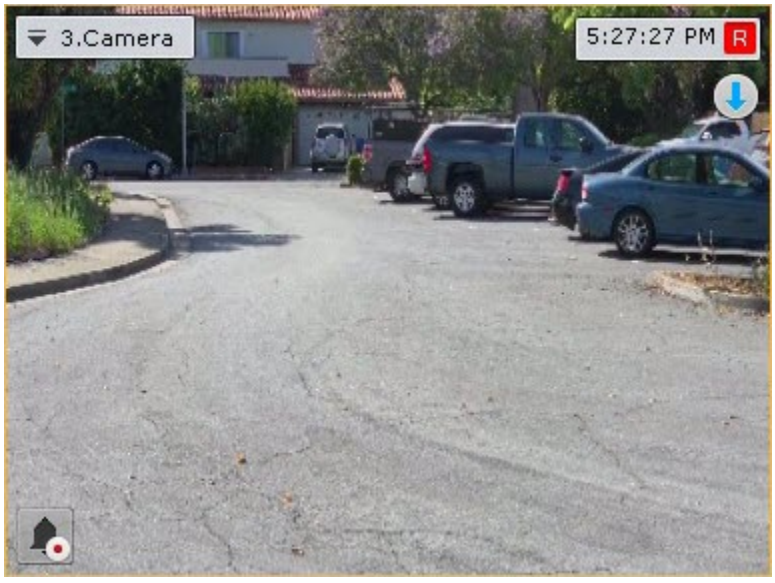
Real-time video surveillance

Switching to Live Video Mode

To switch the Camera Window from a different surveillance mode to Live Video viewing mode, click the **Live** tab in the lower-right corner.



The viewing tile will then appear in Live Video mode.



Video Surveillance Functions Available in Live Video Mode

In Live Video mode, the following video surveillance functions are accessible:

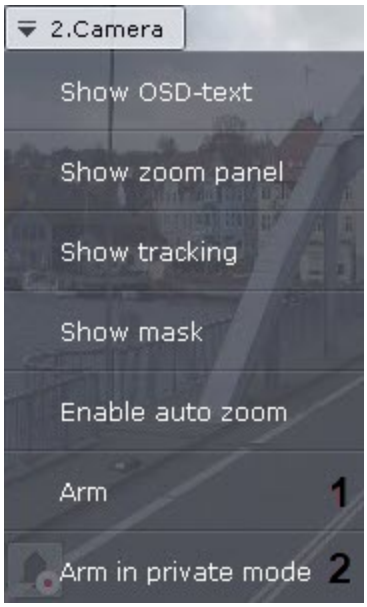
1. Selecting video stream quality in a viewing tile.
2. Autozoom.
3. Functions for tracking of moving objects.
4. Arming/disarming a video camera.
5. Controlling a PTZ Camera.
6. Controlling outputs.
7. Displaying the input status.
8. Autoreplace offline cameras on layouts.
9. Snapshot.
10. Functions Available in All Video Surveillance Modes.

Arming and Disarming a Video Camera

In *Axxon One*, a video camera is armed via all the detection tools registered for that video camera.

To arm a camera, select one of the following two parameters in the context menu of the viewing tile:

1. **Arm** (**1**). In this case, the camera will be available to all users who have access to it.
2. **Arm in private mode** (**2**). In this case, the camera will not be available to the users with the **Live in Armed mode.**



To disarm a camera, select **Disarm** in the context menu of the viewing tile. The video camera will then be disarmed.

Controlling a PTZ Camera

PTZ video camera can be controlled with the PTZ Control Panel or directly in the Viewing Tile (see Controlling a PTZ Video Camera in the OnScreen PTZ Mode, Control using Areazoom, Control using Point&Click).

The user gains access to this panel when the viewing tile of a video camera in Live Video mode that supports a PTZ control interface is selected.

Attention!

PTZ camera is controlled in accordance with the priority settings (see Creating and configuring roles). If multiple users have the same control priority, they can control a PTZ camera simultaneously.

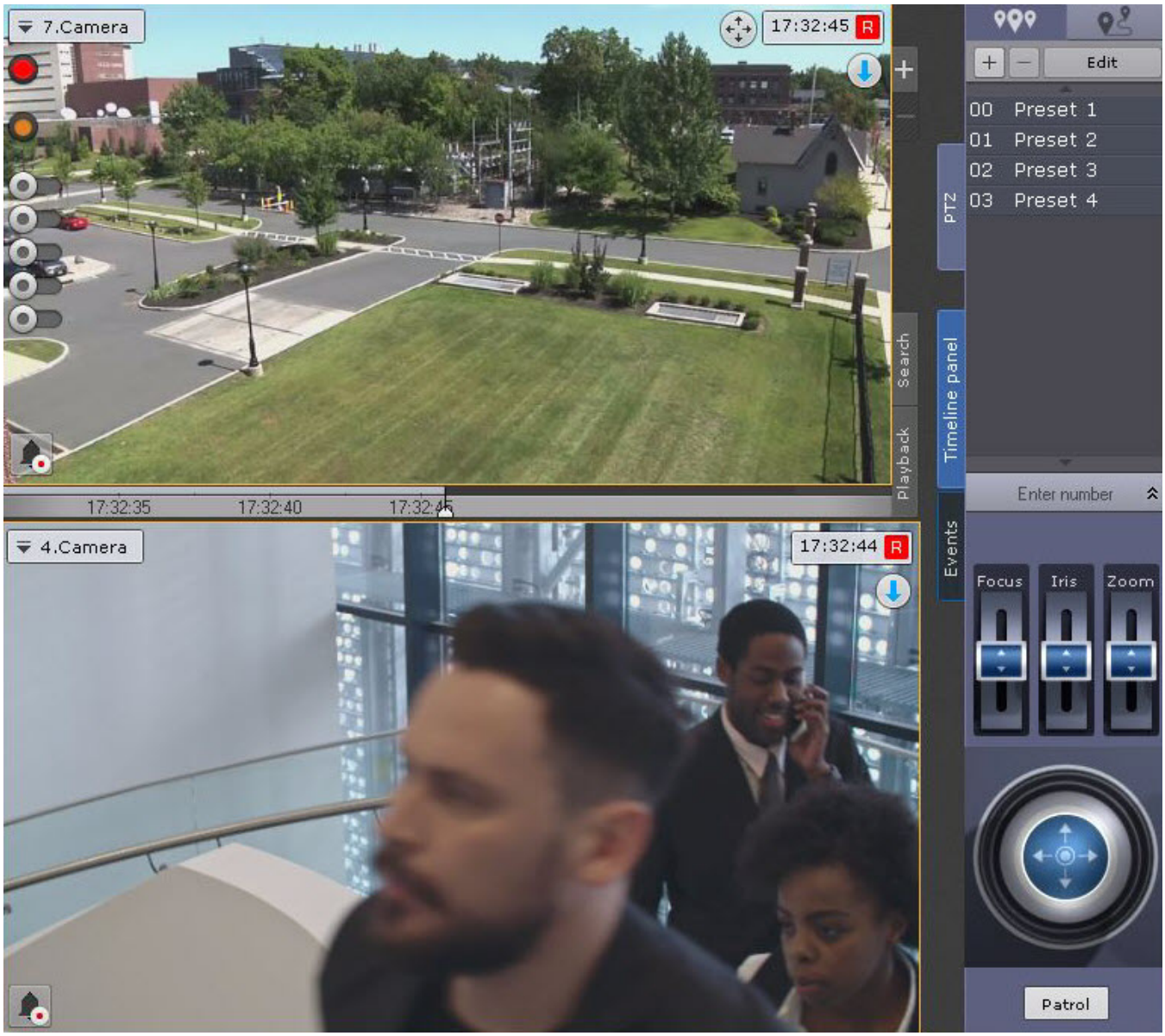
If the user with higher priority controls the PTZ camera with the the PTZ control panel (as long as the camera is selected) users with a lower priority can not control it. If the user with higher priority controls the PTZ camera, the relevant information is displayed on the panel.



If you disabled the option to simultaneously control a PTZ camera by multiple users, users with the same priority take over the control on a first-come, first-served basis.

However, a user with equal or higher priority can take over the PTZ control. To do this, click the **Take control** button.

If the user that controls the PTZ camera is idle for a certain time (see Configuring PTZ control), it is automatically unlocked and the control becomes available to all users.



The following actions can be performed using the PTZ device control panel:

1. Use presets.
2. Modify the parameters of the iris, focus, and optical zoom.
3. Modify the horizontal and vertical tilt angle of the video camera.
4. Starting/stopping patrol mode.

Note

Setting presets is described in detail in the section The PTZ Control Panel.

When you exit the PTZ device control panel, it will be automatically switched to the default preset if the **Home preset timeout** field value is different than **0** (see The PTZ Object).

Presets

Creating and editing presets

The presets list created for a selected video camera is displayed in the upper part of the PTZ control panel in the  tab.



For each preset in the list, the following parameters are displayed:

1. The identification number.
2. A descriptive name.

The presets list is used for the following functions:

1. Creating presets.
2. Editing the identification number and name of an existing preset.
3. Deleting presets.
4. Switching to a preset.

You can create up to 100 presets with numbers from 0 to 99. To create a preset, you must perform the following steps:

1. Place the PTZ camera in the position which is to be saved as a preset.
2. Click  . Fields for entering an identification number and a descriptive name for the preset will then appear.


3. Fill in these fields as desired.

> **Attention!**
>
> If a preset with the identification number entered already exists, its parameters, as well as the corresponding PTZ camera position, will be overwritten.

4. Left-click anywhere in the presets list and press **Enter** to save changes.

Creation of a preset is now complete.

To edit the number and name of an existing preset, you must perform the following steps:

1. Highlight the desired preset in the list.
2. Click  . The identification number and descriptive name fields will then become accessible for editing.
3. Modify the preset number and/or name as desired.
4. Left-click anywhere in the presets list to save changes.

Editing of the preset is now complete.

To delete an existing preset, you must perform the following steps:

1. Highlight the desired preset in the list.
2. Click  .

The preset has now been deleted.

To switch to a preset, left-click the corresponding line in the presets list. The camera will then be switched to the desired position.

> **Note**
>
> See the section Selecting a preset.

Selecting a preset

To switch a PTZ camera to a preset, you can use the presets list. To do this, left-click the corresponding line in the given presets list.



To switch a PTZ camera to a preset, you can use the Enter number panel. To display the Enter number panel, click the **Enter number** button.



To switch to a preset using the Enter number panel, you must perform the following steps:

1. Using the numeric buttons (0-9), enter the number of the preset to which you want to switch.
   The entered number is displayed in a special field.

   To delete the last digit entered, click the  button.

2. Click the  button to switch to the preset with the number entered. The camera will then be switched to the desired position.

Switching to a preset using the Enter number panel is now complete.

Note

Examples of entering a number:

5,  – switch to preset number 5;

0, **5**,  – switch to preset number 5;

5, **7**,  – switch to preset number 57.

PTZ Tours

During a PTZ tour, the camera automatically scrolls between pre-listed preset positions.

> **Attention!**
>
> In *Axxon One*, you can set up PTZ tours only for cameras connected via the ONVIF Generic driver (see Generic Drivers (General device, generic)).

The presets list created for a selected video camera is displayed in the upper part of the PTZ control panel in the  tab.



Creating and editing PTZ tours

Axxon One automatically adds PTZ tours created with the camera's web interface.

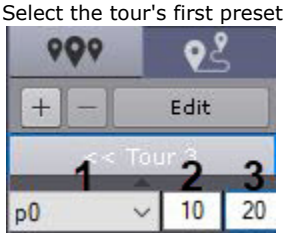


To add a new tour, do the following:

1. Click the  button.
2. Enter a name of the new tour, and click the **Ok** button.



3. Select the tour's first preset (**1**).



4. Specify dwelling time in seconds for this preset (**2**).
5. Specify transition speed to this preset in standard units from 1 to 100 (**3**).

> **Attention!**
>
> This parameter is reserved for future *Axxon One* software versions.

6. Click the **Ok** button.
7. Add all other desired presets in the same way.
8. Click 

to return to the PTZ tours list.

To alter a tour, select it in the list and click **Edit**.



To delete a tour, select it and click  .

Launching a PTZ tour

To start a tour, do the following:

1. Select a tour from the list.



2. Click the **Patrol** button.

To stop a tour, click again the **Patrol** button.

Control using step buttons and virtual joystick

To control a PTZ camera, you can use both step buttons (discrete PTZ mode) and the virtual joystick (the camera must support continuous PTZ), if the camera supports both modes.




To select, click the  and  buttons.

Otherwise, only one of the modes may be used.

> **Note**
>
> If your camera is set to Discrete PTZ control via Continuous, your control options will be limited to buttons only (see The PTZ Object).

Set the sensitivity level of PTZ step buttons by selecting a value from 1 to 10.



If you press and hold the buttons, the PTZ camera will move continuously.

> **Attention!**
>
> Interaction between PTZ cameras and the Client may cause the cameras to jerk in some cases.
>
> Cameras also may jerk when they are connected by the ONVIF protocol (see Notes on configuring video cameras connected via ONVIF).

Virtual joysticks are controlled as follows:

1. Click and hold down the left mouse button in the central (blue) portion of the joystick.
2. Drag the joystick in the necessary direction.

> **Note**
>
> You can also move the joystick by clicking and holding the left mouse button outside of the joystick border.
>
> The turn speed depends on the tilt of the joystick: the greater the tilt, the higher the speed.

> **Note**
>
> If you rotate a camera view/viewing tile 180°, you will have PTZ controls inverted.

Patrolling

Patrolling is an automatic change in the position of a camera along a route defined in the camera's presets list.

> **Note**
>
> You can use a cycle macro to set up patrolling (PTZ camera tour, see Switching to a PTZ camera preset, Wait for timeout, Cyclical macros).

Patrolling must be activated in camera settings (see The PTZ Object). In this case, the operator can stop patrolling by clicking the **Patrol** button on the PTZ control panel. After the manual PTZ control session is over, patrolling will resume automatically.



If patrolling is switched off in camera settings, you can switch it on by clicking the **Patrol** button.

> **Attention!**
>
> Manual control takes priority over automatic control. Any interference in the patrolling process cancels it.

To stop patrolling, click the **Patrol** button again.

> **Note**
>
> Any user (regardless of priority, see Creating and configuring roles) can stop patrolling.

Patrolling will automatically stop when a manual PTZ control session is over, or after you close the PTZ control panel.

> **Note**
>
> Control session automatically stops after a set idle time (see Configuring PTZ control).

Controlling Focus, Iris and Optical Zoom

To control focus, iris and optical zoom, use the corresponding sliders.



To control focus, iris, and optical zoom, move the corresponding slider up or down.

If the camera has AF (auto focus), you can see the corresponding  button under the slider.



Some devices allow to control optical zoom with the mouse scroll wheel.

To control optical zoom with the mouse, go to OnScreen PTZ mode (see Controlling a PTZ Video Camera in the OnScreen PTZ Mode), otherwise the zooming will be digital (see Digitally Zooming Video Images).

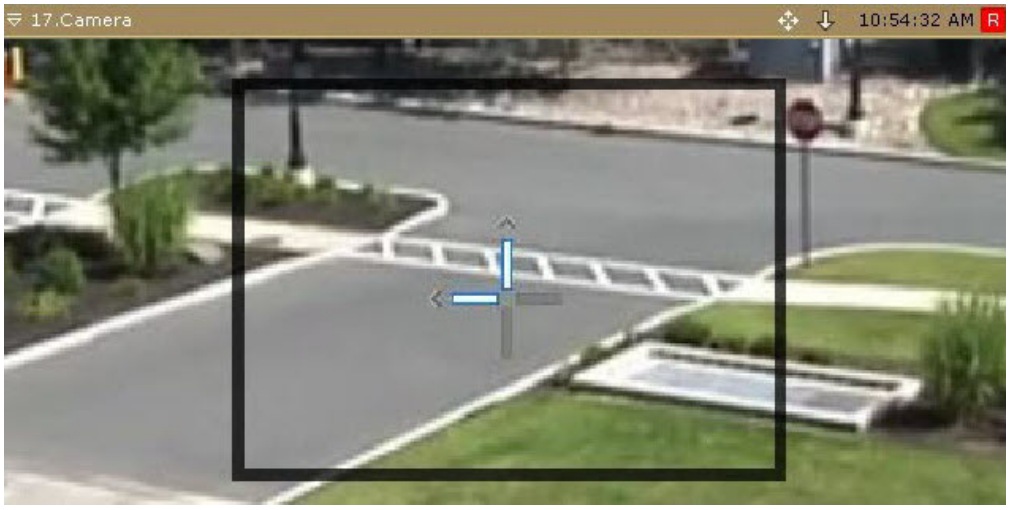
Controlling a PTZ Video Camera in the OnScreen PTZ Mode

The OnScreen PTZ mode enables controlling a PTZ video camera by mouse manipulations in the Viewing tile.

Click  to enable this mode.

> **Note**
>
> In OnScreen PTZ mode, the Areazoom function is disabled (see Control using Areazoom).

To change the viewing angle, click on a video image with the left mouse button and move the mouse pointer in the required direction. During this action the software displays a visual element on the image showing the camera lens movement direction and speed.



The faster you move the mouse, the faster the camera rotation will be.

Click  again to disable the OnScreen PTZ mode.

Control using Point&Click

To change the focus of the camera lens, left-click anywhere within the video image in the viewing tile.

Attention!

To operate Point&Click, go to **OnScreen PTZ** mode (see Controlling a PTZ Video Camera in the OnScreen PTZ Mode).

Once you have done that, the focus of the camera lens will automatically change to the selected area. The focus is changed using *Axxon One* algorithms.

Note

This function is available for only some CCTV cameras.

For more information, contact AxxonSoft.

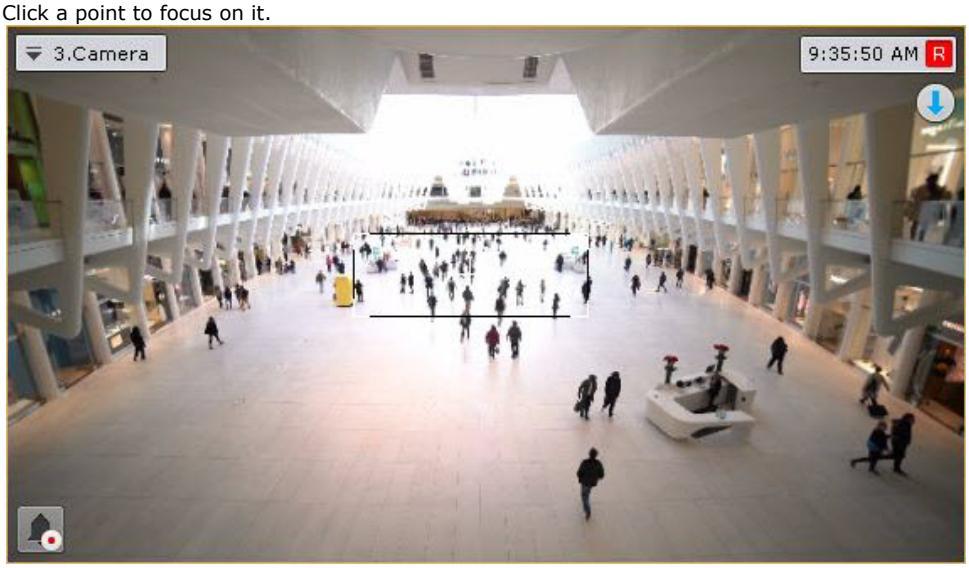
Control using Areazoom

You can focus on a particular area in a video frame.

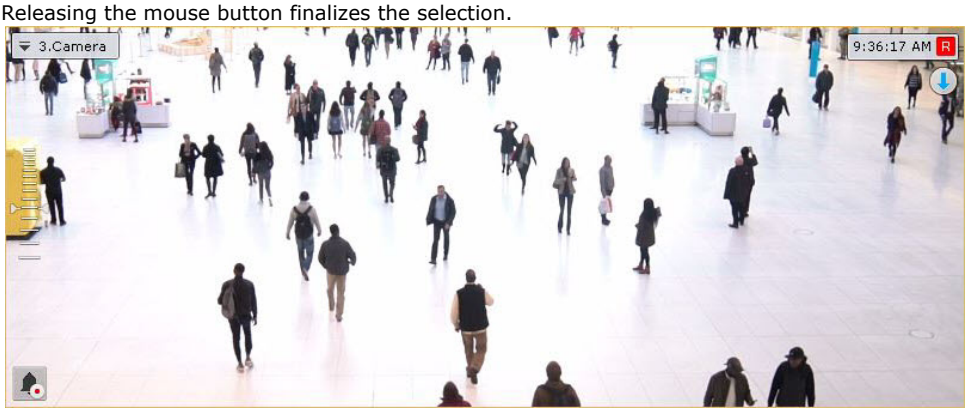
> **Note**
>
> Areazoom function is unavailable if the **OnScreen PTZ** mode is enabled (see Controlling a PTZ Video Camera in the OnScreen PTZ Mode).

To do so:

1. Click a point to focus on it.



2. Holding down the mouse button, moving outward from the center of the focus area, the user sets the size of the area. Releasing the mouse button finalizes the selection.



The lens is reoriented and the image is enlarged so that the selected area now fills the entire viewing tile.

> **Note**
>
> This function is available for only some CCTV cameras.
>
> For more information, contact AxxonSoft.

Functions for tracking of moving objects

Axxon One includes several features for tracking moving objects.

With Tag & Track, an object can be tracked by a PTZ camera under the guidance of panoramic cameras**.**

With Tag & Track Lite, the operator is alerted to the camera in front of which the moving object is most likely to appear next. The camera is predicted based on object trajectory and mapping of cameras to map locations.

Tag&Track Pro

Tag&Track functionality depends on the PTZ mode that is specified in the settings.

Attention!

- If manual or control priority mode is selected, for Tag&Track Pro you must activate object tracking in the viewing tile of the overview camera (see the Tracking objects section).
- The use of fish-eye cameras is not allowed.

- If automatic mode is selected, the PTZ camera will track all active objects. In this case the PTZ camera switches focus between each object with the specified dwell time.

  Note

  The PTZ camera is positioned so that the moving object is in the center of the frame.

- In manual mode, the PTZ camera tracks an object only after the object is manually selected in the viewing tile (left-click to track). If you click anywhere in overview camera's FOV that contains no tracks, the PTZ camera cancels object tracking and focuses on the specified point.



- If control priority mode is selected, the PTZ camera automatically tracks an object until another object is manually selected for tracking in the viewing tile. If an object is deselected (by clicking again) or if it leaves the field of view of the PTZ camera, automatic mode is re-activated.
- If the PTZ camera is in manual mode, the user controls it with on screen or with a joystick / CCTV keyboard. If the user does not operate the PTZ camera (The PTZ Control Panel hidden), then the Automatic mode is used.

Note

Tag&Trac Pro cannot be used with the OnScreen PTZ mode simultaneously (see Controlling a PTZ Video Camera in the OnScreen PTZ Mode).

Tag & Track Lite

Attention!

- For Tag & Track Lite to work, you must activate object tracking in the viewing tile (see the Tracking objects section).
- The use of fish-eye cameras is not allowed.

Tag & Track Lite works as follows:

1. The operator left-clicks an object to start tracking it (the object is outlined with a white frame).



2. After the selected object leaves the field of view of the camera, the video camera's location on the map and trajectory of the object are used to predict the camera in front of which the object is **likely to appear**.
3. The viewing tile of that camera is activated. If the current layout does not contain that camera, a minimal layout with the camera is shown.

   Note.

   If the viewing tile for that camera is currently in archive mode, the tile is switched to Live Video mode and made active.

   Note.

   If video in the viewing tile of the original camera is magnified and the predicted camera is not in the layout, the viewing tile with the camera is made active and the same degree of digital zoom is applied.

   Attention!

   Tag & Track Lite merely predicts, and therefore cannot guarantee, that the object will appear in front of a given camera.

4. To continue tracking the object, select it again in the camera window.

Simultaneously using Tag & Track Pro and Tag & Track Lite

In some cases, it may be useful for Tag & Track Pro and Tag & Track Lite features to be active at the same time.

For example:

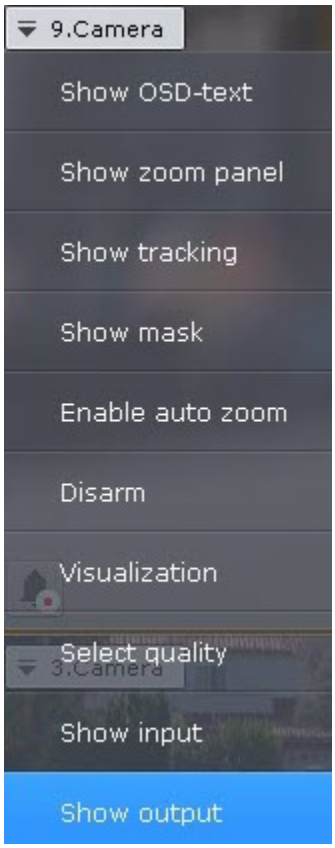
- In Tag & Trac Pro, manual or control priority mode is selected for the PTZ mode.
- In Tag & Track Lite, an object is selected in the field of view of the camera that is designated as the overview camera for Tag & Track Pro.

In this case, both features are active: the object will be tracked by the PTZ camera and its trajectory will be used to predict the camera in front of which it will appear next.

Managing Outputs

To control a output, select **Show output** in the context menu of the viewing title.

> **Note**
>
> You must first activate an object before you can control its output.



This opens **Output Switch**.



> **Note**
>
> To hide **Output Switch**, select **Hide output** in the context menu of the viewing tile.

You can toggle the output state by clicking the radio button.

> **Note**
>
> If a output is controlled by several operators simultaneously, the output will remain activated as long as at least one operator requires it.

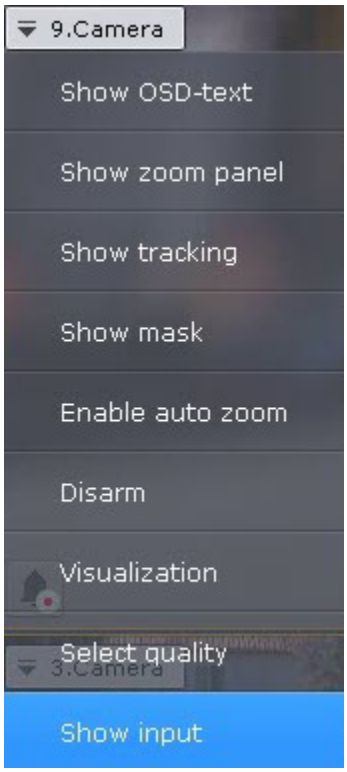
Output Switch	Output status
	Normal

	Activated

Displaying the input status

To display the status of a video camera’s input, select **Show input** in the context menu of the viewing tile.

> **Note**
>
> You must first activate an object to display the status of its input.



The status of the input will now appear in the viewing tile.

> **Note**
>
> To hide the input status, select **Hide input** in the context menu of the viewing tile.



There are four possible statuses of a input.

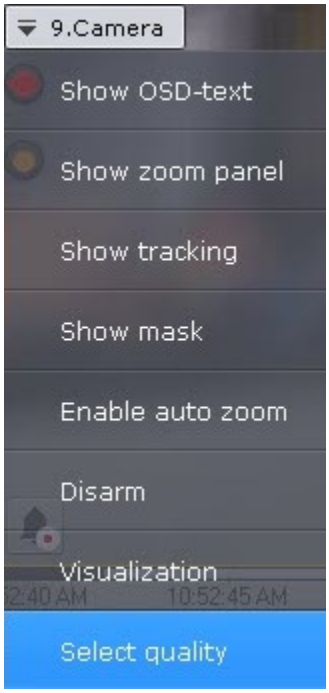
Input status	Description
	Video camera is armed, input is in normal status
	Video camera is armed, input is in alarm status
	Video camera is disarmed, input is in normal status
	Video camera is disarmed, input is in alarm status

Selecting video stream quality in a Surveillance window (GreenStream)

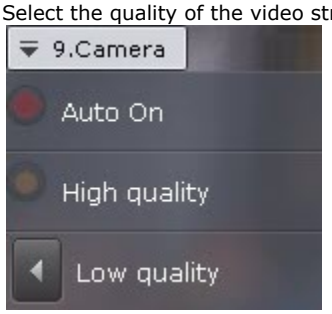
If the video camera supports multistreaming, you can select the quality of the video stream that you want to display in viewing tiles.

To select the video stream quality, do as follows:

1. In the context menu of the viewing tile, select the **Select quality** item.



2. Select the quality of the video stream that you want for display in the viewing tile.



Menu item	Description

Auto (GreenStream, default)	Algorithm for displaying a video stream in the video surveillance window if there are several streams in the camera (see The Camera object): **a.** a suitable video stream is selected using the following algorithm: **i.** determine the available space for video output on the layout; **ii.** select the video streams for which the **Use for GreenStream** option is enabled (see The Camera object) and sort them in ascending order of the original video width; **iii.** for each stream: • reduce the original height and width while maintaining the proportions so that the new height and width do not exceed the available space for video output on the layout; • if the size of the stream after inserting it into the output area does not exceed 110% of the original size, select this stream for further output. **b.** select the stream that has the highest frame rate among other suitable video streams of the same resolution; **c.** if several video streams were selected in the previous steps, select the video stream with the maximum bitrate among them. If a stream was selected based on the maximum bitrate, then another stream will be selected only if its bitrate is more than 5% higher than the current one (to eliminate frequent switching if the values are approximately equal). When changing the characteristics of video streams, the decision to change the stream to display is made only if the need for a change is confirmed within 35 seconds. This measure is also intended to eliminate frequent switching of video streams. When the video surveillance window is enlarged, it switches to a high-quality video stream.
High quality	Algorithm for displaying a high-quality video stream in the video surveillance window if there are several streams in the camera (see The Camera object): **a.** select the video streams for which the **Use for GreenStream** option is enabled (see The Camera object); **b.** among the selected video streams, select those that have the highest resolution; **c.** among the selected video streams with the highest resolution, select the one with the highest frame rate; **d.** if several video streams were selected in the previous steps, select the stream with the maximum bitrate among them.
Low quality	Algorithm for displaying a low-quality video stream in the video surveillance window if there are several streams in the camera (see The Camera object): **a.** select the video streams for which the **Use for GreenStream** option is enabled (see The Camera object); **b.** among the selected video streams, select those that have the lowest resolution; **c.** among the selected video streams with the lowest resolution, select the one with the highest frame rate; **d.** if several video streams were selected in the previous steps, select the stream with the minimum bitrate among them.
Other	You can select a specific video stream from a video camera to display in the video surveillance window.

3. Click in the area between the tiles.

Selection of the video stream quality in the viewing tile is complete.

Autozoom

The **Autozoom** function performs automatic control of digital zoom.

If a viewing tile is inactive and autozoom is enabled, the following actions occur:

1. The smallest rectangular area that contains all tracked objects (even if object tracking is disabled) is chosen.
2. Maximum digital zoom is performed for the selected area.

If autozoom is enabled but there are no moving objects in the video frame, the contents of the viewing tile are shown at their original size.

Note

If the Fit screen function is activated for a viewing tile, the default digital zoom level is used.

Autozoom stops when a viewing tile is selected and resumes when the viewing tile is no longer active.

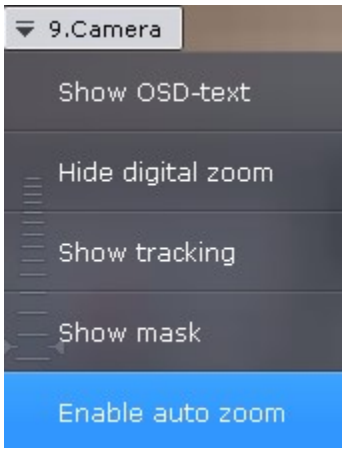
Autozoom can be enabled both for a single camera and for all video cameras in a layout.

To enable autozoom for a specific camera, in the viewing tile context menu, select **Enable auto zoom**.

Important

Autozoom is available if:

1. the object tracker is activated for this camera (see General information on the standard detection sub-tools).
2. the Video Motion Detection tool is activated (see Configuring the Motion detection).
3. at least one of the Embedded Analytic tools is activated (see General information about embedded detection tools).

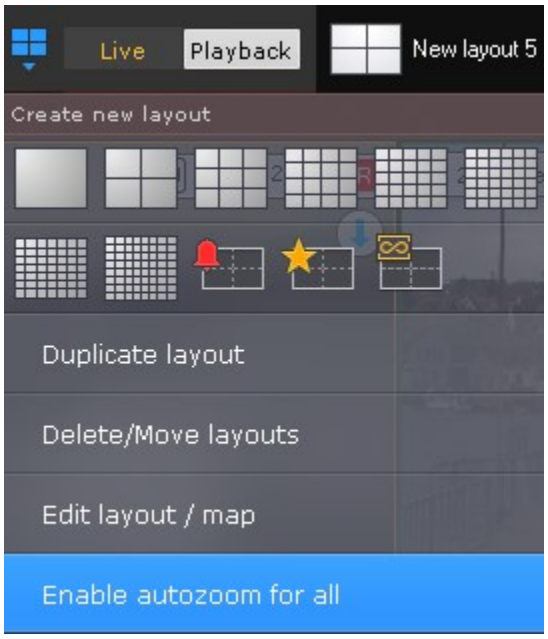


Note

Autozoom resizing takes into account objects from all tracking sources that are activated for a particular video camera.

To disable autozoom, select the corresponding command in the viewing tile context menu.

To enable autozoom for all cameras in a layout, select **Enable autozoom for all**.



To disable autozoom for all cameras in a layout, select **Disable autozoom for all**.

Note

If autozoom is activated for one or more cameras in a layout, by default the menu displays the **Disable autozoom for all** option.

Note

When you switch to the layout editing mode, the auto zoom is disabled for all cameras.

Autoreplace Offline Cameras on Layouts

If the main camera goes offline and a sub camera is defined in the settings (see The Camera object), they are automatically replaced: the sub camera shows in the tile in place of the main one.

Cameras are swapped across all layouts in the system.

When connection restores, changes are automatically undone.

Snapshot

In Live Video mode, you can "freeze" video. To do so, click the time display (scrubber) in a viewing tile.

This will cause the viewing tile to be highlighted with a blue border. A snowflake icon will appear in the time field.



To return to live video, click the display again.

Viewing selected camera's detection tool triggering events

You can get quick access to selected camera's detection tool triggering events from any layout. To do it, follow the steps below:

1. Select a camera on the layout.
2. Click the **Events** button on the right margin of the screen.
   An events panel (see Working with Event Boards) opens containing detection tool triggering events for this camera only.



To hide the panel, click again the **Events** button.

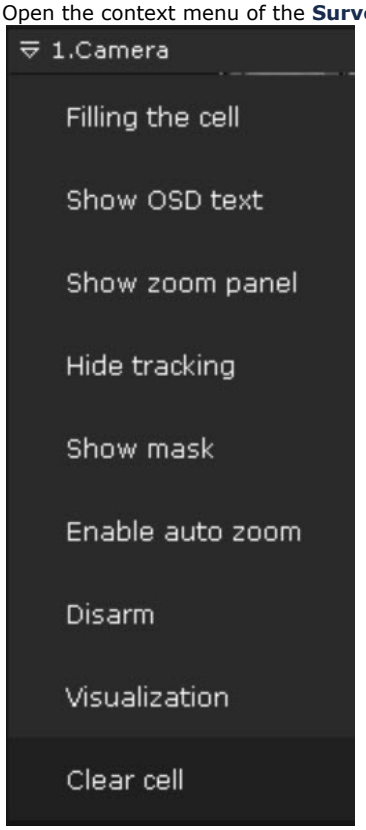
Removing a camera from a layout

You can remove a camera from any layout.

> **Attention!**
>
> Changes aren't saved and the original layout will be available when you switch layouts or the next time you start the Client.

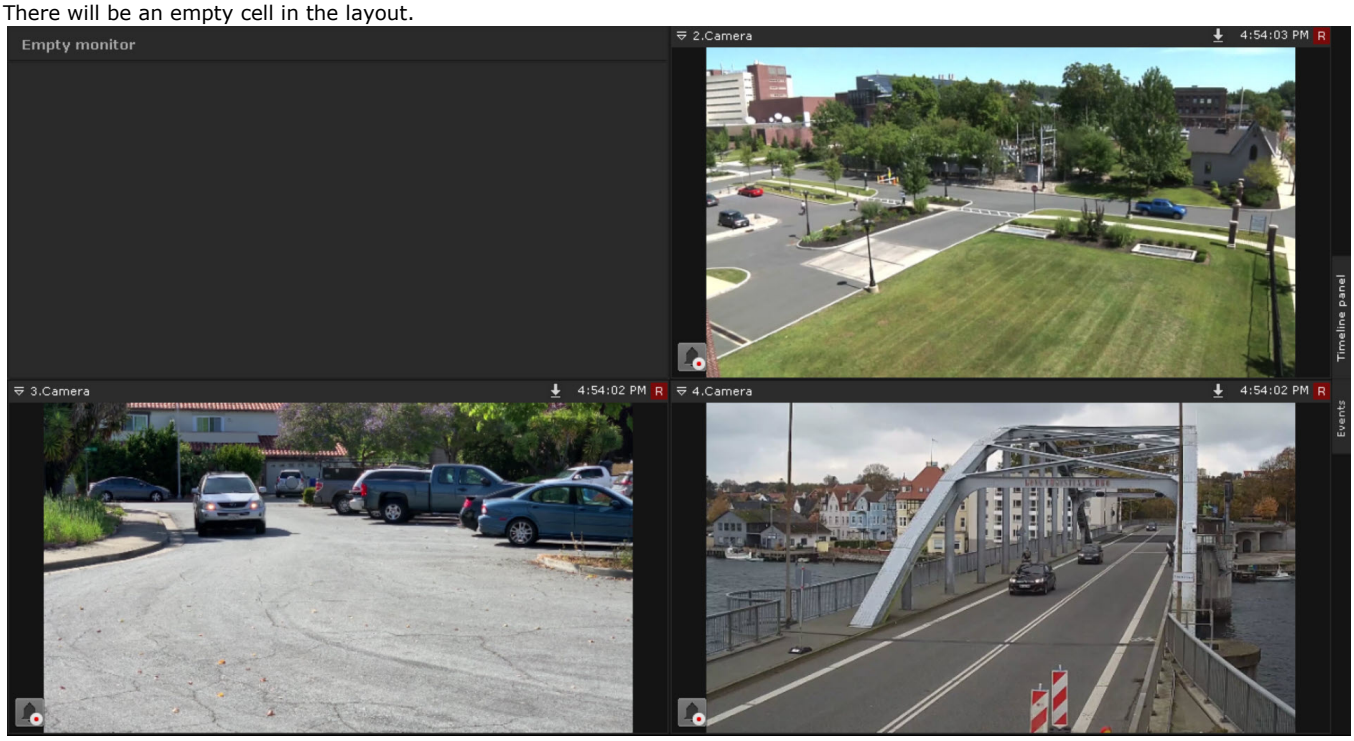
To remove a camera, do the following:

1. Open the context menu of the **Surveillance window**.



2. Select the **Clear cell** item.

There will be an empty cell in the layout.



You can further drag a camera to a cell from the **Objects panel**, **Camera Search Panel**, or using an interactive map (see Adding cameras to cells).

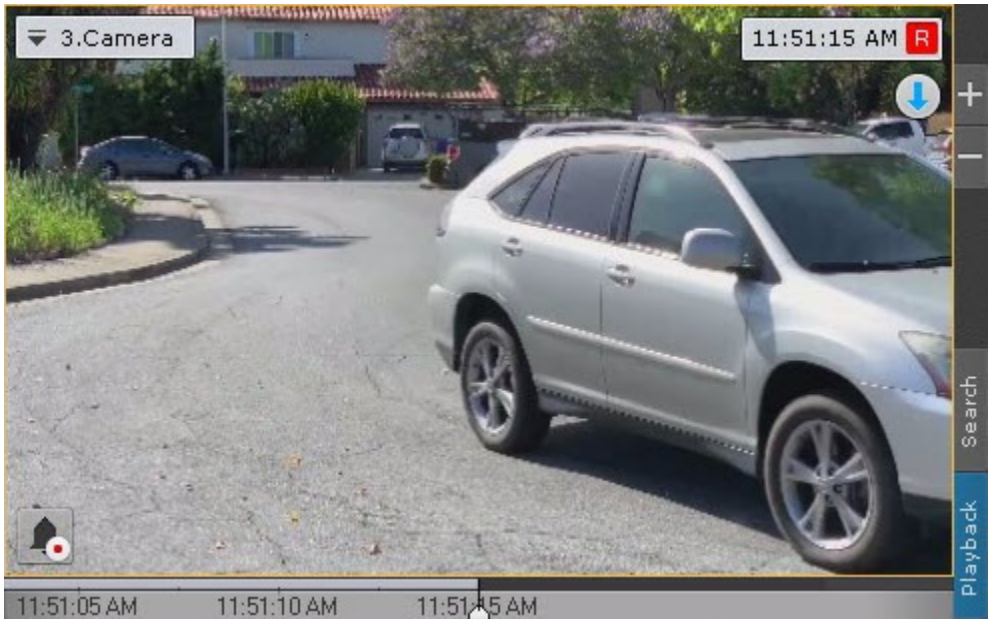
Video surveillance in archive mode

Switching to Archive Mode

To switch from a different surveillance mode to the Archive mode, click the **Playback** tab in the lower-right corner of the Camera Window.

Note

- If a camera is not linked to a video archive and has no on-board storage, this tab will be not available.
- If the video camera is in archive mode and the video is paused, then after you drag another video camera into its place (from the object tree, search panel or map), the new video camera will remain in archive viewing mode, and the video will be paused. If the video is playing, the new camera will also be displayed in the archive view mode and the video will be played.

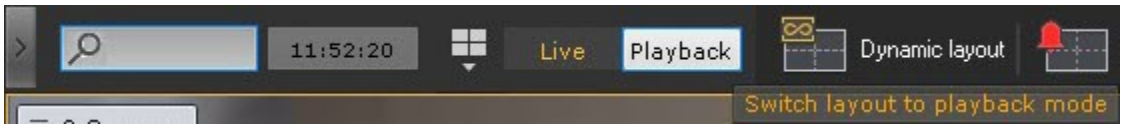


You can also switch from Live Video mode to Archive mode using the advanced archive navigation panel (see Advanced Archive Navigation Panel).

Note

In Live Video mode, if the viewing tile is not active, the tabs for switching to other modes and the advanced archive navigation panel are not displayed. To display them, click on the video surveillance window with any mouse button.

To switch all cameras within a layout to Archive mode, click the **Playback** button on the upper panel.



To return to live viewing, click **Live**.

Furthermore, if all cameras within a layout are in Live Video mode, you have to open the Archive navigation panel to switch the cameras to Archive mode (see Show and Hide the Archive Navigation Panel).

Note

If archive mode is selected as the default video mode for a camera in a layout, when you switch to that layout, the camera is immediately in archive mode (see Selecting the default video mode for a camera).

On first access to Archive mode, the most recently recorded video will be selected on the timeline (see The Timeline). On further accesses to a particular camera archive, the timeline indicator will show the position of the most recent video in the Archive.

Attention!

If you prefer to open the most recently recorded video when accessing the Archive (Video Footage), create a ResetArchivePosition parameter in the following registry key on the Client: HKEY_LOCAL_MACHINE\SOFTWARE\AxxonSoft.

Click  to create a temporary layout for Archive (video footage) viewing.

The temporary layout is not preserved after you switch to any other layout.

Video Surveillance Functions Available in Archive Mode

In archive mode the following video surveillance functions are accessible:

1. Autozoom.

   > **Note**
   >
   > Refer to section Real-time video surveillance for a description of switching to the results of a saved search query and the **Autozoom** function.

2. Selecting an archive for viewing of recordings.
3. Synchronized playback of archives.
4. Compressed playback of archives.
5. Viewing recorded video with operator comments.
6. Viewing external archives.
7. Navigating through the archive.
8. Displaying why Scene Analytics detection tools have been triggered.
9. Viewing the results of a saved search query.
10. Manual archive replication.
11. Tag&Track Lite.
12. Functions Available in All Video Surveillance Modes.

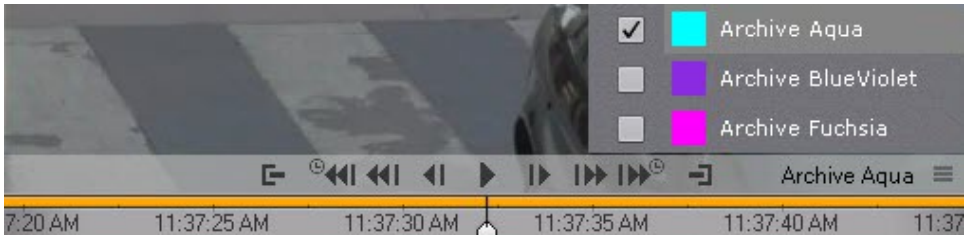
Selecting an Archive

You can select video footage to view only if the camera is recording to several archives.

If you do not select an archive, the default archive is played back (see Configuring recording to an archive).

To select another archive for playback:

1. Click the archive name or the button on the advanced archive navigation panel.
2. Select the required archive from the list.



Note

You can select all available Mirror Archives (if any, see Configuring data replication) and on-board storage (if enabled, see The Embedded storage object).



You can now view video footage from the selected archive in the viewing tile.

Attention!

The next time you enter the Archive mode, the selected (not default!) archive will be displayed.

Note

If there is no recording in the selected archive, a message to that effect will appear in the viewing tile.

Viewing a combined Archive

In some cases, you might need to record videos from a single camera into multiple Archives.

For example, videos triggered by Detection Tool #1 go into into Archive #1, and videos triggered by Detection Tool #2 are recorded into Archive #2.

For more user convenience, *Axxon One* offers an option to visually combine records from different Archives.

To view a combined Archive, you need:

1. Go to the Archive selection menu (see Selecting an Archive).
2. Check boxes for the Archives to be combined.



Records from all checked Archives will appear on the timeline. You can apply any system function to a combined Archive.

Note

Clicking on a particular Archive brings you to viewing videos from this Archive only.

Note

If you select multiple archives for a particular camera, and then switch all the layout to Archive mode, all cameras will be set to multi-archive display.

When combining multiple streams from the same camera into one Archive, the highest quality stream is prioritized.

For example, if:

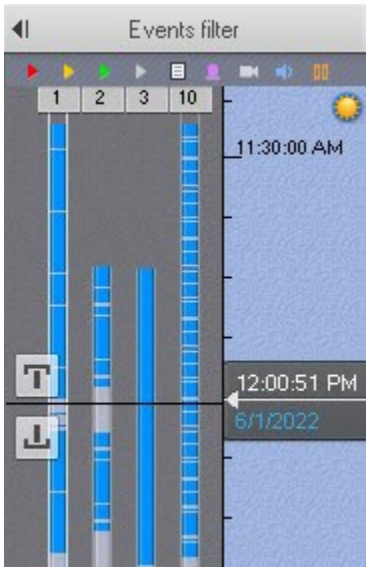
- a lower quality video stream is permanently recorded into Archive #1,
- and a high quality video stream is recorded into Archive #2 by VMD,

then the combined Archive will consist of high quality motion-triggered records and low quality "other" videos.

Synchronized playback of archives

Synchronized playback of archives lets you play back archives from several different video cameras simultaneously.

To enable synchronized playback, switch a few video cameras into archive mode. The timeline will then display time axes for the corresponding archives.



Synchronized archive playback is controlled through the playback panel in the same way as playback for a single archive.

Compressed playback of archives (TimeCompressor)

During compressed playback (TimeCompressor), the viewing tile simultaneously displays tracked objects from different moments in time within the selected portion of the archive. This lets you quickly look through the archive to find important events and investigate them in more detail.

For condensed playback of archived video from a camera, the following conditions must be true:

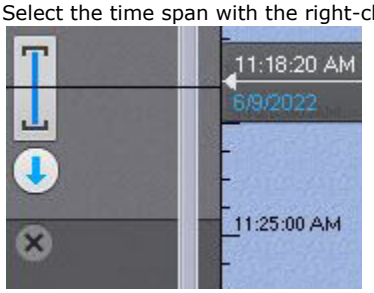
1. Camera is bound to an archive (see Configuring recording to an archive).
2. The camera must have at least one active source of metadata (Object Tracker, Video Motion Detection, Embedded Analytics).

> **Attention!**
>
> For the Object Tracker, you have to select the video stream currently selected for Video Footage recording (see Setting general parameters of Tracker-based Scene Analytics detection tools).

Switching to TimeCompressor mode

To use TimeCompressor, complete the following steps:

1. You can set the time span for viewing video in TimeCompressor on the timeline in one of the following ways:
    a. Set the pointer to the start position. In that case you view the whole archive to the end of it (see the section titled Navigating Using the Timeline).
    b. Select the time span with the right-click.



> **Note**
>
> The TimeCompressor mode allows you to view the results of a specific archive search (see Viewing Search Results In TimeCompressor).

2. Click the  button on the advanced archive navigation panel.

The archive will now start playing in compressed mode.



> **Note**
>
> Only one video camera can run TimeCompressor at one time. If synchronized playback is started and a video camera is switched to TimeCompressor mode, playback of all other video cameras will be automatically paused.

Note

To switch back to the standard archive browsing mode, click the displayed area of the advanced archive navigation panel  .

Playback control

Playback control in TimeCompressor mode is managed using the advanced navigation panel and the playback panel.

To set the desired number of tracked objects to be simultaneously displayed, set the slider in the appropriate position (**1**). The extreme left position of the slider corresponds to two objects, the extreme right – sixteen.



Note

Once you have configured this setting, playback begins at the beginning of the selected interval.

Note

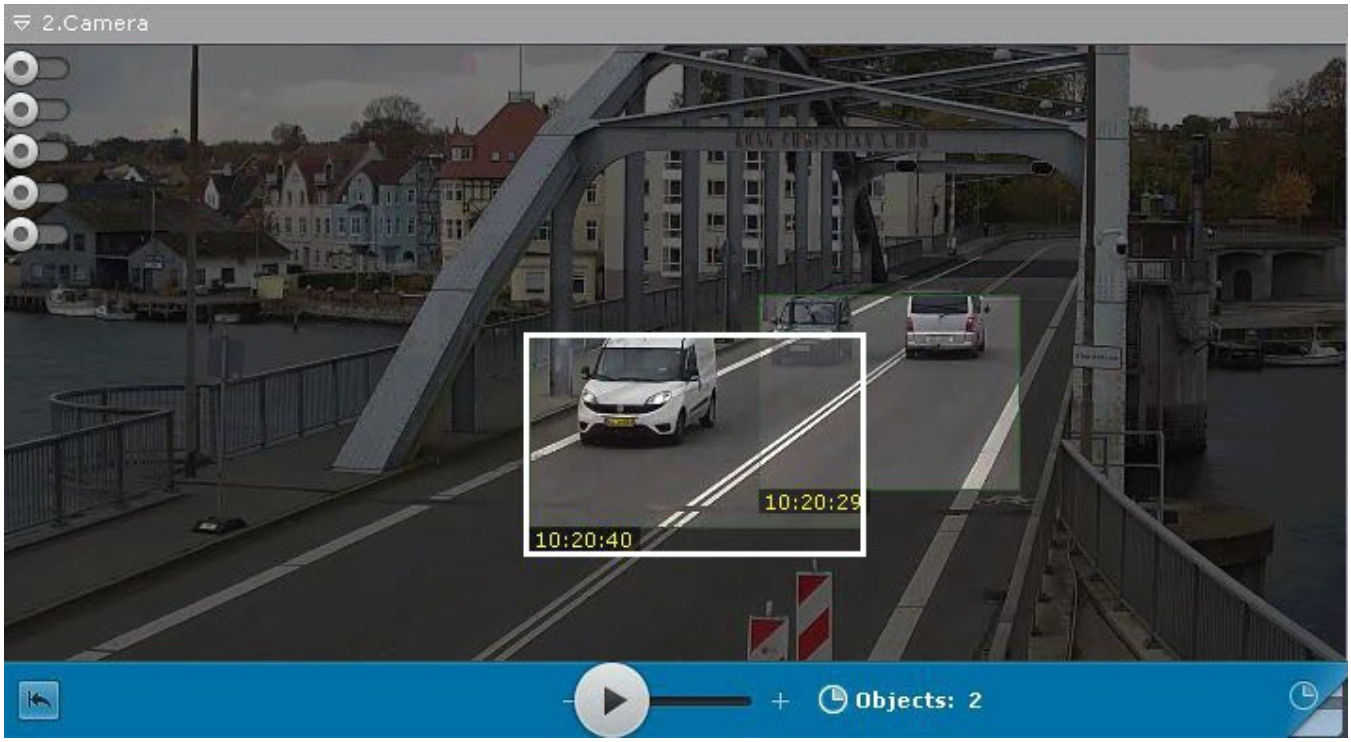
However, according to the logic of the algorithm, the number of displayed objects may be greater.

To stop or start playback, use the  and  buttons on the playback panel or the identical buttons on the advanced navigation panel.

To start archive playback in TimeCompressor mode starting at the beginning of the selected interval, click the  button (**2**).

Switching back to the original recording of an object

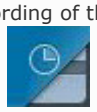
To leave TimeCompressor mode to go back to the original recording of an object, left-click the object.



The system will now automatically switch back to the original recording of the object in standard archive playback mode. Playback of the recording will be paused, and the beginning of the recording will correspond to the moment at which the object was selected.

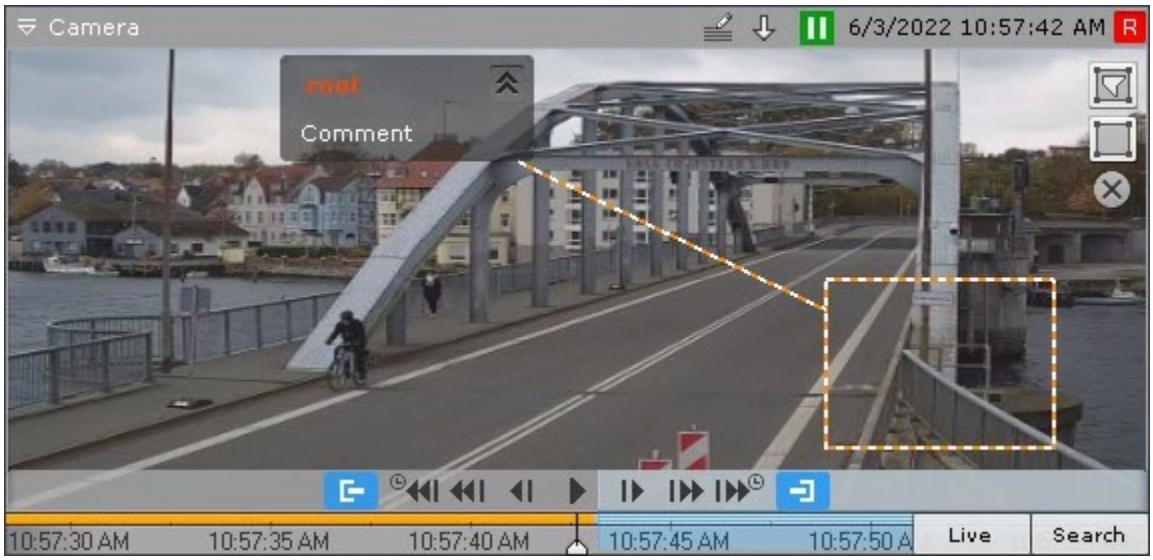
The period during which the objects remains in the camera's field of view is displayed in the viewing tile.

Note

Once you have switched back to the original recording of the object, you can return to TimeCompressor mode to the place where the switch was made. To do this, click the  tab. In this case, playback in TimeCompressor mode will be paused.

Viewing recorded video with operator comments

Operator comments are displayed when recorded video is played back in a viewing tile.



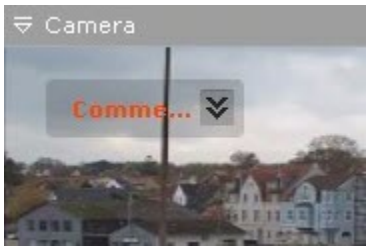
Comment text begins display five seconds before the frame for which the comment was added (before the first frame, if the comment was set for an interval), with gradual outlining of the area (or point) that was specified when adding the comment.

When the commented frame is shown or during the commented interval, the area (or point) is also highlighted,



Five seconds after the commented frame (after the end of the interval, if the comment was for an interval), the comment is hidden.

To minimize comments and the displayed area, if any was specified, click the  button.



To return to the full comment, click the  button.

Viewing External Archives

External Archive is time-referenced video footage (see Importing video to Axxon One).

If you go to Archive mode, the timeline shows available video recordings. If there is no time overlapping for video recordings, the space between them is blank.

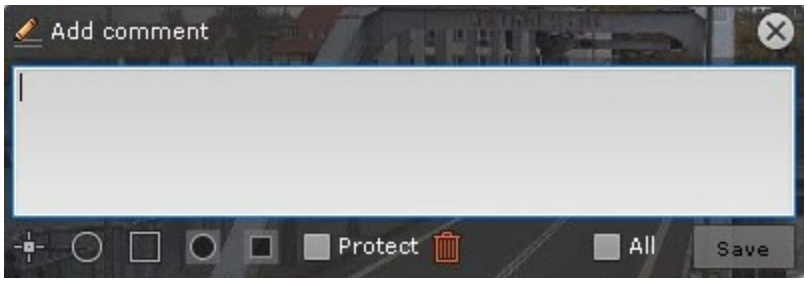
If video recordings overlap, they are displayed as one track that spans from the beginning of the first video clip to the end of the second.

If you want to watch this track, both video clips are played sequentially and in full.

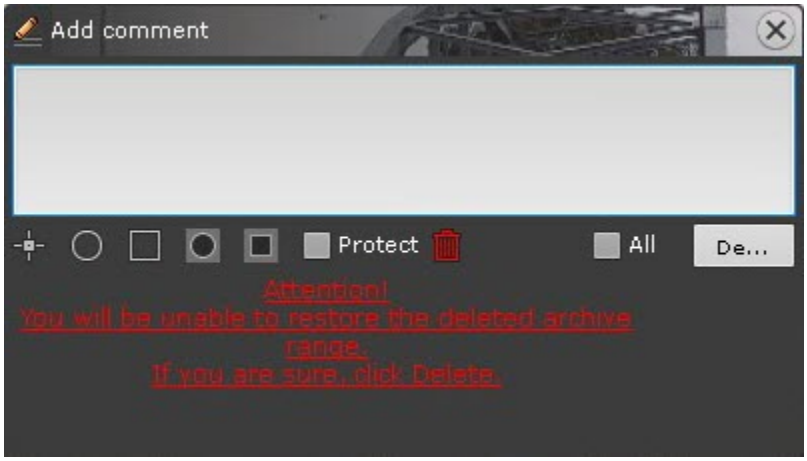
Delete a part of an archive

You can delete an arbitrary part of an archive. To do this:

1. Set the time interval for the footage to be deleted from the archive:
   a. on the main timeline, set the indicator to the beginning of the interval, click the button, then set the indicator to the end of the interval and click again; as an alternative, you can right-drag the mouse over the required interval. To delete the interval, click ;
   b. on the additional navigation panel, you can set the time interval the same way using the buttons. You cannot set the interval with the mouse on the additional panel.
2. Click in the Camera window.



3. To delete footage within the specified time interval for all cameras within the archive, check the **All** box .
4. Click .



5. Click the **Delete** button to confirm the deletion.

> **Attention!**
>
> You cannot recover deleted footage.

> **Attention!**
>
> If several archives were selected for viewing (see Viewing a combined Archive), the footage will be deleted from all of them.

After the deletion is complete, the remaining footage may contain some artifacts near the cut points.

Navigating in the Archive

You can navigate in the archive using the following interface elements:

1. Timeline.
2. Advanced navigation panel.
3. Events list.
4. Playback panel.
5. Time indicator.

You can also navigate through the archive by easily flipping through recordings.

Navigating Using the Timeline

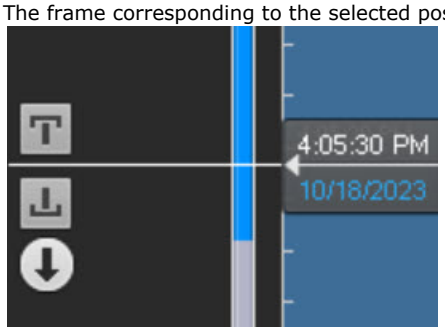
> **Note**
>
> Use of the timeline is described in detail in the section The Timeline.

You can select recordings in the archive for playback in a viewing tile by using the timeline, in one of two ways:

1. Left-click the indicator and drag it to the corresponding position on the timeline. Alternatively, you can left-click the left portion of the timeline.

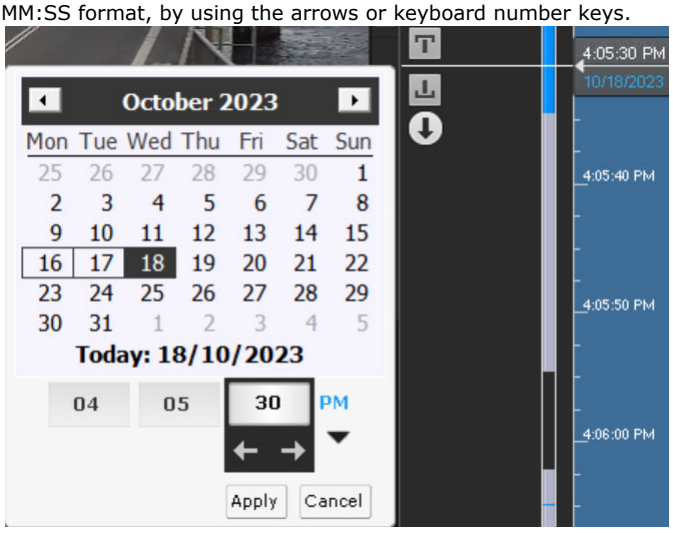
   > **Note**
   >
   > The position on the timeline is a graphical representation of a specific moment in time.

   The frame corresponding to the selected position (moment in time) will then be displayed in the viewing tile.

   > **Attention!**
   >
   > If the system clock is shifted back one hour (for example, in winter saving), the videos from the lost hour will disappear from the timeline but remain accessible.
   >
   > For example, at 3 PM the clock is shifted back one hour. If you place the timeline marker anywhere after 02:00:00, videos shot after the shift will be played back.
   >
   > If you set the marker to 01:59:59 or earlier, videos shot from 01:59:59 to 02:59:59 (time stamped before the shift) will be played back.

2. Click the indicator. The calendar opens. Select the date to which you want to jump in the archive and specify the time in HH:MM:SS format, by using the arrows or keyboard number keys.

   > **Note**
   >
   > The Tab key can be used to navigate across various elements of the Calendar.

You are then taken to the specified point in the archive.

If one video camera is in archive mode and you move the indicator to a point for which there is no video, the indicator will automatically go to the video for the closest point in time. If two or more video cameras are in archive mode, you will not be taken to the video for the closest point in time; the message **No archive** will be shown on screen.

To play back the selected recording, use the playback panel (see the section titled Navigating Using the Playback Panel).

Navigation using the advanced panel

You can use the advanced navigation panel to select recordings in the archive for playback in the viewing tile. To do this, complete one of the following two actions:

1. Left-click the timeline and hold down the button while dragging the scale to the desired position.
2. Left-click the desired moment in time on the timeline.
3. Left-click and hold the desired moment in time on the timeline.



When you left-click and hold left the mouse button and the timeline is moved, you can view the corresponding recording in fast forward. The further left you click, the faster is the playback speed.

> **Note**
>
> The current moment in time is determined by the cursor located in the center of the timeline. The position of the cursor relative to the timeline never changes.

Once the selected moment is reached, playback stops. The speed of playback depends on the speed of the timeline's movement.

To start archive playback click  in the middle of the timeline. To pause playback, click the  button or left-click the timeline.

To control playback, use the playback panel (see the section titled Navigating Using the Playback Panel) or the advanced navigation panel.

Playback		Pause	
Item	Description	Item	Description
	Decreases playback speed by one level		Go to the preceding frame
	Decreases playback speed by one level		Go to the next frame
	Go to the previous recording		Go to the previous recording

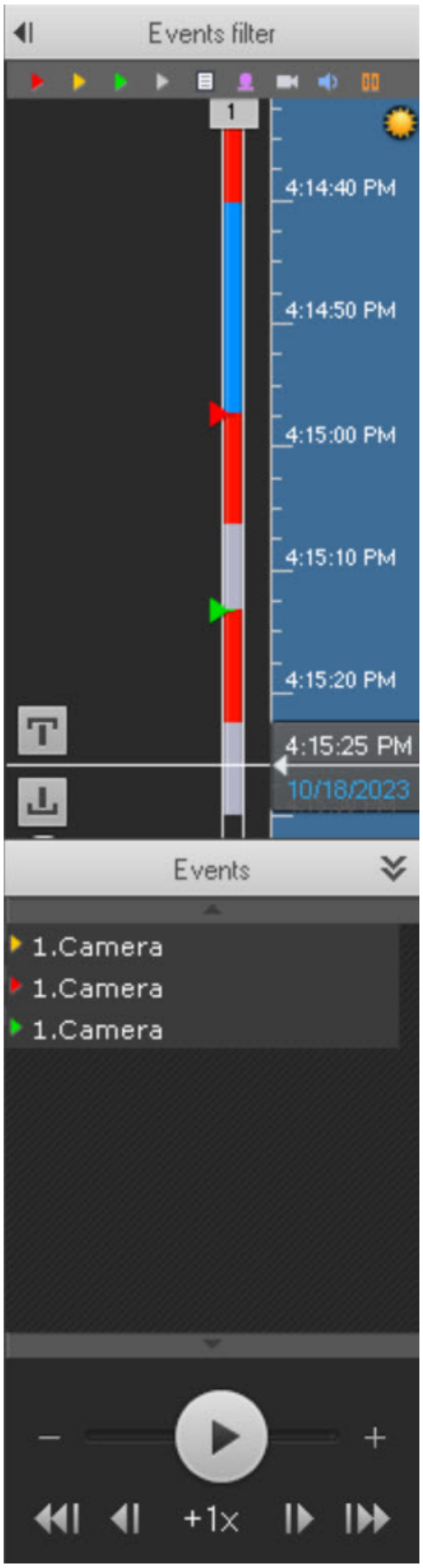
	Go to the next recording		Go to the next recording
	Jump back by N* seconds		Jump forward by N* seconds
*see Navigation using the advanced panel.			

Attention!

Click and hold the  button to jump to the end of the archive.

Navigating Using the Events list

The Events List and the timeline are dynamically linked: when you select an event in the list, the timeline indicator automatically jumps to the selected position.



For details, see the section titled Events List.

Navigating using the Playback Panel

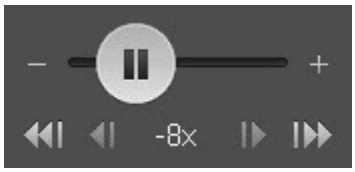
To navigate in the archive using the playback panel, you must first select a recording for playback.

Once a recording is selected, the following operations are accessible:

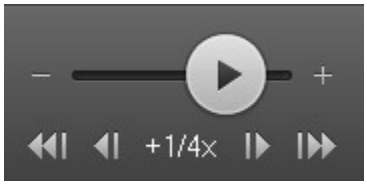
1. Play recording:  .
2. Pause/Stop playback:  .
3. Go to the preceding frame  .
4. Go to the next frame  .
5. Go to the previous recording  .
6. Go to the next recording  .

You can fast-forward/fast-rewind and change playback direction (forward/back).

Fast-rewind playback:



Slow playback:



For reverse playback of a recording, move the slider to the left of the position corresponding to zero playback speed (the center of the slider); for forward playback, move it to the right. The current playback speed is displayed under the slider. During forward playback of a recording, a  sign appears before the speed; during reverse playback, a  sign appears. The value **0X** corresponds to zero speed, i.e., no playback; the value **1X** corresponds to the frame rate of recording.

Tp speed up playback by one step, click  . To slow down by one step, click  . To temporarily change the playback speed, move the slider in the desired direction.

To slow playback N-fold, do as follows:

1. Accelerate playback N-fold.
2. Click the value of the current playback speed below the slider.

This slows the playback N-fold. To return to the fast playback, click the current speed again.

If one camera is in the Archive mode, you can fast forward/backward up to 128 x. If several cameras are in the Archive mode, then you can speed up and slow down playback up to 32 x.

Navigation via the time indicator

The time indicator in a viewing tile can be used to set the time of the current day on the timeline to which you want to navigate in the archive.

To do so, left-click the indicator and specify the time in HH:MM:SS format, by using the arrows or keyboard number keys.



You are then taken to the specified point in the archive.

If one video camera is in archive mode and you try to navigate to a point for which there is no video, you will be automatically taken to the video for the closest point in time. If two or more video cameras are in archive mode, you will not be taken to the video for the closest point in time; the message **No archive** will be shown on screen.

Keyboard navigation

You can use keyboard shortcuts to navigate through an archive and control video playback.

Key or key combination	Resultant action during pause	Resultant action during play
Spacebar	Begins playback	Pauses playback
Ctrl+Spacebar	Uses the current position to set the export interval	Uses the current position to set the export interval
Up-Arrow	Increases playback speed by one level	Increases playback speed by one level
Down-Arrow	Decreases playback speed by one level	Decreases playback speed by one level
Left-Arrow	Moves back to the preceding key frame	-
Right-Arrow	Moves forward to the next key frame	-
Page up	Switches to the preceding recording	Switches to the preceding recording
Page down	Switches to the next recording	Switches to the next recording

Displaying the causes of triggered Scene Analytics detection tools

When positioning the archive in the range [-1 sec.; +1 sec.] from when the Scene Analytics detection tool was triggered, the objects that triggered the detection unit will be marked on the video frame.

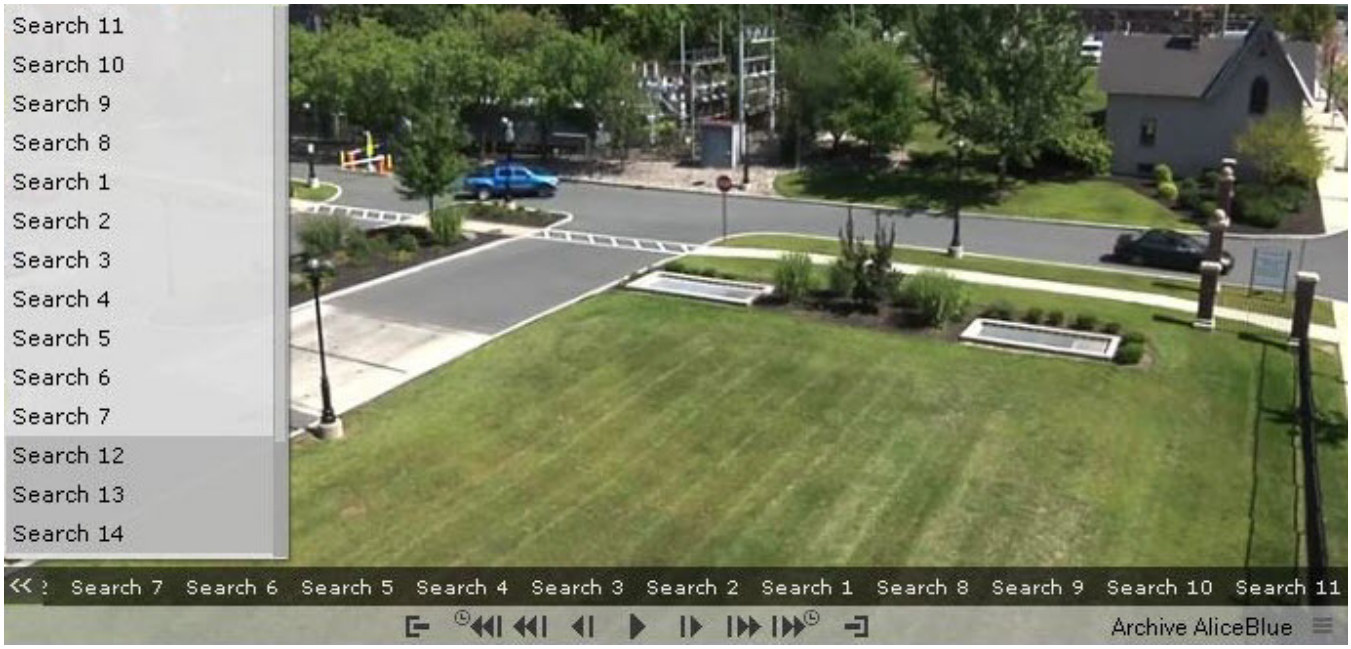


Viewing the results of a saved search query

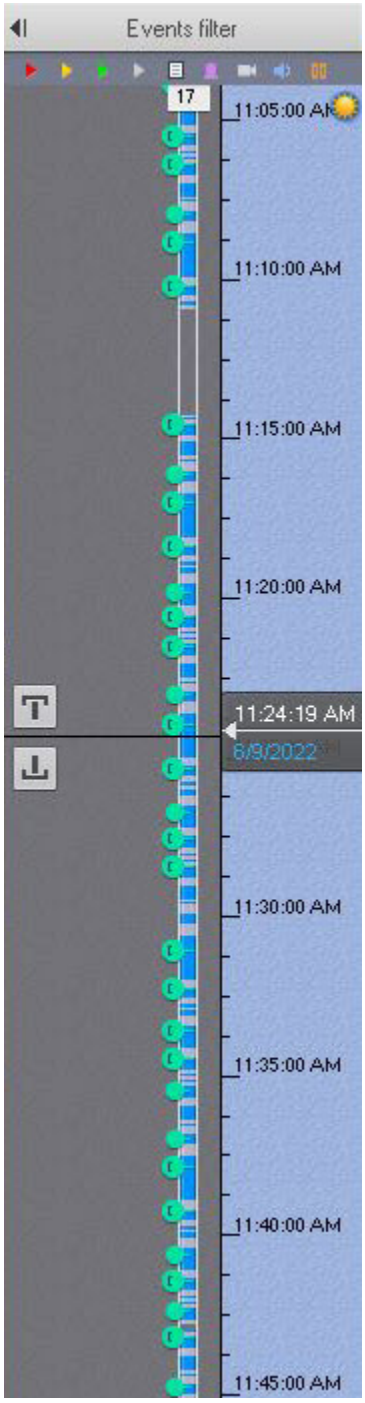
If the system has saved Forensic Search queries for a video camera, tabs for these queries are displayed in the lower-right corner of the corresponding viewing tile.



If not all tabs fit in the viewing tile, a full list of saved Forensic Search queries is available by clicking the  button.



Clicking a tab switches to Archive mode, displaying the results of the relevant search on the timeline (the process is similar to viewing search results in Archive Analysis mode).



The standard Archive mode controls are used for navigating between search results (see Navigating in the Archive).

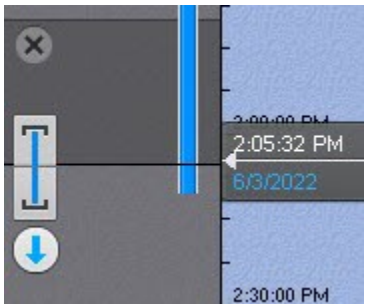
> **Note**
>
> To search in standard archive mode without displaying search results, click the corresponding tab in the viewing tile.

The parameters for the search are displayed when switching from search results to Archive Analysis mode.

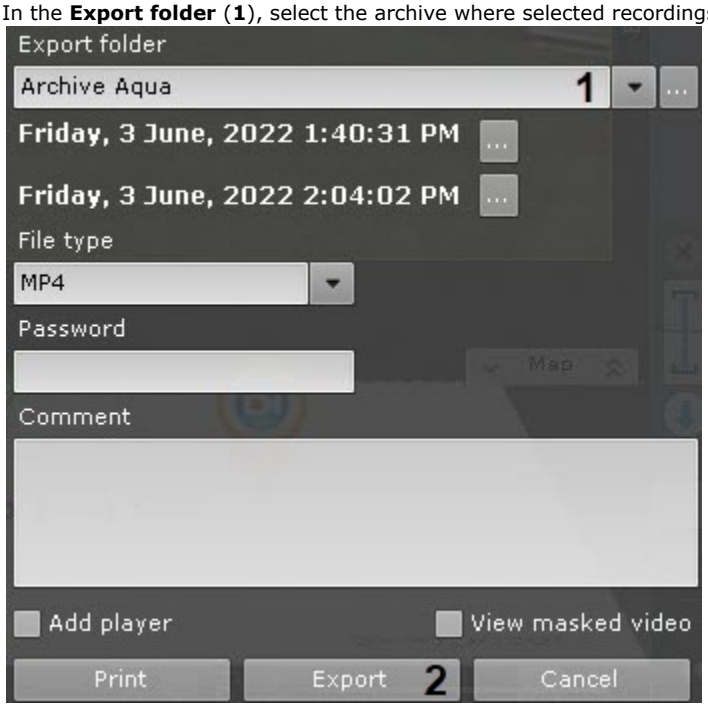
Manual Archive Replication

You can protect selected video recordings from being overwritten. To do this:

1. Create a new archive (see Creating archive) and configure on-demand replication for it (see Configuring data replication).
2. Switch to Archive Mode (see Switching to Archive Mode).
3. Set the time interval on the timeline (see Standard video recordings export). Recordings from this range will be copied to the new file.



4. Click the button  .
5. In the **Export folder** (**1**), select the archive where selected recordings will be copied.



> **Attention!**
>
> You can replicate recorded video only to the "right" end (later point in time) of the archive. It is not possible to overwrite existing data in the archive.
>
> If the selected replication range starts and ends earlier than the starting time of the mirror archive (e.g. you want to copy a hour of video footage from 9 a.m. to 10 a.m., but the mirror archive starts at 11.a.m.), replication will not be possible (the **Export** button is not available).

6. Click the **Export** button (**2**).

Selected recordings have now been copied to the specified file.

Tag & Track Lite in Archive mode

Configuring Tag & Track Lite

Tag & Track Lite

Attention!

- For Tag & Track Lite to work, you must activate object tracking in the viewing tile (see the Tracking objects section).
- The use of fish-eye cameras is not allowed.

Tag & Track Lite in the Archive mode works as follows:

1. Left click an object's track to select the object of interest.



2. The most probable camera where the object **may have been** captured next is suggested.
3. After selecting an object, you are switched to the suggested camera. Camera footage will be played back automatically from the moment when the target object was supposed to appear in the FoV.

Attention!

Tag & Track Lite merely predicts, and therefore cannot guarantee, that the object will appear in front of a given camera.

Video surveillance in alarm management mode

Video surveillance functions available in Alarm Management mode

The following video surveillance functions are available in Alarm Management mode:

1. Forwarding and reversing playback of an alarm at various speeds.
2. Evaluating alarms (assigning a status).
3. Functions Available in All Video Surveillance Modes.

Switch to Alarm Management mode

When an alarm is initiated, the system switches to alarm mode automatically at the moment the event is accepted for processing. Operator can escape the Alarm management mode. To return a viewing tile from a different surveillance mode to Alarm Management mode, in the lower-left corner of the tile, click the  button.



The viewing tile will then appear in **Alarm Management** mode.

If there are multiple alarms for a camera, Alarm Management mode will open to the most recent alarm.

Initiating an alarm event

A system alarm can be initiated in one of two ways:

1. Manually (by an operator).
2. Automatically (when a detection tool is triggered).

> **Note**
>
> You can initiate an alarm only if the specific video camera is linked to the archive.

Manual initiation

To initiate an alarm event manually, do the following:

1. In the lower-left corner of the Surveillance window, click the  button.



2. The operation will initiate an alarm event that will be displayed on the **Alert panel** (see Alert panel). To assess an alarm event, click the  button again.

> **Note**
>
> - When in the Alarm Management mode, the user who initiated the alarm event will be displayed at the bottom of the Surveillance window.
> - An alarm event initiated manually has a medium priority.



Manual initiation of an alarm event is now complete.

Automatic Initiation

Automatic rules or macros can be configured to initiate an alarm (see the section titled Initiating an alarm in the system).

If an alarm is initiated automatically, the **Alert panel** tab is color-coded 

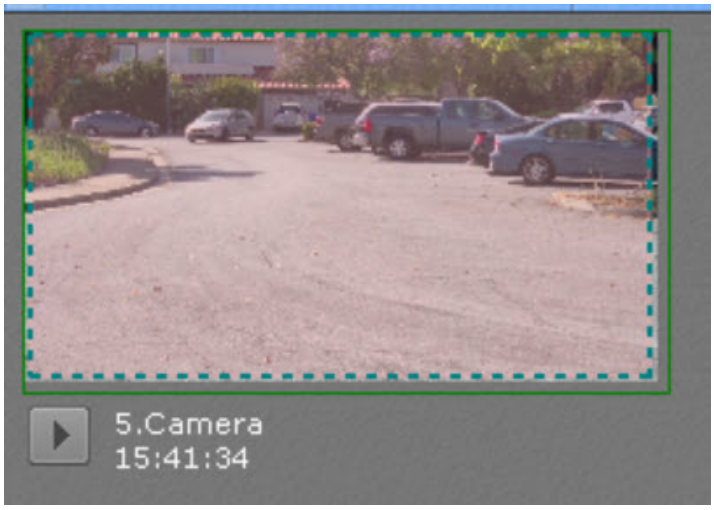
.

To evaluate the situation, click the Alert panel tab, select the event and classify it in Alarms Management (see the section titled Selecting an alarm event for Alarm Management).

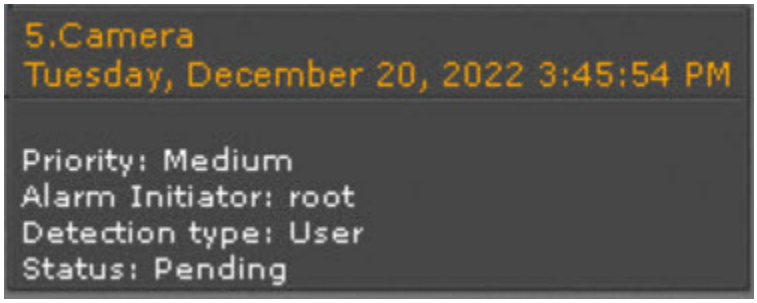
Working with an assessment of an alarm event

Displaying and viewing alarm events

Each alarm event is displayed on the Alarms Panel as follows: the event preview window with the first frame of the alarm event; under the preview window, there is a playback button, time when the alarm event occurred and the name of the video camera.



When you hover the mouse cursor over the event preview window, the additional information about the alarm event is displayed:



When you click the button, the alarm event is cyclically played back in the preview window. To stop the playback, click the button.

When you click the alarm event preview window on the Alarms Panel, the alarm event will be played back in the surveillance window.

If you click the button on the Alarms Panel, the alarm event will be played back on the temporary layout containing only the specified camera.

If you don't click this button, the alarm event will be played back in the surveillance window on the regular layout.

If the Alarms Panel is added to the regular layout, the Alarms Panel will display the alarm events in the top-down priority order. The alarm priority icons will be displayed at the top of the event preview window:

—maximum priority;

—high priority;

—medium priority;

—low priority;

—minimum priority.

Outlining an object that triggered an alarm event

In the Event Preview window, you can outline an object that triggered an alarm event. To do so, click the  button.

> **Note**
>
> The object can be outlined only if the alarm event was initiated by detection tool.

To undo object outlining, click the  button again.

Selecting an alarm event for Alarm Management

When you click the Event Preview window, a layout opens that has the relevant camera's view. The layout is selected automatically with the following algorithm:

1. The system searches for the layouts that contain the selected alarm event and are available for the current user.
2. The system chooses the layout with the minimum number of cells to display the selected video camera.
3. If the required layout does not yet exist, the system creates a new layout with a single video camera.
4. The system switches to the selected layout.
5. The video camera becomes active in the selected layout. The Surveillance window is expanded by one step. It switches to the Alarm Management mode (if you have selected an active alarm) or to the Archive mode (if you have selected a processed or a missed alarm event).

Working with the Alarm Management window

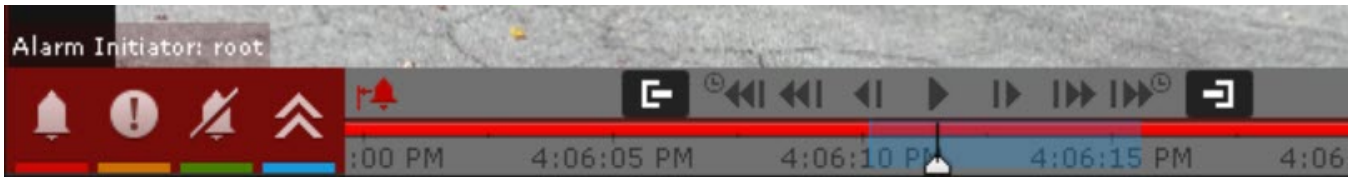
Interface elements of the Alarm Management window

The Alarm Management window is a Surveillance window which contains, besides the standard interface elements (context menu, time indicator, etc.), the elements for alarm event playback and assessment:

1. Playback panel.
2. Timeline.
3. A button for quick positioning of the timeline indicator in the position corresponding to the beginning of the alarm event.

Alarm event playback

As soon as an alarm event is taken into processing, the alarm event recording is played back automatically one time, at 1X speed. Playback is launched either from the moment of the beginning of the alarm event, or from the moment corresponding to the position of the alarm event flag (only when the alarm event is initiated automatically—see Initiating an alarm in the system).



If the alarm event was initiated automatically, the visual element set for the detection tool which initiated the alarm event will be displayed in the Surveillance window: or a detection area or virtual tripwire, which triggers the detection tool when it is crossed. The object which caused the trigger will be outlined with a red frame.

Display of an **Area** visual element:



Display of a **Line** visual element:



The name of the detection tool that initiated the alarm event is displayed above the buttons for alarm assessment.

To navigate the fragment of an alarm event, use the Advanced panel (see Navigation using the advanced panel) or the Playback panel (see Navigating using the Playback Panel).

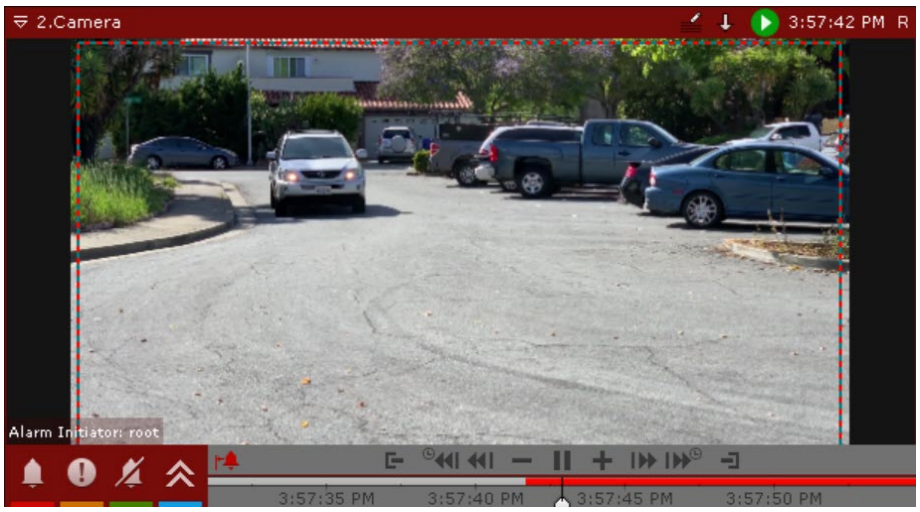
To go to the required fragment of an alarm event in order to play it again, hold the timeline pointer with the left mouse button and drag it to the required position.

To go to the beginning of the alarm event, click the  button.

Assessing an alarm event

To assess an alarm event, use the group of colored buttons in the lower left corner of the Alarm Management window. After assessing the alarm, the **Surveillance window** on the given Client automatically switches to Live Video mode. The corresponding alarm event is no longer in the **Alarms** tab.

> **Attention!**
>
> In the case of multi-user alarm event processing, only the first operator who switched to the Alarm Management mode can assess the alarm event (if they have the appropriate permissions). For the rest of the operators, the alarm event assessment buttons are not displayed.



Button	Executed function
	The **Confirmed alarm event** status is assigned
	The **Suspicious alarm event** status is assigned
	The **False alarm event** status is assigned
	Alarm escalation

It is possible to specify the time within which the alarm event should be taken into processing, otherwise it will be assigned the **Skipped** status (see Configuring Alarm processing).

> **Note**
>
> The statuses of alarm events are displayed on the timeline using color indicators (see The Timeline).

Limitations when working with alarm events in case of multi-user processing

In the case of multi-user processing, only one operator may accept an alarm for processing. Other operators may switch to Alarm Management mode with limited functionality for the purpose of playing back the alarm. This can be done in one of two ways:

1. Click the  button (see Video surveillance in alarm management mode).
2. Go to the **Alarms** tab and select the alarm from the alarms list.



In Alarm Management mode with limited functionality, the Alarm Management buttons are not displayed. Instead, the name of the operator who is currently processing the alarm event is displayed. Other functions of the alarm handling tile remain unchanged.

If the operator has taken an alarm event into processing, this task will not be available for another operator.

After processing an event on another Client, the assigned status of the alarm event is displayed on this Client instead of the operator name.

If an operator accepts an alarm for processing and then exits the Alarm Management mode (switches to Live Video mode, Archive or Archive Search mode, to the viewing tile of another camera, etc.), and the operator absence time is equal to the operator's Idle time parameter value, then other operators are able to accept the alarm event for processing.

If more than one alarm appears for one camera, any operator may access all alarms not yet accepted for processing.

Video surveillance in archive search mode

Switching to Archive Search mode

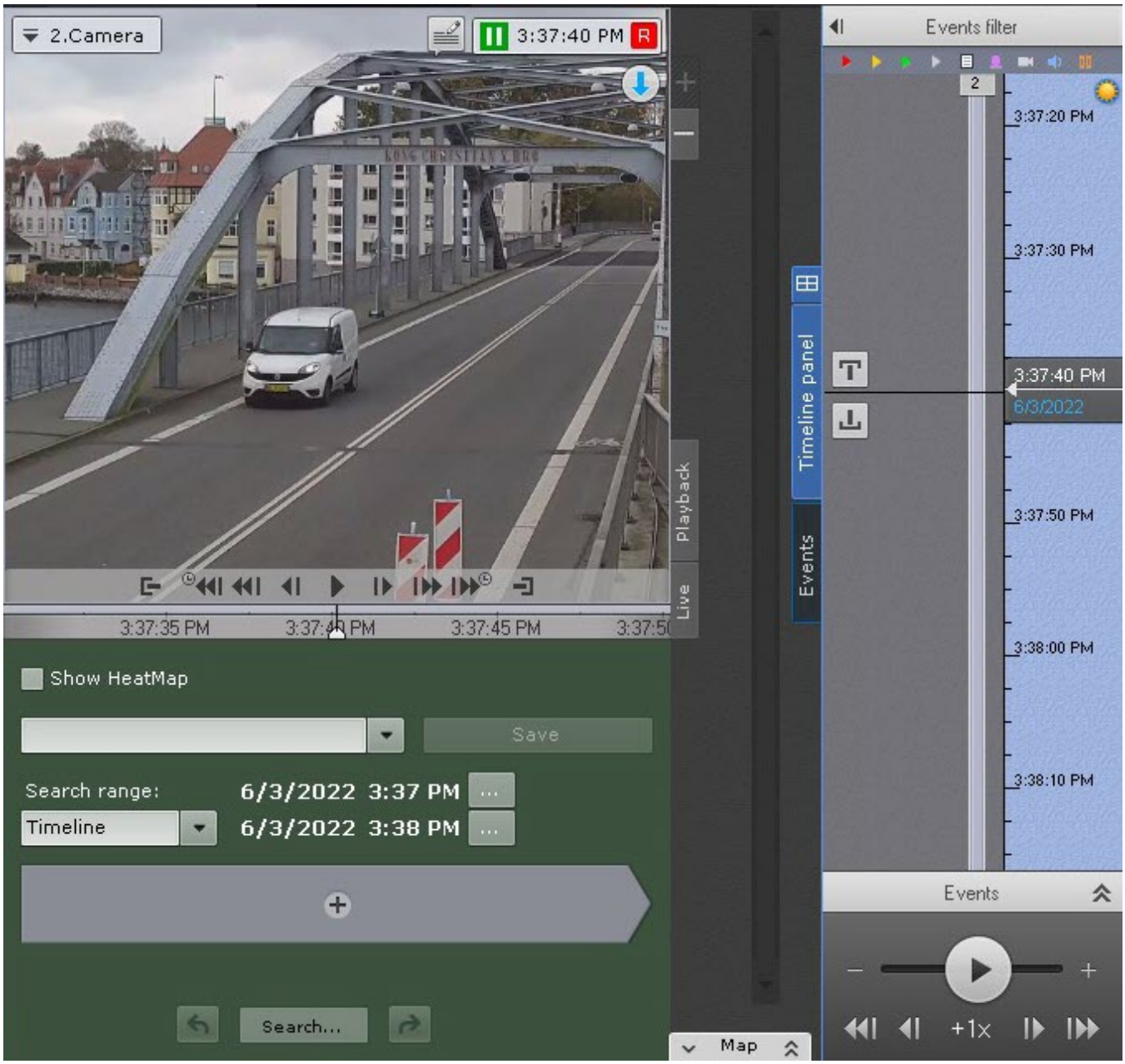
To switch the Camera Window from a different surveillance mode to the Archive Search mode, click the **Search** tab in the lower-right corner.

> **Note**
>
> If the video camera is not linked to a video archive, this tab will be unavailable.

> **Note**
>
> In Live Video mode, if the viewing tile is not active, the tabs for switching to other modes are not displayed. To display the tabs, click the viewing tile by using either button of the mouse.



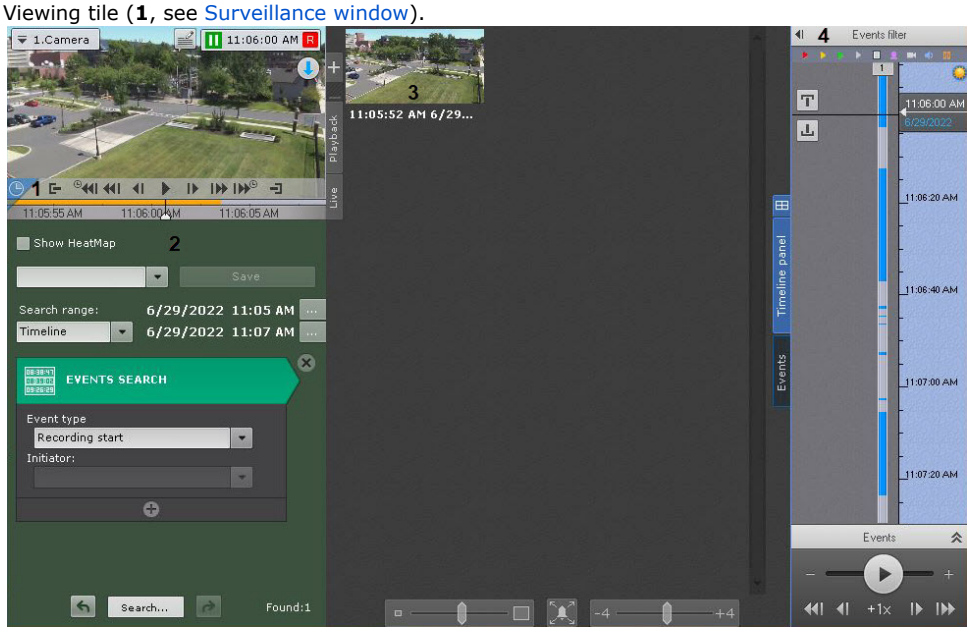
The archive analysis interface will then appear.


2.Camera
3:37:40 PM
R
3:37:35 PM
3:37:45 PM
Playback
Live
Timeline panel
Events
Events filter
2
3:37:20 PM
3:37:30 PM
3:37:40 PM
6/3/2022
3:37:50 PM
3:38:00 PM
3:38:10 PM
Show HeatMap
Save
Search range:
6/3/2022 3:37 PM
Timeline
6/3/2022 3:38 PM
Search...
Map
Events
+1x

Archive Search mode interface

The visual layout of Archive Search mode is divided into the following 4 components:

1. Viewing tile (**1**, see Surveillance window).



2. Search control panel (**2**, see Search in an archive of a single video camera).
3. Search results panel (**3**, see Viewing search results).
4. Archive navigation panel (**4**, see The Archive Navigation Panel).

You can hide search parameters for a portrait-oriented camera. To do so, click the  button.



To unhide, press the button.

Video surveillance functions available in Archive Search mode

In Archive Search mode, the following video surveillance functions are available:

1. Selecting an archive for video recording analysis.
2. Autozoom.
3. Navigating through the archive.
4. Display of the causes of triggered Scene Analytics detection tools.
5. Viewing recorded video with operator comments.
6. Events search.
7. Forensic search.
8. Time search.
9. Searching comments.
10. Switching between search results.
11. Playing back fragments retrieved by searches of specific moments in time.
12. Zooming in on objects that trigger detection tools.
13. Functions Available in All Video Surveillance Modes.

Note

The functions for navigating through an archive, displaying the causes of Scene Analytics detection tool triggering, and **Archive Selection** were inherited from archive mode; their descriptions are Video surveillance in archive mode. The Autozoom function is described in the Real-time video surveillance section.

Search in an archive of a single video camera

Selecting the search type

To start a search, click  and choose the search type.



Note

The current *Axxon One* suite release supports only search of a single type at one time.

Note

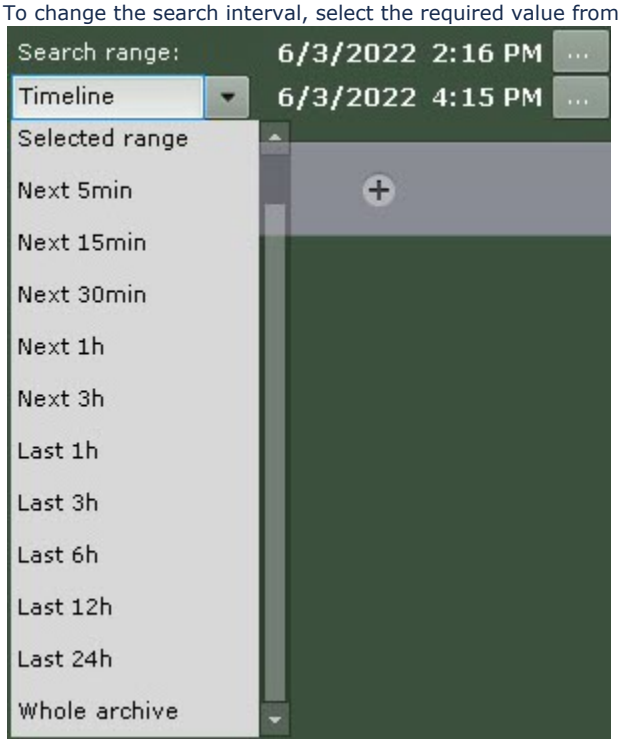
In the on-board storage of the camera, you can only find video episodes with thumbnail search (TimeSlice).

Setting a search interval

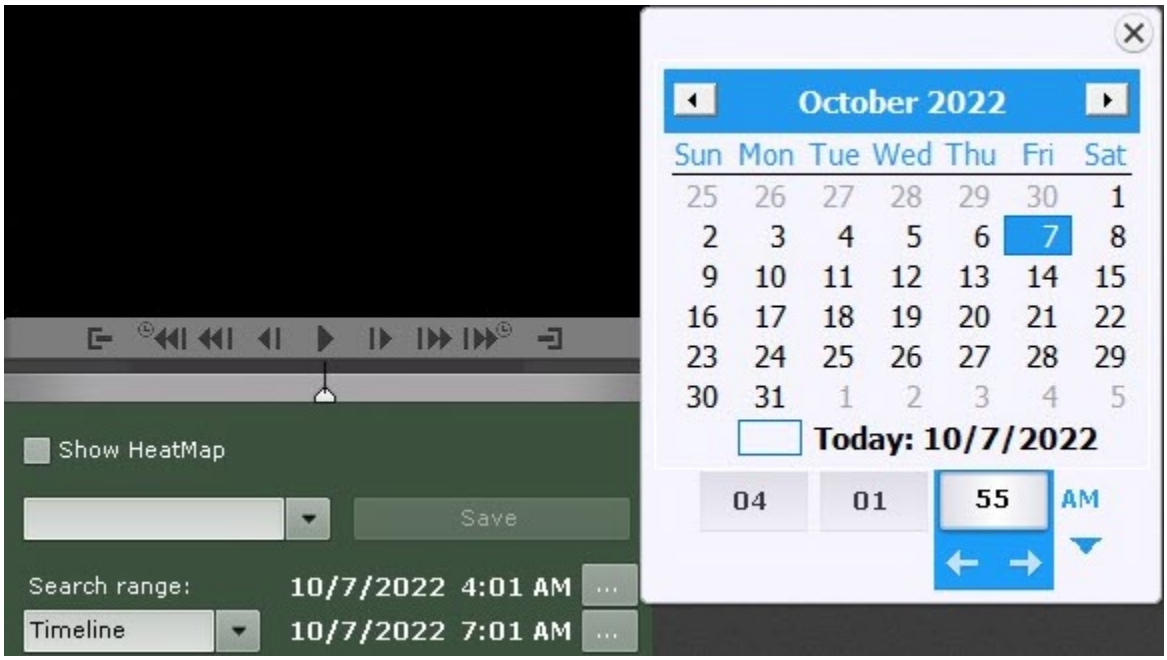
Setting a search interval is a common procedure for all types of the archive search.

By default, the search spans across the part of the archive that is displayed on the timeline (see Navigating Using the Timeline).

To change the search interval, select the required value from the **Search range** drop-down list.



Search range	Description
Timeline	The search spans across the part of the archive that is displayed on the timeline. The interval can also be set manually with the upper and bottom buttons ... .
Selected range	The search will be performed within the interval currently selected on the timeline. You can set the interval using the and buttons.
Next 5min /15min/30min /1h/3h	The search will be performed within the following interval [specified start of the interval; specified start of the interval + 5min/15min/30min/1h/3h]. To set the beginning of the interval, click the ... button.
Last 1h/3h/6h /12h/24h	The search will be performed within the last hour (or 3, 6, 12, 24 hours) of the archive.
Whole archive	The search will be performed across the entire archive.

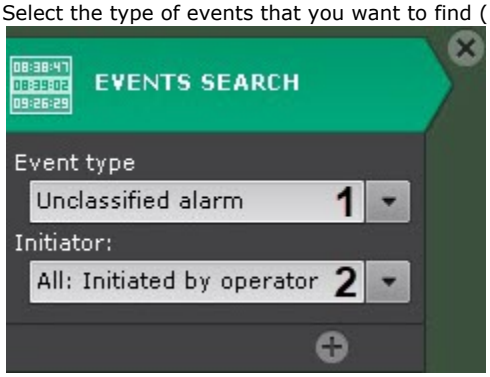

October 2022
Sun Mon Tue Wed Thu Fri Sat
25 26 27 28 29 30 1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31 1 2 3 4 5
Today: 10/7/2022
04 01 55 AM
Show HeatMap
Save
Search range: 10/7/2022 4:01 AM
Timeline 10/7/2022 7:01 AM

Events search

This type of search allows you to select events in the archive based on the type of event.

To search for events, do the following:

1. Select the type of events that you want to find (**1**).



Event	Description
All alarms	The search finds moments in the archive containing all types of alarms
Non-critical alarm	The search finds moments in the archive containing non-critical alarms
Critical alarm	The search finds moments in the archive containing critical alarms
Unclassified alarm	The search finds moments in the archive containing unclassified alarms
False alarm	The search finds moments in the archive containing false alarms
Triggering	The search finds moments when detection tools were triggered
Recording start	The search finds the beginning and end of recordings from the specified camera regardless of the initiator

2. Select an event initiator from the list (**2**).

> **Note**
>
> - An event initiator could be an operator, a camera input, or any detection tool of a camera, or any detection tool that is activated in the system. The search results will show the moments in the archive containing the events that were triggered by the initiator.
> - When you search for any type of event or for a **Triggering** type of event when searching in the face lists or license plates lists, select **Real-time recognition** as an intiator with a specific list. For this, enable the **Check in lists** parameter in the settings of the Category: Face and Category: Vehicle (see Configuring vehicle license plate recognition based on the created lists and Configuring face recognition based on the created lists).

3. If necessary, click  and add more similar search conditions.
4. Set the search interval (see Setting a search interval).
5. Click the **Search** button.

> **Attention!**
>
> - To search in the embedded storage of an IP device (for example, a camera or recorder) for triggers of embedded detection tools, you must synchronize the server and IP device (see Limitations of Axxon One). If you don't perform synchronization, there can be discrepancies between the time of detection tool triggering and the time of frames in the archive.
> - Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

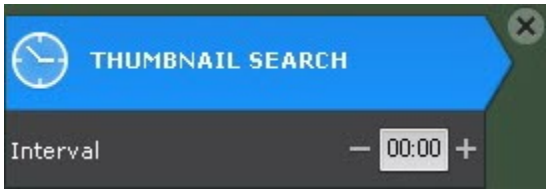
This starts a search in the archive based on the defined criteria. Search results are available on the search results panel.

Note

To zoom objects that caused an alarm or triggered a detection tool, set the **Expand alarm object** checkbox in the lower part of the search results panel.

Time search for video fragments (TimeSlice)

The search of fragments by time is meant for quick search of moment of interest by dividing a selected time period into equally sized fragments.



Search by time is performed using the following algorithm:

1. Setting a search interval.
2. In the **Interval** field, specify the duration of the video episodes in the MM:SS format:
    a. If you do not specify the duration (00:00), TimeSlice (Thumbnail Search) splits video footage from the selected time interval into 12 equal episodes.
    b. If you set the duration other than 0, TimeSlice splits the selected time interval into video clips of the specified duration. The number of slices depends on the specified parameters.

    > **Note**
    >
    > It's recommended to set the interval value to no less than 10 seconds.

3. Start the first search iteration (click the **Search** button).

    > **Note**
    >
    > Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

    The search results panel displays frames that match moments in time that are equally spaced from each other; the search control panel shows the number of fragments found.



4. If the specific moment is not found, then start the second search iteration: double-clicking on the found moment triggers the search in the time interval from this moment to the next one.
5. Keep searching until the specific moment is found.

Note

Information on playback of video fragments is provided in the section titled Playback of video fragments.

Searching comments

Comments search allows filtering for comments that contain certain text.

To search comments:

1. Enter the text that you want to find in comments.

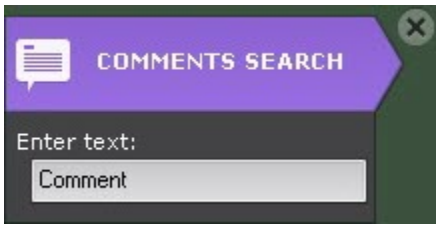
   Attention!

   You should enter at least three characters to make a search. The search is performed for the entire string of entered text, not for separate words.

   Note

   To search all comments for the selected interval, do the following:

   - in *Axxon One* 1.9.0 or later versions, enter ***** (asterisk) in the search field (it represents any number of any characters);
   - in earlier versions of *Axxon One*, leave the search field blank.

2. Set the search interval (see Setting a search interval).
3. Click the **Search** button.

   Note

   After starting the search, it can be stopped at any time. To do this, click the **Stop** button which replaces the **Search** button.

This starts a search for video fragments based on the defined criteria. The search results pane displays frames, for which there are comments containing the search text. The relevant comment is displayed under each frame.



Note

If the comment was left for an interval, the first frame of the interval is displayed.

Forensic Search for Fragments (MomentQuest)

Forensic Search lets you search for moments in the archive using the following criteria:

1. Motion in Area.
2. Loitering of an object in a specific area.
3. Simultaneous presence of a large number of objects in a specific area.
4. Crossing of a virtual line by an object’s trajectory.
5. Motion from one area to another.

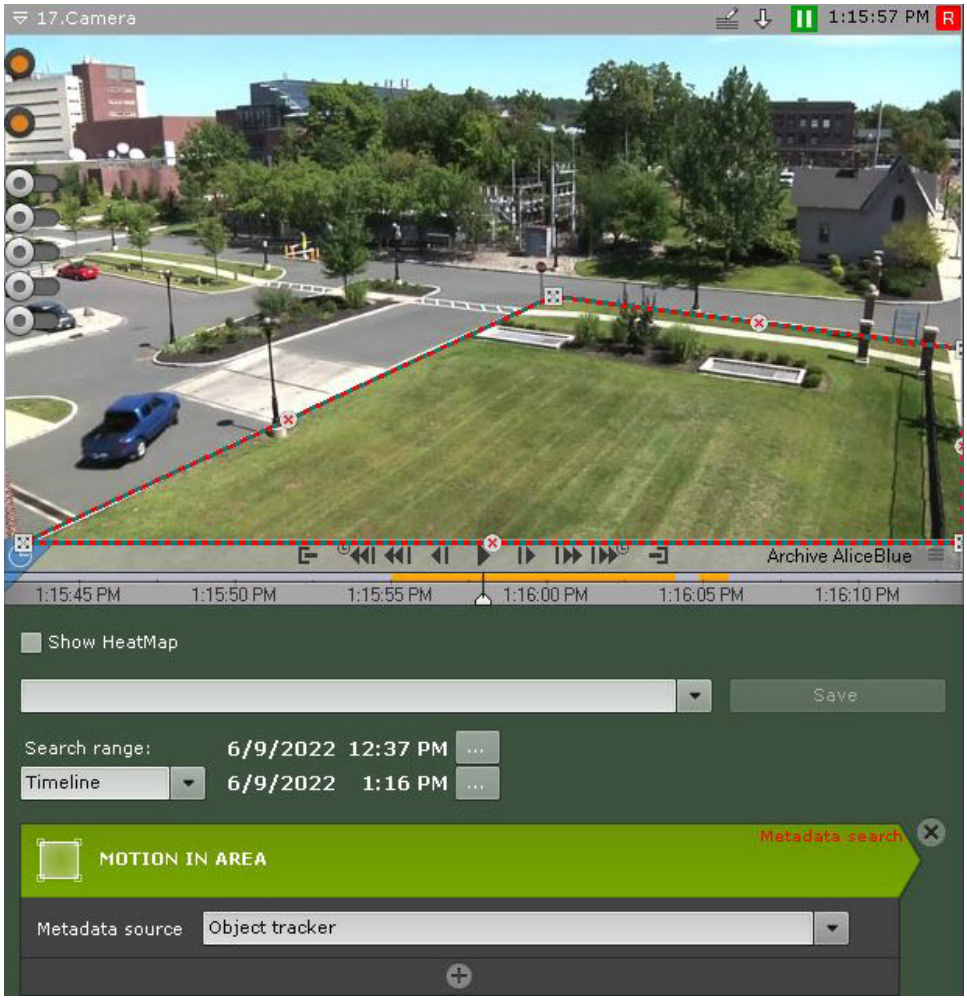
Motion in Area

To perform forensic search for motion in area:

1. In the Viewing Tile, define the area to be analyzed during search in accordance with the selected condition.

   The nodes of an area are connected by a two-colored dotted line.

   By default, an area is defined by 4 nodes with the coordinates (30%, 30%), (70%, 30%), (70%, 70%) and (30%, 70%) as percentages of the width and height of the frame, respectively.



   To edit an area, use the following actions.

Action	Result
Right-click on a line	Creates a new area node
Right-click on a created node	Deletes the area node
Position the cursor on a node and hold down the left mouse button while you move the mouse	Moves the area node

2. Select the metadata source if there are several for this video camera. This parameter will not be displayed if there is only one source.
3. Specify any number of additional parameters by clicking  , if necessary (see Configure the search parameters).
4. Set the search interval (see Setting a search interval).
5. Click the **Search** button.

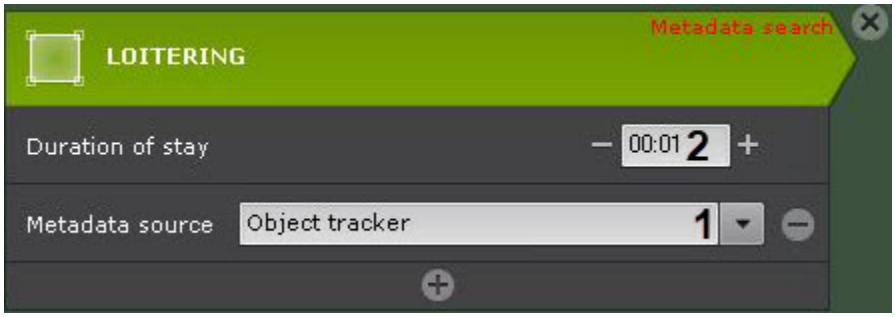
> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

The found moments will be displayed in the search results panel.

Loitering of an object in a specific area

To search for moments of an object loitering in an area:

1. In the Viewing Tile, define the area to be analyzed during search in accordance with the selected condition (see Motion in Area).
2. Select the metadata source if there are several for this video camera (**1**). This parameter will not be displayed if there is only one source.



3. Set the minimum duration of stay in the area (**2**, in seconds and minutes). Search results contain recorded video in which the object is present in the area for longer than the indicated time.
4. Specify any number of additional parameters by clicking  , if necessary (see Configure the search parameters).
5. Set the search interval (see Setting a search interval).
6. Click the **Search** button.

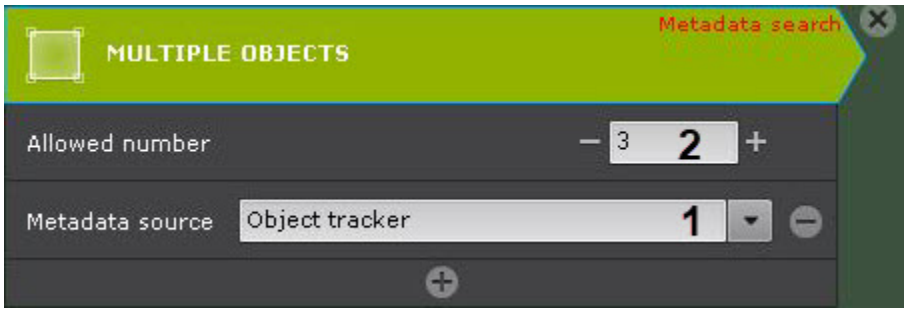
> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

The found moments will be displayed in the search results panel.

Simultaneous presence of a large number of objects in a specific area

To search for moments when objects gather in an area:

1. In the Viewing Tile, define the area to be analyzed during search in accordance with the selected condition (see Motion in Area).
2. Select the metadata source if there are several for this video camera (**1**). This parameter will not be displayed if there is only one source.



3. Specify the number of objects allowed in the area (**2**). Search results contain recorded video in which the number of objects in the area exceeds the specified number.
4. Specify any number of additional parameters by clicking , if necessary (see Configure the search parameters).
5. Set the search interval (see Setting a search interval).
6. Click the **Search** button.

> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

The found moments will be displayed in the search results panel.

Motion from one area to another

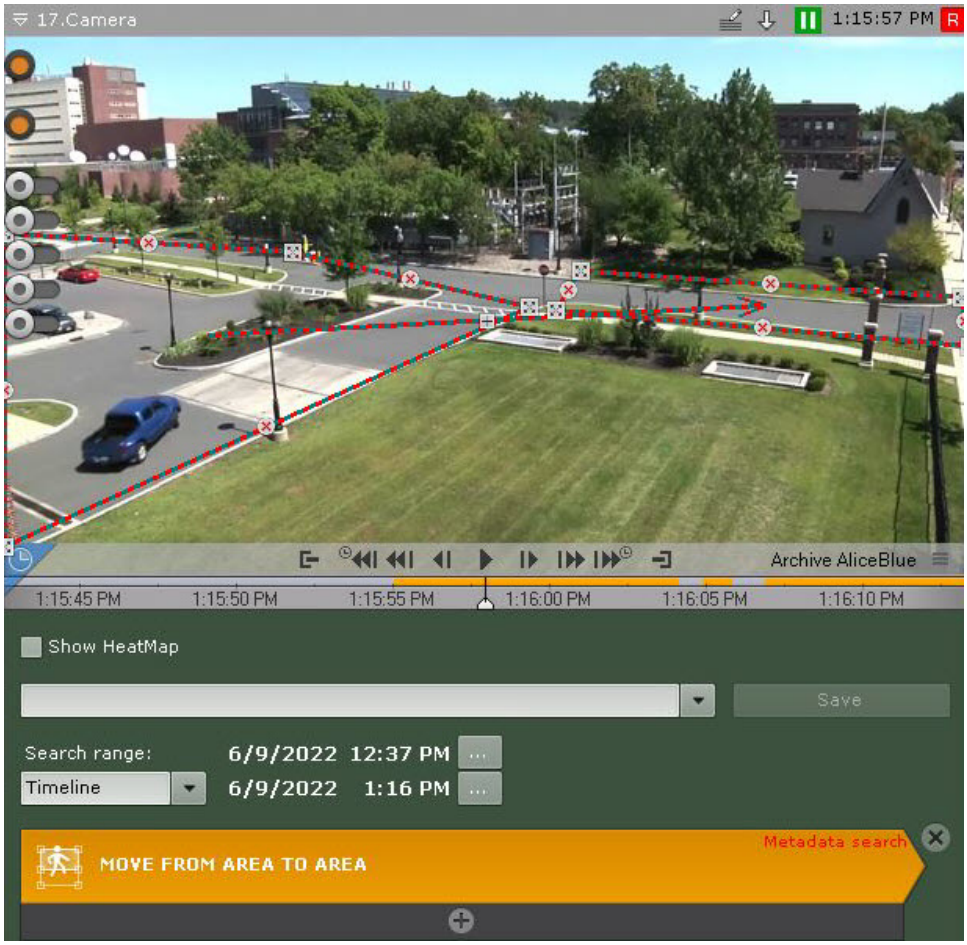
To search for moments when the object moves from one area to another:

1. Set two areas in the Viewing Tile: the area the object moves from and the one it moves to.

   The nodes of each area are connected by a two-colored dotted line. The direction of motion between the areas is indicated by a dotted arrow.

   By default, each area is defined by 4 nodes. The nodes of the first area have the coordinates (20%, 40%), (40%, 40%), (40%, 60%), (20%, 60%), and those of the second have the coordinates (60%, 40%), (80%, 40%), (80%, 60%), (60%, 60%) as percentages of the width and height of the frame, respectively.

   > **Note**
   >
   > You can collapse the graphical elements if they block the visual elements and prevent editing them. To hide them, select the **Hide graphical elements** check box.

   Area editing operations are described in the Motion in Area section.

   To change the direction of motion between the areas, click the button on the direction arrow.
2. Select the metadata source if there are several for this video camera. This parameter will not be displayed if there is only one source.
3. Specify any number of additional parameters by clicking , if necessary (see Configure the search parameters).
4. Set the search interval (see Setting a search interval).
5. Click the **Search** button.

   > **Note**
   >
   > Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

The found moments will be displayed in the search results panel.

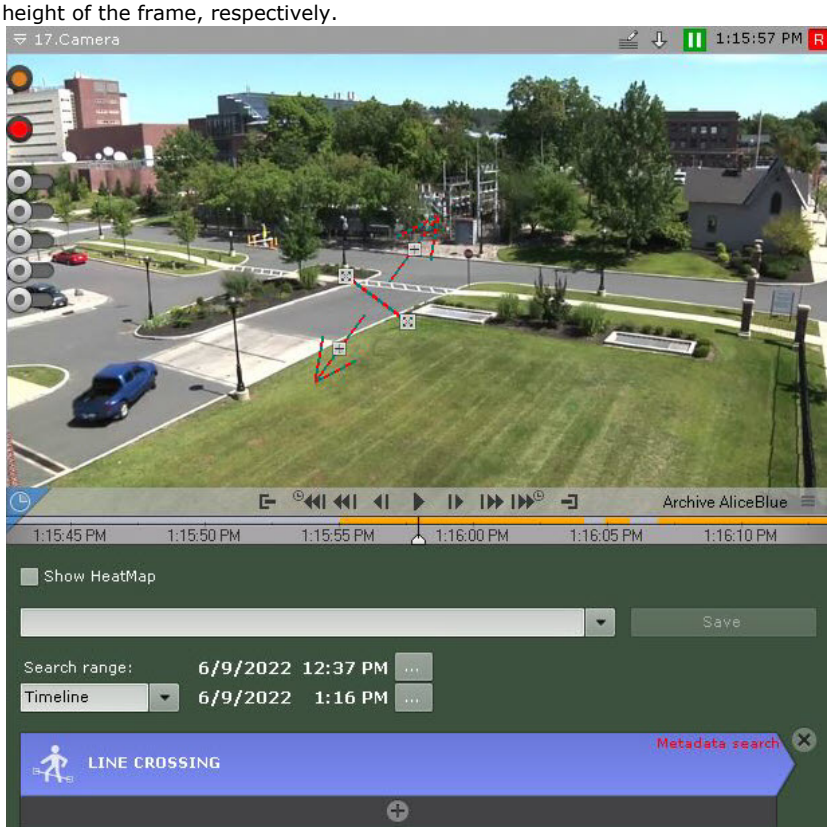
Crossing of a virtual line by an object's trajectory

To search for moments when the object crosses a virtual line:

1. Set the virtual line to be crossed in the Viewing Tile.

   The end points of the line are connected by a two-colored dotted line. The direction of the object's motion across the line is indicated by dotted arrows.

   By default, the end points of the line have the coordinates (50%, 30%) and (50%, 70%) as percentages of the width and height of the frame, respectively.



   To move the end point of a line, position the cursor on the end point and hold down the left mouse button as you move the mouse.

   By default, both directions of motion across the virtual line are taken into account when searching the archive. If you do not need to search in a specific direction, click the ⊞ button corresponding to that direction.

   > **Attention!**
   >
   > At least one direction must be selected for the search.

   > **Note**
   >
   > A disregarded direction of object motion is indicated by a dimmed arrow.

2. Select the metadata source if there are several for this video camera. This parameter will not be displayed if there is only one source.
3. Specify any number of additional parameters by clicking ⊕, if necessary (see Configure the search parameters).
4. Set the search interval (see Setting a search interval).
5. Click the **Search** button.

Note

Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

Configure the search parameters

It is not required to specify parameters, but for more precise results, it is possible to set one or more parameters for each criterion:

The search criteria	Possible parameters
Motion in Area	Direction of movement Maximum and minimum object size Maximum and minimum object speed Object color Object type Entry/exit from area
Loitering in area	Maximum and minimum object size Object color Object type
Many objects in area	Maximum and minimum object size Object color Object type
Object trajectory crossing a virtual line Motion from area to area	Maximum and minimum object size Maximum and minimum object speed Object color Object type

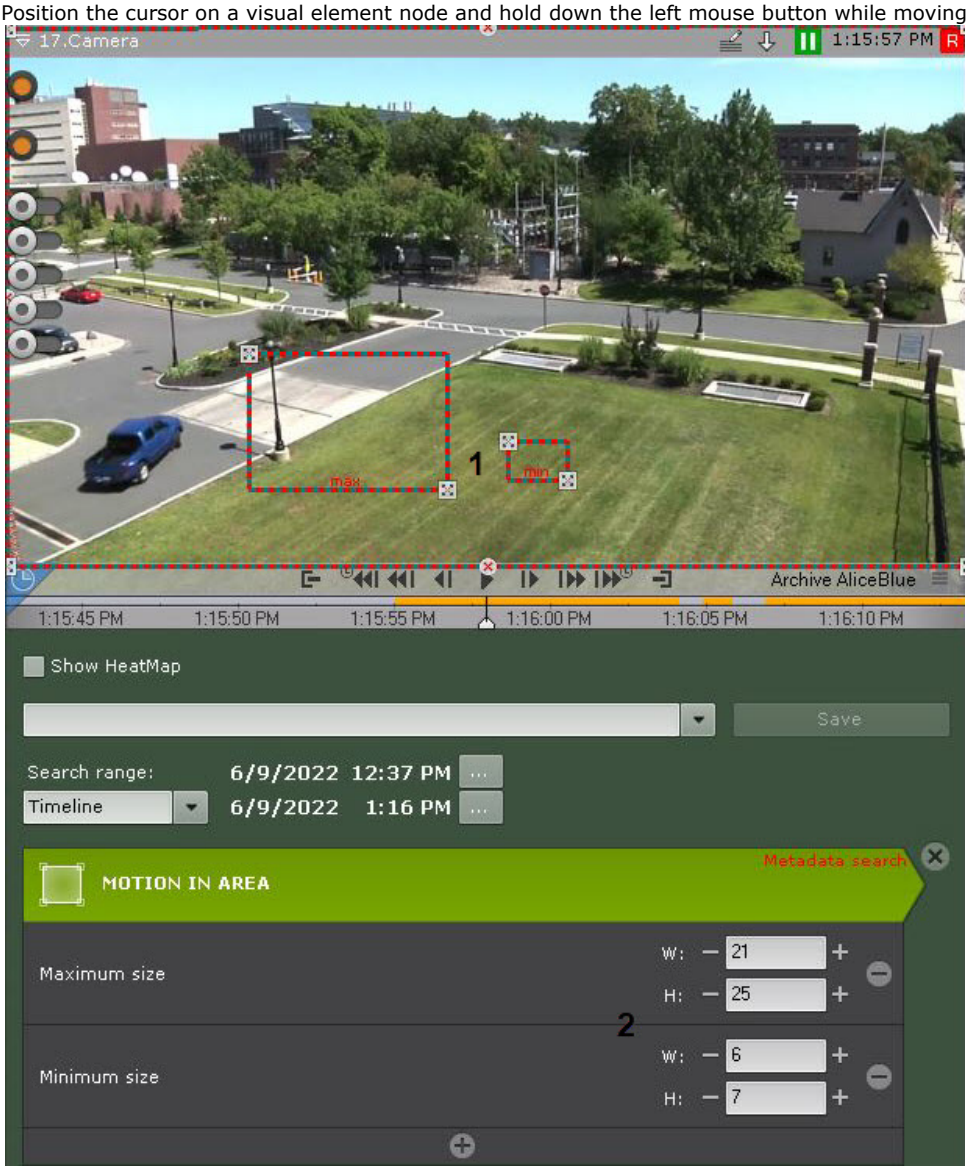
Configuring minimum and maximum object size

The procedures for setting the minimum and maximum size of a moving object are identical.

The minimum (or maximum) size of a moving object can be set using any of the following methods:

> **Note**
>
> The first method lets you roughly configure the size, and the second method allows you to set the size precisely.

1. Position the cursor on a visual element node and hold down the left mouse button while moving the mouse (**1**).



2. Set the width and height of an object of the minimum (maximum) size using the arrows in the upper and lower margins, respectively. The dimensions of a visual element in the viewing tile can be changed in a similar manner (**2**).

The minimum (maximum) size of an object is now set.

Configuring minimum and maximum object speed

In the *Axxon One* VMS, the speed is a relative value computed from parameters of different units. The computing algorithm includes both frame width and height. For more accurate search, we recommend you to perform several search iterations while setting speed values empirically.

The procedures for setting the minimum and maximum speed of a moving object are identical.

The minimum (or maximum) speed of a moving object can be set using any of the following methods:

1. Position the cursor on an end point of the arrow and hold down either mouse button while you move the mouse. The length of the arrow will correspond to the minimum (maximum) displacement of the object per second (**1**).



2. Use the arrows to set the minimum (maximum) speed of the object as percentages of the frame per second (**2**).

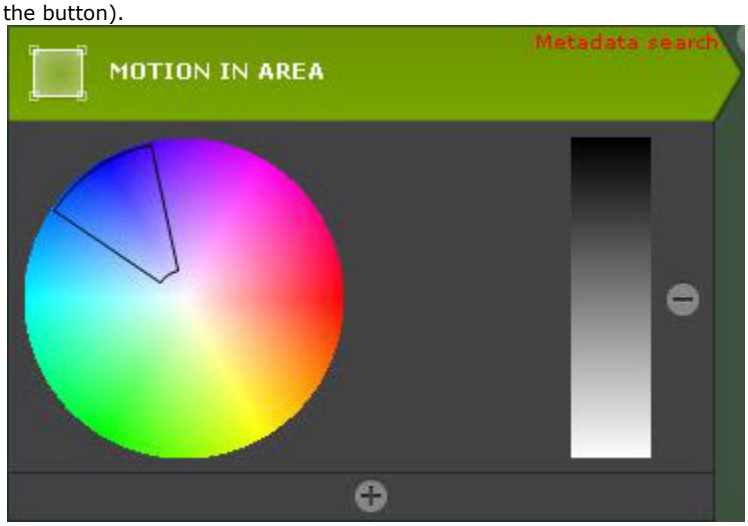
The minimum (maximum) speed of a moving object is now set.

The following objects will be included in the search results:

- If you set only the maximum speed – the objects that move slower, than the maximum speed.
- If only the minimum speed is specified – the objects that move faster than the minimum speed.
- If both the maximum and the minimum speed are specified – the objects whose speed does not exceed the maximum, but is more than the minimum speed.

Configuring object color

The color range is selected using drag-and-drop on the color palette (click and hold any mouse button, move the mouse, then release the button).



Any click on the palette is interpreted as the beginning of a new range; the previous range will disappear.

Attention!

Axxon One uses a logic according to which all objects are monochrome. The color of an object in *Axxon One* is an average of all object colors in the video image.

All objects of specified colors will be included in search results.

Attention!

It is not possible to search by color when using metadata from a motion detection (see Setting up VMD-based Scene Analytics detection tools).

Use Case for Color Filter

The AI analysis extracts metadata from moving objects and stores it in a database. The color filter allows you to focus the search on objects with selected colors. For example, if a person is wearing clothing of a specific color, or a car is red, blue, or green, *Forensic Search* will search for people, objects, or vehicles that match the selected color spectrum.

By utilizing the search and filtering capabilities based on color, you can search by predominant color within a person's or object's track. For example, you can search for a person wearing a red shirt (if it constitutes 80% or more of the total track size) or locate a blue car.

Configuring direction of object movement

By default, when searching the archive, the system searches for motion in all directions. You can stop the search for motion in one or several specific directions.

To do this, click the direction in which you want to stop the search for motion with any mouse button. As a result, the sector corresponding to this direction will be grayed out.

If necessary, repeat this action for other directions. To reactivate the search for inactive direction, click it again with any mouse button.



If incorrect search results occur, we recommend setting the **Advanced mode (requires more processing time)** checkbox. This will increase the accuracy of the search, but the search process will require more time.

The required directions of an object motion are now set.

Configuring object entry/exit from area

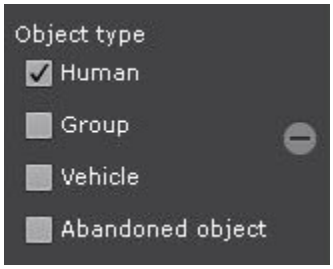
"Entry" occurs when an object enters the field of view and crosses its boundaries; "exit" occurs when an object disappears from the field of view and crosses its boundaries.

To find moments when an object enters an area, select **Enter**, or for moments when an object exits an area, select **Exit**.



Choosing the object type

You can search for moving objects of one or several types: a person, a group of people, a vehicle, or an item left behind. To do this, check the corresponding boxes.



Note

The object type is determined by analyzing its appearance. An item that does not move for some time is considered to be abandoned, e.g. a parked car.

Attention!

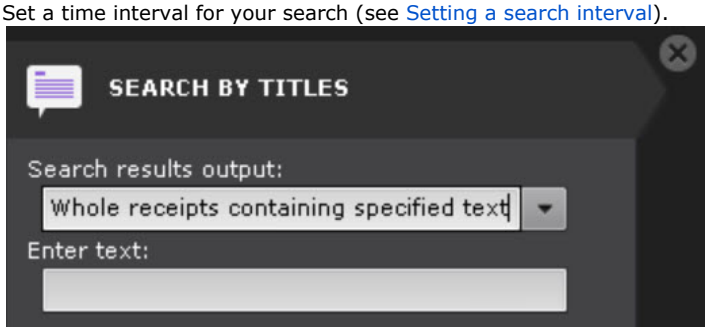
You cannot search by object type in VMD-generated metadata (see Setting up VMD-based Scene Analytics detection tools).

Search by titles

Search by titles allows you to find the necessary words in the titles DB received from the POS devices.

To search by titles, do the following:

1. Set a time interval for your search (see Setting a search interval).



2. In the **Search results output** drop-down list, select one of the search methods:
   - **Whole receipts containing specified text**—video fragments containing receipts with the searched text are displayed as search results. The number of video fragments is equal to the number of receipts that include the searched text.
   - **Single titles containing specified text**—video fragments containing the searched text are displayed as search results. The number of video fragments is equal to the number of search words in the receipts.

   > **Note**
   >
   > For example, the word "Milk" appears on two receipts, and is mentioned twice in each of them. The search results will be as follows:
   >
   > - **Whole receipts containing specified text**—two video fragments will be displayed, since the word is contained in two receipts;
   > - **Single titles containing specified text**—four video fragments will be displayed, since in total the word appears four times in receipts.

3. Enter the text that you want to find in the titles. You can search the whole word or part of it.

   > **Attention!**
   >
   > - You must enter at least three characters to make a search.
   > - The search is performed by the entire text that you entered, not by individual words.
   > - You cannot search by empty string.

4. Click the **Search** button.

   > **Note**
   >
   > After starting the search, you can stop it at any time. To do this, click the **Stop** button which replaces the **Search** butt on.

The search process based on the specified criteria will start. The search results panel will display frames with titles containing the search text.

> **Attention!**
>
> The time of the found events corresponds to the start time of the receipt, not the time of occurrence of the searched text.

Search by LPs

With search by LPs, you can find the recognized license plates in the archive, as well as filter them according to specified criteria.

To search by license plates, do the following:

1. Set a time interval for your search (see Setting a search interval).
2. Select the detector from the list (**1**), by which you want to search.
3. Enter the license plate that you want to find (**2**). You can enter either a full license plate or a part of it using the **?** character (any character in the license plate) and the ***** character (any number of any characters in the license plate). For example, a search query **?20*** will show all vehicles with license plate containing **2** and **0** in the second and third position, respectively. License plate can contain any number of characters.

> **Note**
>
> To search by all recognized license plates, enter * (asterisk).



4. If necessary, set additional search criteria by clicking the  button:

> **Note**
>
> To search by additional criteria, the **Vehicle recognition** option must be enabled in the **License Plate Recognition RR** settings (see Configuring License Plate Recognition RR).

   a. Select the **Vehicle class** (**3**) from the drop-down list:
      i. Car;
      ii. Truck;
      iii. Bus;
      iv. Motorcycle;
      v. Mini truck;
      vi. Unknown.
   b. **Vendor** (**4**): enter full name of the car manufacturer in Latin letters, case-insensitive. Correct spelling examples: Mitsubishi, Nissan, Hyundai.
   c. **Model** (**5**): enter full name of the car model in numbers or Latin letters, case-insensitive. Correct spelling examples: Outlander, Teana, Creta, 406 (for Peugeot 406).

> **Note**
>
> A complete list of models and vendors is given here.

   d. **Color** (**6**): set the color of the vehicle (see Configuring object color).
   e. Select the **Vehicle headlights** (**7**) state from the drop-down list:
      i. Unknown;
      ii. Enabled;
      iii. Disabled.
   f. **Vehicle speed** (**8**): in the **From** and **To** fields, set the vehicle speed range depending on the unit of measurement selected in the **Speed detection** field in the detection tool settings (see Configuring License Plate Recognition RR):
      i. Kmph: possible range from 0 to 450.
      ii. Mph: possible range from 0 to 280.
   g. **Vehicle direction** (**9**): select the vehicle direction from the drop-down list:
      i. Unknown—the vehicle's direction is not recognized;
      ii. Incoming—the vehicle is moving towards the camera;
      iii. Outgoing—the vehicle is moving away from the camera.

> **Note**
>
> To remove a search criterion, click  .

5. Click the **Search** button.

> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

This starts a search based on the selected criteria. The search results panel displays frames with vehicles whose numbers contain the text from the search query and also satisfy the specified additional parameters.

A recognized license plate will be highlighted with a red frame in the Surveillance window.



Face search

> **Attention!**
>
> The processor must support the AVX2 or AVX512 instruction set (see ark.intel.com, Hardware requirements for neural analytics operation).

Face detection tool (see Category: Face) recognizes faces that are in the field of view of the cameras connected to the *Axxon One* Server.

If the recognized face meets the requirements (see Video stream and scene requirements for the Face Detection VA and its sub-tools), a biometric vector is created on its basis. It is stored in the Server database and used for comparison.

A biometric vector is a set of numbers of a given length that implicitly characterizes the visual identity of the owner of the biometric sample.

When you search for faces on the Client, the selected image is sent to the Server, where a biometric vector is created based on the received data.

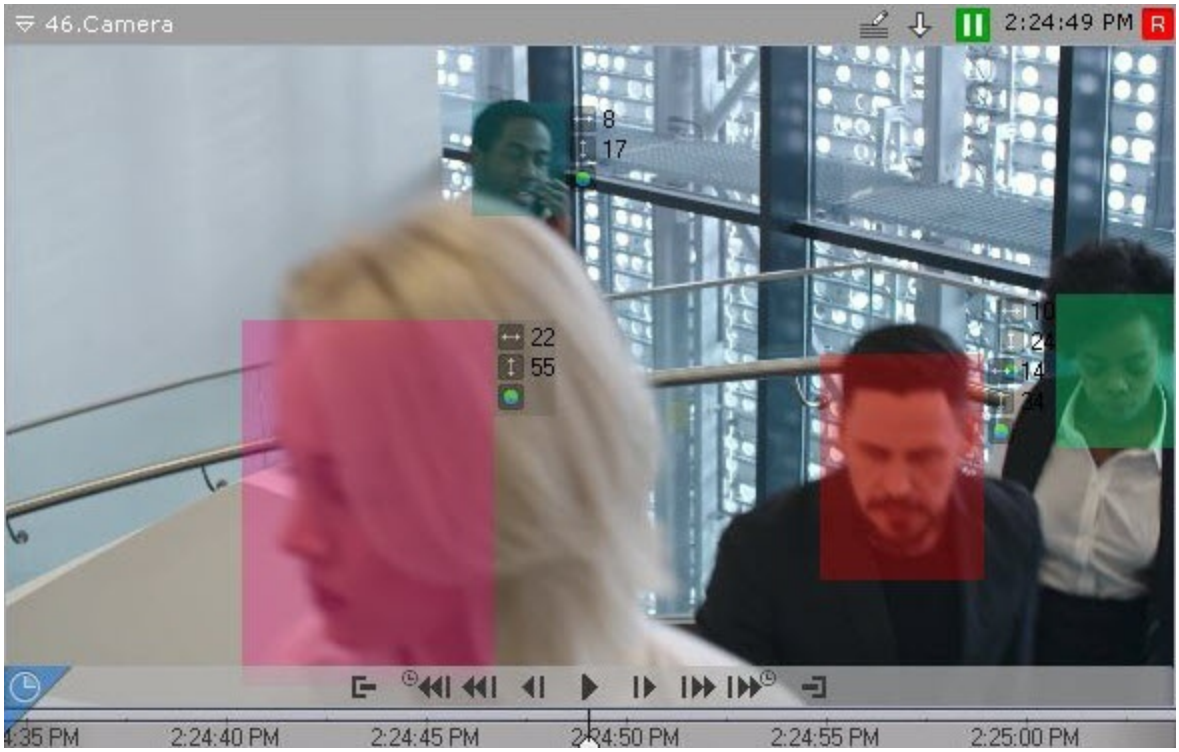
The information about the biometric vectors stored in the database on the selected cameras for the specified time interval (see Setting a search interval) is uploaded to the RAM on the Server side and compared with the biometric vector created on the basis of the image received from the Client.

> **Attention!**
>
> The data in RAM is stored for about two hours. If you search for faces on the previously selected cameras and for a time interval shorter or equal to that stored in RAM, the search results will be obtained faster.

Face search helps you find in the archive:

1. Similar faces (see Search for similar face).
2. Recognized faces (see Search for all recognized faces).
3. Face contacts (see Search for face contacts).

Face track and face size are always highlighted in the surveillance window during face search.

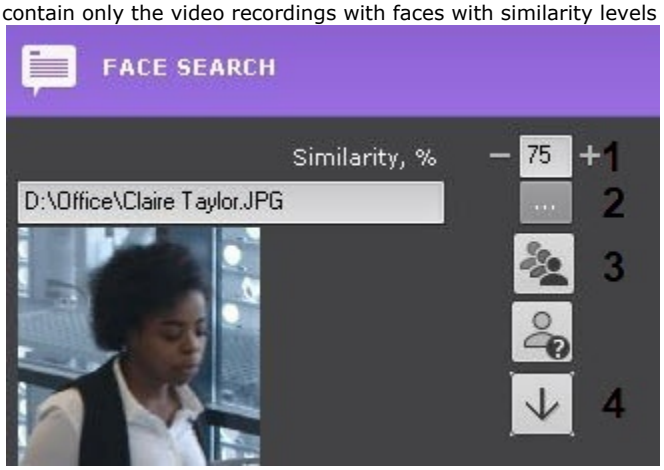


Search for similar face

Face search allows you to find faces similar to a given photo in the archive.

To perform face search:

1. Set the search interval (see Setting a search interval).
2. Set the minimum similarity level (in %) between the face in the photo and faces from the archive (**1**). The search results will contain only the video recordings with faces with similarity levels above the set value.



3. Select a photo with the face that should be found in the archive (**2**). Supported formats: **png**, **jpg**, **jpeg**, **jpe**. When you click the face in the surveillance window, this face will be selected for search. If you do not select a photo, then all faces recognized during the specified time will be displayed. To delete a photo from the search, click the button.
4. Select, how to sort the search results: — by the similarity level; — by time (**3**).
5. If necessary, set additional search criteria by clicking the button:
   a. **Gender**: select the required option;
   b. **Age span**: specify in years in the **From** and **To** fields.



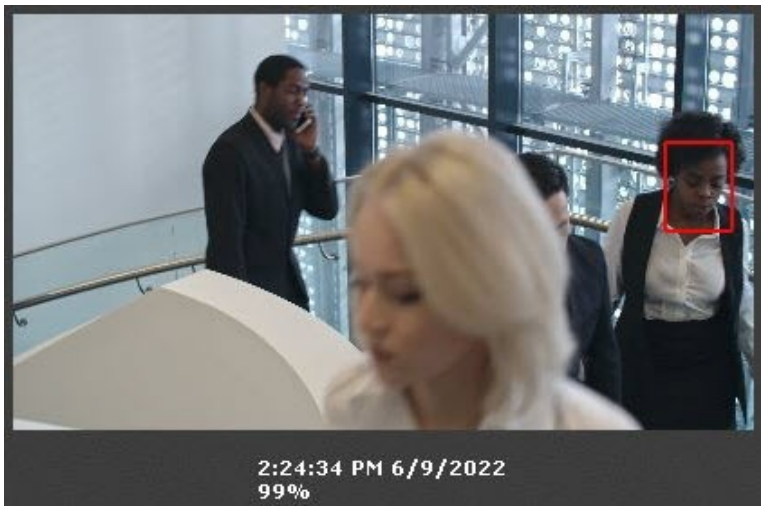
> **Note**
>
> Saving information about gender and age to the database should be enabled in the detection tool settings (see Configuring Face detection).
>
> To delete a criterion, click the button.

6. Click the **Search** button.

> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

This starts a search based on the defined criteria.

The video frames with the faces that meet the search conditions will be displayed in the search results panel. A recognized face will be highlighted with a red frame, and the face similarity level (in %) will be displayed below.



To instantly export a face image from the frame, do the following:

1. Click a face track in the surveillance window.
2. Click the  button (**4**).

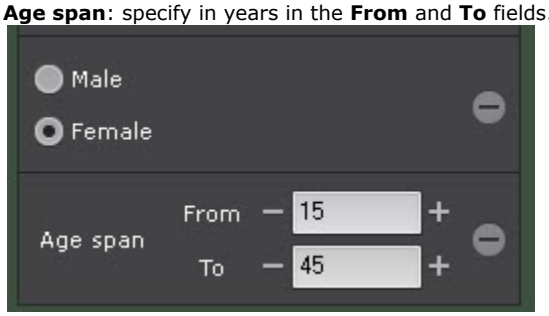
The face image will be saved to the folder specified in the settings (see Configuring export options).

Search for all recognized faces

Face search allows you to find all recognized faces in the archive.

To find all recognized faces, do the following:

1. Set the search interval (see Setting a search interval).
2. If necessary, set additional search criteria by clicking the  button:
    a. **Gender**: select the required option;
    b. **Age span**: specify in years in the **From** and **To** fields.



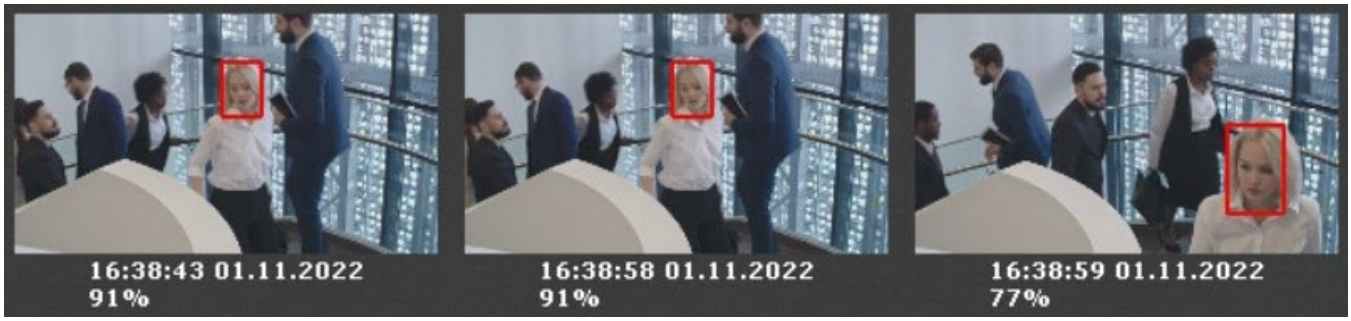
> **Note**
>
> Saving information about gender and age to the database should be enabled in the detection tool settings (see Configuring the Face Detection TV).
>
> To delete a criterion, click the  button.

3. Click the **Search** button.

> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

This starts a search for all recognized faces.

The search results panel will display video frames that contain recognized faces that match the search criteria. Recognized faces will be highlighted with a red frame:



To instantly export a face image from the frame, do the following:

1. Click a face track in the surveillance window.
2. Click the  button.

The face image will be saved to the folder specified in the settings (see Configuring export options).

Search for face contacts

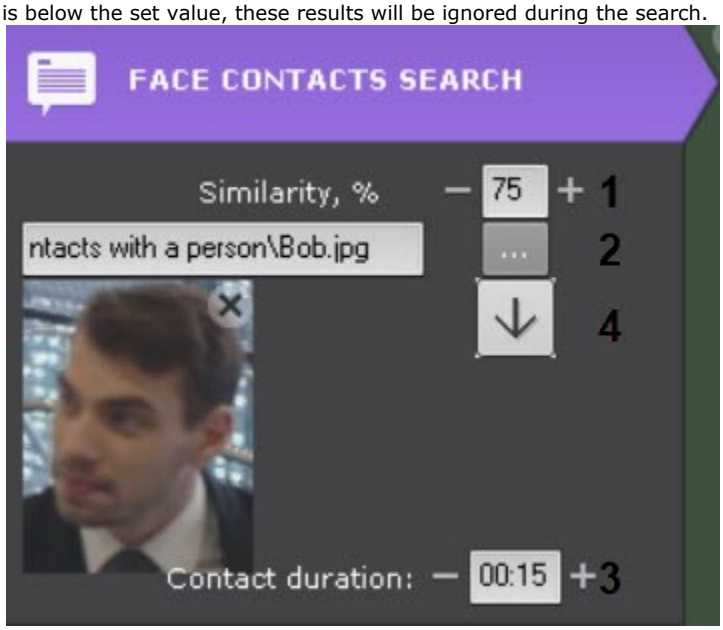
Face contacts search allows you to find in the archive all people who contacted with any person for a specified time.

The search algorithm works as follows:

1. Finds all people in the archive who look like the person from the uploaded photo.
2. Analyzes the archive fragments, in which there is a person from the photo and other people are present as well.

To search for face contacts, do the following:

1. Set the search interval (see Setting a search interval).
2. Set the minimum similarity level (in %) between the face in the photo and the faces from the archive (**1**). If the similarity level is below the set value, these results will be ignored during the search.



3. Select a photo of the person whose contacts you want to find (**2**). Supported formats: **png**, **jpg**, **jpeg**, **jpe**. When you click the face in the surveillance window, this face will be selected for search. If you do not select a photo, then all faces recognized during the specified time will be displayed. To delete a photo from the search, click the  button.
4. Set the minimum contact time of other persons in the frame with the person on the photo in the MM:SS format (**3**). If the contact time is below the specified value, these results will be ignored during the search. The maximum contact time is 59 seconds.
5. Click the **Search** button.

> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears in place of the **Search** button.

This starts a search based on the defined criteria.

The search results panel will display video frames that contain persons who contacted with the person on the photo. Recognized faces will be highlighted with a red frame.



To instantly export a face image from the frame, do the following:

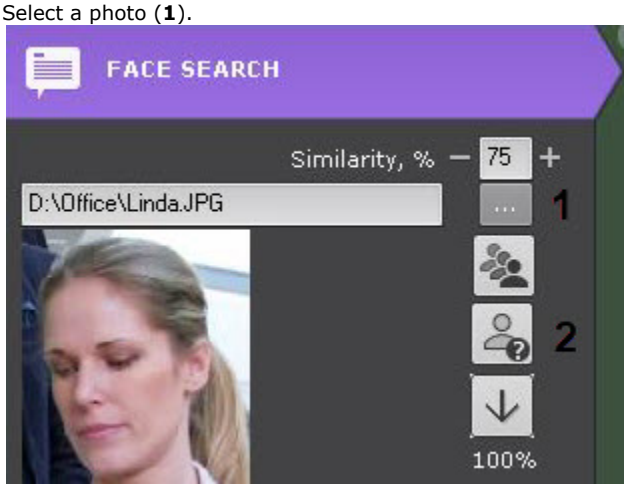
1. Click a face track in the surveillance window.
2. Click the  button (**4**).

The face image will be saved to the folder specified in the settings (see Configuring export options).

Identifying "familiar face" or "stranger" from a photo

To identify the "familiar face" or "stranger" status, do the following:

1. Select a photo (**1**).



2. Click the  button.

The search panel (**2**) will display the probability that the person is a "stranger".

The algorithm is as follows:

1. The person is compared to all recognized persons in the last 30 days.
2. The number of days (**N**) in which the person was captured by camera and recognized is calculated.
3. The probability is calculated according to the formula (1−**N**/30)*100.

Image search

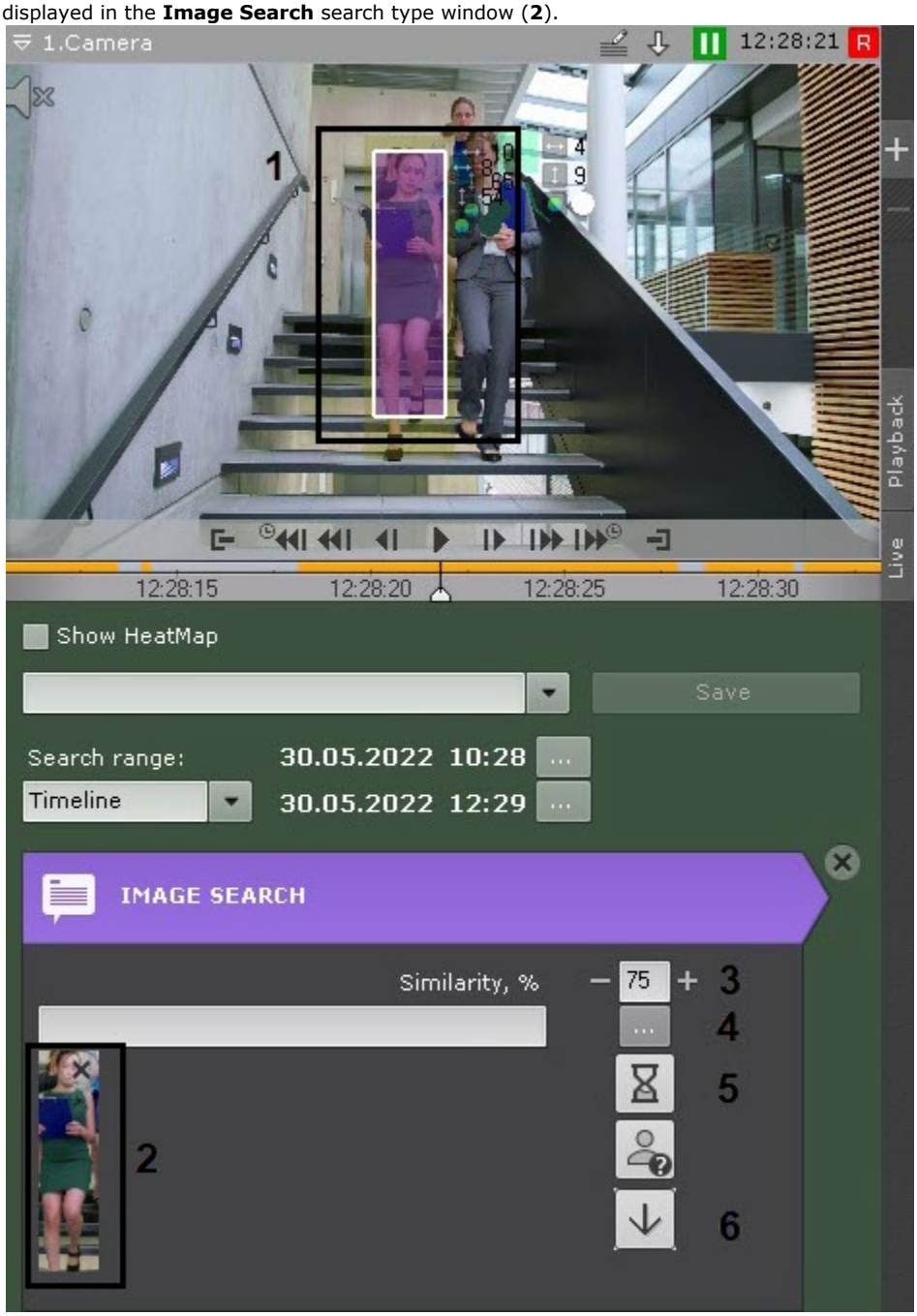
Image search allows you to find in the archive similar images using a certain track or an image.

> ⚠ **Attention!**
>
> - The processor must support the AVX2 or AVX512 instruction set (see ark.intel.com, Hardware requirements for neural analytics operation).
> - To use Image search, it is necessary to configure the neurotracker by enabling the **Similitude search** option in it, and setting the time required for the algorithm to process the track in the **Time of processing similitude track (sec)** field.

You can search by images in the following way:

1. Set the search interval (see Setting a search interval).
2. Select the **Image Search** search type (see Selecting the search type).
3. Select a search method:
    a. Search for a similar image by track:

i. Select a track by left-clicking an object in the Surveillance window (**1**). When you use image search, the image track is highlighted and its dimensions are displayed in the Surveillance window. The track image will be displayed in the **Image Search** search type window (**2**).



ii. Enter the minimum level of similarity (in percent) of the selected track with images in the archive (**3**). The search results will display only those videos that have images with a similarity level greater than the specified one. To remove a track from the search, click the button.

b. Search for a similar image by image:

i. Select an image that is similar to the image you want to find in the archive (**4**). Supported formats: png, jpg, jpeg, jpe. If no image is selected, the search results will display all images recognized within the specified time range. To clear the search criteria, click the button.

ii. Enter the minimum level of similarity (in percent) of the selected image with images in the archive (**3**). The search results will display only those videos that have images with a similarity level greater than the specified one.

> **Note**
>
> When you search for a person, make sure that the track or image displays the person in full height. If the image is not complete, then incorrect recognitions can be included in the search results.

If the search does not give required results at the selected level of similarity, then reduce its value. Note that lowering the similarity level below 50% can lead to incorrect recognitions.

4. Select the type of search results sorting:  —by similarity level;  —by time (**5**).
5. Click the **Search** button.

> **Note**
>
> Once you start the search, you can stop it at any time. To do this, click the **Stop** button, which is displayed in place of the **Search** button.

The search according to the specified criteria will start.

> **Note**
>
> The first time you search by images, the results will appear with some delay (about three minutes).
>
> Next time, results may be delayed for other reasons. For example, if there is a lot of data in the archive or if the hard disk is overloaded.

The search results panel will display video frames with images that match the search criteria. The recognized image will be highlighted with a red frame, and the level of similarity will be displayed below.



To quickly export an image from a frame:

1. Click on the image track in the Surveillance window.
2. Click the  button (**6**).

The image will be saved to the folder specified in the settings (see Configuring export options).

Use case for Image search

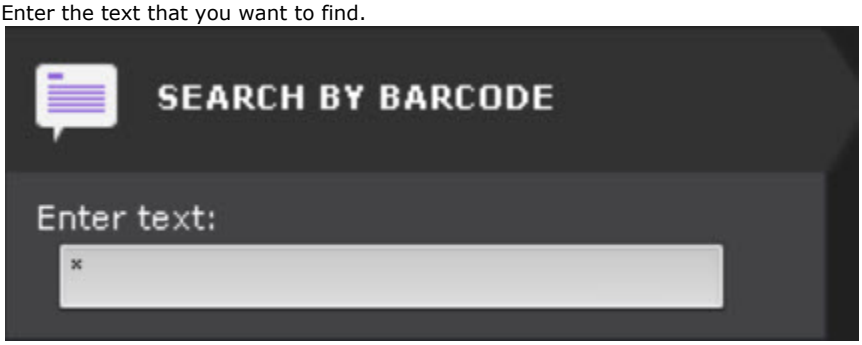
AI analytics extracts human appearance metadata and stores it in a database. Sorting through metadata sourced from multiple cameras, an intelligent algorithm identifies and presents similar individuals. Having said that, if a person is wearing a backpack, bag, or hat for example, the engine will search for people who have these same characteristics.

Search by barcode

Search by barcode allows you to find text in the archive that was detected when detecting barcode.

To search by barcode, do the following:

1. Set the search interval (see Setting a search interval).
2. Enter the text that you want to find.



> **Note**
>
> - To search by all detected barcodes, you must enter * (asterisk)
> - The minimum number of characters in the search text is three.

3. Click the **Search** button.

> **Note**
>
> After the search is started, you can stop it at any time. To do this, click the **Stop** button that replaces the **Search** button.

The search process will start according to the specified criteria. The search results panel will display the frames with barcodes that contain text from the search query. When you hover over the search result, the recognized text in the barcode will be displayed.



Heat map

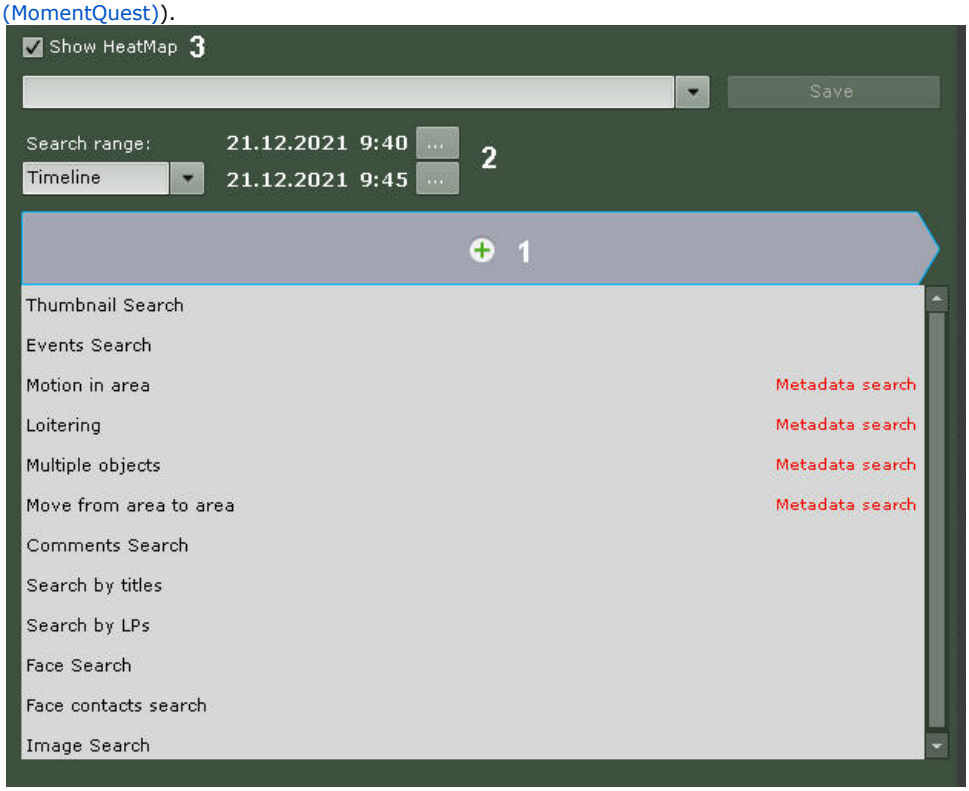
Configuring the heat map

> **Attention!**
>
> At least one metadata source is required for displaying a heat map (for example, an object tracker—see General information on metadata).

The heat map allows you to check the movement activity in the frame and determine the areas where the objects move mostly.

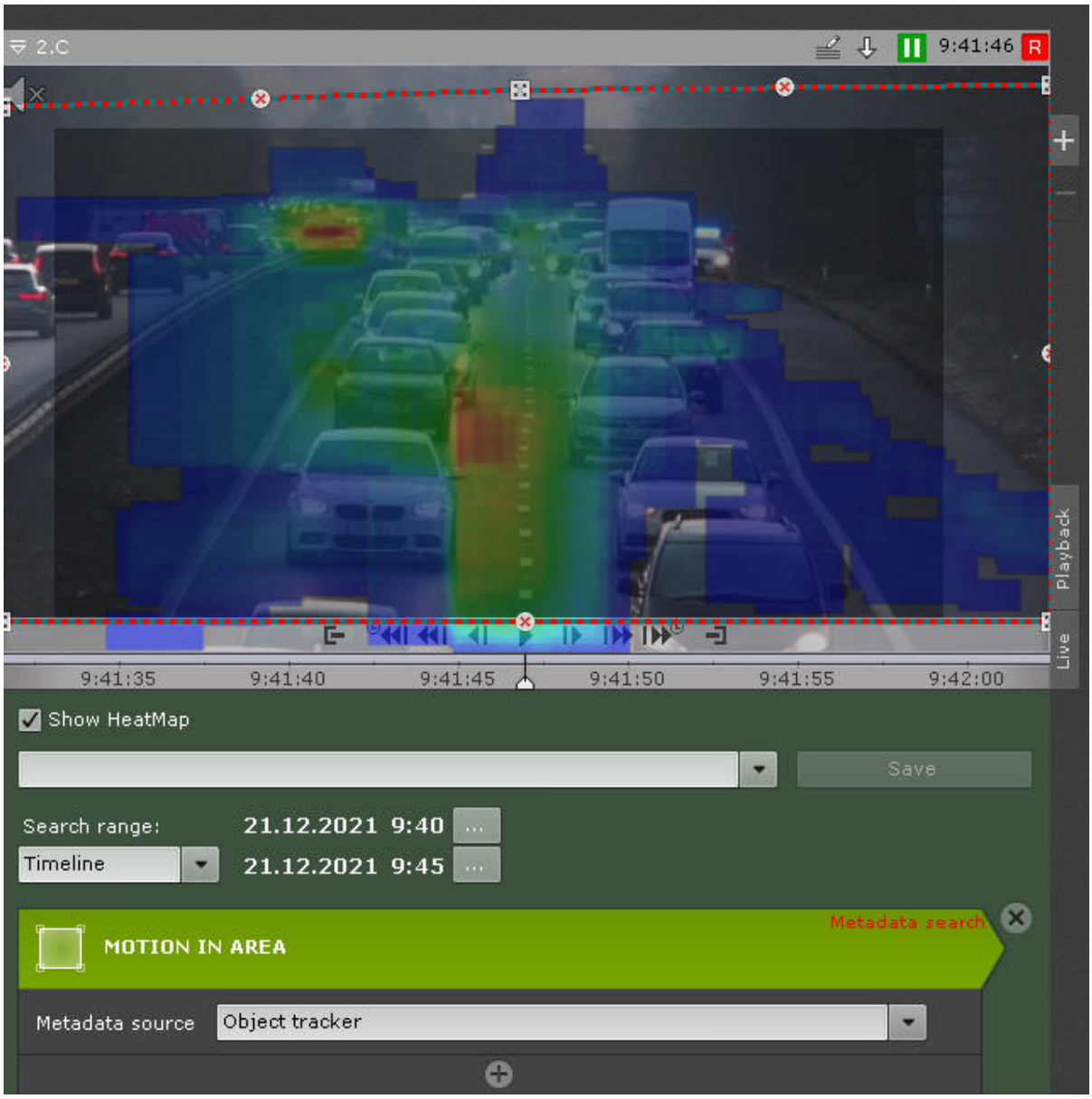
To display a heat map, do the following:

1. Select the type of search using metadata (**1**, see Search by LPs, Search for similar face, Forensic Search for Fragments (MomentQuest)).



2. Set the time period, according to the data from which the heat map should be generated (**2**, see Setting a search interval).
3. Set the **Show HeatMap** checkbox (**3**).
4. Click the **Search** button.

When the search is completed, a heat map will be displayed on the map:



The colors on the map change from blue to red depending on the activity:



where blue is low activity, red is high.

Configuring advanced heat map options

You can specify one or more additional parameters to improve the accuracy of search results. The number of possible additional parameters depends on the search criteria (see Configure the search parameters).

To set additional search parameters, click the  button (see Configure the search parameters). When setting additional parameters, only the zones of the heat map with objects detected motion will be displayed.

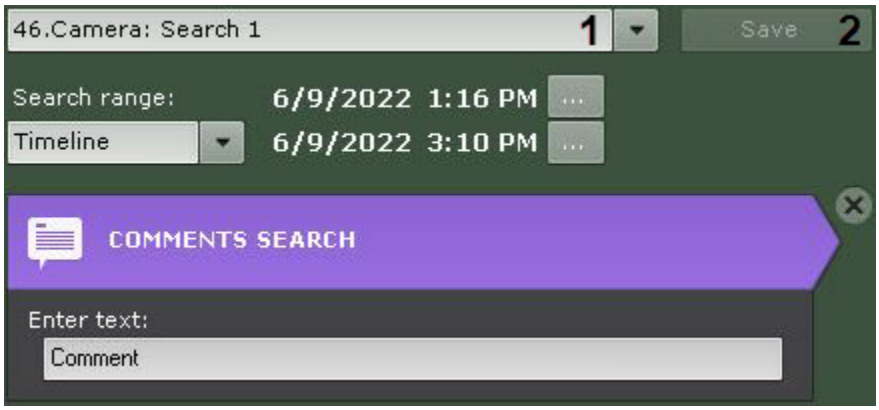
For example, setting the color range of an object allows you to more accurately highlight areas of the video where objects of the specified color are moving (see Configuring object color). In this case, the size of the heat map may change slightly while maintaining focus on moving objects.

Saving search queries

Saving a search query allows you to:

- quickly retrieve its results;
- apply search criteria to other cameras.

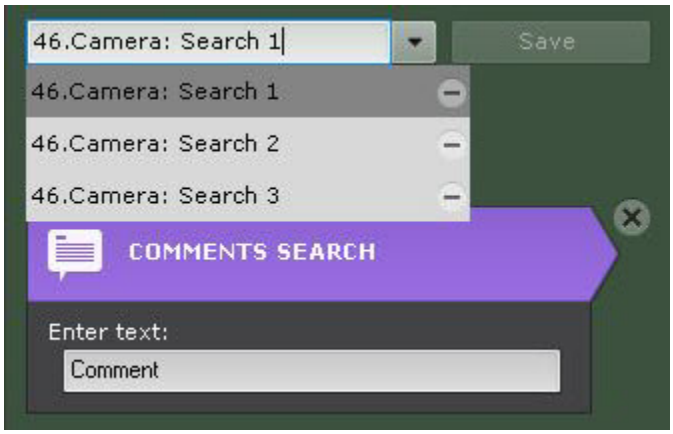
To save a search query, specify a name (**1**) and click the **Save** button (**2**). After this, the tab for the search query becomes available in the lower-right corner of the viewing tile in Archive mode (see Viewing the results of a saved search query).



Attention!

The search range can not be saved.

To apply the saved search criteria to another camera's archive, switch the camera to Archive Search mode and select the required search query.



To edit a search query, view the list and select the relevant query.

Changes are not saved until the **Save** button is clicked. If the query name is changed, the query is saved under the new name and the old, unchanged query remains available.

To delete a search query, click the  button.

Switching between search results

If a search was run more than once and the user did not exit Archive Search mode during that time, it is possible to switch between search results.

> **Note**
>
> The number of stored results is limited only by the amount of RAM in the server.

Click  on the search control panel to switch to the previous search result, and click  to switch to the next result.

Each time you switch between results, the search results panel displays the moments corresponding to the previous/next result.

Working with search results

Viewing search results

The Search Control Panel shows how many episodes are found when the search is complete.



The search results panel displays the precise moments in an archive that correspond to the defined search criteria. The precise time of each moment is displayed under it (**1**). The found results are the beginning of video recordings.

Note

- To copy the time and the start date of the video fragment to the clipboard, right-click them.
- An alarm object is outlined with a red frame.



A scroll bar is located on the right side of the search results panel (**2**). Under it, there is a scale slider (**3**).

When positioning on the timeline (see Navigating Using the Timeline), the positioning is automatically performed among the search results. The search result closest to the positioning point will be highlighted among the search results.

Note

If you select search results close to the limits of the timeline (see Setting a search interval), the search range may shift.

You can filter the search results and keep only the important episodes. To do this:

1. Double-click the episode, that you want to keep. Its thumbnail is tagged with a star  .

Note

To remove the tag, click the star again .

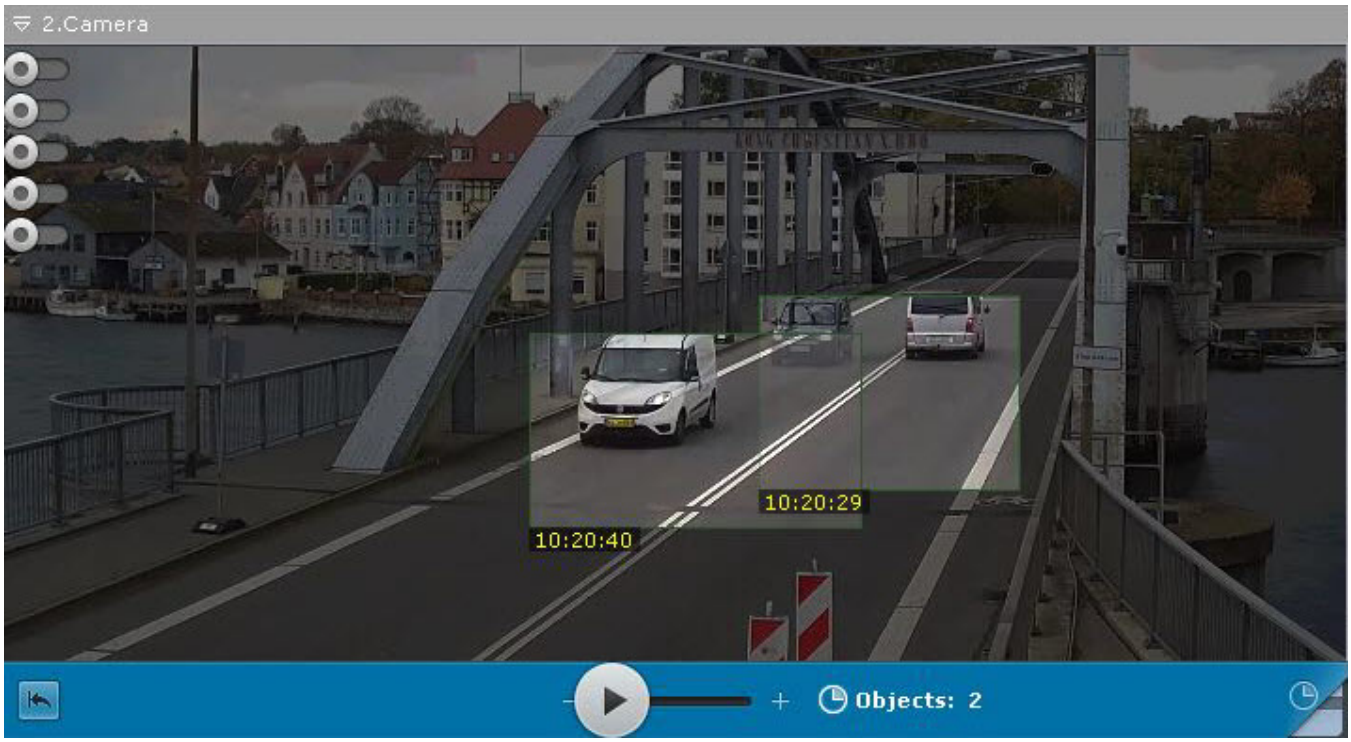
2. Tag all the episodes you want to keep.
3. Click the **Clear** button to delete untagged episodes from the search results.



Viewing Search Results In TimeCompressor

When you search recorded video for motion events by metadata (Search by LPs, Face search, Forensic Search for Fragments (MomentQuest)), you can view results in the TimeCompressor mode.

To do this, click the  button on the timeline in the camera window.



Playback of video fragments

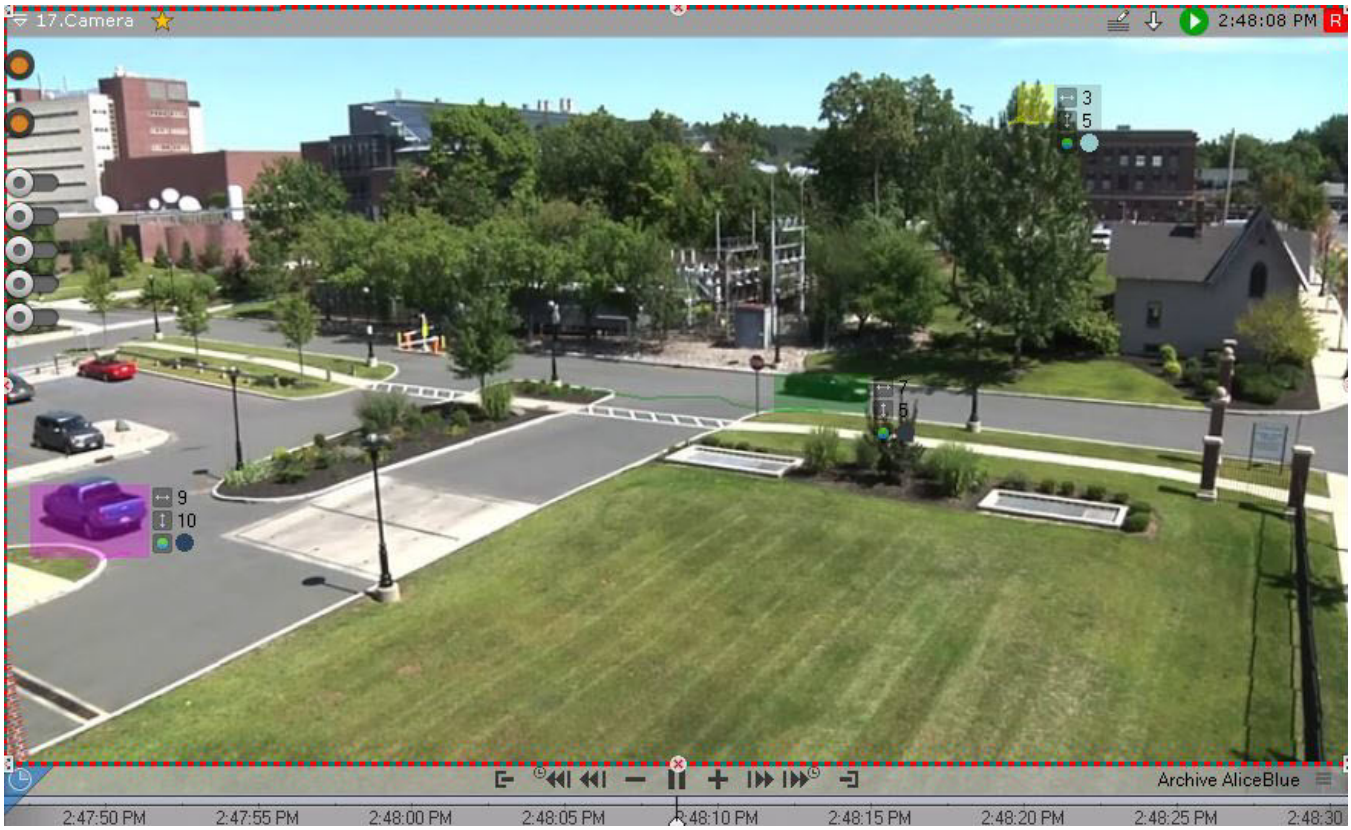
To view the video fragment corresponding to a found moment in the archive, complete the following steps:

1. Left-click the found moment on the search results panel.
2. Using the playback panel (**1**), start playback of the fragment in the viewing tile (**2**).



By default, the playback starts with the time specified under the thumbnail. You can use the control (**3**) to change the start time. If the control is in the leftmost position, playback starts 4 seconds earlier then the start time. If the control is in the far right position, playback starts 4 seconds later.

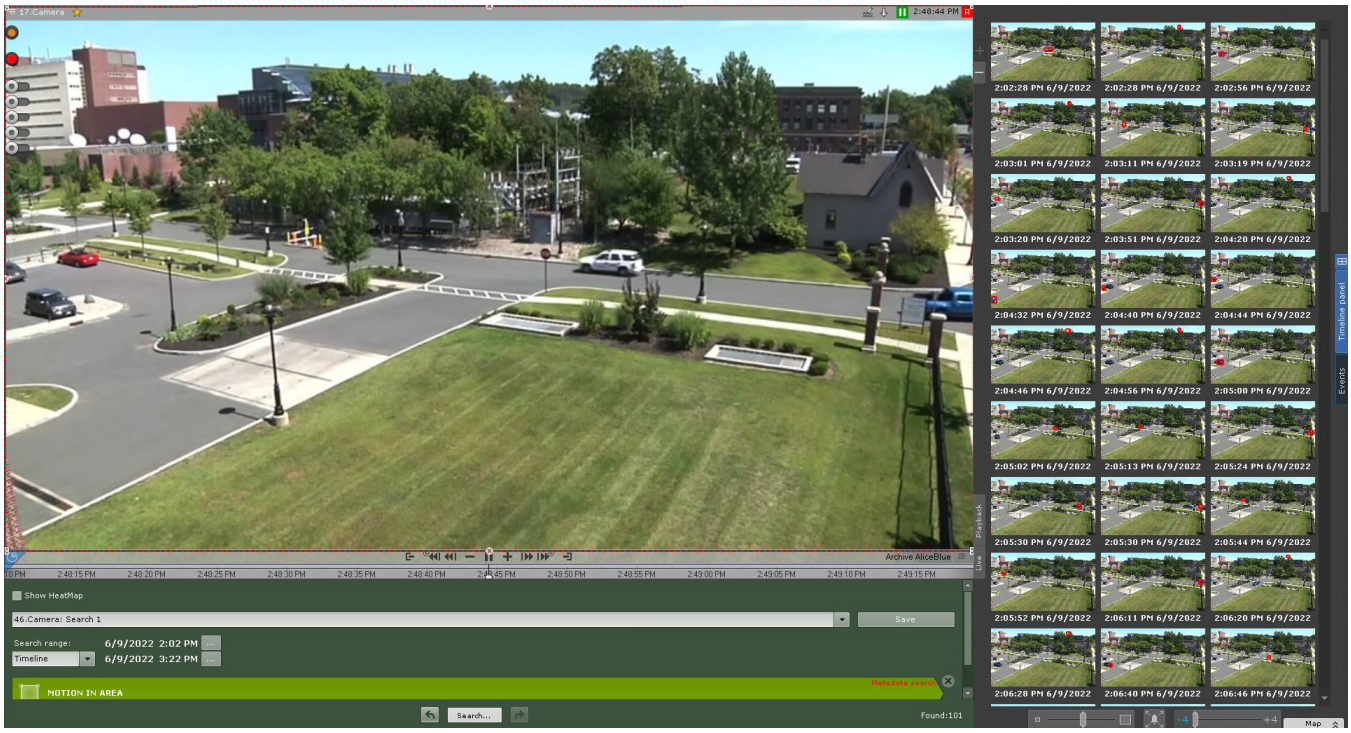
> **Note**
>
> If object tracking is activated in the viewing tile, then the properties of tracked objects (width and height as a percentage of the width or height of the frame) are displayed when viewing video fragments found through forensic search.



Note

To switch between video fragments, use the corresponding buttons on the playback panel or on the advanced navigation panel (see the sections titled Navigation using the advanced panel and Navigating using the Playback Panel).

Extreme zooming a camera window makes the Search Conditions and Archive Navigation panels become hidden (see Scaling the surveillance window).



Enlargement of found moments

When you find moments in archive video, you can enlarge the following:

- object that triggered the detection tool (during event search);
- track (during forensic search);
- commented area of the frame (during comment search).

To do so, above the search results, click the  button.



Attention!

Enlargement occurs only in the following cases:

1. If the height and width of the visual item specified in the forensic search settings are less than 1/3 of the frame dimensions.
2. If the tracking object occupies less than 1/3 of the frame (for detection tool search).
3. If the object marked by the comment occupies less than 1/3 of the frame (for comments search).

In all other cases, the found moments are displayed in their entirety.

To close zoom, click the  button again.

Exporting the video fragments and repeated search

To export the video fragment corresponding to a found moment in the archive:

1. Double-click the found moment on the search results panel. The interval for export will be set apart from this moment until the next found moment.

   > **Important**
   >
   > Double-clicking the found moment will also cause a repeated search within the selected time interval for export.

2. Export the video (see Exporting Video Recordings).

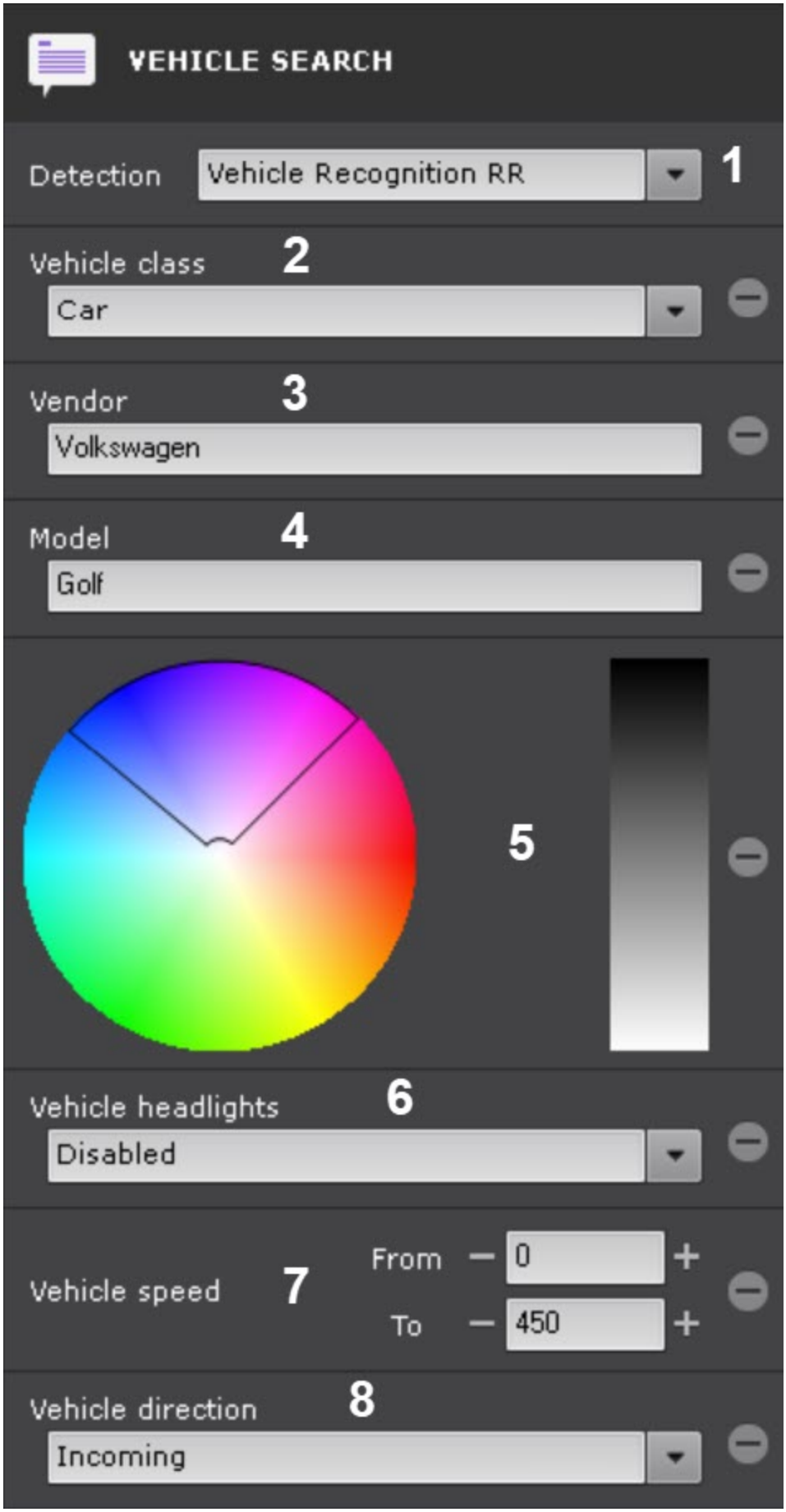
Vehicle search

Vehicle search allows you to find recognized vehicles in the archive, and to filter vehicles according to specified criteria.

You can search for vehicles in the following way:

1. Set the search interval (see Setting a search interval).

2. From the **Detection** drop-down list (**1**), select the detection tool, the alarms from which you want to use as a search criterion.


VEHICLE SEARCH
Detection
Vehicle Recognition RR
1
Vehicle class
2
Car
Vendor
3
Volkswagen
Model
4
Golf
5
Vehicle headlights
6
Disabled
Vehicle speed
7
From
0
To
450
Vehicle direction
8
Incoming

3. If necessary, set additional search criteria by clicking the  button.
    a. From the **Vehicle class** drop-down list (**2**), select one of the following:
        i. Car.
        ii. Truck.
        iii. Bus.
        iv. Motorcycle.
        v. Mini truck.
        vi. Unknown.
    b. In the **Vendor** field (**3**), enter the full name of the car manufacturer in Latin letters, case insensitive. Examples of correct spelling: Mitsubishi, Hyundai.
    c. In the **Model** field (**4**), enter the full name of the vehicle model in numbers or Latin letters, case insensitive. Examples of correct spelling: Outlander, Creta, 406 (for Peugeot 406).

    > **Note**
    >
    > You can see a full list of possible vendors and models on this page.

    d. In the **Color** area (**5**), set the color of the vehicle (see Configuring object color).
    e. From the **Vehicle headlights** drop-down list (**6**), select one of the following:
        i. Undefined.
        ii. Enabled.
        iii. Disabled.
    f. In the **Vehicle speed** area (**7**), in the **From** and **To** fields, set the vehicle speed range depending on the selected unit of measurement in the **Speed detection** field in the detection tool settings (see Configuring License Plate Recognition RR):
        i. Kmph. Possible range: 0 to 450.
        ii. Mph. Possible range: 0 to 280.
    g. From the **Vehicle direction** drop-down list (**8**), select one of the following:
        i. Undefined—the direction of movement of the vehicle is not detected.
        ii. Incoming— the vehicle is moving towards the camera.
        iii. Outgoing—the vehicle is moving away from the camera.

    > **Note**
    >
    > To delete a search criterion, click the  button.

4. Click the **Search** button.

> **Note**
>
> After you start the search process, you can stop it at any time. To do this, click the **Stop** button, which replaces the search start button.

The search process will begin based on the specified criteria. The search results panel will display footage of vehicles that meet the specified search criteria.

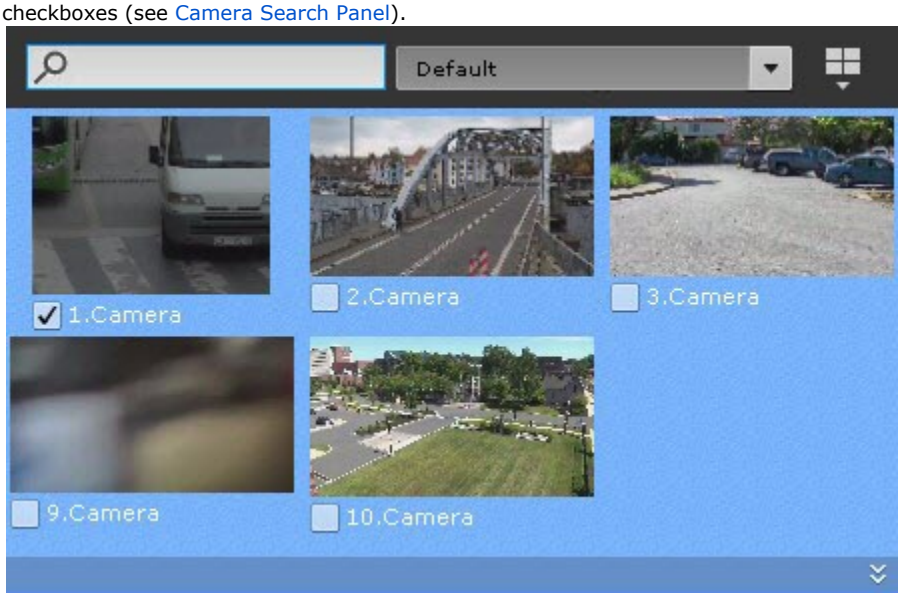

7:07:59 PM 2/14/2024
Car [Volkswagen Golf]
7:08:35 PM 2/14/2024
Car [Volkswagen Golf]
7:09:11 PM 2/14/2024
Car [Volkswagen Golf]
7:10:26 PM 2/14/2024
Car [Volkswagen Golf]

Simultaneous search in an archive of several video cameras

> **Attention!**
>
> The number of video cameras for search is not limited.

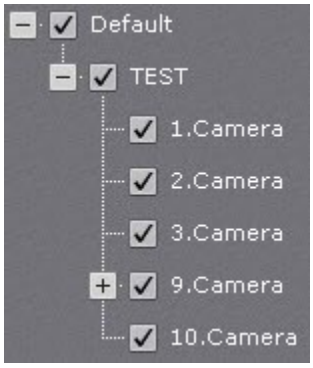
To search in the archive of several video cameras simultaneously, do the following:

1. Choose the search type and set its parameters (see Search in an archive of a single video camera).
2. On the Camera Search Panel, select the video cameras, the archive of which should be searched, by setting the corresponding checkboxes (see Camera Search Panel).



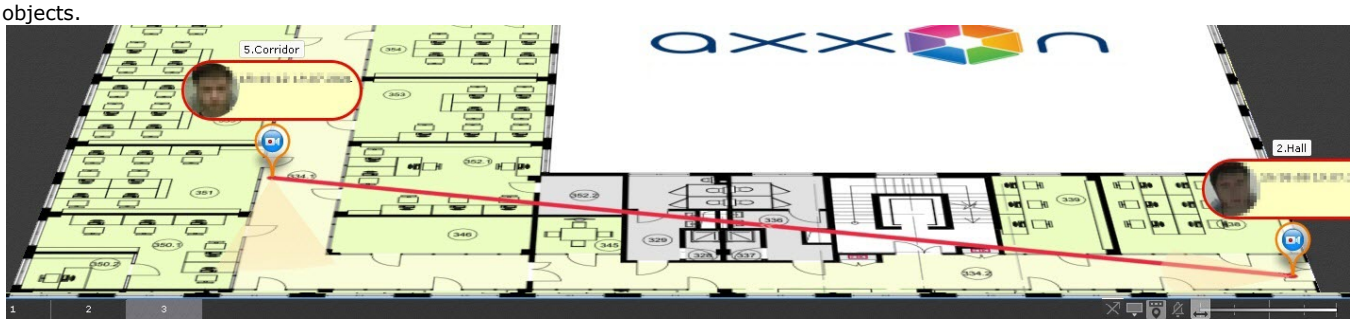
> **Note**
>
> By default, the checkbox is set next to the camera which was switched to the archive search mode. You cannot clear the checkbox next to this camera.
>
> If you want to change the active camera, it is necessary to reopen the archive search mode.

To search all video cameras in an Axxon-domain, open the Objects Panel (see Objects Panel) and set the checkbox next to the Axxon-domain.



3. Click the **Search** button.

If you are searching for faces (see Search for similar face) or for LPs (see Search by LPs) in the archive of several video cameras simultaneously, the interactive map (see Opening and closing the map) will display the approximate movement pattern of the found objects.



The time and date of recognition will be displayed next to the icon of each video camera.

> **Note**
>
> When searching in the archive of several video cameras simultaneously, the timeline is used (see The Timeline) to set the beginning and end of the viewed channel segments. This can affect the search result. The closer the timeline is, the smaller channel segments are used for the search.

Working with fisheye cameras

Viewing modes for video from fisheye cameras

Axxon One allows viewing the video stream and video archive from fisheye cameras, dewarping the video image into one of the following formats:

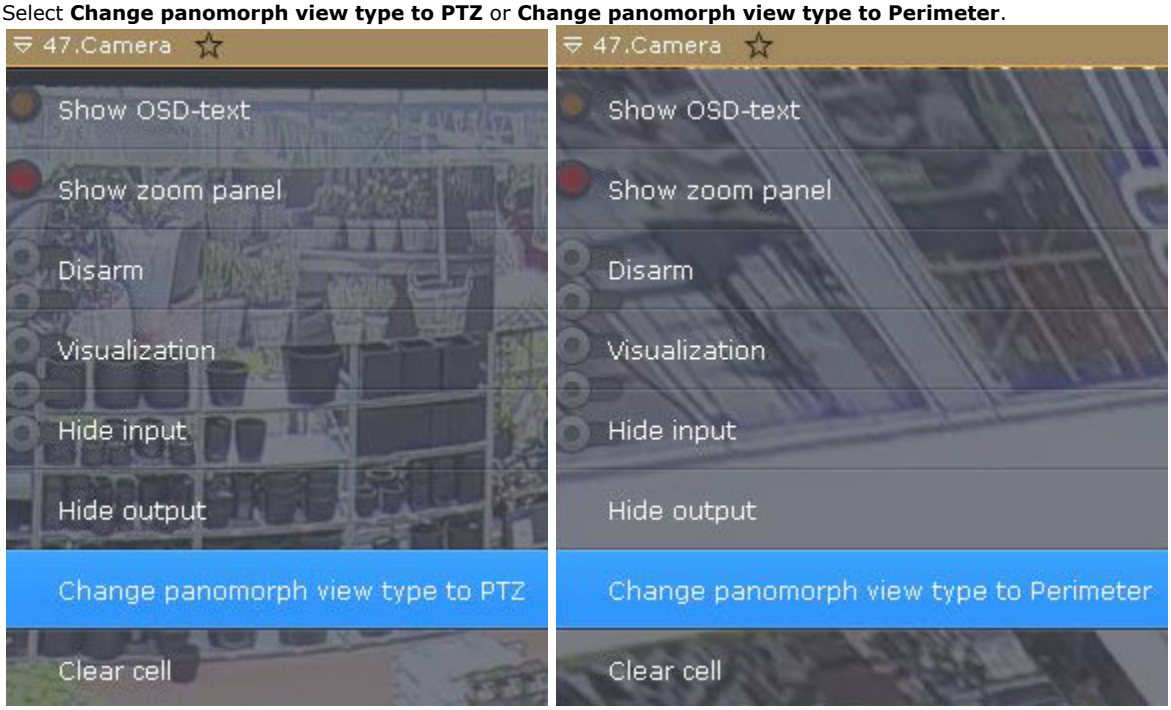
1. 360° panorama.
2. Regional view.
3. 180º panorama (for video camera with an Immervision lens).

Selecting viewing mode for videos from a fisheye camera

By default, fisheye camera video viewing mode setting is taken from device settings (see Configuring fisheye cameras), or from layout settings (see Selecting default functions for viewing tiles).

To change the viewing mode, do the following:

1. Open the camera's context menu.
2. Select **Change panomorph view type to PTZ** or **Change panomorph view type to Perimeter**.



Note

This setting is not preserved if you switch to another layout.

360 degree Panorama and Regional view (virtual PTZ)

By default, video from fisheye cameras is displayed in viewing tiles as a 360° panorama.

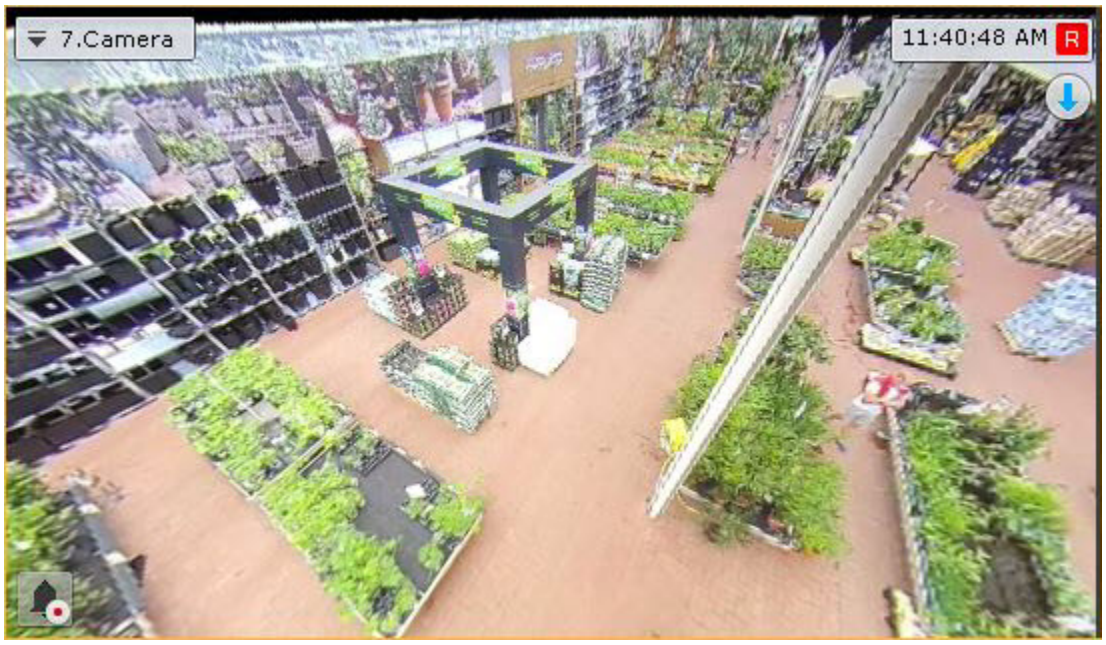
> **Note**
>
> This display format is only available in Live Video and Archive Video modes.



When digital zoom is applied to video (see Digitally Zooming Video Images) by one notch or more, regional viewing begins.

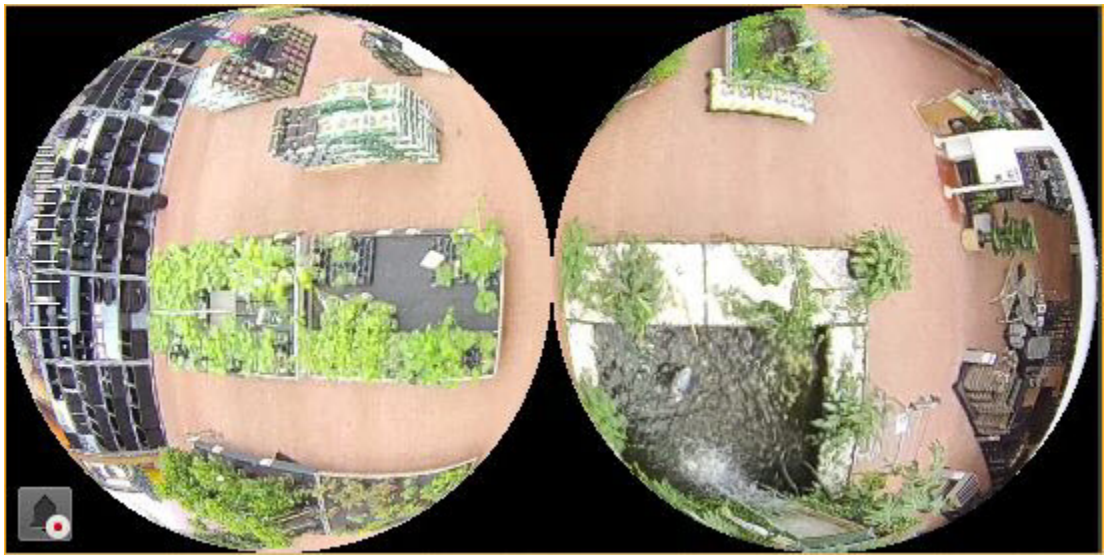
The following actions are available when viewing video in this format:

1. Point & Click functionality (see Control using Point&Click).
2. Change the angle of view of the fisheye camera, by left-clicking in the viewing tile.



In both viewing modes, all standard video surveillance functions are available for the fisheye camera.

When using a dual lens fisheye camera, the default viewing mode is set to two 180° views.



When you zoom in one of the images, both views will be merged into a single panoramic view.



180 degree Panorama

This viewing mode is available for:

- cameras with Immervision lenses;
- dual lens fisheye cameras.

> **Note**
>
> If the video camera is wall-mounted, the angle of view cannot be configured (see Configuring fisheye cameras).



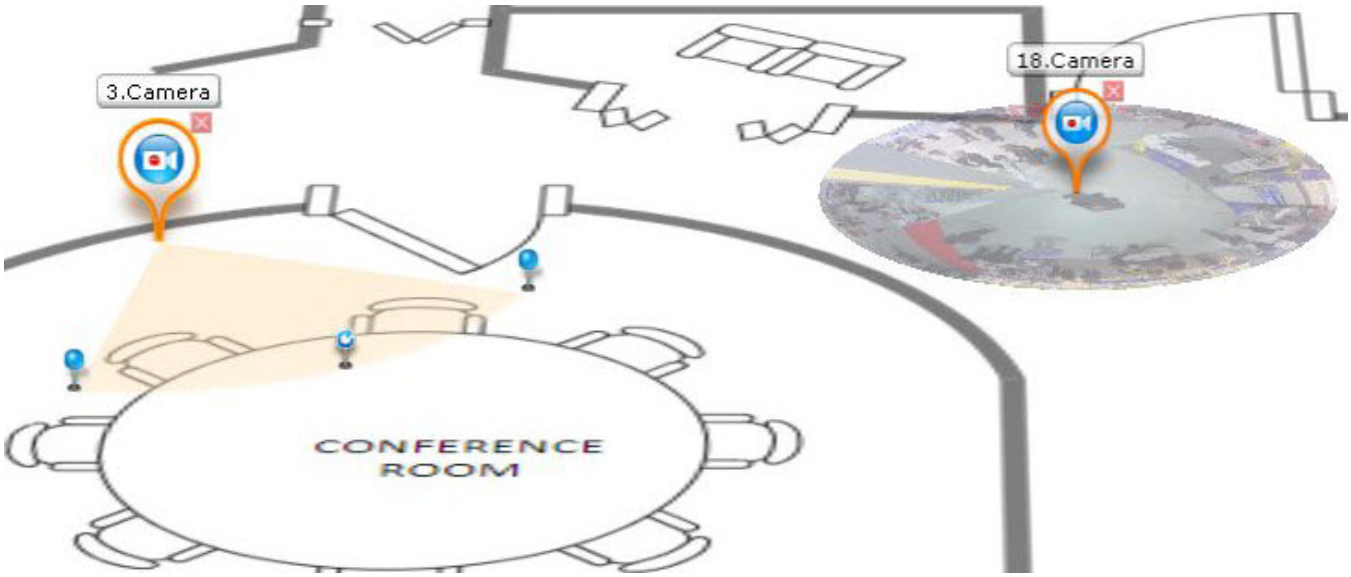
To set the viewing angle, click and hold the  button while moving the cursor to the left or right.

Point&Click (see Control using Point&Click) and all standard video viewing functions are available when viewing video in this format.

Fisheye cameras on an interactive map

Viewing video and controlling a fisheye camera from the map

If a fisheye camera is ceiling-mounted (this position is selected in the video camera settings, see Configuring fisheye cameras) and a 360° field of view is specified for it on the map, the video from the camera is displayed on the map in real time.



To refocus the angle of view of a fisheye camera so that a chosen point in the viewing tile becomes the center of the frame, left-click that point (this is the Point & Click function, see Control using Point&Click).

Note

If the viewing tile for the fisheye camera is inactive when it is clicked, the first click on the video on the map activates the viewing tile. The second click activates the Point & Click function.

Fish-eye cameras in immersive mode

In immersive mode (see Immersive mode), the video from a fish-eye camera is displayed on the entirety of the video surveillance screen, above the map display, as virtual PTZ (see Viewing modes for video from fish-eye cameras).



In immersive mode, only the following video surveillance functions are available for fish-eye cameras.

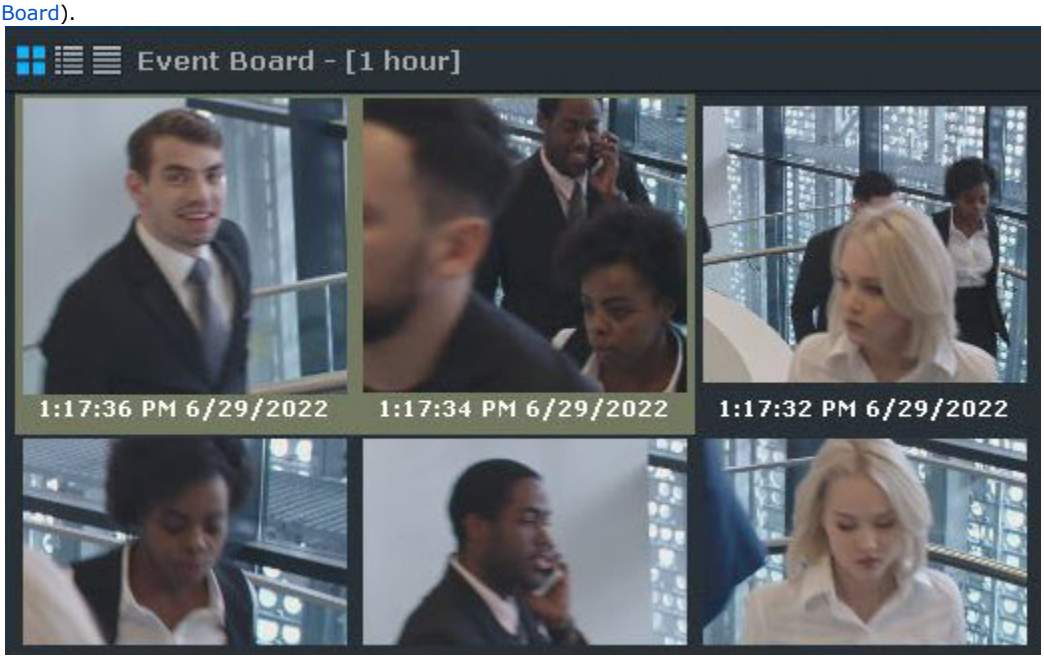
1. Digital zoom via mouse scrolling (see Enlarging a video image using the mouse scroll wheel).
2. Point&Click functionality (see Control using Point&Click).
3. To change the angle of view of a fish-eye camera, move the mouse around the video image while holding down the left mouse button.

To exit immersive mode, click the  button.

Face recognition and search

Face recognition events are registered in the System Log (see The System Log).

These events can as well be displayed on the Events Board (see Working with Event Boards) or Dialog Board (see Working with Dialog Board).



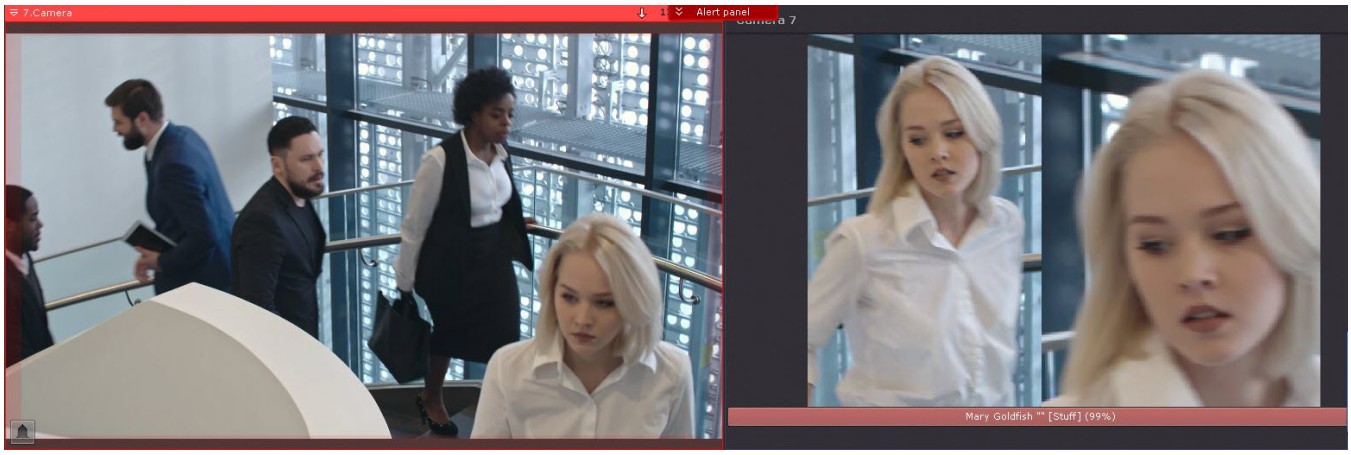
If you activate the age and gender information collection, its results will be displayed on the panel and saved into the System Log (see Configuring the Face Detection TV).



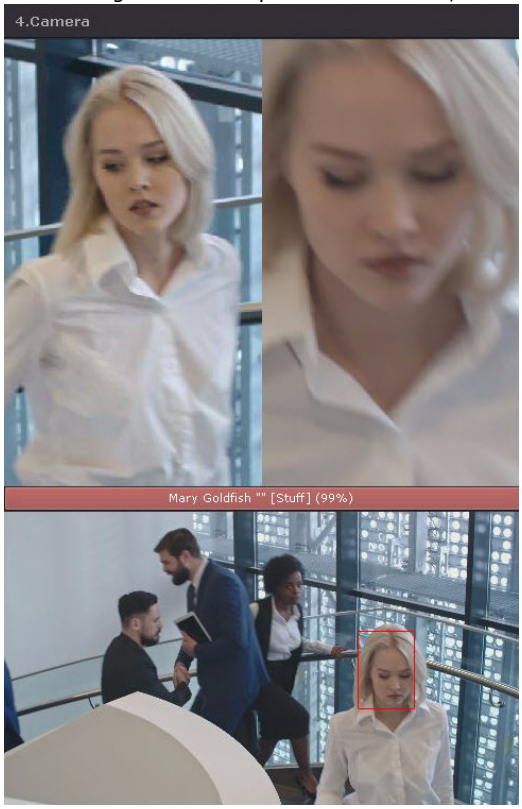
If the Camera window is linked to the Event Board (see Linking cells), you can double click on an event to start the Video Footage search for sequences containing the recognized face.

If you have created any lists of faces, configured an alarm on facial recognition, and linked the Camera window to the dialog board, you will have the following information on screen upon recognition a person that belongs to the list:

1. Reference photo from the List of Faces.
2. Close up shots of faces captured in the scene.
3. Additional information about the person, and similarity percentage between the recognized and reference photos.

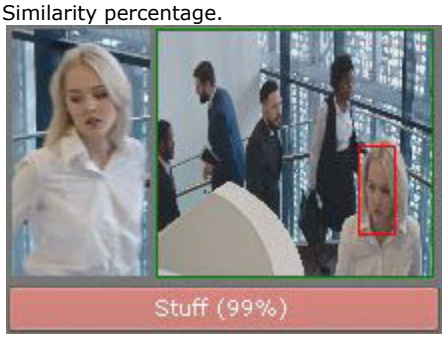


If the Dialog Board has a portrait orientation, its lower part will display the alarm video.



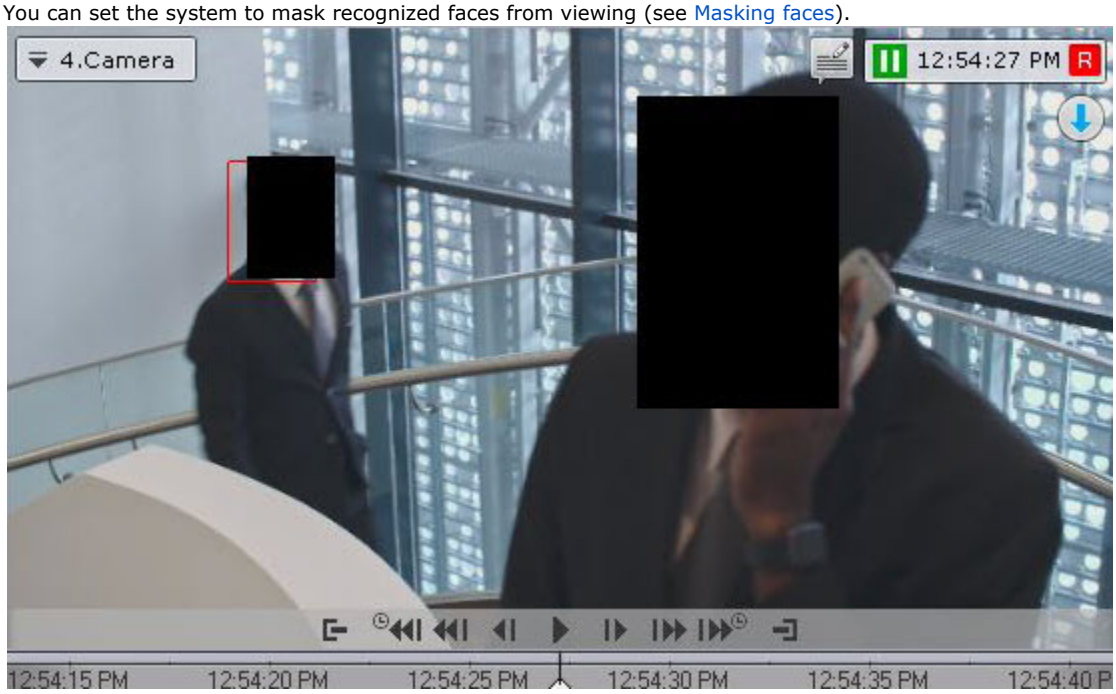
The Alarm notification panel will also include:

1. Reference photo.
2. Thumbnail preview of the source recognition video.
3. Name of the list of faces.
4. Similarity percentage.



You can search FR events in recorded video from one (see Face search) or multiple cameras (see Simultaneous search in an archive of several video cameras).

You can set the system to mask recognized faces from viewing (see Masking faces).



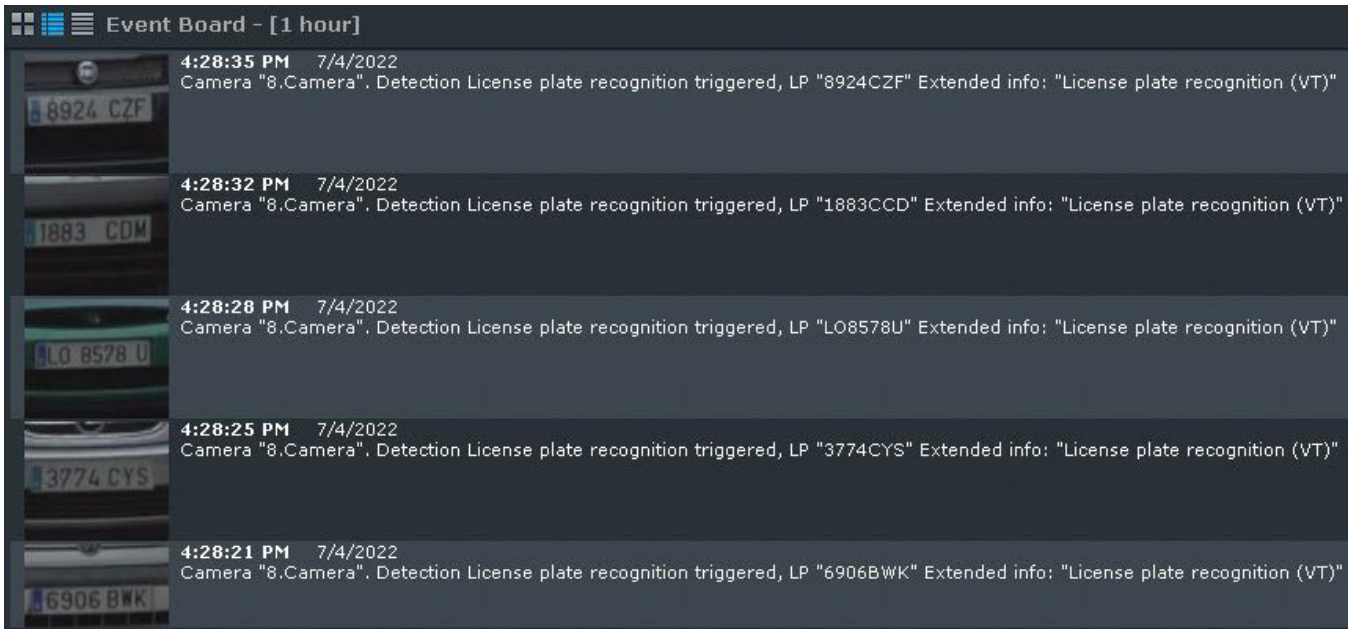
Vehicle number plate recognition and search

VMS logs every ANPR number (see The System Log).

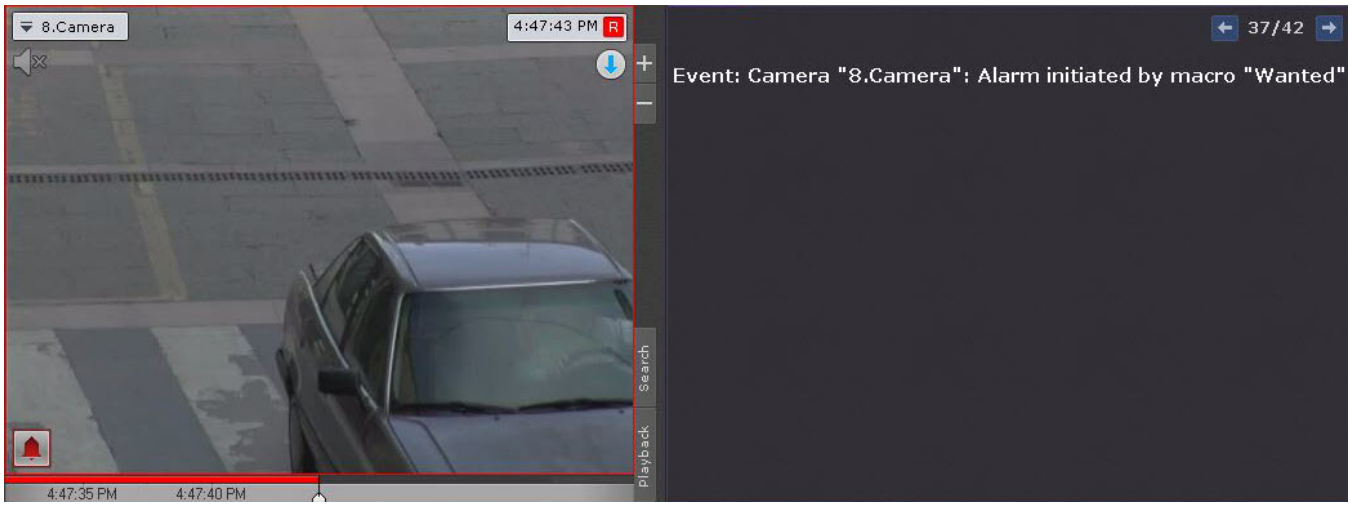
> **Attention!**
>
> Depending on detection tool settings, a delay may occur between the number recognition and the registration of the corresponding event (see Configuring License Plate Recognition VT, Configuring License Plate Recognition IV).
>
> The event is time-stamped with the time of recognition, not registration.
>
> For example, if a car passes the camera at 12:05:00, and the detection tool is set to a 10 sec timeout, the event will be registered at 12:05:10 and the event data will include 12:05:00 as the time of recognition.

> **Attention!**
>
> The standard license provides a more than 30-sec delay between the number recognition and the corresponding event (see Configuring License Plate Recognition VT.

All relevant events can be displayed on the Event Board (see Working with Event Boards) or Dialog Board (see Working with Dialog Board).



If you have created any LP lists in your system, you can program automatic responses (e.g. alarm triggering) to LP recognition events related to list's entries (see Configuring vehicle license plate recognition based on the created lists).


8.Camera
4:47:43 PM
R
37/42
Event: Camera "8.Camera": Alarm initiated by macro "Wanted"
Search
Playback
4:47:35 PM
4:47:40 PM

Temperature screening

In *Axxon One*, only two methods of temperature screening are available:

1. With the use of Mobotix M16 TR cameras. In this case, temperature values are displayed next to each recognized face's bounding box (see Face Detection and Temperature Control with Mobotix M16 TR cameras).



   Each face recognition event contains thermal measurement data which can be displayed on the Events Board (see Working with Event Boards).
2. With the use of built-in detection tools of selected camera models (see General information about embedded detection tools). Some cameras are capable to display a bounding box over the facial image along with corresponding temperature readings. If this option is available, it can be activated via the web interface of a particular camera.



Working with information boards

Resizing information boards

You can resize information boards in the same way as viewing tiles (see Scaling the surveillance window).

> **Note**
>
> When the Statistics Board is enlarged, the graph is enlarged as well, displaying data for a broader range of time. When the size of the Statistics Board is reduced, the opposite occurs.
>
> In both cases, the right-hand border of the graph is constant.

If an information board tile is linked to a viewing tile, at the first enlargement step (to 50%), the viewing tile and information board tile are displayed together and occupy all of the screen on one side.

> **Note**
>
> In this case, the first step takes into account the total size of the related cells: the related cells must be less than 50% of both sides of the layout.

Hiding information boards

Operators can hide information boards in a layout, if this is allowed in the settings.

To hide an information board, in its upper-right corner, click the  button.

> **Note**
>
> If configured, Dialog Board hides after you click a **Response Button** (see Configuring a Dialog Board).

If all cells in the layout have the same size, the space freed up after hiding an information board is allocated to the neighboring cells. Horizontal neighbors have priority over vertical ones.

If free space cannot be distributed horizontally, it is distributed between the vertical neighbors.

In more complicated cases (when cell sizes are different), an attempt is made to distribute the free space between horizontal neighboring cells. If this is not possible, free space is distributed between vertical neighboring cells. If even this second attempt is unsuccessful due to the layout configuration, the space remains empty.

Hidden information boards are displayed in two cases:

1. After switching to another layout and back to the original one.
2. When an event occurs that requires the operator's attention. A description of such events for each type of information board is given in the following table.

Types of information boards	Events that trigger board display
Dialog and Events	An event matching the board filtering settings occurs
Health	Server condition worsens
Statistics	New events occur

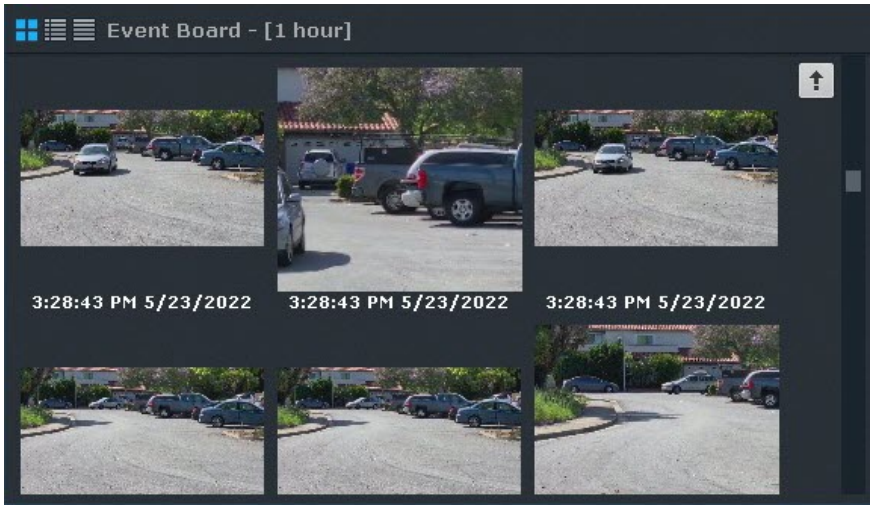
Working with Event Boards

Options for displaying information on Events Boards

Events Boards display information about selected system events. Configuration of the events to display is performed in the corresponding section.

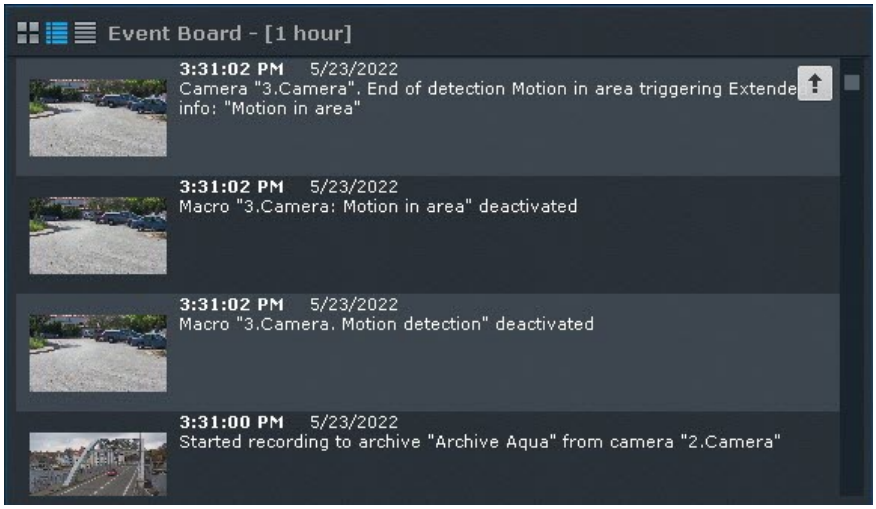
Events on the board can be displayed in three ways, chosen via the buttons in the upper-left corner of the board:

1. First frame of events and their time:



> **Note**
>
> The frame is not displayed when there is no recording in the archive.

2. First frame of events and text:



3. Text only:



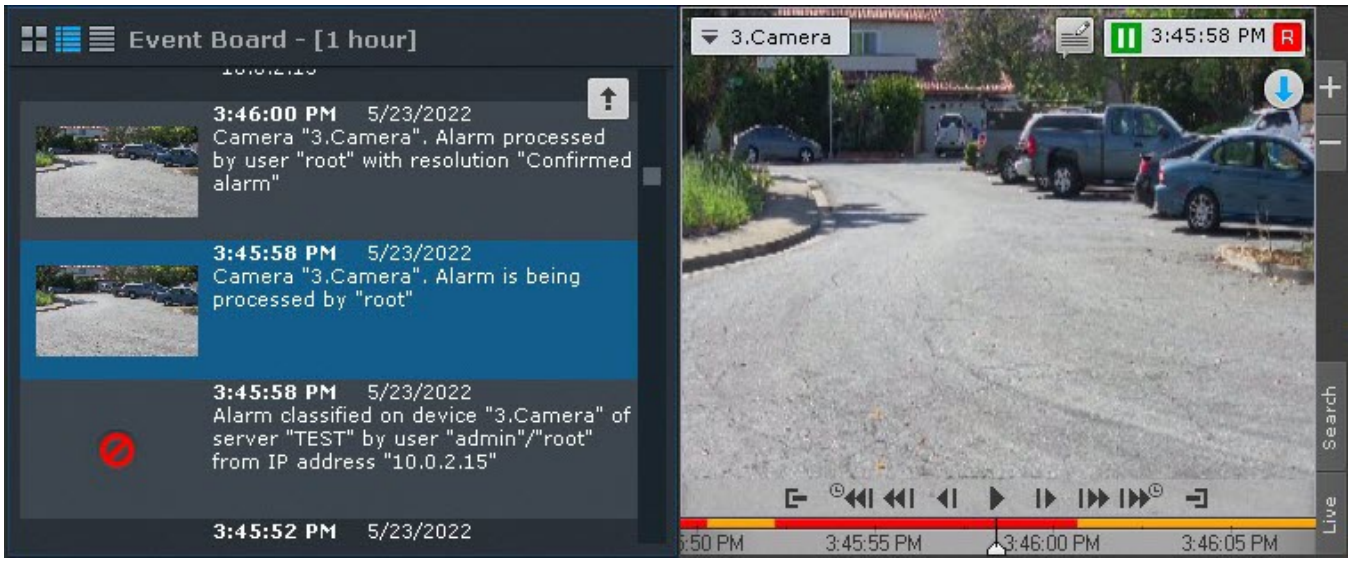
When a layout is switched to, by default the **Events Boards** is displayed as configured in the settings.

At the top of the list are the most recent events. If you are at the end of the list, you can use the  button in the panel's top-right corner to go to the most recent events. New events are highlighted for 4 seconds. The panel may include up to 100 events. If the number of events exceeds the maximum permitted value, the newer events will be displayed in place of older ones.

You can also access the events panel on the right side of the screen (see Viewing selected camera's detection tool triggering events). In this case, it includes only detection events for a selected camera.

Switching a camera linked to an Event Board to the archives

If an Event Board is linked with a camera, clicking an event will switch the camera to Archive mode at the point in time corresponding to the event.



Note

If there is no archive for a camera when an alarm occurs, the archive is positioned at the closest recorded archive entry.

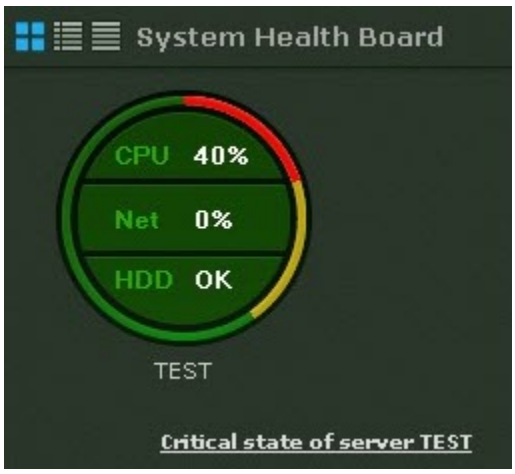
Note

If an Event Board is linked to several cameras, all cameras transition to Archive mode.

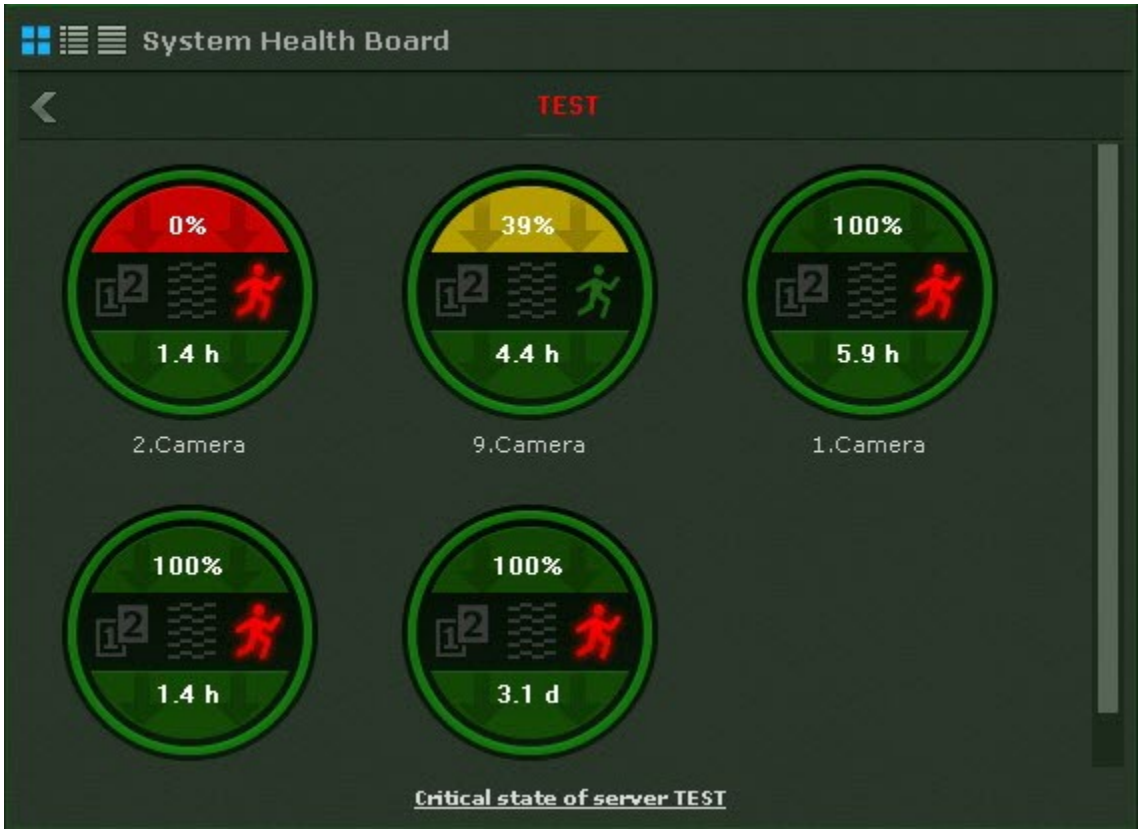
Working with System Health Boards

System Health Boards display the status of selected system servers and connected cameras.

By default, the panel displays the status of Servers.



To switch to viewing the status of cameras, click the diagram for the relevant server.



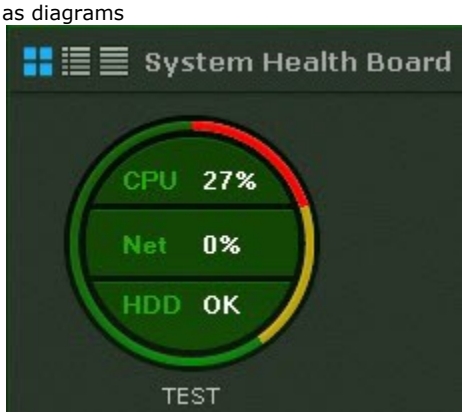
> **Note**
>
> In table mode, you can view server status by clicking the relevant line in the table.

To switch to a view of server status, click the  button.

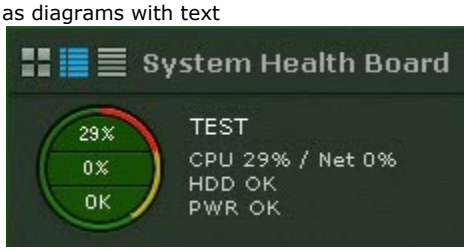
Viewing server status

Information about the status of servers can be displayed in three ways, chosen via the buttons in the upper-left corner of the board:

1. as diagrams



2. as diagrams with text



3. as a table



> **Note**
>
> Disconnected Servers are displayed at the end of the list with dimmed brightness.

Tables can be sorted by any column in any direction.

On each server the following metrics are monitored: CPU, Network usage, Disk subsystem status, Power status.

> **Note**
>
> The remaining time of the archive replication is also displayed in the table.

Areas of the diagram change color based on the respective status.

	CPU	Network	HDD
Red	Load >95%	Connection failure	Critical load on the disk subsystem, data loss when recording to archive over 10%
Yellow	Load from 85% to 94%	At 70% to 100% of capacity	Elevated load on the disk subsystem, data loss when recording to archive under 10%
Green	Load <85%	At less than 70% of capacity	Normal functioning of the disk subsystem (proper operation)

The edge of the diagram changes color based on the status of the connected cameras (see Viewing camera status).

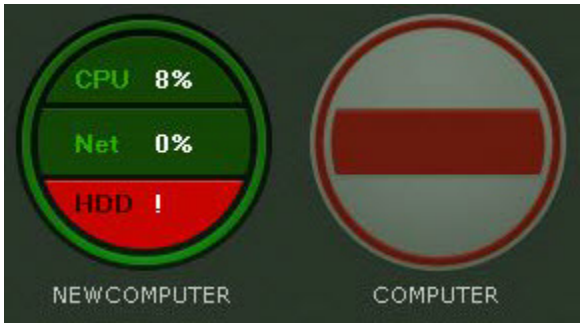
If the entire edge is green, all cameras are in normal condition. If part of the edge is yellow or red, some cameras have borderline or critical status.

Overall server status is determined from the above parameters as follows:

1. Normal – all components and cameras are normal.
2. Borderline – possible problems with the status of at least one component or camera.
3. Critical – at least one component or camera is in critical condition.

Server information is updated every thirty seconds.

If the connection to a server is lost, a corresponding icon is used to depict it.



If all servers are in normal condition, the bottom of the board displays a status bar with information about the number of monitored and distressed servers.



If the status of any server worsens, the status bar is replaced by a message. When the message is clicked, the server status is displayed (if the board is currently displaying camera status).



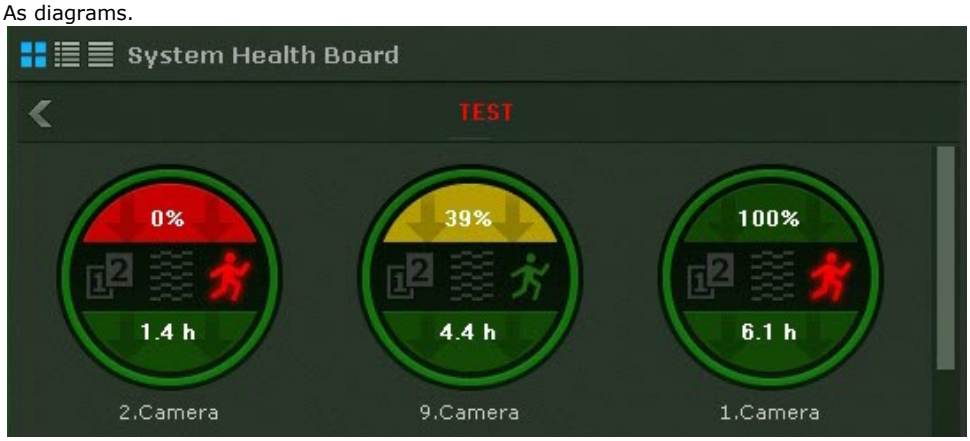
The message then closes and the status bar again appears.

> **Note**
>
> If the status of several servers worsens, a message is shown for the last one.

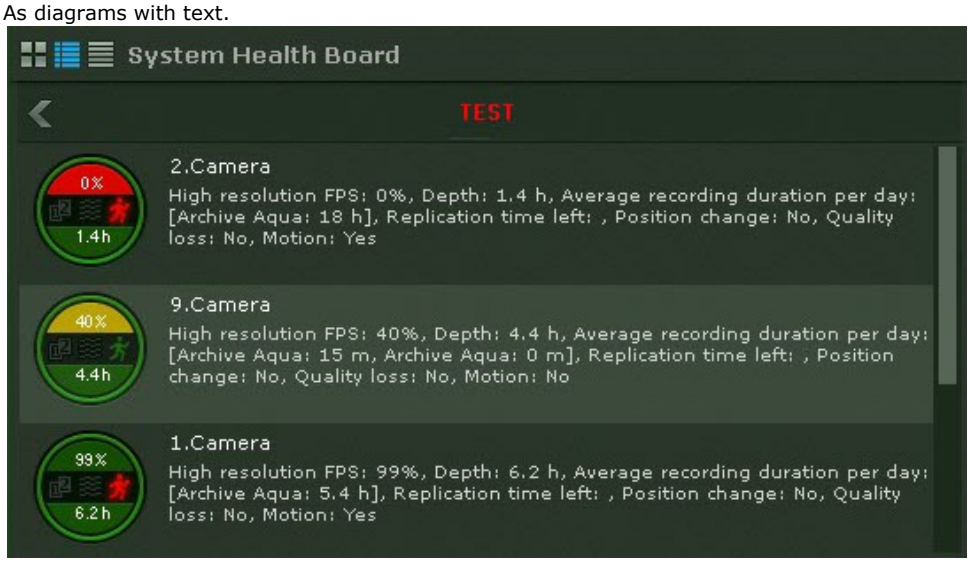
Viewing camera status

Information about the status of cameras can be displayed in three ways, chosen via the buttons in the upper-left corner of the board:

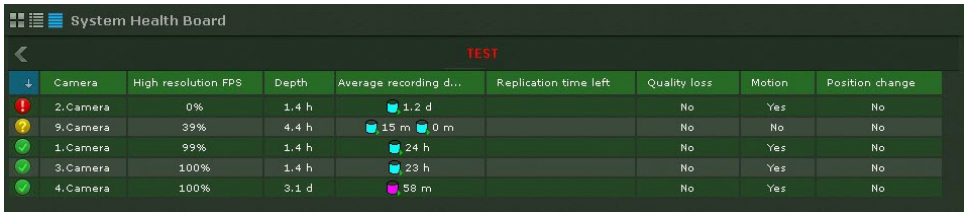
1. As diagrams.



2. As diagrams with text.



3. As a table.



> **Note**
>
> Disconnected cameras are displayed at the end of the list with dimmed brightness.

Tables can be sorted by any column in any direction.

The following information is displayed for each camera:

1. The percentage rate of actual video fps to the camera's high definition stream fps setting (see The Camera object).
2. Status of detection tools (loss of quality, position change, motion).
3. **Depth** refers to the number of hours or days from the start of the earliest video stored in any archive to the end of the most recent video (if archive recording is not configured for the camera, this section is colored gray on the diagram).
4. Average recording time, in hours per day, is the ratio of the total recording time to the age of the archive/retention time (time from the earliest stored video to now).

> **Note**
>
> For constant recording, this parameter value is equal to 24 hours. If the recording takes 50 percent of total time, the value is 12 hours.

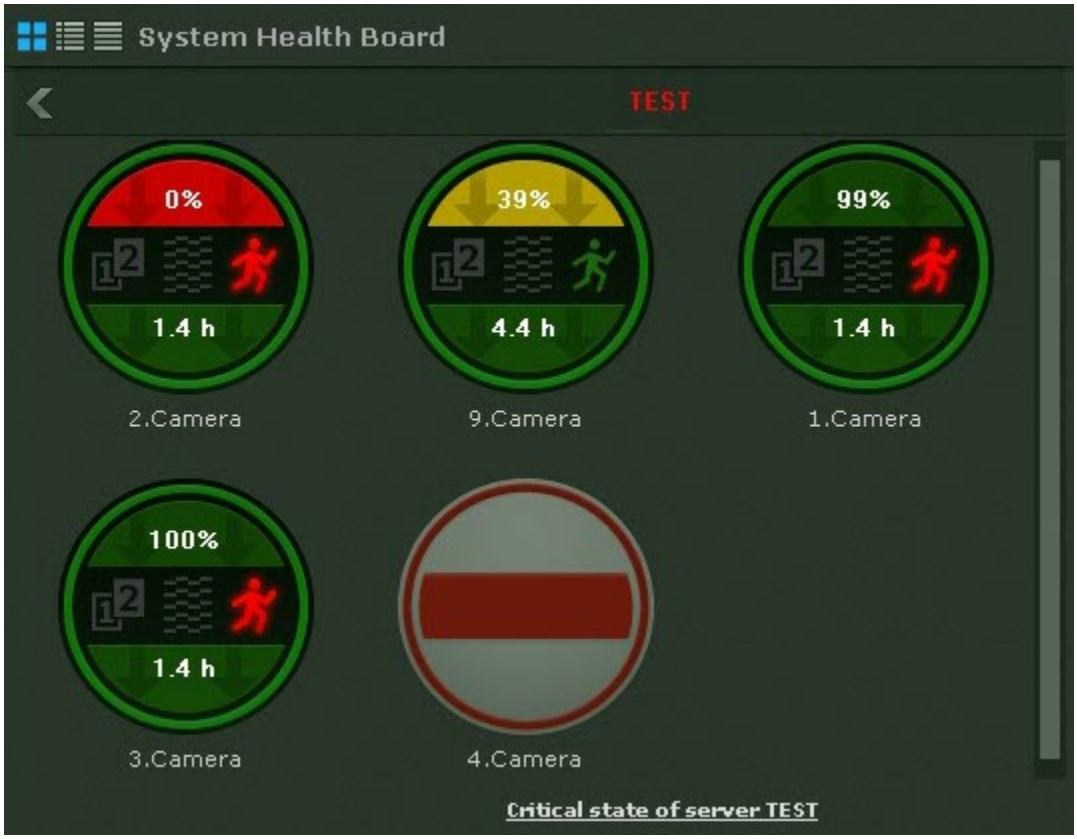
5. Remaining time for replication of the archive.

The camera status is measured based on the signal from the camera and stream rate:

1. Normal – camera signal present, frame rate is from 70% to 100%. The camera is colored green on the diagram and in the table.
2. Borderline – camera signal present, frame rate is from 20% to 70%. The camera is colored yellow on the diagram and in the table.
3. Critical – no camera signal or frame rate is less than 20%. The camera is colored red on the diagram and in the table.

Information is updated every ten seconds.

If there is no signal from a camera, the appearance of the diagram changes accordingly.



Information about detection tools is received in real time. Depending on the status of detection tools, the corresponding icons change color:

- green – detection tool status is normal,
- red – detection tool activated,
- gray – detection tool disabled.

Working with Statistics Boards

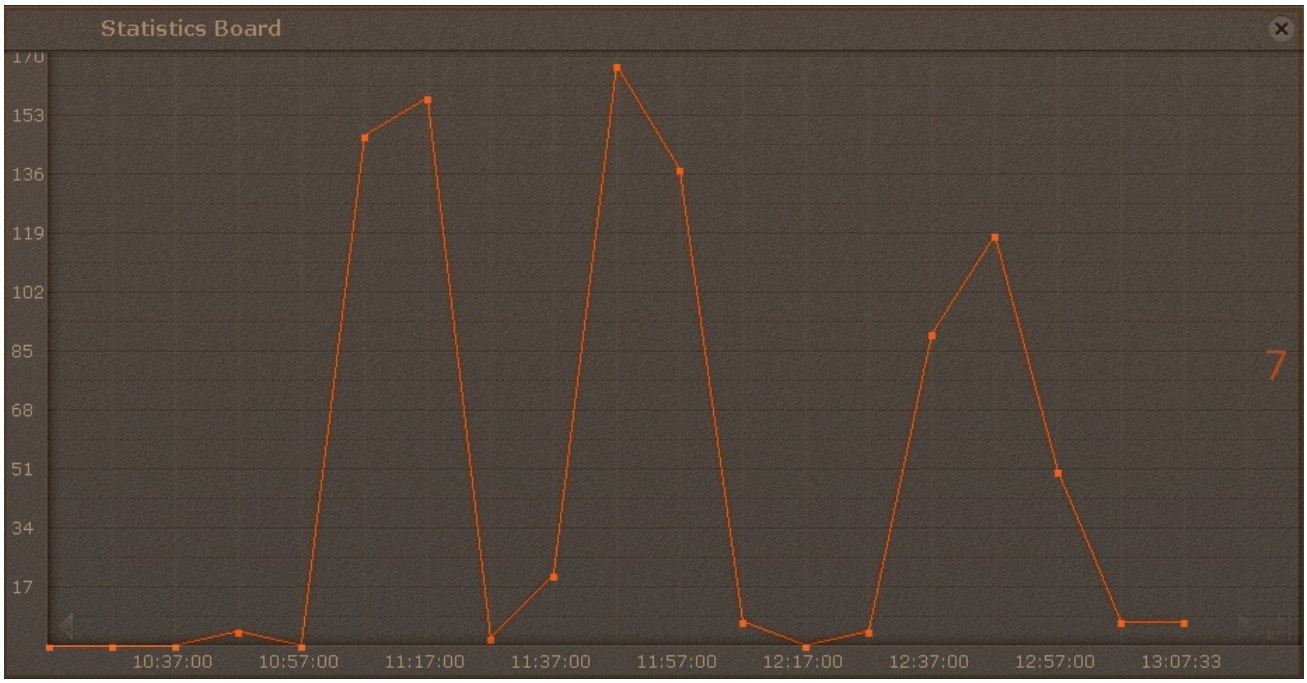
The Statistics Board is a graph of the number of events of a certain type for a specified timeframe. The type of events and amount of time between the points of the graph are configured in the board settings (see Configuring a Statistics Board).

The points of the graph change over time and depend on the current time and interval specified in the settings.

The points are calculated every minute/hour/day/etc. based on the selected unit of measurement (if the interval is specified in minutes, then every minute; if specified in hours, then every hour, and so forth) and is performed as follows:

1. The current time (last point on the graph) is rounded to the nearest whole unit of time (if the interval in the settings is specified in minutes, then the nearest whole minute; if specified in hours, then the nearest whole hour, and so forth).
2. This rounded time is used as the next-to-last point.
3. The formula for the other points is as follows: the adjacent point to the right, minus the interval of time specified in the settings.

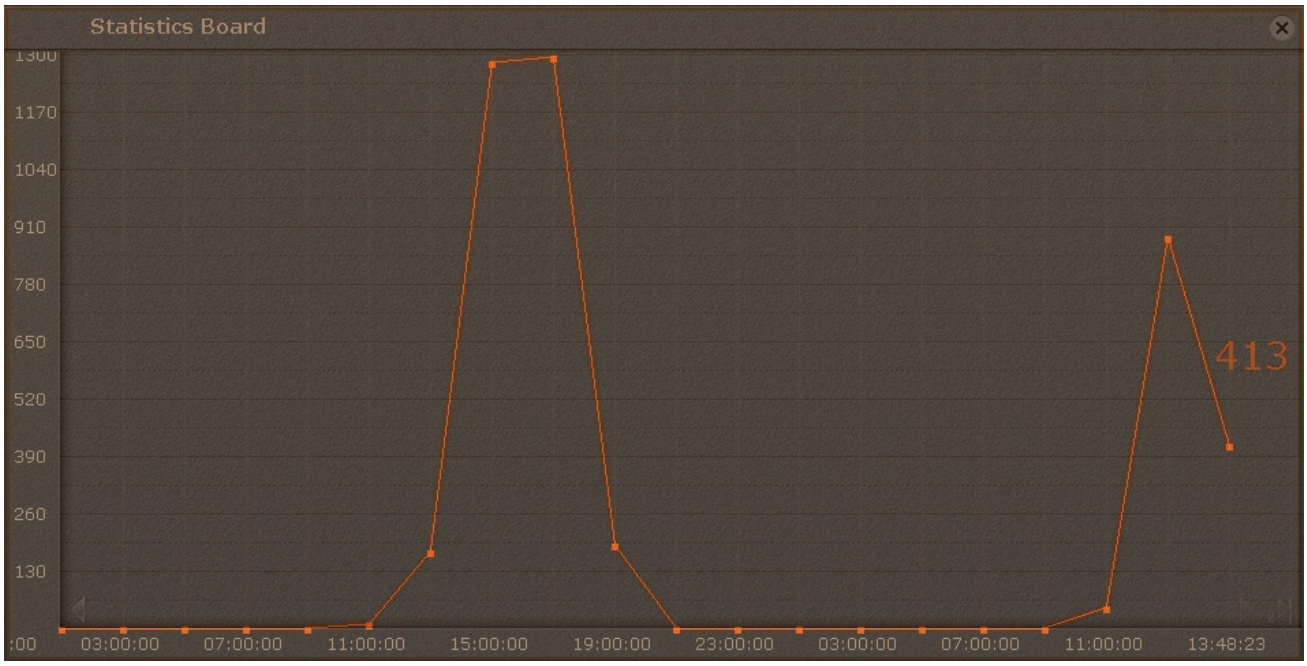
For example, the interval is set to **10** minutes on this sample graph here. The current time (**1:07:33 p.m.**) is the last point on the graph, so after rounding this to the next whole minute we get the value for the next-to-last point: **1:07:00 p.m.** Correspondingly, the points before it are **12:57:00 p.m.**, **12:47:00 p.m.**, etc.



When the current time becomes **1:08:00 p.m.**, the points will be updated to **12:58:00 p.m.**, **12:48:00 p.m.**, etc.

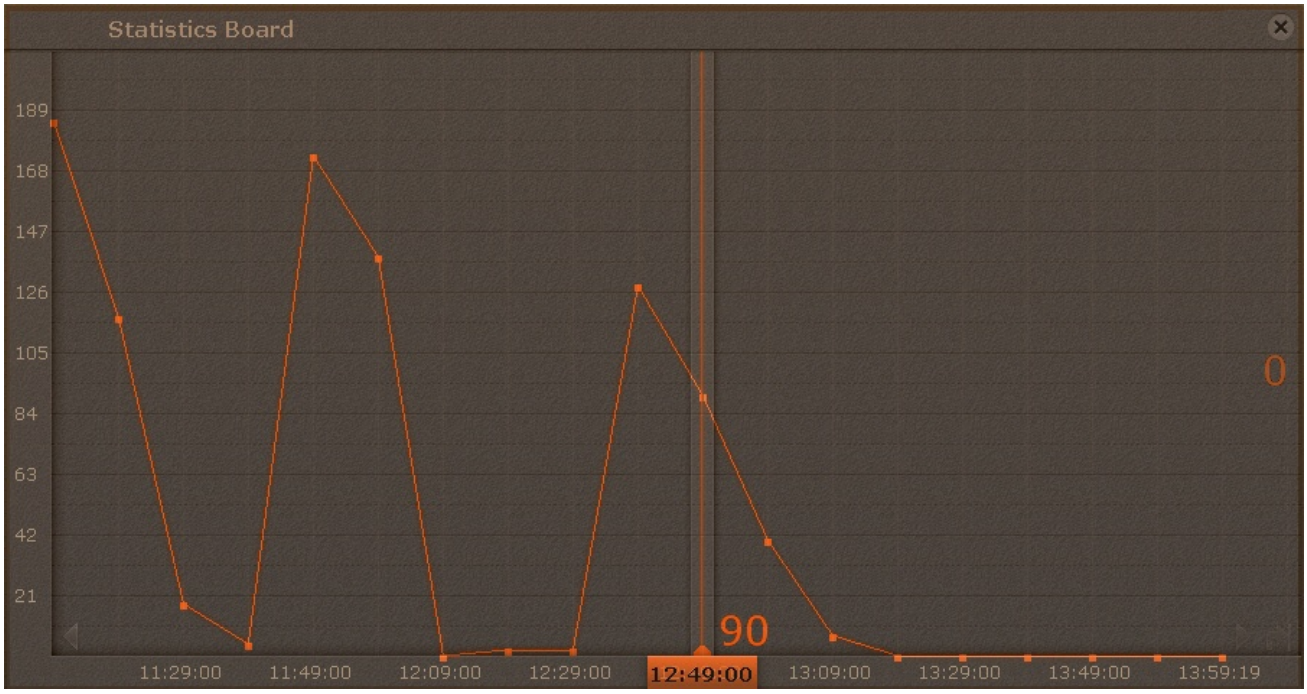
The graph displays the current number of events. The number of events is recalculated every minute and does not depend on the interval chosen.

For example, for this graph with a time interval of **2 hours** and a current time of **1:48:23 p.m.**, the current number of events equals **4 13**, for the period from **11:48:00 a.m.** to **1:48:00 p.m.**



To scroll through the graph, use the arrows  on the graph edges. To jump to the last point on the graph, click the  button.

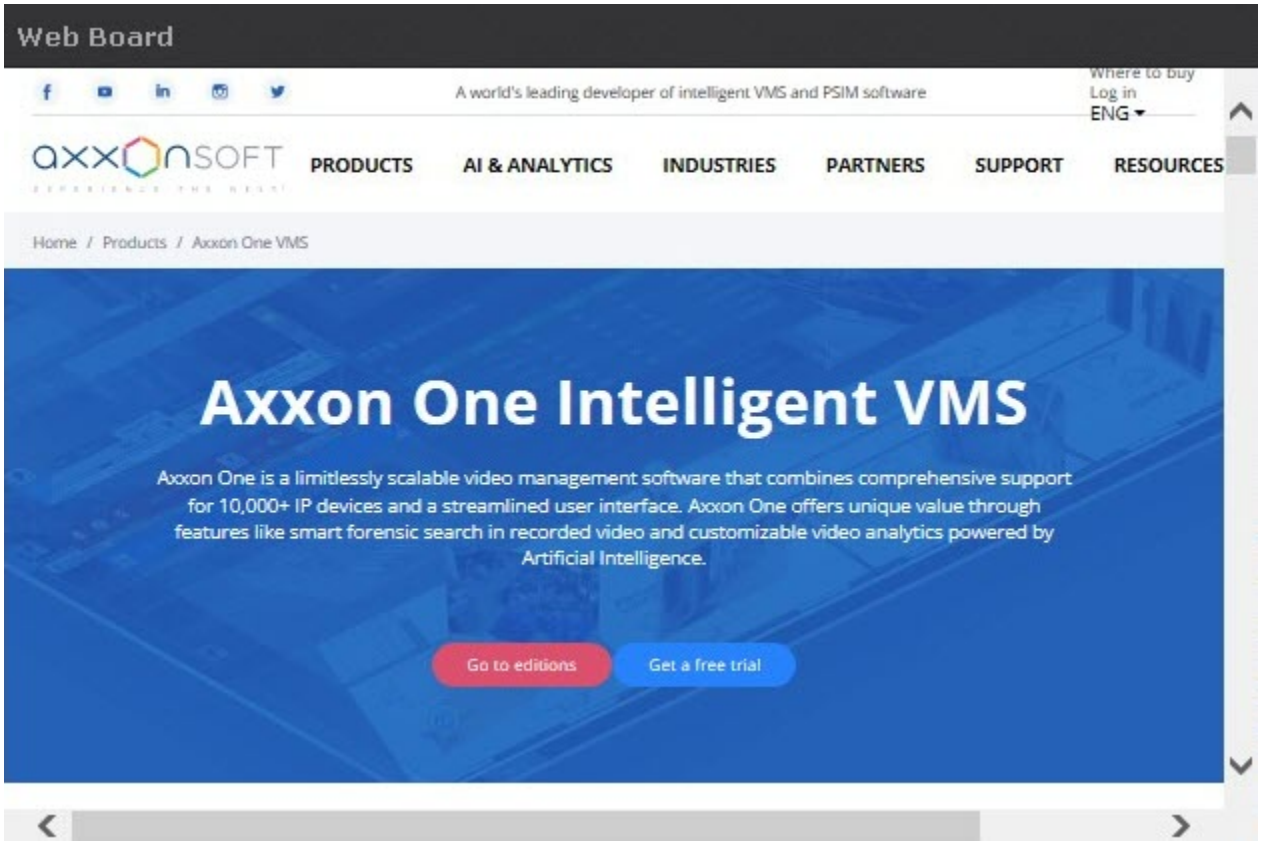
Clicking anywhere on the graph jumps to the nearest point and the relevant value is indicated.



Working with Web Boards

The **Web Board** allows you to view a specific web page on the layout via Chromium or Gecko browser.

If the web page does not fit the board, vertical and horizontal scroll bars are displayed. In this case, the upper-left corner of the web page is displayed.



Note

If there is no network connection, no access to the requested page or if there are other problems, then the Web Board displays standard web browser error messages.

Working with Dialog Board

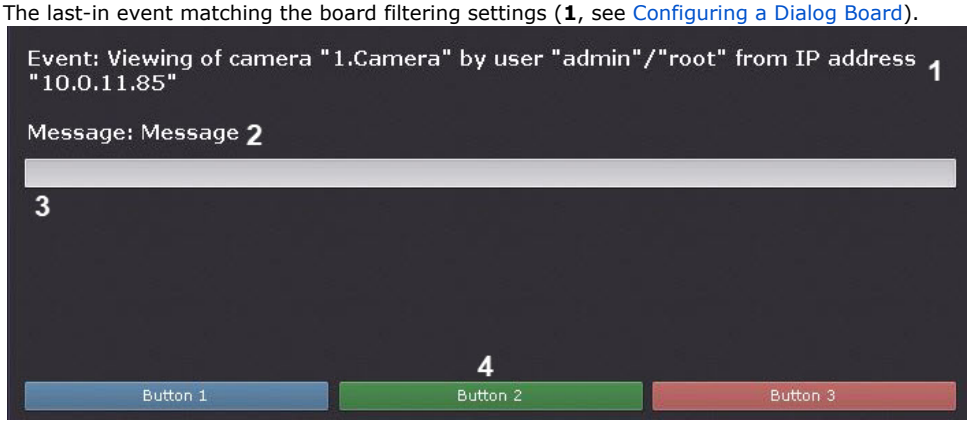
Configuring a Dialog Board

Dialog Board works in three modes:

1. Automated Responses to Events.
2. View and Evaluate Alarm.
3. View Video (Active camera).

In Automated Responses to Events, the board shows:

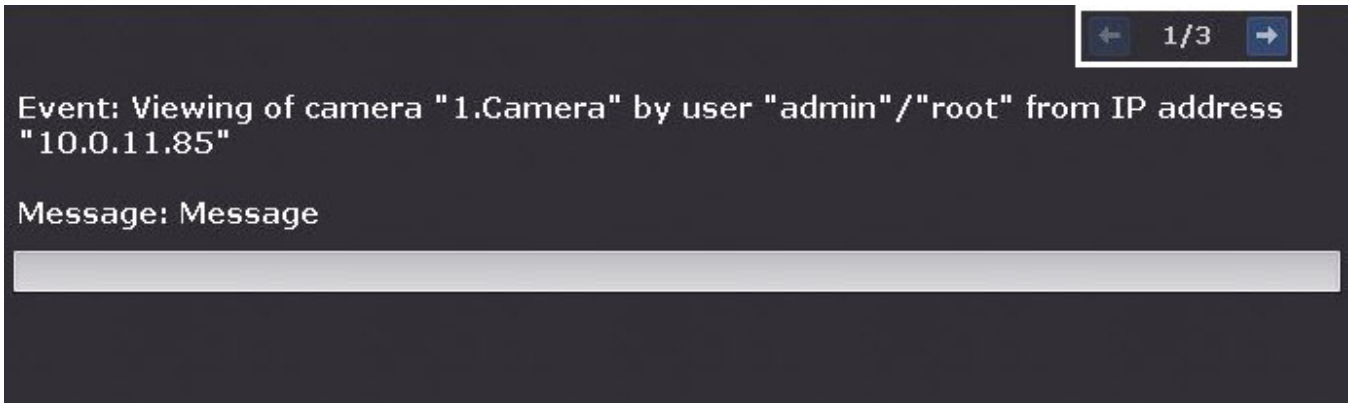
1. The last-in event matching the board filtering settings (**1**, see Configuring a Dialog Board).



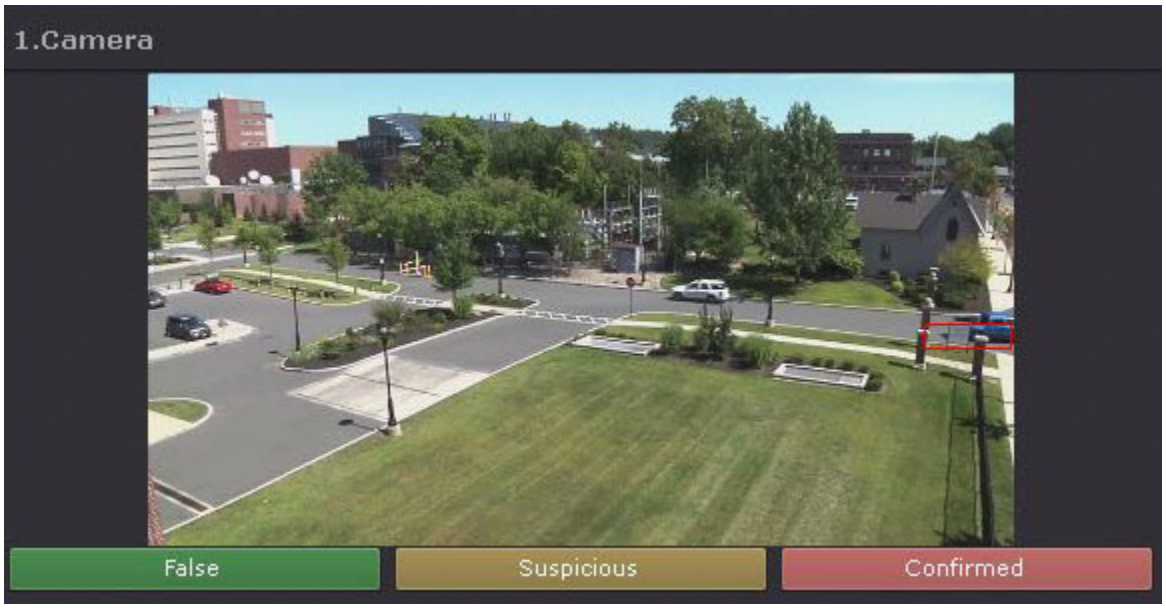
> **Note**
>
> All of the above mentioned elements of the board are optional. You configure the board to show them.

2. Text message as configured (**2**).
3. Comments filed (**3**). Comments input can be optional or mandatory (as configured). Comments are logged to System Log, when you click a response button.
4. Response Buttons (**4**). If you click a response button, the macro starts, and the board auto-hides (if configured, see Hiding information boards).

If the pane has a history of events (see Configuring a Dialog Board), you can use browse it with arrows in top-right corner. Event history is erased after you switch to another layout.



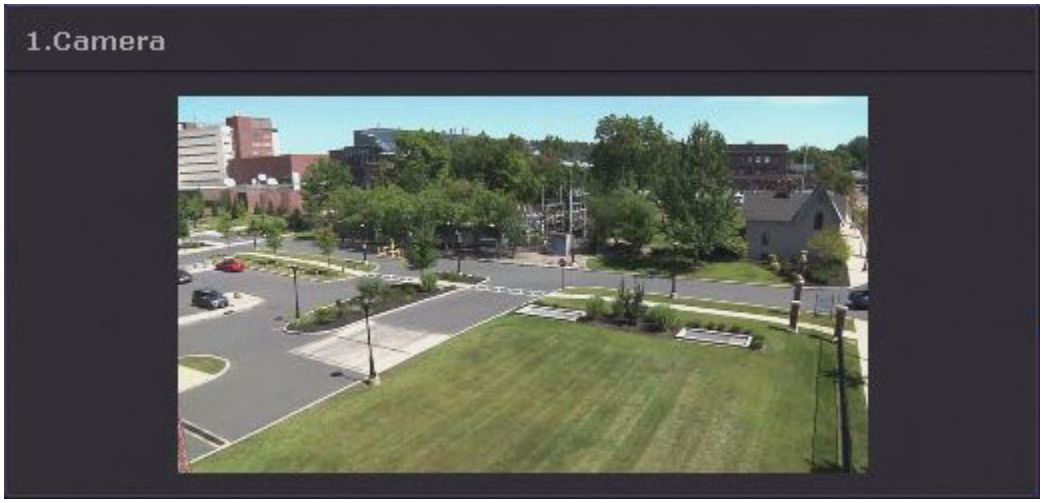
In the second mode, the panel will display an alarm event from the selected or linked camera, depending on the panel setting and the event evaluation buttons.



In the third mode, the panel shows video:

1. from the selected camera;
2. from the stand-by camera for the selected camera;
3. from the stand-by camera for the linked camera.

You can select a camera if you click on its tile on a layout, in the Objects panel (see Objects Panel) or on the map (see Working with the interactive map).

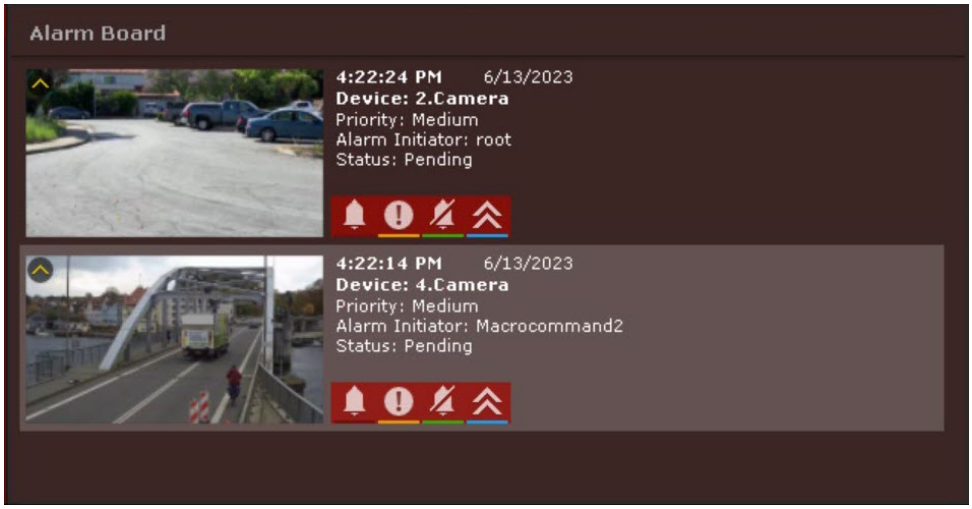


The panel can also display a selected still image.

Working with an Alarm Board

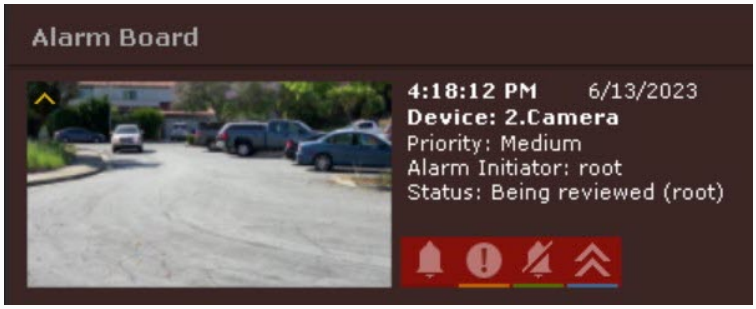
Configuring an Alarm Board

Each alarm event is displayed on the **Alarm Board** as follows: an alarm event window with the first frame of the event, additional information about the alarm event, an event priority icon and the buttons for quick assessment of the alarm event.

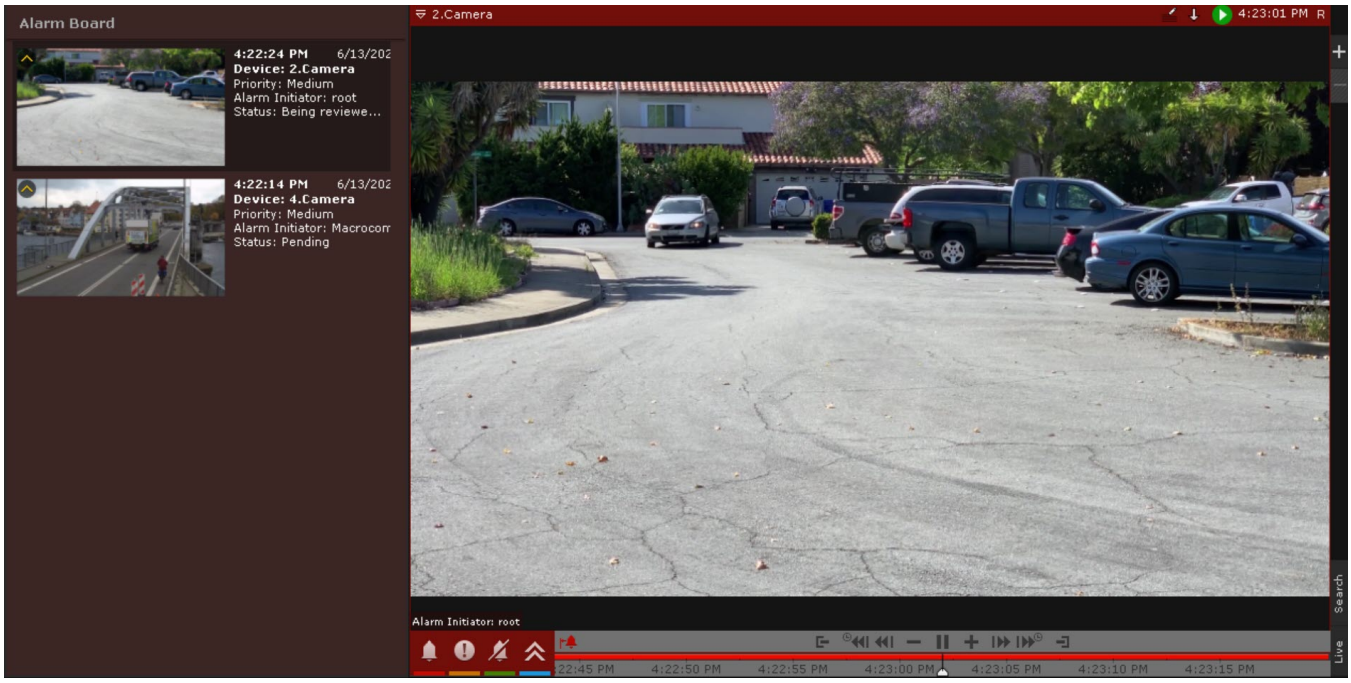


Note

If an alarm event is being reviewed in the **Surveillance window**, the buttons for quick assessment of the alarm event won't be available on the **Alarm Board**.

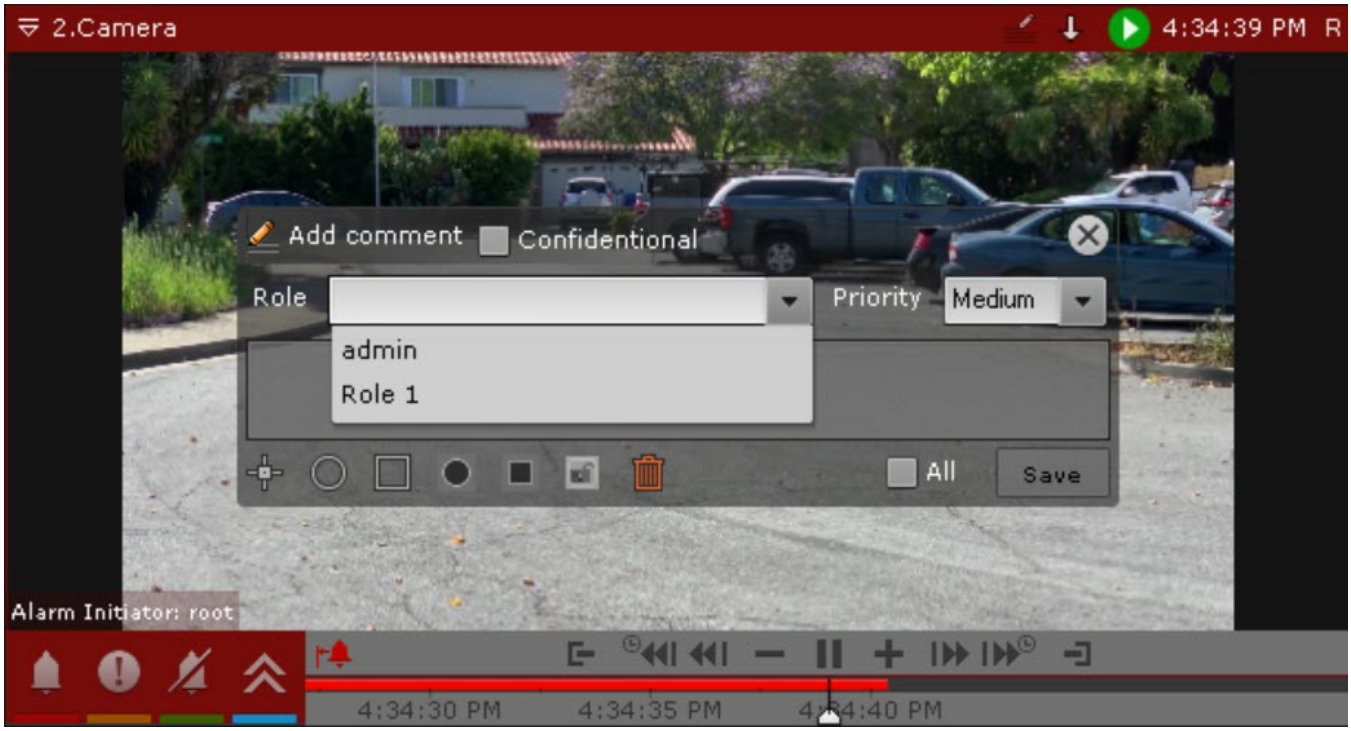


To open a detailed view of an alarm event, double-click the alarm event window on the **Alarm Board**. A detailed view of the alarm event will open. There you can assess the alarm event (see Assessing an alarm event).



Alarm events are displayed in order of priority on the **Alarm Board** (see Initiating an alarm in the system).

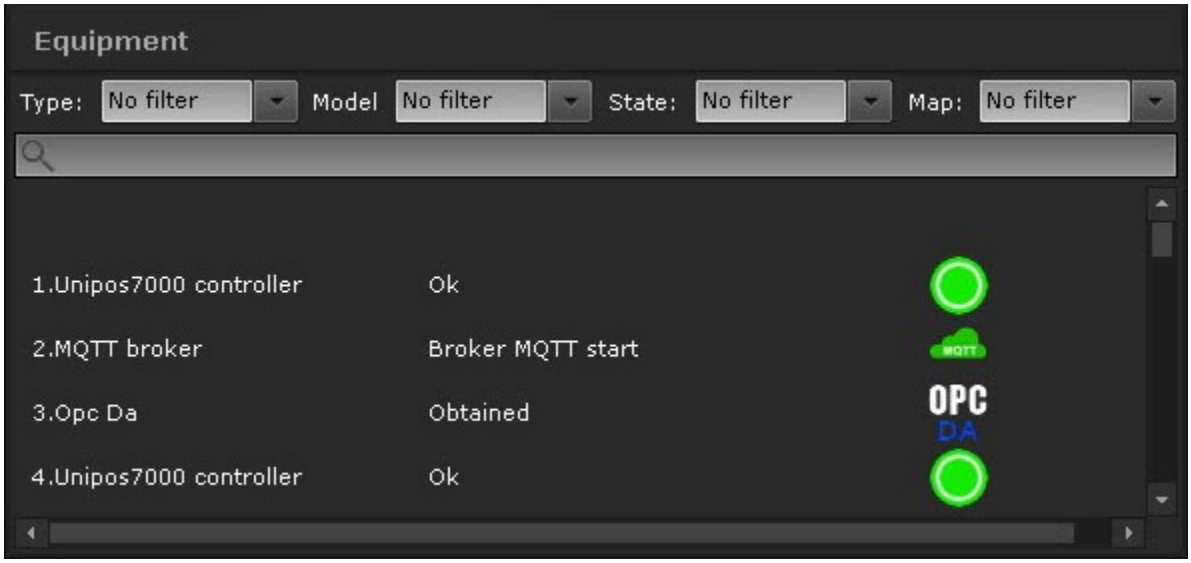
To escalate an alarm, click the  button. A window will open, in which it is possible to set the area of visibility for the roles whose users can see the alarm, as well as change the alarm priority for the selected role. When displayed on the **Alarm Board**, the higher the priority of the alarm, the higher it will be located in the alarms list.



Working with Equipment Board

Configuring an Equipment Board

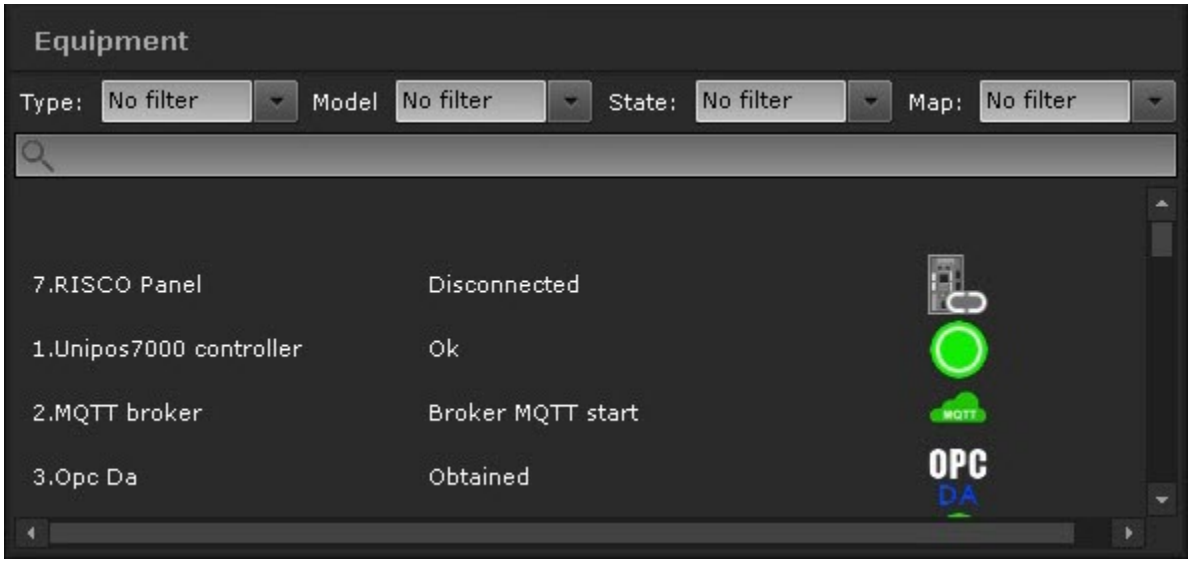
Each *ACFA* integration module is displayed on the **Equipment Board** as follows: equipment, equipment state, and equipment state icon.



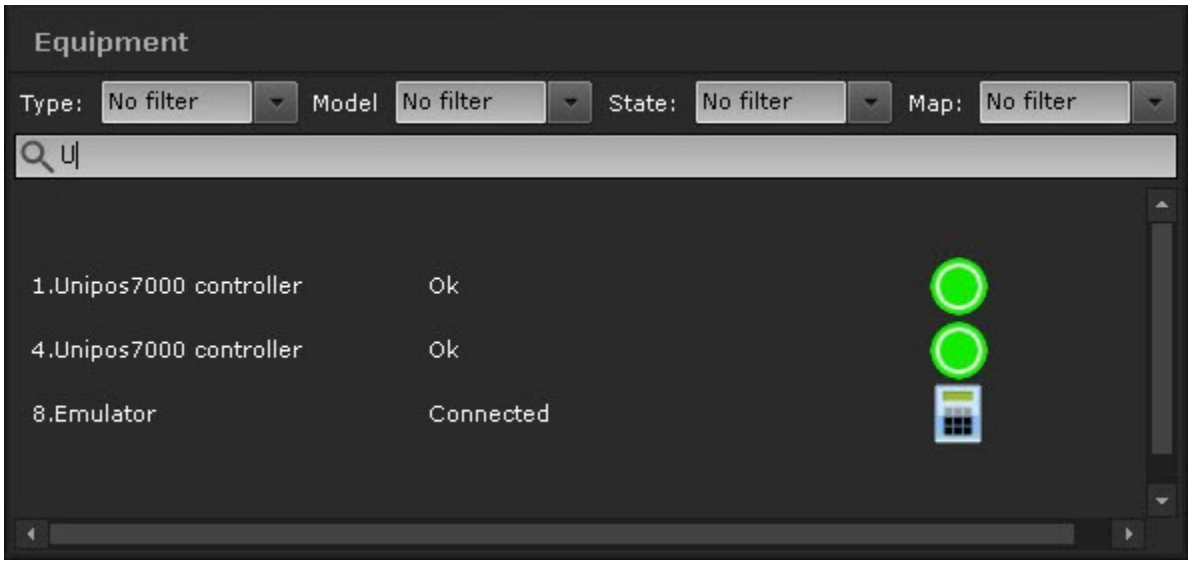
If you didn't set the **Hide filters** checkbox when configuring the **Equipment Board**, you can control board filters in real time.

ACFA integration modules are displayed on the **Equipment Board** in the order in which you added them to *Axxon One*.

On the board, you can sort the devices by equipment and equipment state columns. To do this, left-click the column. The arrow will show the sorting direction.



To search for a specific equipment, enter a part or a full name of the equipment.


Equipment
Type:
No filter
Model
No filter
State:
No filter
Map:
No filter
U
1.Unipos7000 controller
Ok
4.Unipos7000 controller
Ok
8.Emulator
Connected

Layouts management

The *Axxon One* user can run the following commands here:

1. Select a layout for display on screen.
2. Start and stop slideshows of layouts. Slideshow is rotation through all available layouts according to an assigned frequency (dwell-time).
3. Create temporary layouts.

You can work with layouts done on the Layouts ribbon (see The Layouts panel).

Changing cameras on a layout

You can change cameras on the current layout. These changes will not be saved and will be automatically discarded when you switch to another layout.

You can change:

- one of the cameras;
- all cameras on the layout.

To change one camera, drag-and-drop the camera from the Objects Panel (see Objects Panel) or from the Camera Search Panel (see Camera Search Panel) to the layout cell of your choice.

> **Note**
>
> Camera that was dragged-and-dropped to the camera cell in the archive mode (see Switching to Archive Mode), will also be in the archive mode, if recording to the archive is configured for this camera.

To change all cameras on the layout, select multiple cameras on the Objects Panel, and drag-and-drop them into the layout.

> **Note**
>
> To select multiple cameras, use **Ctrl** and **Shift** keys.

After you drag-and-drop a group of cameras, the layout will display all cameras from this group. After you drag-and-drop an Axxon-domain, the layout will display all cameras from this domain.

> **Note**
>
> Currently disabled cameras will not be added to the layout.

Selection and Slideshow of Layouts

To display a layout, click it with the left mouse button.



If the Client is connected to multiple Axxon-domains, layouts for the main Axxon-domain are listed by default. To view the layouts of other Axxon-domains, select the desired domain on the camera search panel.

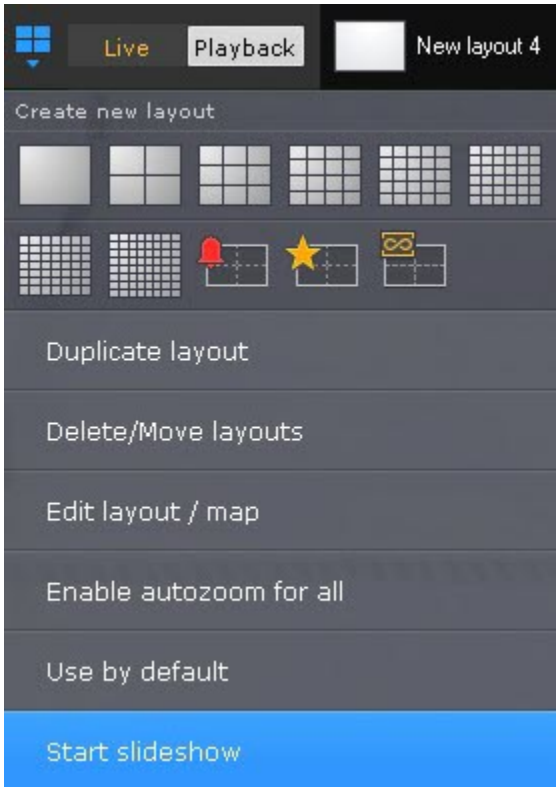
If another user has shared the layout, you will see the following icon:



Shared layouts are by default sorted by name on the Layouts panel.

> **Note**
>
> If you hover the mouse cursor over such a layout, you will see the name of the user that has shared it.

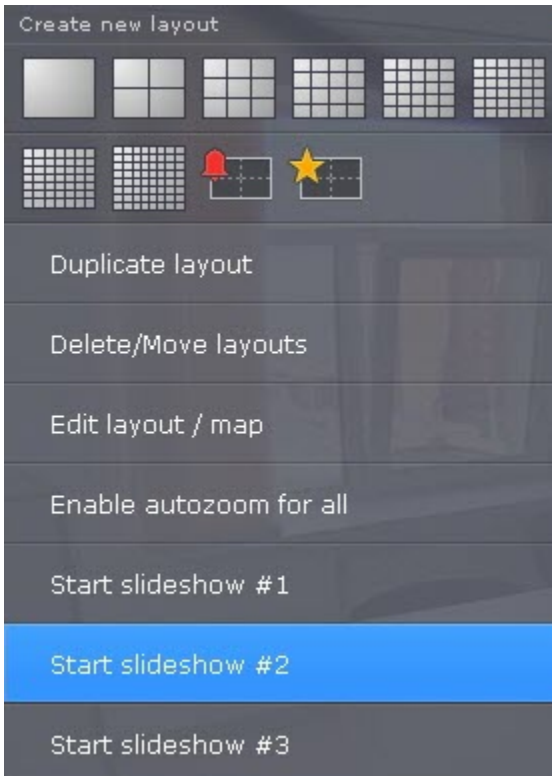
To launch a slideshow, click the  button, and select **Start slideshow** in the context menu of the layout panel.



> **Note**
>
> If you have only one layout in VMS, you do not have **Start slideshow** in the context menu.

This will launch a carousel of all available layouts according to the assigned dwell-time (see Configuring the slideshow parameters). Special layouts (see Working with Special layouts) are excluded from slideshows.

To launch a user-defined slide show, select the required one from the list.



Note

To launch a slide show on a video wall (see Monitor management), select the required monitor in the Video Wall Management Panel (see Monitor panel).

To turn off Slideshow mode, select **Stop slideshow** in the context menu of the layouts panel or left-click any viewing tile.

Working with Special layouts

Configuring special layouts

Alerted Cameras layout

The first 10 seconds after the alert appears in the special layout, it is highlighted.



Cameras disappear from the Alerted Cameras layout in 2 cases:

1. After the alert is classified and the next camera is on (see Assessing an alarm event).
2. After the timeout expires (see Configuring Alarm processing).

> **Note**
>
> The alarm sticks to the layout while the Alarm Management window is open and before the timeout expires. If you select a different camera without classifying the alarm, the alarm evaluation timeout resets.

New alerted cameras will populate the layout as follows:

1. If there are any free cells on the layouts after you have classified or missed the alert, the first free cell is taken.
2. If there are no free cells on the layout, the new alerted cameras takes the next free cell. If there are no free cells, the alerted camera is added to the waiting list

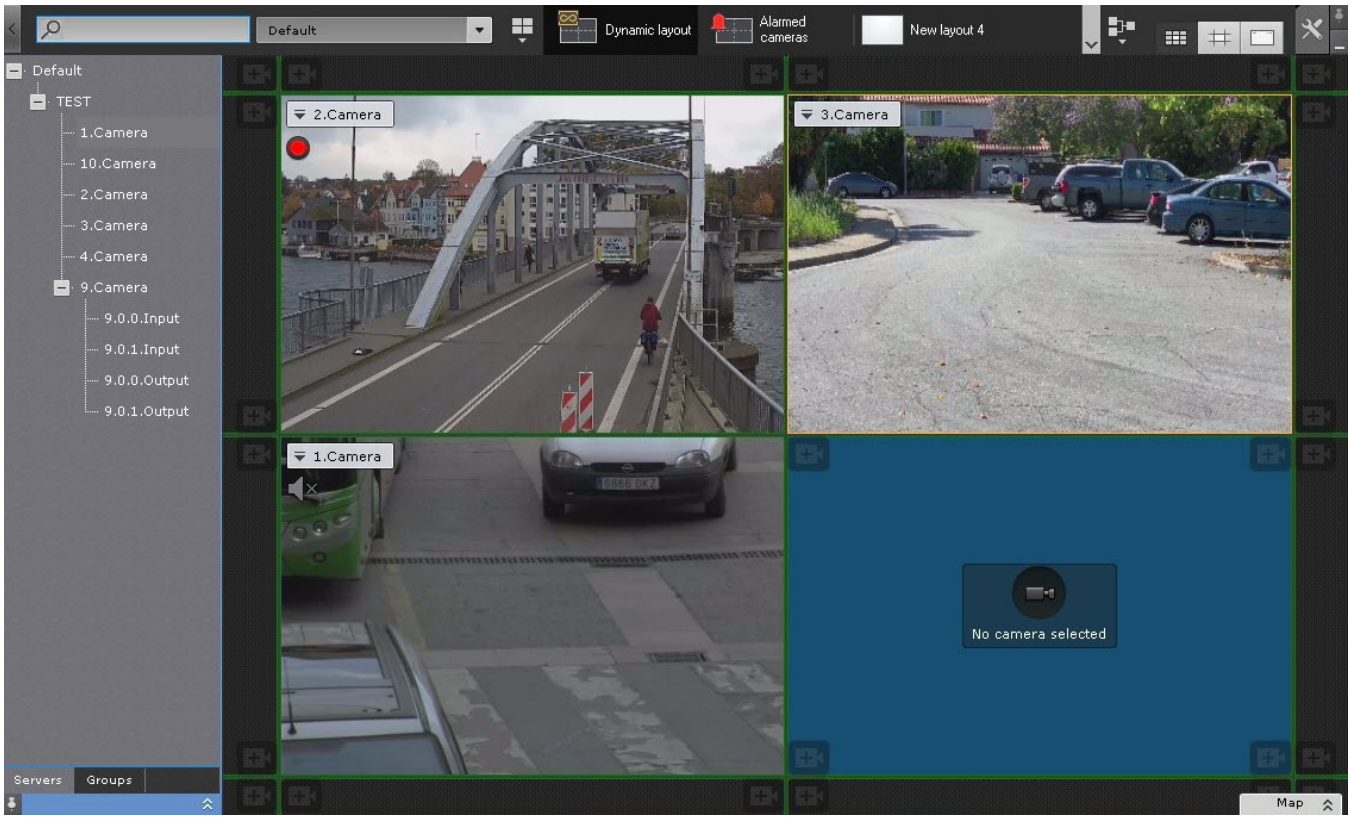
Selected Cameras layout

All selected cameras are displayed on this layout.

Dynamic layout

By default, Dynamic layout is empty. You can add cameras from the object panel (see Objects Panel) one by one or several at once (a group, all video cameras of the Server or Axxon Domains).

To do this, select the target unit on the Object panel and drag&drop it to the layout. During camera drag&drop, the layout shows the grid. The empty cell with the cursor in it, is highlighted when you drag the camera.



If you switch from Dynamic layout to any other, all cameras remain in the current mode. Those in the Archive mode, will keep it when you return to Dynamic layout. The pointer position on Timeline remains intact either.

All changes to Dynamic layout are preserved until you exit the Client. After you launch the Client, the Dynamic layout is always empty.

However, you can back up your Dynamic layout at any given time (see Layout copying).

Monitor management

Managing monitors on a local Client

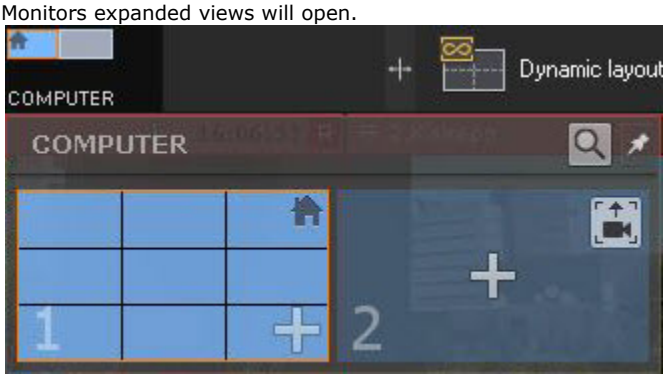
Displaying layouts on monitors

You can display layout on any hardware monitor of a Client. To do it, do the following:

1. Click anywhere on the local Client monitor layout diagram on the Monitor Panel (see Monitor panel).

> **Note**
>
> Client monitor management is regulated by the user rights (see Creating and configuring roles).

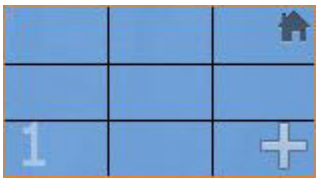
Monitors expanded views will open.

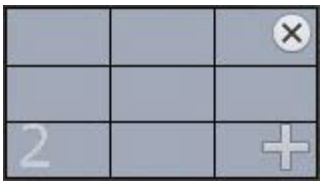
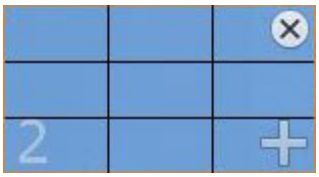


> **Note**
>
> All connected Clients have the NetBiosName name.

> **Note**
>
> Each monitor has its unique ID number. To display the ID number of a monitor, click the  button.

The thumbnails may appear differently, depending on the status of the monitors in *Axxon One*.

Thumbnail	Monitor status
	Active main monitor
	Inactive main monitor
	Non-distributed additional monitor

	Inactive additional monitor
	Active additional monitor

> **Note**
>
> The thumbnail of the monitors shows the currently open layout.

2. To display the layout on the monitor, do the following:
    a. Click the **+** button on the non-distributed additional video monitor's thumbnail. The additional monitor becomes active, and the layout of the main monitor will be duplicated on it.
    b. Configure the layout of an additional monitor (see Configuring layouts). You can configure the layout of the additional monitor through the main monitor (the additional monitor must be active). Changes affect only the additional monitor; the layout of the main monitor is not changed.
    c. Click the main monitor's thumbnail. The additional monitor becomes inactive, and the original layout is displayed on the main monitor. If the additional monitor becomes inactive, editing of the layout does not affect it.
3. To display a camera selected on the main monitor on the additional monitor, do the following:
    a. Click the  button on the non-distributed additional video monitor.
    b. Selecting a camera on the main monitor makes its video feed visible on the additional monitor.

The additional monitors are now configured.

Editing layouts

To edit a layout on an additional monitor, do the following:

1. Activate the additional monitor (by clicking its thumbnail).
2. Edit the layout.
3. Make the additional monitor inactive.

Selecting cameras to display on the layout

You can select the cameras that should be displayed on the main and additional monitor by dragging and dropping them:

1. in the cell of the main or additional monitor diagram from the Objects Panel (see Objects Panel);
2. in the cell of the main or additional monitor diagram using the camera icon from the interactive map (see Working with the interactive map);
3. in the cell of the main or additional monitor diagram from the Camera Search Panel (see Camera Search Panel).

Similarly, you can drag and drop not only individual cameras, but also group of cameras, all cameras of the Server or Axxon-domain.

> **Note**
>
> The changes are saved only until you restart the Client. The next time you start the Client, the layout will have the original view.

Closing the layout of the additional monitor

You can close main and additional monitor separately. To close an additional monitor in *Axxon One*, click the  button on its thumbnail.

Managing monitors on remote Clients within the Axxon-domain

Having appropriate user rights, you can remotely manage monitors on remote Clients connected to a Server within the Axxon-domain (see Creating and configuring roles).

The following actions are possible:

1. Add a layout to an additional monitor of a remote Client.
2. Select another layout or a camera on the additional monitor.
3. Edit a layout on the main or additional monitor.
4. Shut down the additional monitor.

To display a layout on the additional monitor of a remote Client, click anywhere on the required Client's monitor layout diagram, and select a non-distributed video monitor (see Monitor panel).



Note

You can add a layout to the additional monitor of a remote Client the same way as you do it for a local Client (see Managing monitors on a local Client).

To select another layout on a remote Client's monitor, do the following:

1. Select the desired layout on the local Client (see Selection and Slideshow of Layouts).
2. Click anywhere on the remote Client's monitor layout diagram, and then on the required monitor's view.

The selected layout will be displayed on a selected monitor of the remote Client.

If a single camera is displayed on the remote Client's additional monitor, you can switch to another camera by selecting it through the local Client.

To edit the remote Client's main or additional monitor layout, do the following:

1. Select (see The Layouts Panel) or configure (see Creating and deleting layouts) the desired layout on the local Client.
2. Click anywhere on the remote Client's monitor layout diagram.
3. Click the  on the main or secondary monitor layout diagram.



The remote Client's layout is saved, and will be available after rebooting the Client.

You can change the set of cameras to be displayed on the main or additional monitor using the Objects Panel; these changes are not saved, and the initial layout is restored after rebooting the Client. To do it, follow the steps below:

1. Open and lock the Monitor Panel (see Monitor panel).
2. Open the Objects Panel (see Objects Panel).
3. Using the **Ctrl** or **Shift** keys, select one or several cameras on the panel.
4. Left-click on any selected camera.
5. Drag the camera icon onto a desired cell on the main or additional monitor's layout diagram.
6. Release the mouse button.

Another way to put a camera into a desired cell on the main or secondary monitor layout diagram is to capture the camera's icon on the interactive Map (see Working with the interactive map).

You can also move a group of cameras, all cameras from a Server or an Axxon-Domain.

To close an additional monitor on a remote Client, click the  button on the monitor's thumbnail.

Audio Monitoring

General Information

Audio monitoring of a situation is carried out using the microphones that correspond to a video camera surveying the situation.

In different viewing tile modes, different audio monitoring functions are accessible:

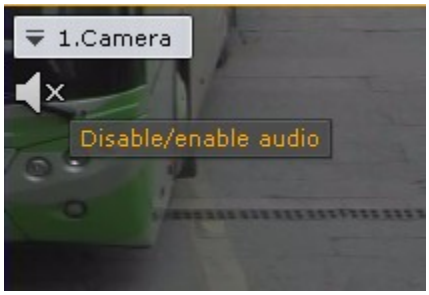
1. Live playback mode – listening to sound from a microphone in real time; playing back sound from Client microphone on camera speakers.
2. Archive mode, Alarm Management mode, Archive Search mode – playback of sound recorded from a microphone.

> **Note**
>
> In Archive mode and Archive Search mode, an audio recording can be played back only from the microphone corresponding to the currently selected video camera, and only in forward playback mode at a speed of 1x.

Listening on the Client to sound from a camera microphone

> **Attention!**
>
> The **Microphone** object must be enabled (see the section titled The Microphone Object).

To listen on the Client to sound from the microphone of a camera, left-click to activate the speaker icon in the viewing tile.



> **Note**
>
> Audio from only one camera can be played back at a time

The speaker icon now becomes active and a volume slider appears.



Volume is controlled using the volume adjuster.

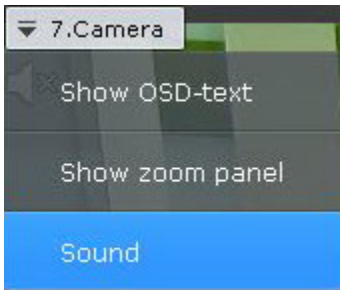
The far left position of the adjuster represents the minimum volume, and the far right position represents the maximum volume.

> **Note**
>
> The *Axxon One* VMS has an embedded sound booster.

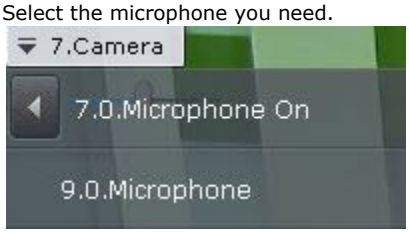
To turn off audio playback, click the speaker icon again.

If a camera has several microphones connected, use the following procedure to select the audio source:

1. Open the camera's context menu.
2. Select **Sound**.



3. Select the microphone you need.



> **Note**
>
> The currently selected microphone is marked as **On**. If you select a **7.0** microphone, the **9.0** microphone is set to off, and **7.0** microphone to on.

> **Note**
>
> If a currently specified loudspeaker goes offline, the system automatically switches to another available one.
>
> After the first loudspeaker goes back online, no automatic switching will occur.
>
> To automatically activate the first loudspeaker in such a case, you have to create a NGP_PORTSOUND_HOSTAPI system variable and set it to DS (see Appendix 9. Creating system variable).

Playing back sound from Client microphone on camera speakers

Audio transmission from the Client's microphone behind NAT to the Server's or camera's loudspeaker

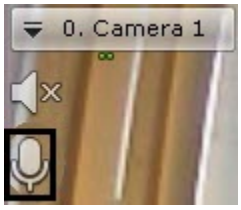
Sound from the Client microphone can be broadcast both on a single camera and on all cameras in a layout.

Attention!

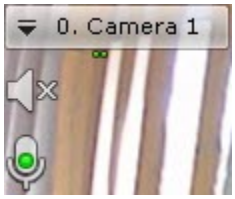
To use this option:

1. Configuration of audio on the Client is now completed (see Configuring audio on the Client).
2. **Speaker** objects are activated for the corresponding cameras (see The Speaker object).

To broadcast sound on the speaker of a single camera, left-click the microphone icon in the viewing tile.

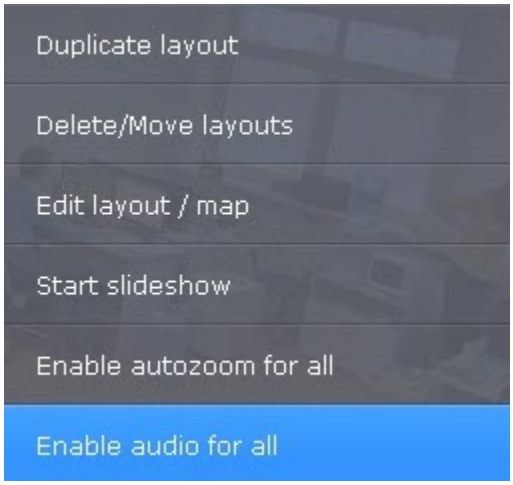


The microphone icon now becomes active.



To turn off broadcasting of sound on a camera speaker, click the microphone icon again.

To broadcast sound on speakers on all cameras in a layout, in the context menu of the layouts ribbon, select **Enable audio for all**.



The microphone icon is then activated for all cameras that have an activated **Speaker** object.

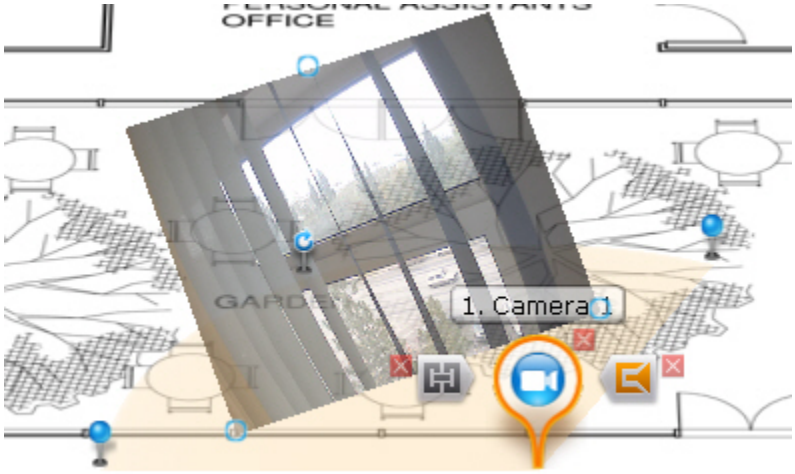
To turn off sound broadcasting on all cameras, select **Disable audio for all**.

Working with the interactive map

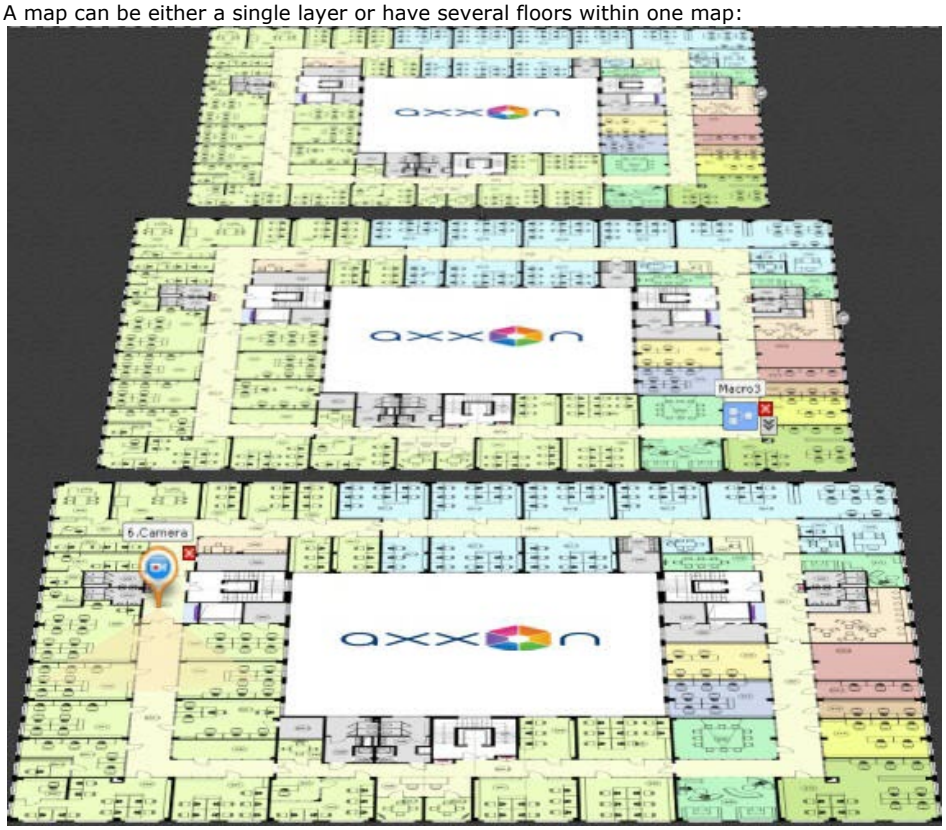
You can use the interactive map in three modes:

1. 3D mode, in which both the map and layout are available.
2. 2D mode, in which only the map is available.
3. Immersion mode, in which video is overlaid on the map.

The map can contain icons for cameras, inputs, outputs, and counters. The area in which live video is displayed and field of view are indicated for each camera.

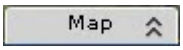


A map can be either a single layer or have several floors within one map:



Opening and closing the map

You can switch to Map View from all modes of operation except for Archive Search.

To go Map View, click the **Map** button in the bottom right corner 

.

The Map will open in a 3D view while the current layout contracts to fit the screen area over the map.



To switch to 2D map view and close the layout, click the button to the left of the **Map** button.

If you expand a tile to full screen, the map auto-hides (see Scaling the surveillance window).

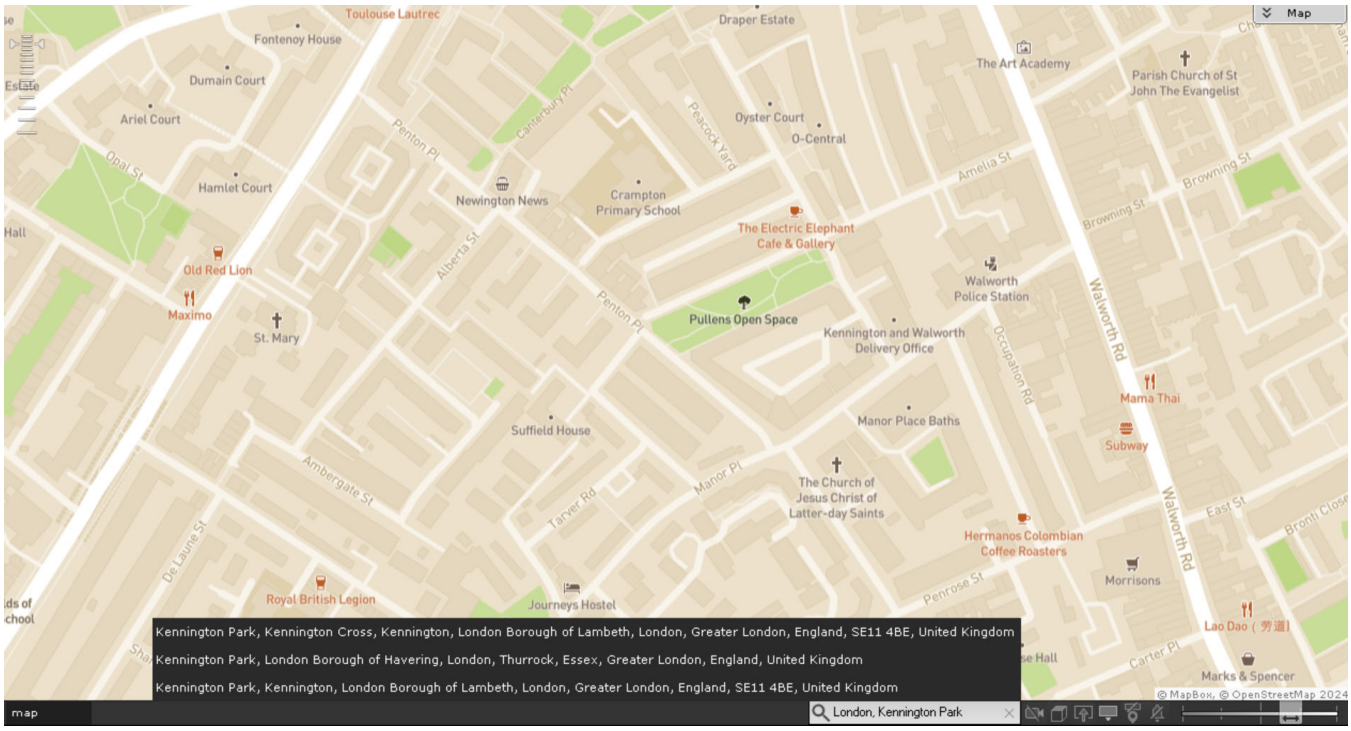
> **Note**
>
> When you minimize the tile, the map appears again.

Geomap search

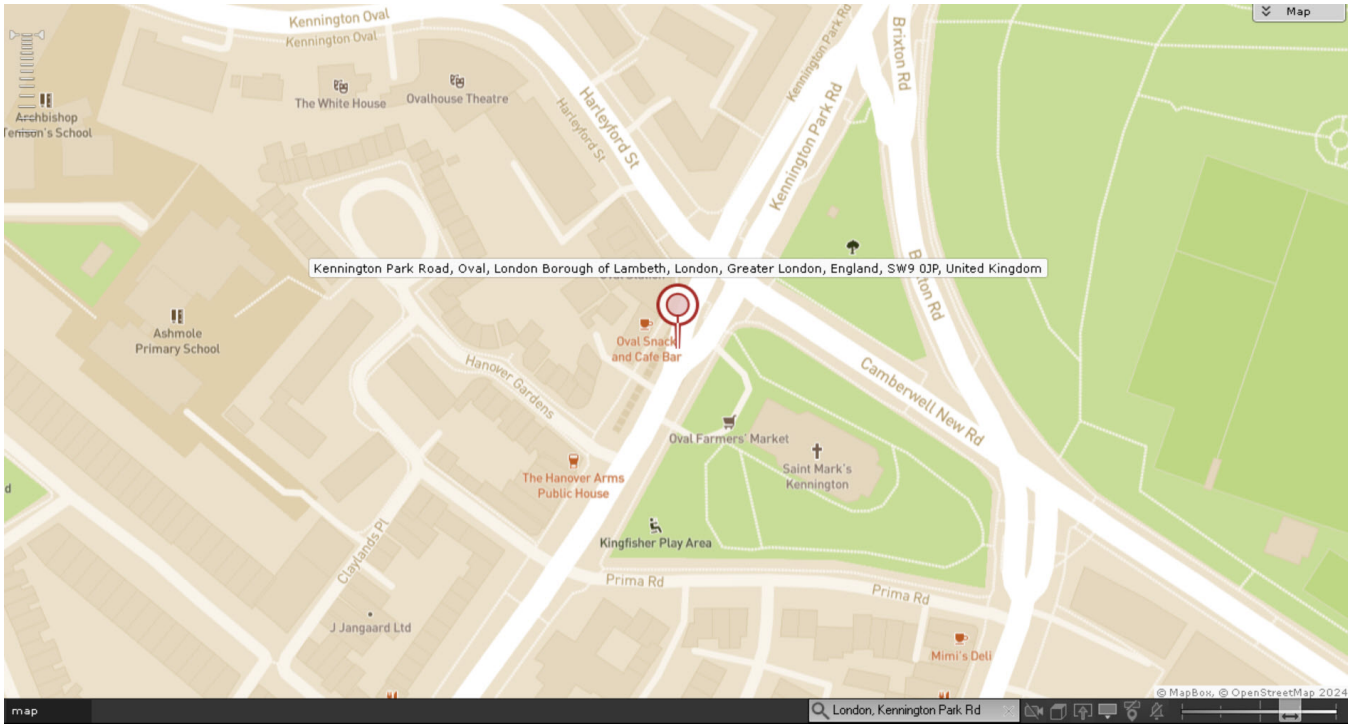
On OpenStreetMap, you can search for any geographical objects or streets in a given city (see Setting keywords for geomap search. For detailed information, see the provider's website).

To do this, do the following:

1. Enter the name of the street or geographical object in the search bar.
2. Select the required option from the drop-down list.



As a result, a mark will appear on the map indicating the object or street you are looking for.

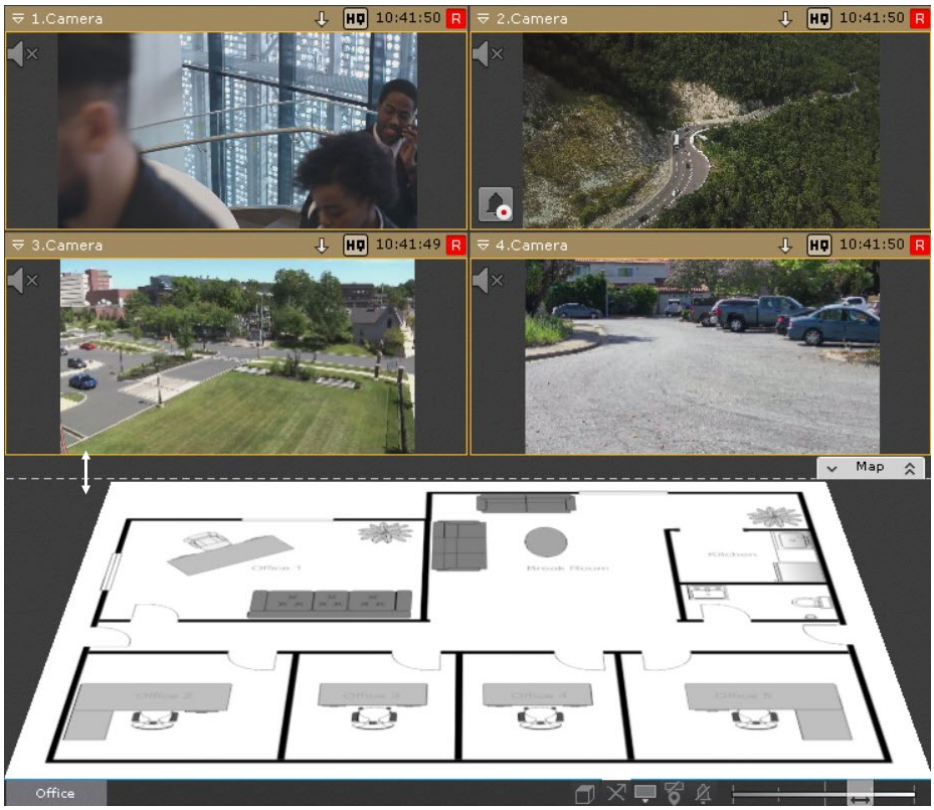


Note

- You can connect different providers for geomap search. To do this, contact the AxxonSoft technical specialists.
- You can search the geomap after adding the geomap to the layout (see Adding a new map) and in the layout editing mode (see Switching to layout editing mode).

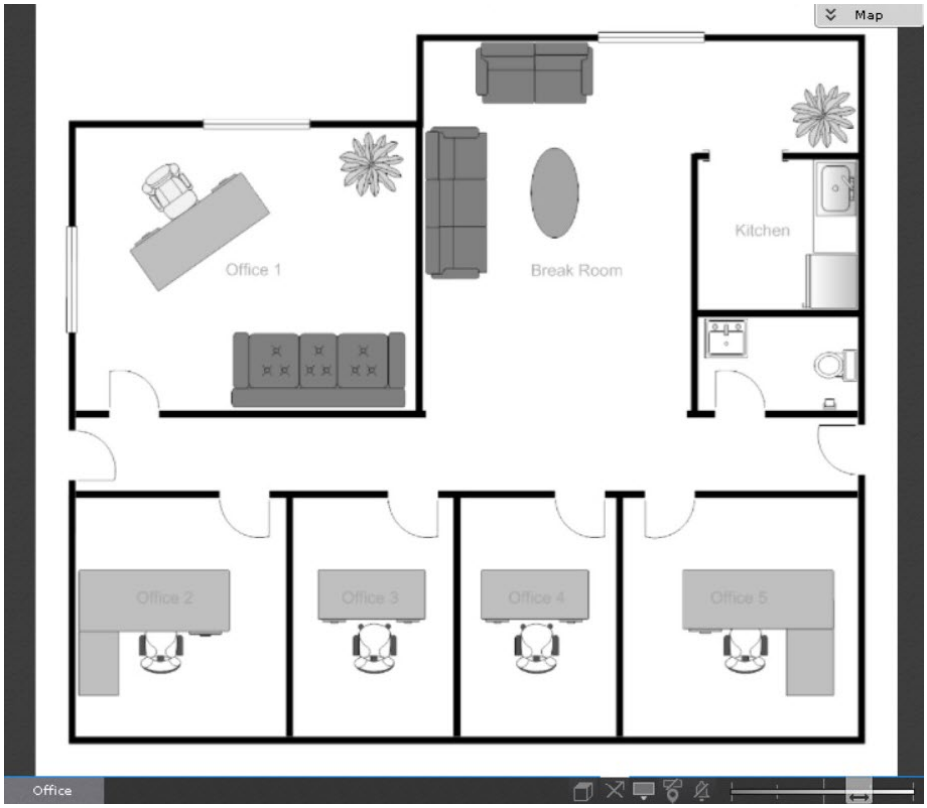
Changing the map tilt

You can change the tilt of the map by adjusting the border between the map and the layout areas.



There are two ways to switch to 2D map view:

1. Click the  button to the right of the **Map** button. In this case the layout will close, and the map will be displayed in full screen.



To return to 3D map view, click the **Map** button. To hide the map, click the button.

2. Click the button on the control bar in the bottom right corner of the screen. In this case the layout will not close, and the map will be displayed in the same place.

> **Note**
>
> If the map is hidden, the control bar in the bottom right corner of the screen will not be available.



To return to 3D map view, click the same button, which will look like this  .

Scaling and focusing of map

Map scale and focus can be changed both manually and automatically.

> **Note**
>
> The map is automatically resized and refocused if this function is activated in the settings (see Configuring map auto zoom).

Automatic adjustment of map scale and focus occurs when a video camera alarm occurs, if no video camera icon is selected on the map.

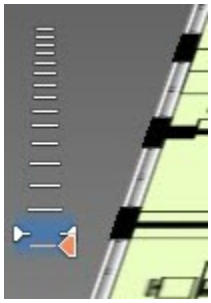
In this case, the map is scaled and refocused to center the icon for the alarm camera on the map.

If alarms occur for several video cameras simultaneously, the map scale and position are adjusted to show all icons for the relevant video cameras.

After a video camera alarm ends and there are no alarms for other video cameras, the map scale and position return to their initial status.

Automatic scaling and focusing of the map stops when the user clicks to select the icon of a video camera on the map or viewing tile.

To manually adjust the map scale, use the mouse scroll wheel (the cursor must be above the map) or use the map scale slider.



After increasing the scale, you can refocus the map with the mouse (by clicking and holding the left mouse button) in the direction of your choice.

Customizing an interactive map

You can change some of the map settings in live video. Use the controls in the bottom right corner of the screen.



You can change the transparency of video on the map using a slider in the bottom right corner.



In the leftmost position of the slider, the video isn't displayed on the map. In the rightmost position, the video isn't transparent.

To change the size of icons on the map, use the slider in the lower left corner.



In the leftmost position of the slider, the icons are of the minimum size. In the rightmost position, the icons are of the maximum size.

To enable/disable the display of device name and identifiers on the map, use the / button.

To enable/disable the display of unavailable devices on the map, use the / button.

To enable/disable camera icon fluttering on alarm, use the / button.

To change the action when you click the camera icon on the map, use the (takes you to the layout with the camera)/ (goes to Immersion mode (see Immersion mode)) button.

To change the format of the video on the map, use the (3D view)/ (flat view) button.

Video in 3D view:



Video in flat view:


3.Camera

Switching between maps

In any mode, you can switch between the maps that have been created in the system.

You can switch between maps in two ways:

1. In the lower-left corner of the screen, select the corresponding tab.



> **Note**
>
> If many maps have been created, some tabs may not fit on the screen. If this happens, click the » button. In the drop-down menu that opens, select a map.



2. By left-clicking a map icon for switching, if it has been created (see Adding switches to another map).
The icon header shows the name of the destination map.



Immersion mode

In Immersion mode, video from a selected camera is displayed on top of the map image.

If you created links between video and the map (see Configuring cameras in immersion mode), an angle will be selected so that objects in the video match the objects as depicted on the map.

If you didn't create links, the map is displayed in such a way so that the video is located in the specified FOV of the camera on the map. The FOV is directed upwards.

You can go to immersion mode in two ways:

1. Click the  button on the right border of the surveillance window. The button may not be available at certain display settings of the surveillance window (see Configuring the display of the surveillance window).
2. On the map, left-click a camera icon, its FOV, or video display area. This method is possible if you didn't click the  button (see Customizing an interactive map).



In Immersion mode, you can view video from only one video camera at a time.

To select another camera, do one of the following:

1. Click the camera icon, its FOV, or image on the map, if possible.
2. Exit Immersion mode and select the required camera on the map.

To exit Immersion mode, do one of the following:

1. Click the  button.
2. Minimize the surveillance window by clicking the  button.
3. Click a part of the map that doesn't contain the camera FOV.

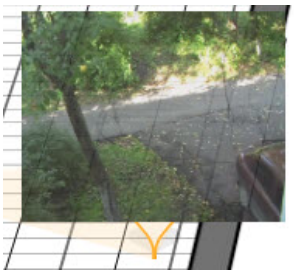
Note

- After you exit Immersion mode, the camera on the layout will display live video.
- You cannot apply actions 2 and 3 if a fisheye camera with certain parameters is in Immersion mode (see Fish-eye cameras in immersive mode).

Controlling devices from the map

Using the context menu of icons on the map, you can control outputs and logical objects (counters, macros), as well as control video cameras and configure their interface.

Commands for controlling and configuring video camera interface are given in the table below.

Command (context menu item)	Condition	Result after the command is performed
Arm	The camera is disarmed	Icon status: 
Private Arm (see Arming and Disarming a Video Camera)	The camera is disarmed	Icon status: 
Disarm	The camera is armed	Icon status: 
Show video	Video image is not displayed	Video image display: 
Hide video	Video image is displayed	Video image is not displayed
Show layout	Additional conditions are not required	The selected camera is displayed on the temporary layout. To display multiple selected cameras on the temporary layout, see Selecting Cameras for a Temporary Layout
Copy	Additional conditions are not required	If you right- or left-click on any cell of the layout, then the video from the copied video camera will be displayed in this cell. The copied camera will be displayed on the layout until you switch to another layout or restart the client

Commands for controlling outputs are given in the table below.

Command (context menu item)	Condition	Icon status after the command is performed
Turns the output on	Output in normal status	
Disable output	Output is activated	

Note

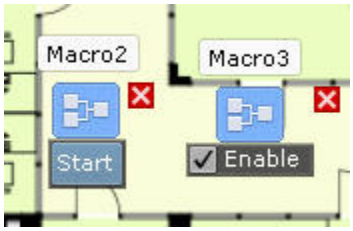
You cannot switch the status of the Output from the map if there are macros with the corresponding action running in the system (see Switch output).

Commands for controlling macros are listed in the table below.

Command (context menu item)	Condition	Command description

Start	Event-driven macro	Running the macro
Enable	Disabled cyclic macro	Enabling the macro
Disable	Enabled cyclic macro	Disabling the macro

On top of that, you can manage macros with the **Start** button and the **Enable** check box.



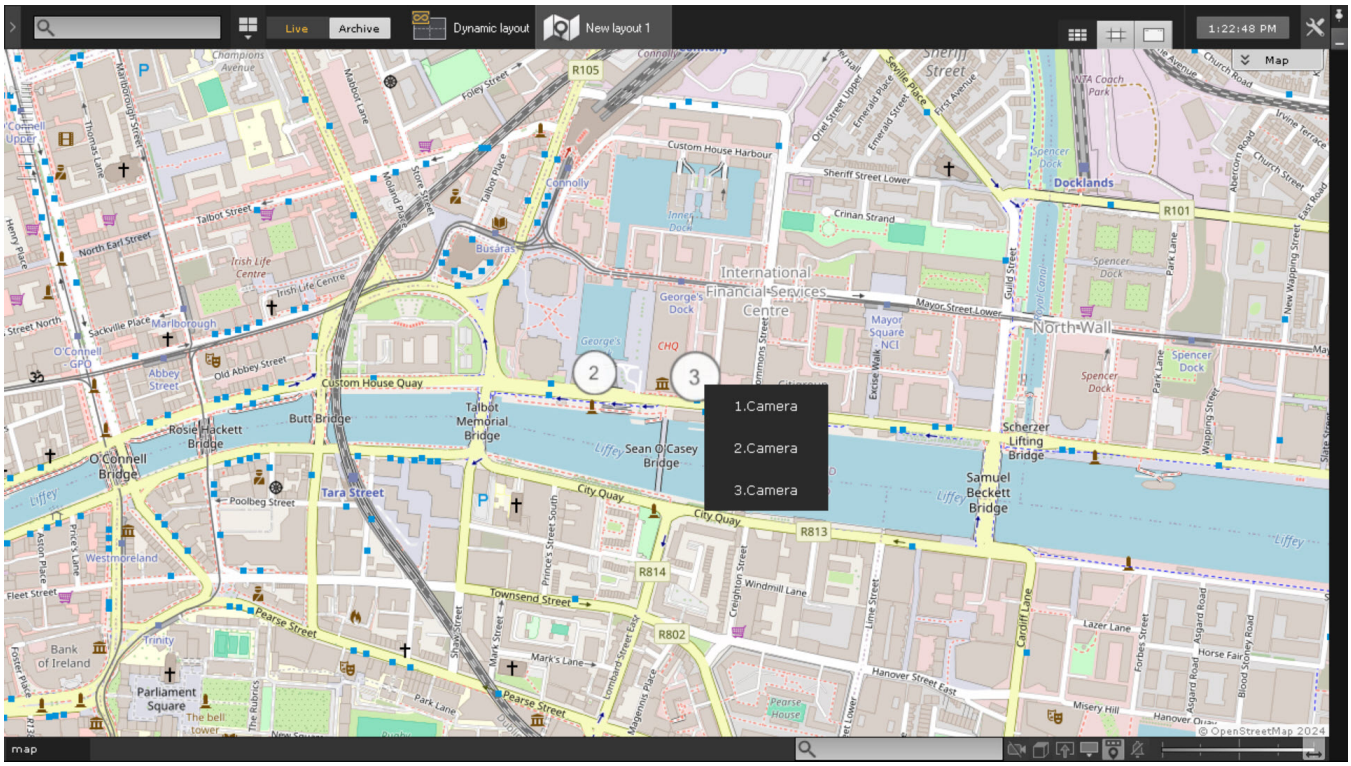
Commands for controlling counters are listed in the table below.

Command (context menu item)	**Condition**	**Command description**
Stop	The counter is running	Stopping the counter. If the counter is on pause, its value does not change
Start	The counter is stopped	Starting the counter. If the counter is running, its value changes as specified
Clear	Any state	Resets the counter value to 0

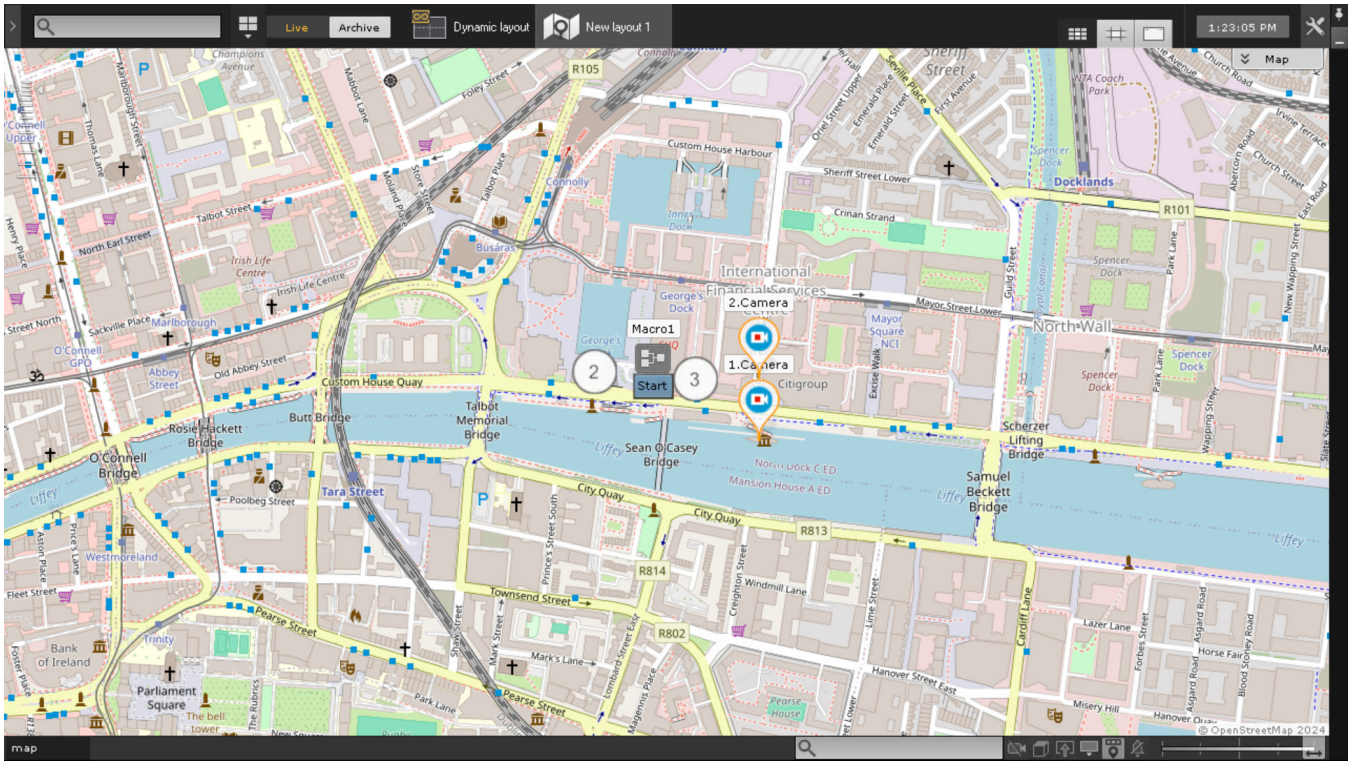
Grouping objects on the map

If the video cameras have the same coordinates or are located close to each other, they automatically merge into a cluster. Each cluster is displayed on the map as a circle, and the total number of cameras in the cluster is indicated in its center. Relays, sensors and macro commands can also be combined into clusters.

You can right-click on a cluster to see a list of all objects included in that cluster.



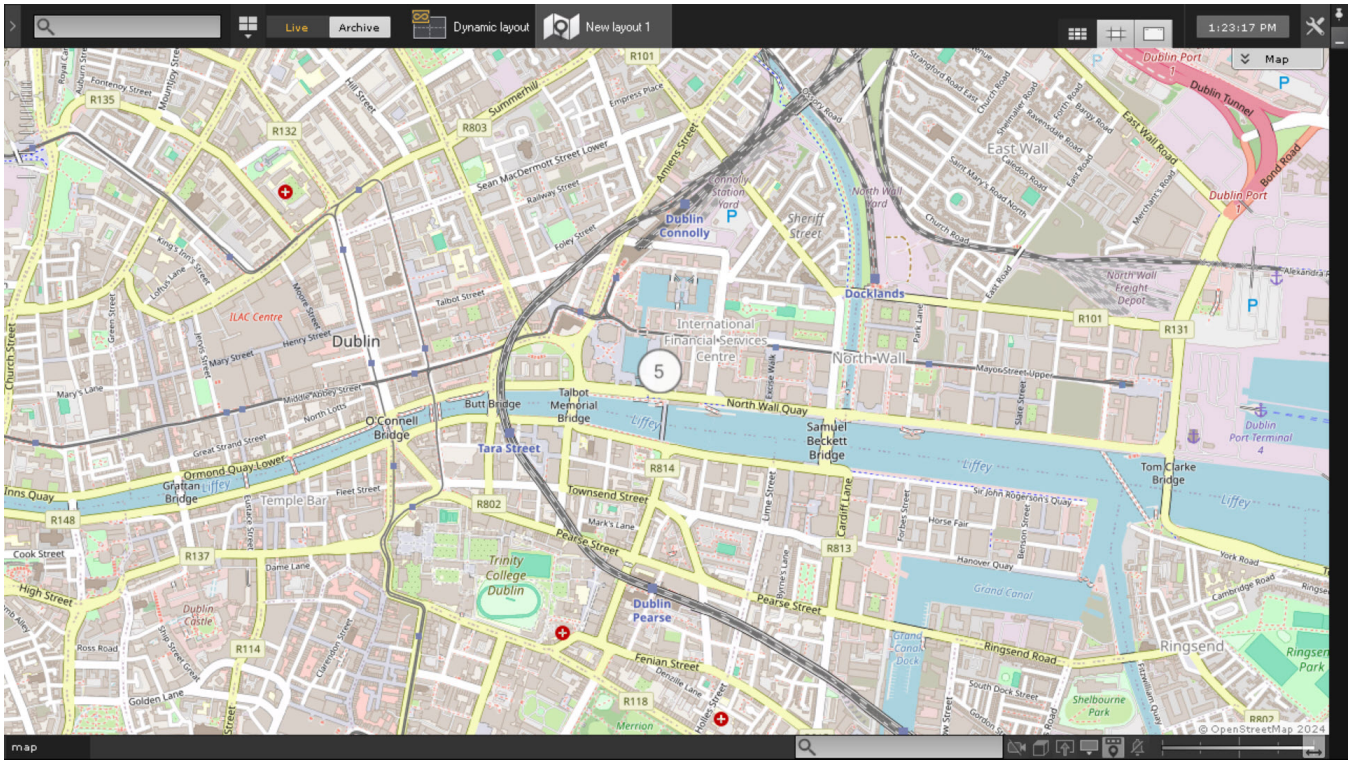
When you select a certain object from the list, it will be displayed next to the cluster.



You can left-click on an object icon on the map to see a context menu for managing the object (see Controlling devices from the map).

To hide the list of objects and display them as a cluster on the map, zoom out on the map (see Scaling and focusing of map).

If there are several clusters located close to each other on the map, they will merge into a new cluster when you zoom out on the map. The center of the new cluster indicates the total number of objects of all child clusters.



When you click on a merged cluster, the map will automatically zoom in and the child clusters will be displayed.

Displaying device status

The icons on the map indicate the current status of the corresponding devices.

The possible states of the video camera icon are described in the table below.

Map icon	Camera status
	Camera disarmed, no archive recording
	Camera disarmed, archive recording active
	Camera armed, no archive recording
	Camera armed, archive recording active
	Camera alarm, archive recording active
	Camera connection lost

The possible states of the Output icon are described in the table below.

Map icon	Output status
	Output is activated
	Output in normal status

Note

When a macro changes the Output status, the Output icon on the map does not change.

The possible states of the Input icon are described in the table below.

Map icon	Input status
	Video camera is armed, Input is in normal status
	Video camera is armed, Input is in alarm status
	Video camera is disarmed, Input is in normal status

	Video camera is disarmed, Input is in alarm status

Inputs (sensors) connected to Tibbo boards also show temperature/humidity values on the map (see Setting up Tibbo relay/loop boards).

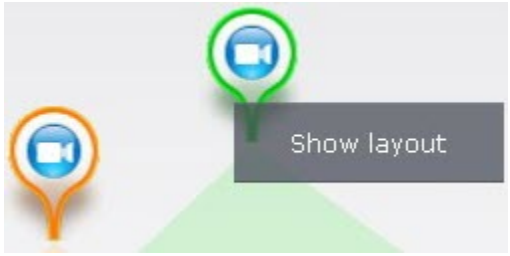


Selecting Cameras for a Temporary Layout

You can use the Map to select cameras for viewing their video feeds on a temporary layout.

Do the following:

1. Press and hold Ctrl, and left-click camera icons.



2. Click the **Show layout** button.

The selected cameras' views appear on the temporary layout which is not preserved after you switch to any other layout.

Exporting frames and video recordings

Users with the corresponding rights can export snapshots and video. if a Client is connected to multiple Axxon-domains, export of snapshots and video is available only for cameras on the Axxon-domains on which the user has the corresponding rights.

Still frames can be exported to JPG and PDF, videos can be exported to AVI, MP4, MKV and EXE formats.

Exported videos will contain synchro audio.

The name of the exported file contains the following information: name of camera, export date, and export duration.

> **Note.**
>
> The date and time of the event in the file name are given based on the Windows locale settings.

> **Note.**
>
> The file name can be up to 70 characters long.

When exporting a snapshot to PDF, you can also print the document immediately.

A digital watermark is added to exported snapshots and video. Watermark authentication is available in the corresponding bundled utility (see the Digital signature verification utility section).

> **Note**
>
> Exported videos and snapchots are digitally signed with the SHA-256 algorithm.

Titles containing a date and time stamp will be superimposed on exported video.

> **Note.**
>
> Captions are stored in a separate video track and, if necessary, are disabled in the player through software.

Frame export

You can export frames at any time when working with a camera in *Axxon One*.

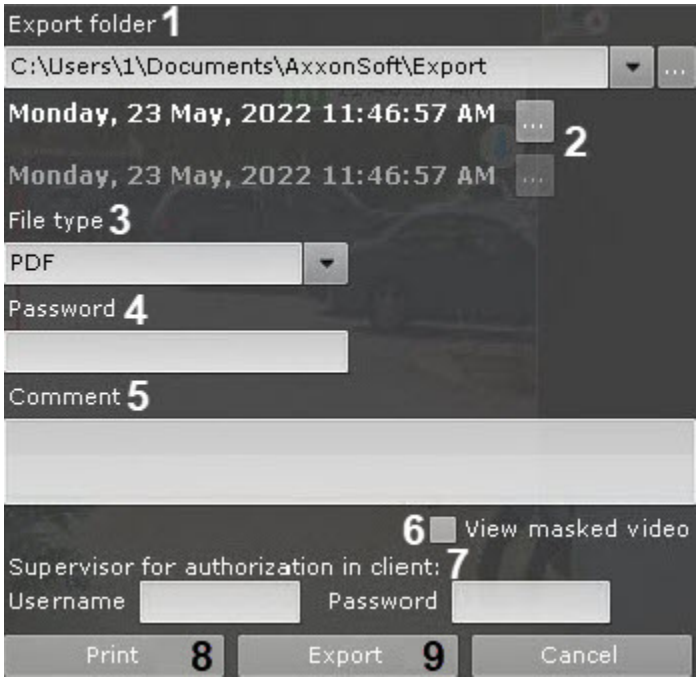
To export a frame, do the following:

1. If you want to export from an archive mode or archive analysis mode, specify an export area and mask if necessary (see Configuring export area and masks).
2. In the surveillance window, in the upper-right corner, click the button.

> **Attention!**
>
> To instantly export a frame with standard settings (see Configuring export options), right-click the button.

3. Specify the folder to which you want to export the frame (**1**).

> **Note**
>
> By default, frames are exported to the folder specified in the export settings (see Configuring export options). If you change this folder, the new path to the exported files will be kept in memory until the Client restarts.



4. Select the date and time of a frame (**2**). By default, the current frame is selected in the surveillance window. If you are watching an archive video, then the frame that was displayed when you clicked the button is selected.

> **Note**
>
> If you are watching a live video, then the frame that was displayed when you clicked the button will be exported. Date and time fields are not displayed.

5. Select the frame format: PDF or JPG (**3**).
6. If you want to export a frame to an encrypted zip archive, set an archive password (**4**).

> **Attention!**
>
> Setting a password will be mandatory if it is specified in the user role settings (see Creating and configuring roles).

7. If you exports a frame to PDF format, you can add comments (**5**).

8. To export unmasked frames (see Setting up privacy masking in Video Footage), the user must have appropriate access rights. To perform such an export, set the **View masked video** checkbox (**6**).
9. Enter the credentials of the supervisor who confirms the launch of export (**7**).

> **Note**
>
> The supervisor enters their password only if it is required by user role settings (see Creating and configuring roles). If no export confirmation is required, these fields will not be displayed.

10. If you export to PDF, you can immediately send the file to print (**8**). In this case, the frame is not saved to disk.
11. To export the frame, click the corresponding button (**9**).

Export begins. Progress is shown in the export panel (see Viewing export progress).

Export of the frame is now complete. The frame exported to JPG will also be placed on the clipboard.

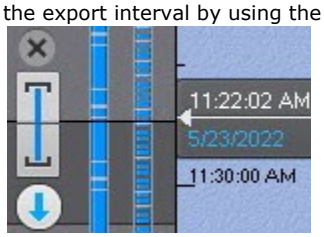
Exporting Video Recordings

Standard video recordings export

The standard export of the video recordings is performed according to the following procedure:

1. Setting the export interval.
   Set the export interval on the primary or the secondary timeline. You can set the export interval later by entering the date and time (see item 3c below):

   a. on the primary timeline, move the marker to the beginning of the interval that you want to export. Click the button. Move the marker to the end of the interval that you want to export. Click the button. You can also select the export interval by using the right mouse button. To clear the interval, click the button;

   b. you can specify the interval on the additional navigation panel in the same way, by clicking the buttons. You cannot use the mouse to select the export interval on the additional navigation panel.

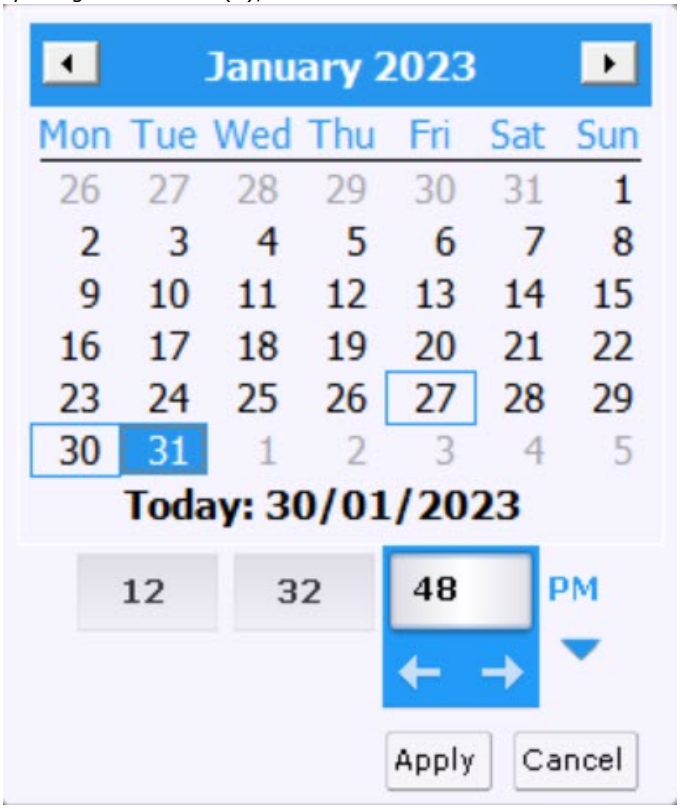
2. Setting the export area and masks (see the Configuring export area and masks).
3. Setting the export format.

   a. Click the button on the timeline or in the surveillance window.
   The export window opens.

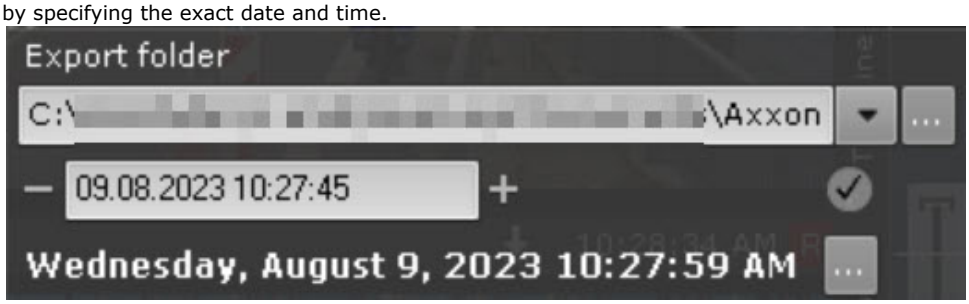
   

   b. If necessary, change the export path (**1**). By default, the file is exported to the folder specified in the settings (see Configuring export). If the folder was changed, the new path for the exported files is saved until the Client restart.
   c. You can set the start and end time of the exported interval in one of the following ways:

- by using the calendar (**2**);



- by specifying the exact date and time.



d. Click the **Apply** button.
e. If necessary, specify a different file format into which you want to export the video recording (**3**). Video recordings can be exported into the following 4 formats: MP4, MKV, EXE and AVI.

> **Attention!**
>
> - Video recordings are exported into the MKV format without recompression.
> - Video recordings are exported into the AVI format with recompression by the codec selected in the settings. Export into the AVI format may take longer because of recompression. In addition, the AVI format export increases the CPU load, especially when you export several files at once (see Simultaneous export of videos from multiple cameras, Simultaneous export of all event videos).
> - When video recordings are exported into the EXE format, an executable file is compiled, containing video recording, playback tools, and necessary codecs. When exporting into the EXE format, note that Windows OS does not allow launching executable files of more than 4 GB.
> - If you export video recordings from the fisheye camera in the EXE format, the entire panoramic view is exported, that can be rotated to the desired angle of view in the player. If the export is performed in the MKV, MP4 or AVI formats, the selected section on the camera in the layout interface is exported.

f. If you export a video recording into the MKV or AVI format, and you need to add the Axxon Player utility (see The Axxon Player User Guide) to the same folder, set the corresponding checkbox (**4**).
g. If you want to export into the encrypted ZIP archive, set the archive password (**5**). When exporting into the EXE format, you will need to enter the password when you open the file.

Attention!

Setting a password will be mandatory, if this condition is set in the user role settings (see Creating and configuring roles).

h. If necessary, add a comment to the export. The comment will be displayed as captions when the exported video recording is played back (**6**).
i. If necessary, export the video recording with the display of object tracks. To do this, select the type of detection tool that will be the source of the displayed tracks from the **Tracks** drop-down list (**7**).
j. If necessary, export the video recording with object masking. To do this:

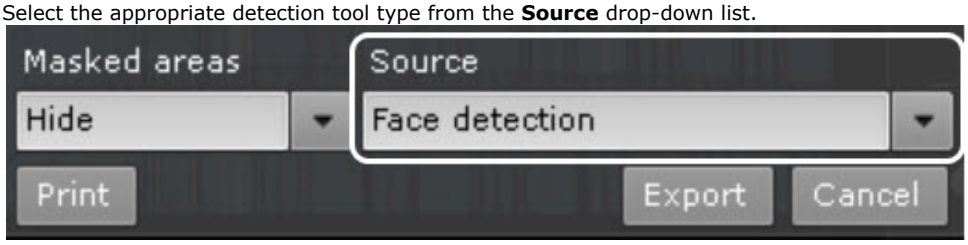
   i. From the **Masked areas** drop-down list (**8**) select one of the values:

      - **Hide**—if you want to mask objects in the exported video;
      - **Invert and hide**—if you want to mask the area around objects in the exported video.

      Note

      If you select **Hide** or **Invert and hide**, the export may take long time, regardless of the export format. This is because the system needs to re-encode the video to mask faces, which requires additional computing resources and time.

   ii. Select the appropriate detection tool type from the **Source** drop-down list.



k. Enter the username and the password of the supervisor who confirms the launch of the export (**9**).

Note

Entering the supervisor password is only required if this is set in the access rights settings (see Creating and configuring roles). If the confirmation is not required for the export, these fields will not be displayed in the window.

l. Click the **Print** button (**10**) if you want to to print the current video frame.
m. Click the **Export** button (**11**).

The export process starts. The progress is displayed on the export panel (see Viewing export progress).

Note

You can stop export at any time by clicking the **Stop** button.

Note

The duration of the exported file can be longer than the specified duration, because the key frame is not always at the beginning of the export interval.

Instant video export

You can instantly export video without specifying an export range. To do so, click the  button in the upper right corner of the surveillance window at any time.

If export is performed:

- in real time, then only the video frame at the moment the  button is clicked will be exported. Then, you should set the necessary parameters for exporting the frame (see Frame export).
- in the archive mode or the archive analysis mode, the first frame of the exported video will be the position of the bar on the timeline when the  button is clicked. Then, you should set the export parameters (see Standard video recordings export). If you select MP4, MKV, EXE or AVI format for export, the video recording range is 5 minutes from the current position of the bar on the timeline.

After you click the **Export** button, the export process will start, the status of which will be displayed in the export panel (see Viewing export progress).

The duration of exporting the video or a frame will depend on the Server resources.

Note

- You can stop the export at any time by clicking the **Stop** button.
- If export is performed in the archive mode or the archive analysis mode, you can pre-configure an export area and masks (see Configuring export area and masks).

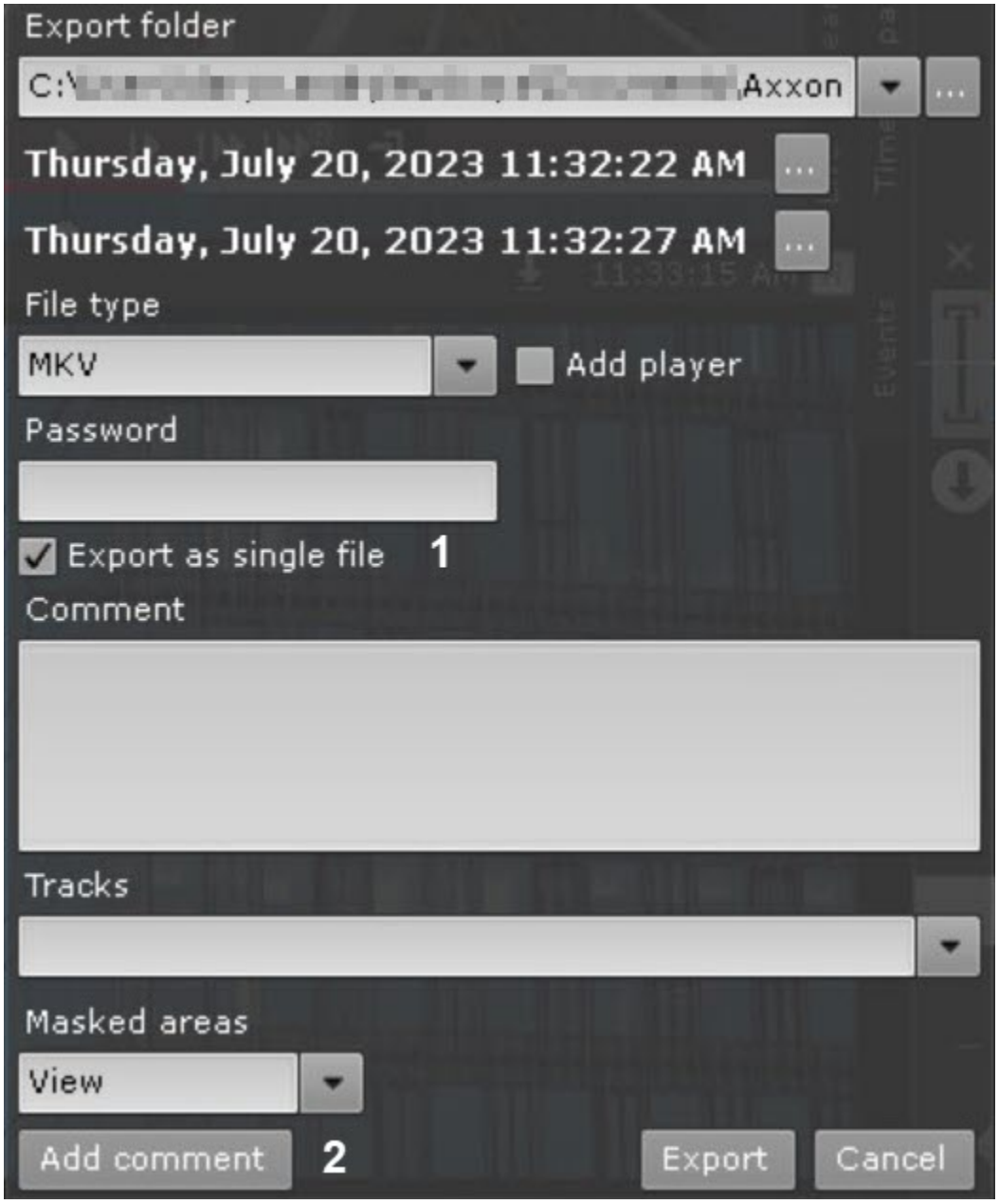
Simultaneous export of videos from multiple cameras

If multiple cameras in a layout have been switched to an archive mode, you can simultaneously export videos from all of them.

To do this, select the export interval on the primary timeline or in the calendar and start exporting (see Standard video recordings export).

By default, the video is exported to a single file. To export video from different cameras to separate files, clear the **Export as single file** checkbox in the export window (**1**).

> **Note**
>
> When you export to a single file, the streams are written in parallel. To view exported video, use a player that allows playing multiple simultaneously (for example, VLC).



Comments made during export are added to each exported video (**2**).

Note.

For each video you can pre-set an export area and masks (see Configuring export area and masks).

Simultaneous export of all event videos

You can use the Story board (see Story board) to simultaneously export all found videos of an event from archives of different cameras, having previously collected them on the board.

To do this, do the following:

1. Click the thumbnail of the found video fragment.
2. Set a time interval on the timeline for export (see Standard video recordings export).
   This will add the thumbnail of the selected video to the Story board.



3. Click the **+** button in the middle of the thumbnail. The video will be added to the export batch.

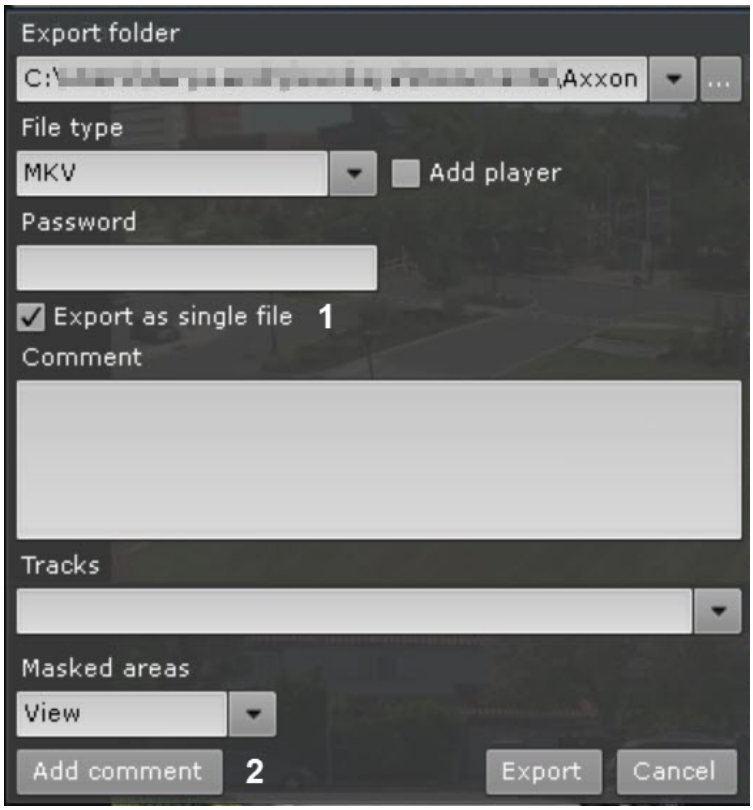
> **Note**
>
> To remove the video from the batch, click the button.

4. Repeat these steps for all videos of interest.
5. Click the button to export all selected videos.

The export window will open, further export steps are identical to the standard export process (see Standard video recordings export).

By default, the video is exported to a single file. To export video from different video cameras to separate files, clear the **Export as single file** checkbox in the export window (**1**).

> **Note.**
>
> When you export to a single file, the streams are written in parallel. To view exported video, use a player that allows playing multiple streams simultaneously (for example, VLC).



Note

We recommend you to export to the EXE format.

Comments made during export are added to each exported video (**2**).

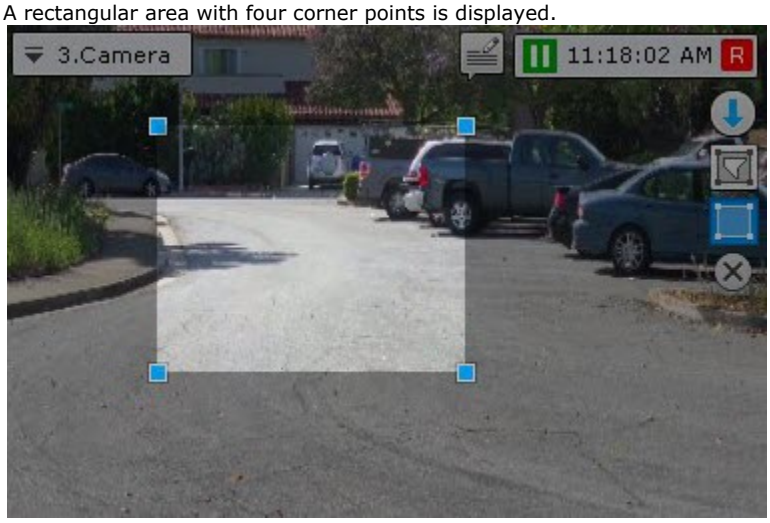
Configuring export area and masks

If you are exporting a snapsnot or video from Archive mode or Archive Analysis mode, you can specify an export area and masks.

You can specify an export area and masks at the same time.

By specifying an export area, you export only the portion of the frame that is of interest, while omitting the remainder.

To specify an export area:

1. In a viewing tile, click the  button.
   A rectangular area with four corner points is displayed.
   

2. Reposition the corner points to specify the area that you want to export. To reposition the corner points, left-click a corner point and drag it.

Configuration of the export area is now complete.

Masking allows you to hide complex or irrelevant areas of the frame so that they do not appear in an exported file. You can set an unlimited number of masks.

To specify a mask:

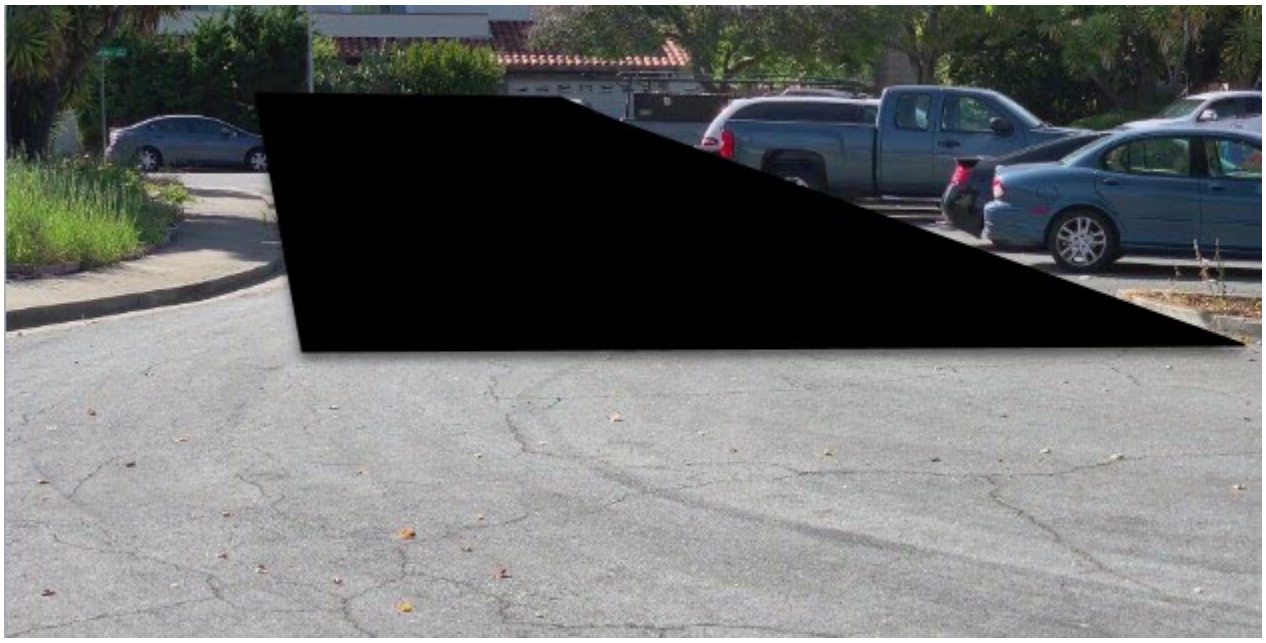
1. In a viewing tile, click the  button.
2. Use the corner points to enclose the area that you want to mask. To add a corner point, left-click the video. You can add an unlimited number of corner points.
   

   After you add a mask, you can perform the following actions:

- move corner points (left-click a corner point and drag it),
- delete corner points (right-click a corner point),
- delete a mask (click the  button),
- add a new mask.

Mask creation is now complete.

In the exported snapshot or video, the masked area is filled in with black.



Viewing export progress

After export is started, the export progress is displayed on the export panel. The export panel is displayed near the top of the monitor after the export process is started, and is hidden after all messages are closed.



To stop the export process, click the **Finish** button. In this case the file will be saved. The length of the exported fragment will depend on the export time and resources of the Server.

To cancel export, click the **Cancel** button. In this case, the file is not saved.

If several export processes are active, you can switch between them by clicking the  buttons. The following information is displayed between them: number of the current export operation/total number of export operations (export progress for all operations).

To close the export progress message, click the  button.

> **Note.**
>
> If export is active, you cannot close the message.

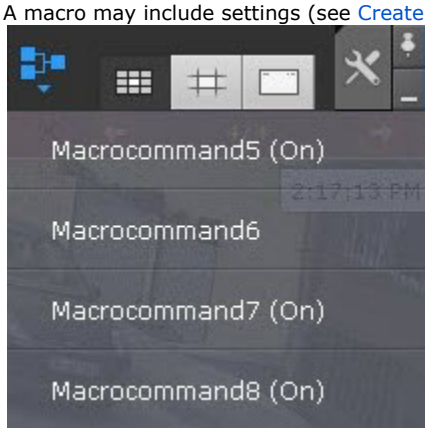
If an error occurs during export, it will be indicated on the dynamic error panel (see Control in Live Video mode).



Macros control

You can manage macros from the map (see Controlling devices from the map) or from the menu on the top panel.

A macro may include settings (see Create Macros) to display the  control menu in the upper panel.



Those macros that are currently active (enabled as **Always** or within a time schedule, see Create Macros), are marked as **(On)**. To enable or disable macros you need to select them in the list. When you disable a macro, the mode is changed to **Never**.

> **Note**
>
> If you disable a macro, which is active within the time schedule, then this mode will be restored after reactivation.

> **Note**
>
> The status of the macro in the menu changes only a few seconds after a command is completed.

Event-driven macros can be triggered by using the corresponding buttons on the Dialog board (see Working with Dialog Board) or by using hotkeys.

Event control

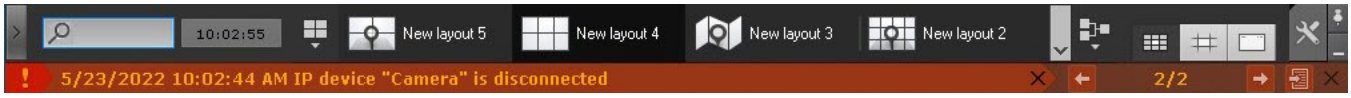
Event control in the *Axxon One* software package can be conducted in three ways:

1. In Live Video mode.
2. Using the system log.
3. By logging events in external logs.

> **Note**
>
> Configuration of logging to external files is carried out through the log management utility (see the section Log Management Utility).

Control in Live Video mode

Messages about system errors which have occurred are displayed in real time on a dynamic error panel. When there are no unaccepted errors, this panel is not displayed; when there are such errors, it is displayed in *Axxon One*'s **Layouts** tab.



> **Note**
>
> This feature is configured on the **Permissions** tab (see the section Creating and configuring roles).

To accept an error and delete it from the error panel, click the cross.
To accept all errors and close the error panel, click the cross on the right-hand side of the panel.

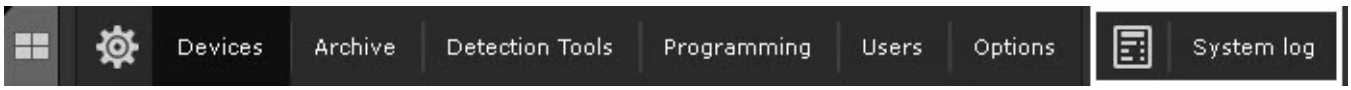
To switch between error messages, click the buttons.

To jump to System log (see The System Log), and open error messages, click the button.

The System Log

Information about events which have occurred in the system is stored in the system log.

To access the system log, select **Settings System log**.



When you do this, a window appears which can be used to search, view, and export system log events.

Setting Event Search Filters

To view and/or export system log events, first you need to perform a search for them.

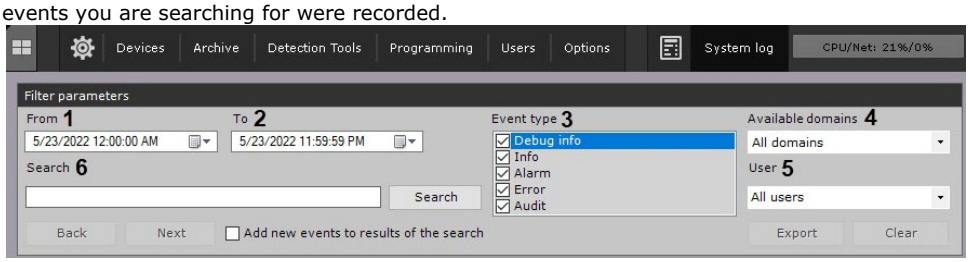
To search for system log events, you need to set one or more filters:

1. Time period during which the events were recorded.
2. Event type:
    a. Information,
    b. Alarm,
    c. Error,
    d. Debug info,
    e. Audit – user actions log.
3. A key phrase contained in the system event descriptions.

> **Note**
>
> The time period is a mandatory filter, while the event type and key phrase are optional.

Search filters can be set as follows:

1. In the **From** (**1**) and **To** (**2**) fields you can enter the date and time of the beginning and end of the period during which the events you are searching for were recorded.



> **Note**
>
> The date format is DD-MM-YYYY and the time format is HH:MM:SS.XXX.

> **Note**
>
> By default, the event search period is defined as the past 24 hours.

2. Selecting event types for search (**3**).
3. Select the Axxon domain where you need to search for events (**4**).
4. If user actions search was selected (the **Audit** type), choose a particular system user (**5**). If no user is selected, the search function will return actions of all system users.
5. Enter the text that matches the events you want to find in the **Search** text field (**6**). To find license plate numbers, enter the full or partial number. Use **?** (any one character) and ***** (any number of any characters). For example, a search query **?20*** shows all vehicles with a license plate containing **2** and **0** in the second and third position respectively. The total number of characters in number plates can be arbitrary.

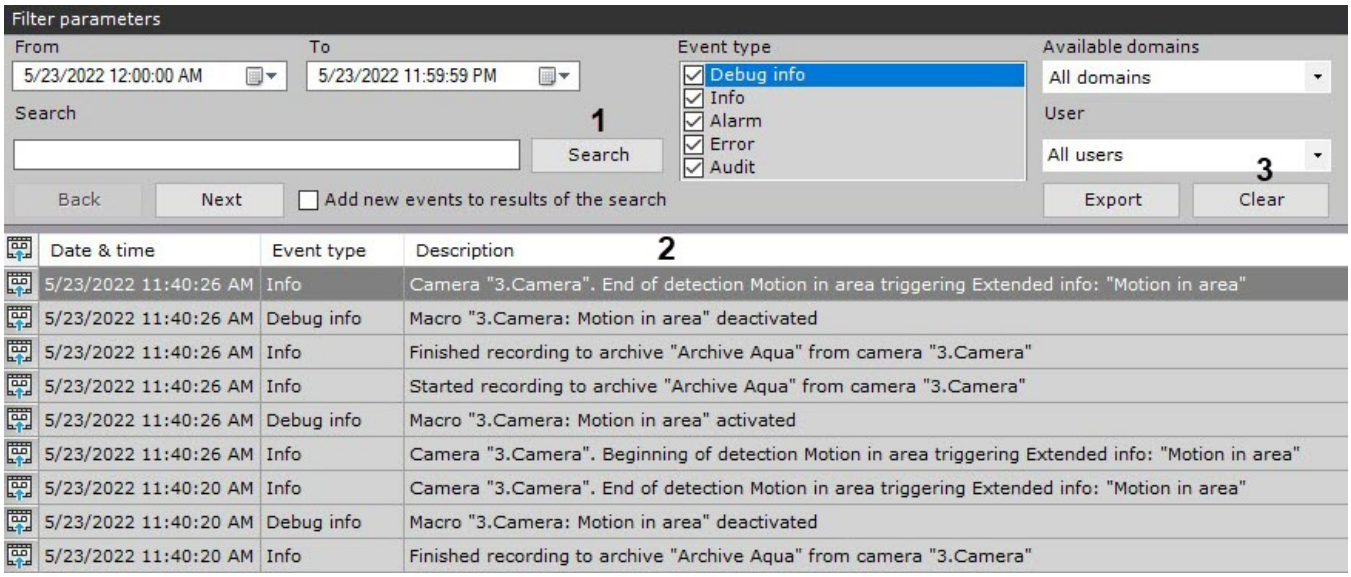
> **Attention!**
>
> You can use OR and AND logical operators when searching data in the system log:
>
> - to search with the OR logical operator, separate the words with the symbol "|";
> - to search with the AND logical operator, use a space.

The event search filters have been set.

Next you must start the event search (see the section titled Event search procedure).

Event search procedure

To start a search for system log events which satisfy the filters which have been set (see the section Setting Event Search Filters), click the **Search** button (**1**).

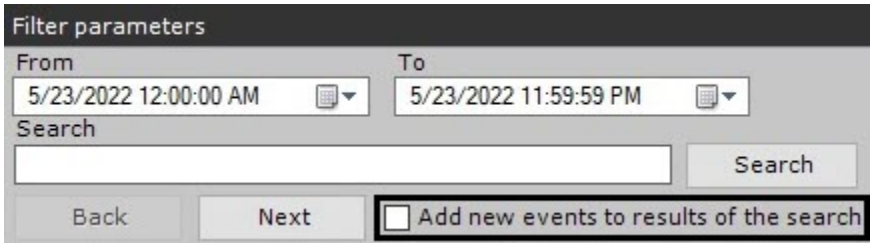


When you do that, a search results table appears (**2**).

To accept all errors and close the error panel, click the **Clear** button (**3**).

Refreshing Event Search Results

You can automatically refresh the event search results table, i.e., add events to it which happened after the search was started (see the section Event search procedure). To do this, select the **Add new events to results of the search** checkbox.



Note

Select this checkbox to update events automatically with no need to search again.

Viewing Event Search Results

System log event search results are displayed in a table (**1**).

> **Note**
>
> Events in the table are sorted by the date they were registered, beginning with the most recent one.

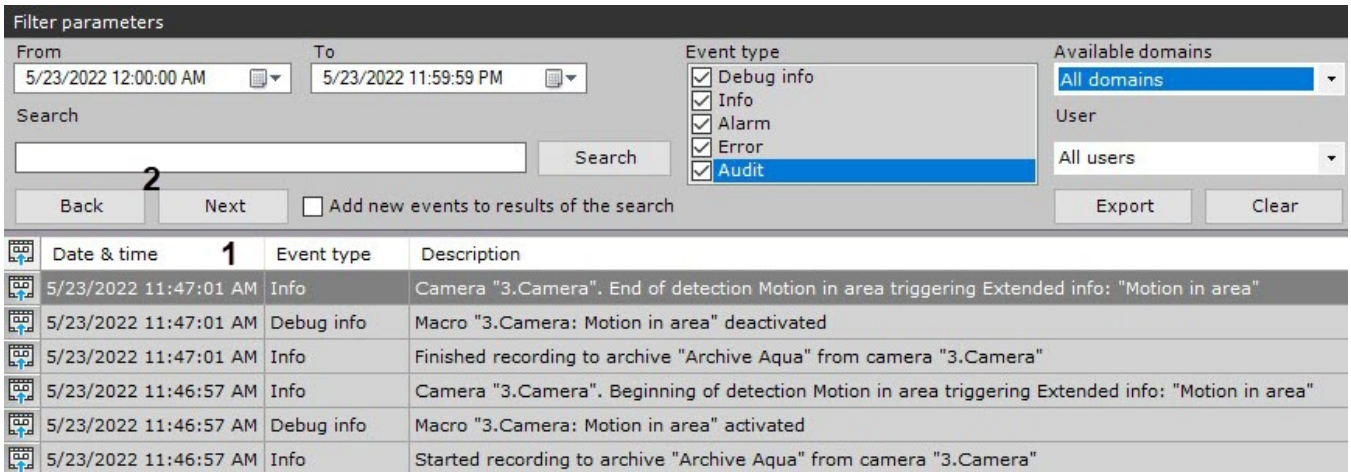


Table column	Contents of column
	Switching to archive video of specific events
Date & time	Date and time of the event was recorded in the system in the format DD.MM.YYYY HH:MM:SS
Event type	Event type (Information, Alarm, Debug info, Error)
Description	System description of the event

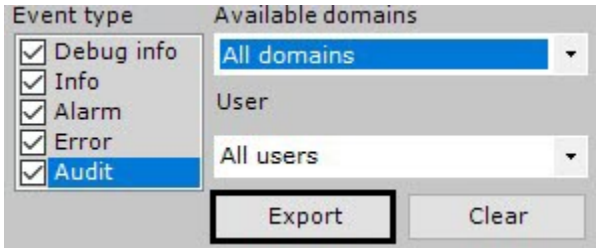
The search results table may be more than one page. To navigate through a table which is more than one page, use the following buttons (**2**):

1. **Back** – go back to the previous page of the table.
2. **Next** – go to the next page of the table.

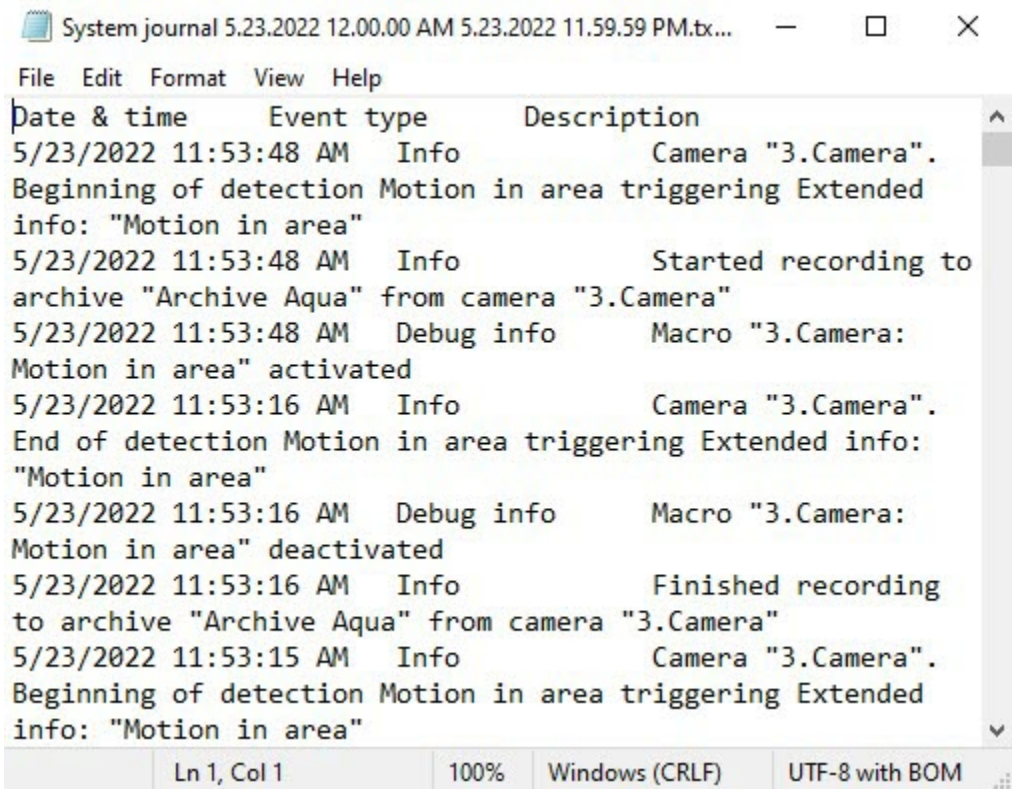
> **Note**
>
> Once the *Axxon One* VMS is installed, the log may show a **Table end violation** error**.** This is part of the installation routine and not a bug.

Exporting Event Search Results

To export the system log event search results, click the **Export** button.



When you do this, the standard Windows “Save as” dialog box appears, using which you can save the search results as a file with a .txt (text) extension or .csv (comma-separated).



Switching to archive video of specific events

To switch to archive video of specific events, click the  icon next to the event or double-click the relevant row.

> **Note**
>
> Archive viewing can be triggered by events coming from cameras, inputs (sensors) and outputs (relays). To make it work, I/O must be linked to a particular camera (see The Input Object, The Output Object).

Date & time	Event type	Description
5/23/2022 11:47:01 AM	Info	Camera "3.Camera". End of detection Motion in area triggering Extended info: "Motion in area"
5/23/2022 11:47:01 AM	Debug info	Macro "3.Camera: Motion in area" deactivated
5/23/2022 11:47:01 AM	Info	Finished recording to archive "Archive Aqua" from camera "3.Camera"
5/23/2022 11:46:57 AM	Info	Camera "3.Camera". Beginning of detection Motion in area triggering Extended info: "Motion in area"
5/23/2022 11:46:57 AM	Debug info	Macro "3.Camera: Motion in area" activated
5/23/2022 11:46:57 AM	Info	Started recording to archive "Archive Aqua" from camera "3.Camera"
5/23/2022 11:46:52 AM	Info	Camera "2.Camera". End of detection Motion detection triggering Extended info: "Motion detection"

The system will now switch to Archive mode and fetch the video of the selected event.

Working with Axxon One through the Web-Client

Web-Client overview

Web-Client is an interface that allows you to interact with some components of the *Axxon One* through a Web browser.

Before you start working with Web-Client, it is recommended that you learn the hardware and technical requirements for the correct operation of the Web-Client (see Hardware and software requirements for the Web-Client operation).

To ensure the correct launch of Web-Client, first configure the *Axxon One* Web-Server (see Configuring the Web-Server). Then you can launch and authorize in Web-Client through a Web browser using the address of the *Axxon One* Web-Server (see Starting and logging in to the Web-Client).

The Web-Client user interface (see Web-Client GUI) can be changed using user preferences (see Web-Client configuration).

The Web-Client offers the following options:

1. Viewing live videos.
2. Working with layouts.
3. Controlling PTZ cameras.
4. Viewing Archive.
5. Archive search.
6. Archive position selection.
7. Searching for video cameras.
8. Viewing and processing alarms.
9. Listening to a camera's microphone.
10. Exporting still frames and videos.
11. Digital zooming.
12. Working with bookmarks.
13. Viewing video camera detection tool triggerings.
14. Running macros.
15. Viewing Camera and Archive Statistics.
16. Working with interactive map via the Web-Client.

Hardware and software requirements for the Web-Client operation

The Web-Client operates correctly with the latest versions of Google Chrome, Safari, Firefox and Microsoft Edge browsers.

Note

Since no 3rd party technologies are used in the Web-Client, it may operate with other browsers; in this case, we cannot guarantee its stable operation.

Attention!

No support for Internet Explorer is provided in the current version.

To monitor 16 FullHD* camera videos on a single browser tab, you need at least an Intel Core i3 CPU and 1Gb of RAM.

* conditions are:

- dual stream cameras,
- each stream's frame rate is 25 FPS,
- the second stream's resolution is 360p,
- if the layout includes more than one camera, the browser shows streams with lower bitrates.

Starting and logging in to the Web-Client

You can work with *Axxon One* via the Web-Client remotely using a web browser and the TCP/IP communication environment. Remote video surveillance via a web browser doesn't require installation of *Axxon One*.

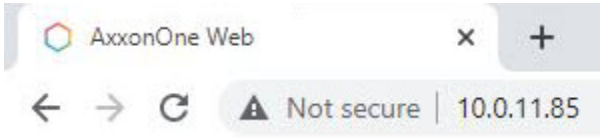
To start and log in to the Web-Client, do the following:

1. Start a web browser.
2. In the address bar, enter the address of the *Axxon One* Web-Server in the following format: <Web-Server IP address>:<Port>/<Prefix>.

   Connecting the Web and Mobile Clients to the Server behind NAT

   Attention!

   - The Server URL is case-sensitive. It is necessary to enter the URL exactly in the letter case specified in the settings (see Configuring the Web Server).
   - A connection via the secure HTTPS protocol will be automatically established, if the Web-Server is configured accordingly (see Configuring the Web-Server).

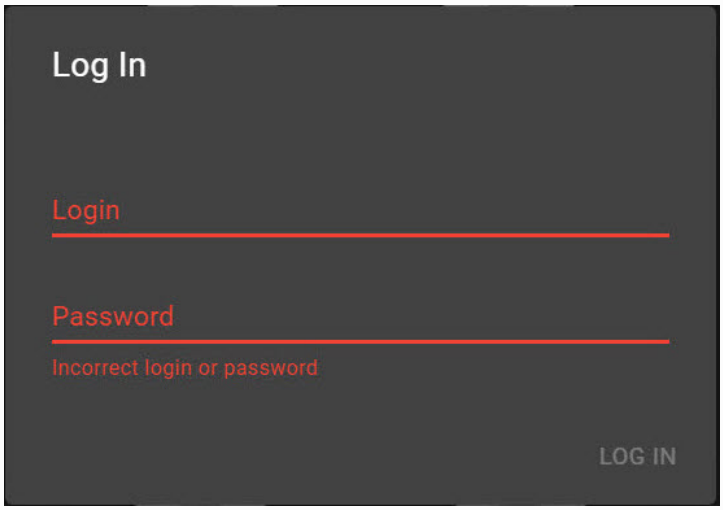
   

3. Enter a login and password to connect to the *Axxon One* Web-Server.

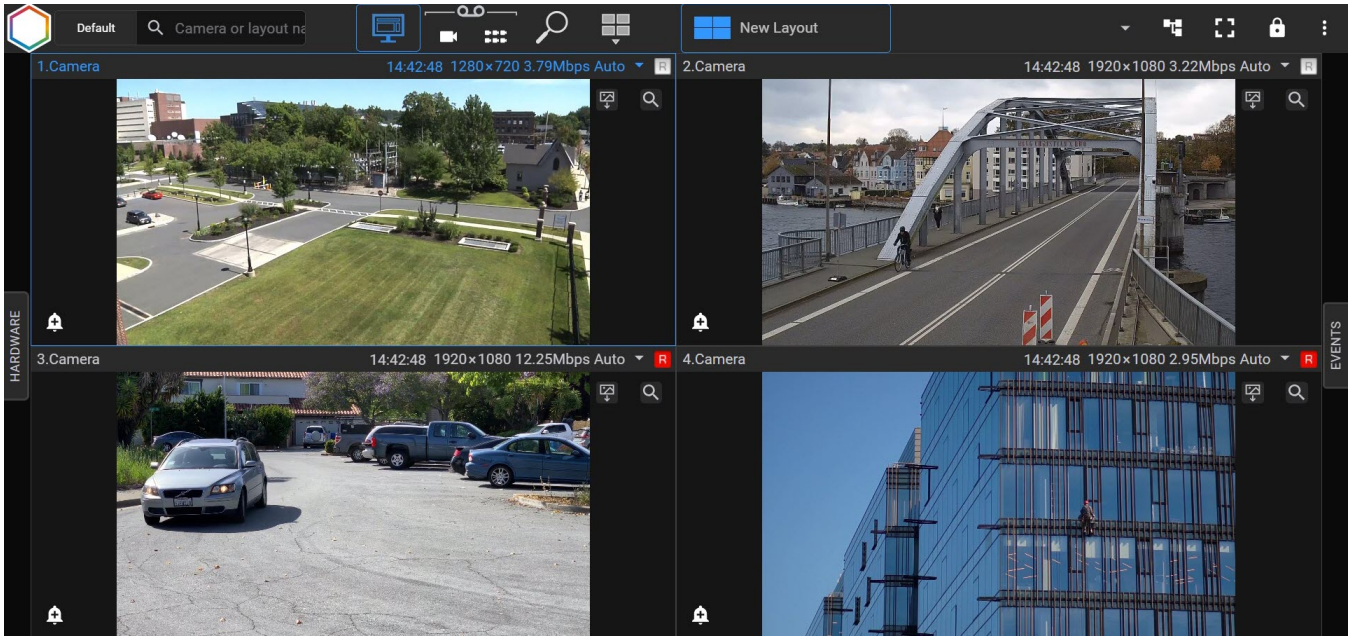
Note

If you try to log in with an invalid login and password, an error message will be displayed.



After five failed log in attempts, the user is blocked for 10 minutes.

As a result, the Web-Client interface will be displayed. By default, the first listed layout will be displayed. If there are no layouts, the Cameras panel will open on the left and the video image from the first listed video camera will be displayed.

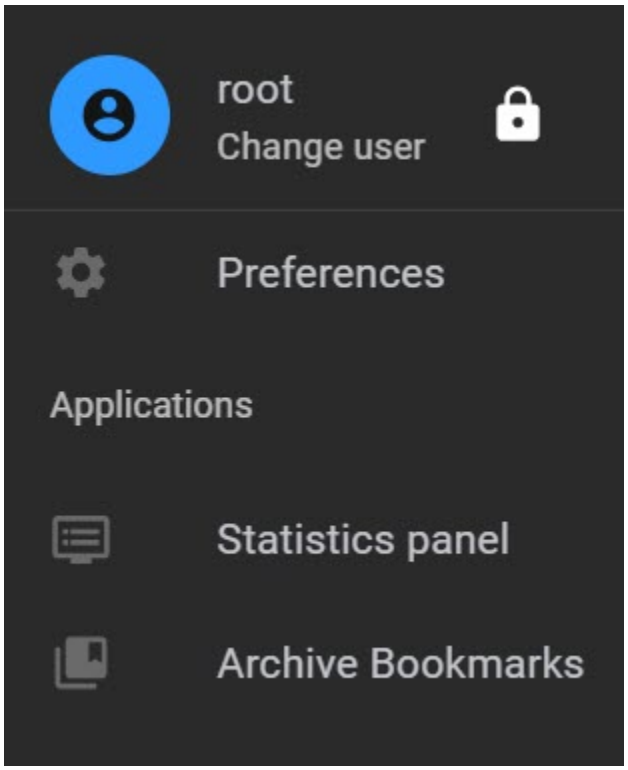


Changing the user in the Web-Client

To change the user in the Web-Client, click the  button in the top right corner and select the **Change user** menu item.

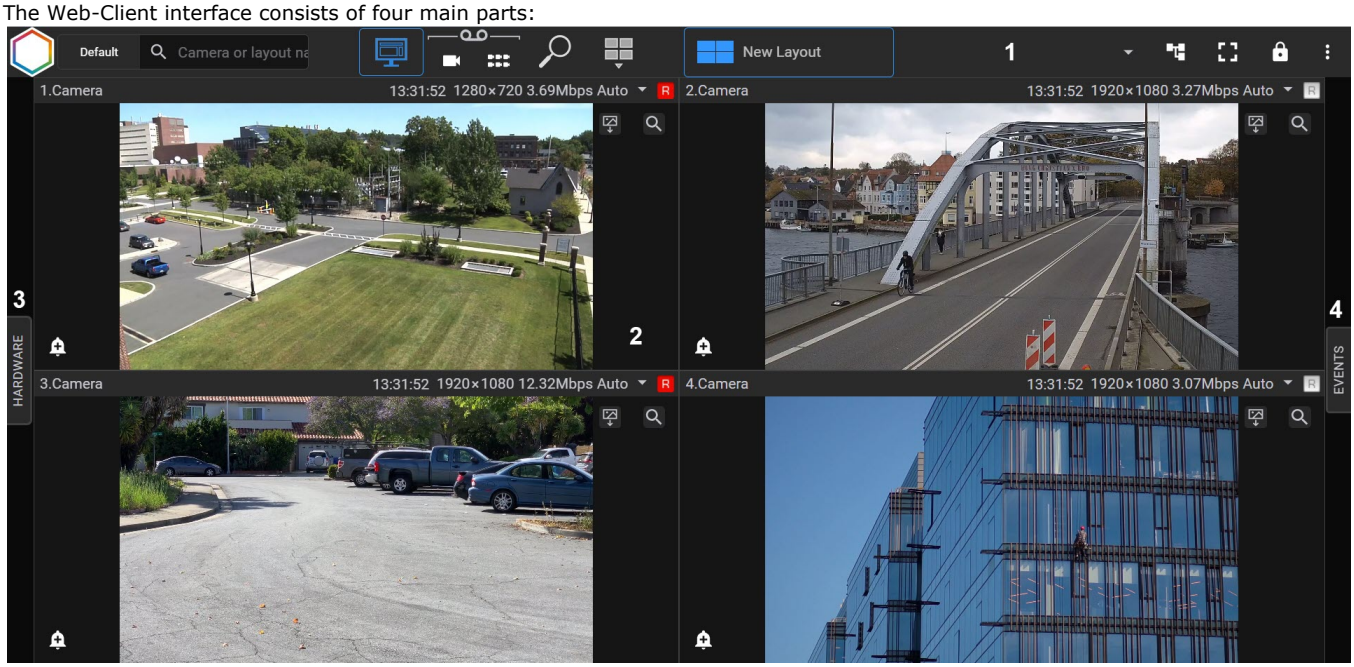
Note

The name of the current user is displayed next to this item.


root
Change user
Preferences
Applications
Statistics panel
Archive Bookmarks

Web-Client GUI

The Web-Client interface consists of four main parts:



1. The top panel (**1**) includes:
   a. the search bar for cameras or layouts (see Searching for video cameras in the Web-Client);
   b. the button to go to the real-time video surveillance mode  (see Real-time video surveillance in the Web-Client);
   c. the button to view the camera archive  (see Viewing video archives through the Web-Client);
   d. the button to switch all video cameras on the layout to archive mode  (see Viewing video archives through the Web-Client);
   e. the button to go to the archive search mode  (see Archive search in the Web-Client);
   f. the layouts menu and the list of available layouts  (see Working with layouts in Web-Client);

      > **Attention!**
      >
      > The Web-Client displays the layouts available to a particular user. The number of cameras on the layouts is unlimited.

   g. run macro button  (see Running macros in Web-Client);
   h. the full-screen mode button  ;
   i. the button to hide the top panel  . In this case, the top panel will be displayed only when you hover the mouse cursor over it. To pin the top panel, click the  button.
   j. the three-dot menu button  (see Web-Client configuration, Viewing Camera and Archive Statistics).
2. The Surveillance window (**2**), (see Surveillance window in the Client). Each surveillance window includes:
   a. the export button  (see Export in the Web-Client);

b. the button to go to the quick search mode  (see Archive search in the Web-Client);

c. the button to trigger an alarm  (see Viewing and processing alarms in Web-Client).

3. The **Hardware** panel (**3**) that displays all available cameras (see Searching for video cameras in the Web-Client).

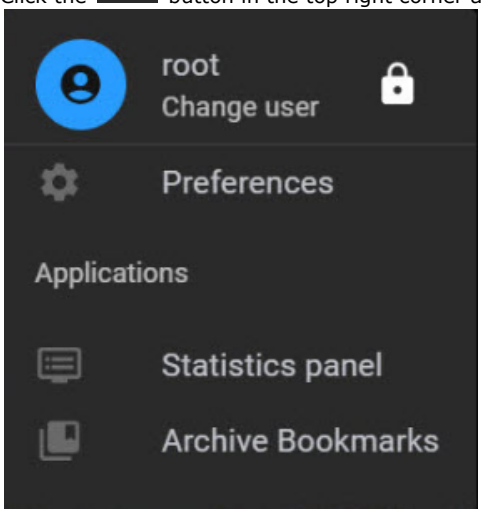
> **Note**
>
> In the Web-Client interface, you can change the width of the **Hardware** panel. To do this, point the cursor to the **Hardware** panel, hold down the cursor and drag it to the left or right.
>
> 
>

4. The **Events** panel (**4**) that displays the selected system events.

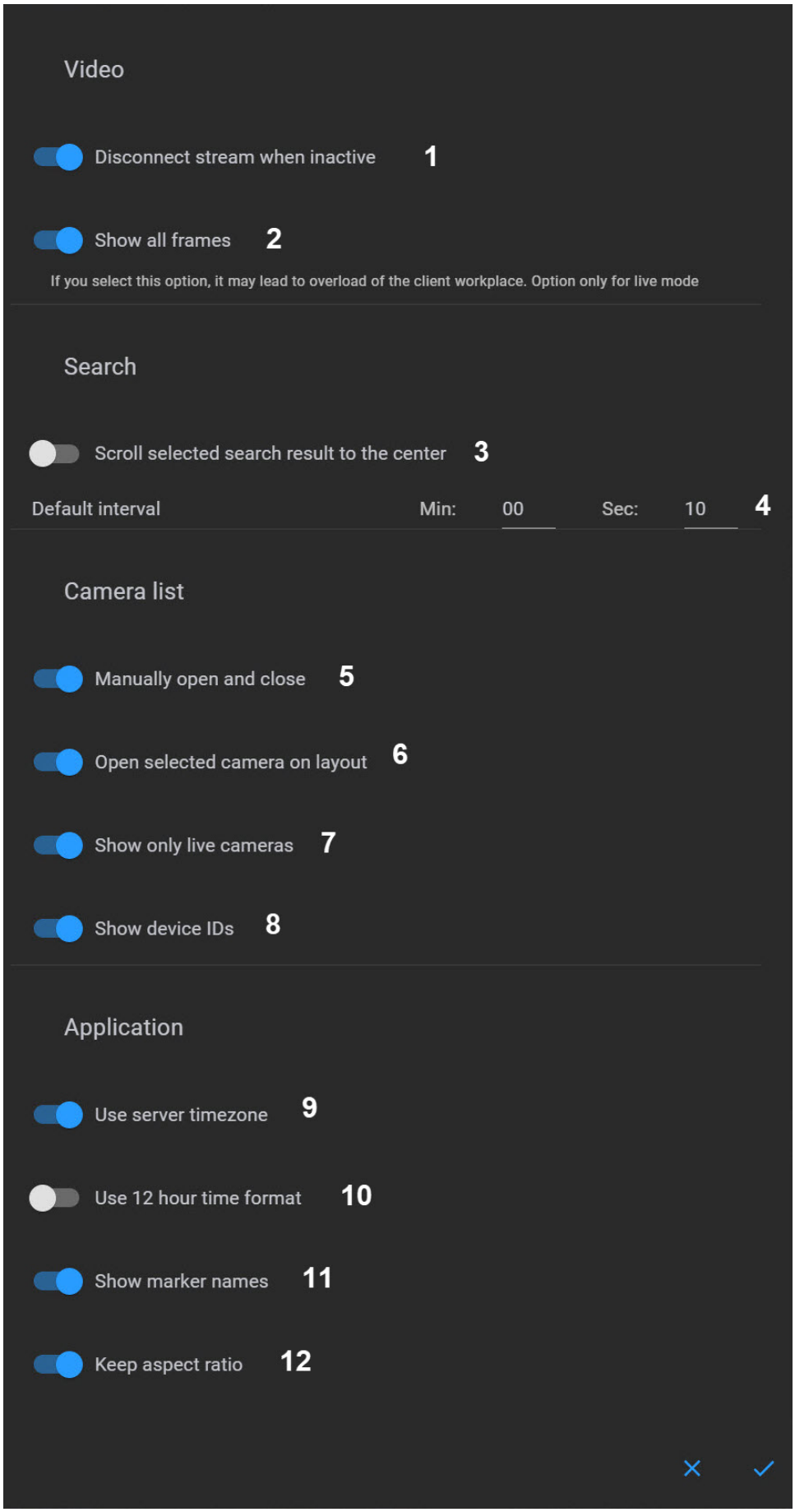
Web-Client configuration

To configure the Web-Client, do the following:

1. Click the  button in the top right corner and select **Preferences**.



2. By default, when you switch to another tab in the browser and minimize it, the video stream transmission stops. In order not to interrupt the video stream transmission, disable the **Disconnect stream when inactive** parameter (**1**). This setting is common to all Web-Client users in a particular browser.


Video
Disconnect stream when inactive
1
Show all frames
2
If you select this option, it may lead to overload of the client workplace. Option only for live mode
Search
Scroll selected search result to the center
3
Default interval
Min:
00
Sec:
10
4
Camera list
Manually open and close
5
Open selected camera on layout
6
Show only live cameras
7
Show device IDs
8
Application
Use server timezone
9
Use 12 hour time format
10
Show marker names
11
Keep aspect ratio
12

3. By default, in the video on the layouts, all frames are displayed. To reduce the load, you can disable the **Show all frames** parameter (**2**). As a result, on a layout with several video cameras, video playback will only be by key frames, and only when you select a specific camera, all frames will be displayed. The parameter does not affect the archive video, as archive videos are always played back by all frames. This setting is common to all Web-Client users in a particular browser.

   > **Note**
   >
   > The parameter does not affect the MJPEG video format, as all frames in it are key frames.

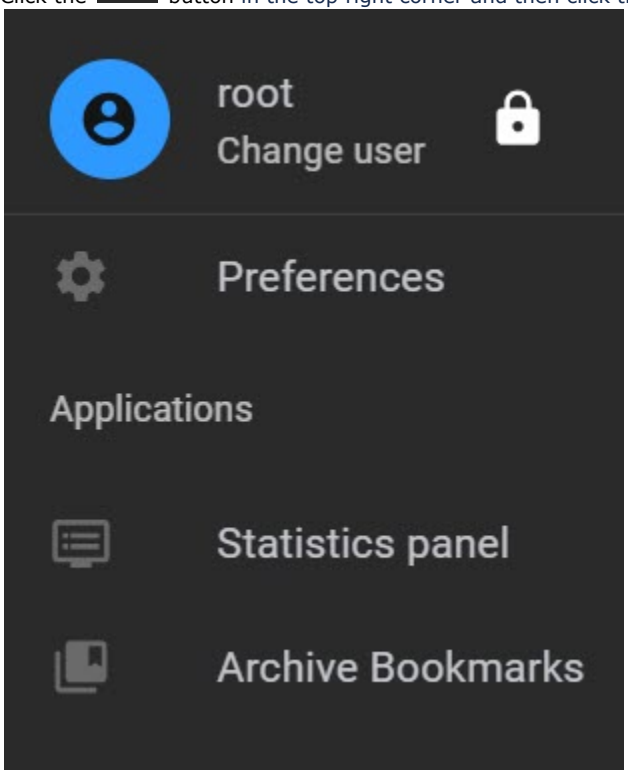
4. To position the found fragment in the center of the screen, enable the **Scroll selected search result to the center** parameter (**3**). This setting is common to all Web-Client users in a particular browser.
5. Set the default interval for the TimeSlice (**4**, see Types of archive search in the Web-Client). This setting is common to all Web-Client users in a particular browser.
6. By default, the Cameras panel does not close after you select a device. To minimize the panel, disable the **Manually open and close** parameter (**5**). This setting is common to all Web-Client users in a particular browser.
7. When you select a camera in the Cameras panel, a layout containing the selected camera will open. If there are several such layouts, then the one with fewer cells is selected. To expand the video camera to full screen, disable the **Open selected camera on layout** parameter (**6**). This setting is common to all Web-Client users in a particular browser.
8. By default, the Web-Client displays only the enabled cameras. If you want the Web-Client to display all cameras, disable the **Sh ow only live cameras** parameter (**7**). This setting is common to all Web-Client users in a particular browser.
9. By default, the Web-Client displays the cameras IDs. In order to disable the cameras IDs display, disable the **Show device IDs** parameter (**8**). This setting is common to all Web-Client users in a particular browser.
10. By default, the Web-Client cameras and bookmarks display the Server time. If you want the Web-Client cameras and bookmarks to display the client time, disable the **Use server timezone** parameter (**9**). This setting is common to all Web-Client users in a particular browser.
11. By default, the Web-Client displays time in the 24-hour format and date in the DD-MM-YYYY format. If you want the time to be displayed in the 12-hour format and date to be displayed in the MM-DD-YYYY format, enable the **Use 12 hour time format** parameter (**10**). This setting is common to all Web-Client users in a particular browser.
12. If you can view the interactive map in the Web-Client, the names of all camera markers added to the map are displayed by default. To disable the display of marker names on the interactive map, disable the **Show marker names** parameter (**11**). This setting is common to all Web-Client users in a particular browser.
13. By default, in the Web-Client, the size of the surveillance windows in the layout is proportional to the resolution of the video image. To ensure that the video image takes the entire space of the surveillance window, disable the **Keep aspect ratio** (**12**) parameter. As a result, the video image will be stretched over the entire surveillance window. This setting is common to all Web-Client users in a particular browser.
14. Click the  button.

Configuring the Web-Client is complete.

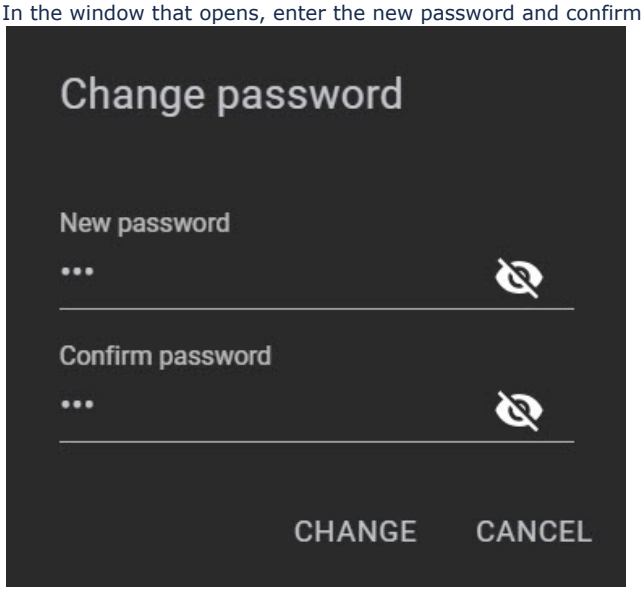
Changing the user password in the Web-Client

To change the user password in the Web-Client, do the following:

1. Click the  button in the top right corner and then click the  button.



2. In the window that opens, enter the new password and confirm the new password.

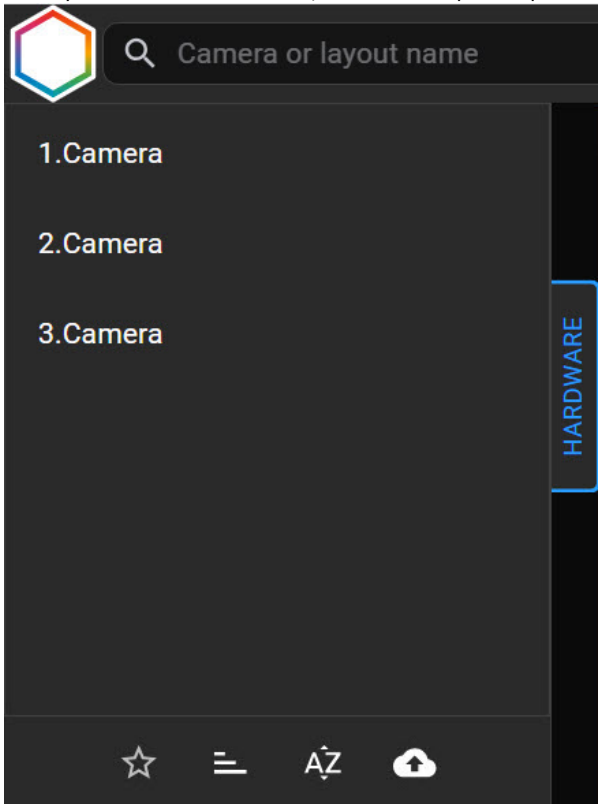


3. Click the **Change** button.

Changing the user password in the Web-Client is complete.

Searching for video cameras in the Web-Client

When you start the Web-Client, the cameras panel opens on the left. It displays the list of all available devices.



By default, the panel displays all available cameras. You can also create a list of the favorite cameras. To do this, do the following:

1. Point the mouse cursor to the camera.
2. Click the  button to add the camera to the list. The asterisk becomes filled  . Another click on the asterisk excludes the camera from the list.

> **Attention!**
>
> The list of the favorite cameras is common for all Web-Client users in a particular browser.

Click the **Favorites** button at the bottom of the panel to display the favorite cameras only. Click the same button again to display all available cameras.

Additionally, it is possible to make favorite the cameras from the pre-prepared list in Excel format. To do this, do the following:

1. Create an Excel file containing two columns: the **id** column for camera IDs and the **name** column for camera names.

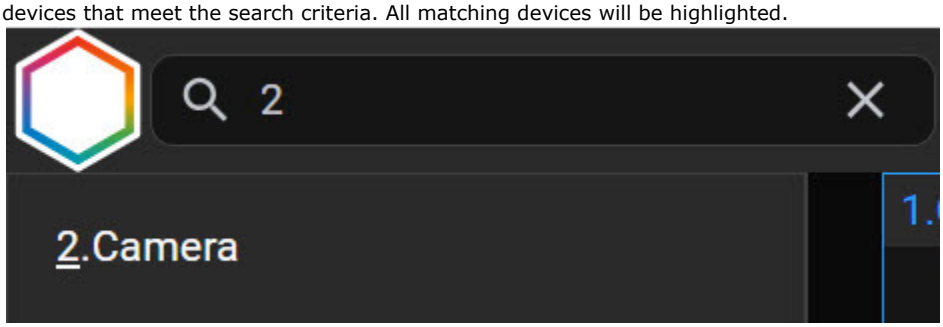
	A	B
1	id	name
2	8	Camera1
3	9	Camera2

2. Click the  button and select the file.

> **Attention!**
>
> After downloading the file, only the cameras listed in the file will become favorite.

Click the  button to sort the cameras on the panel by ID, or click the  button to sort the cameras by name.

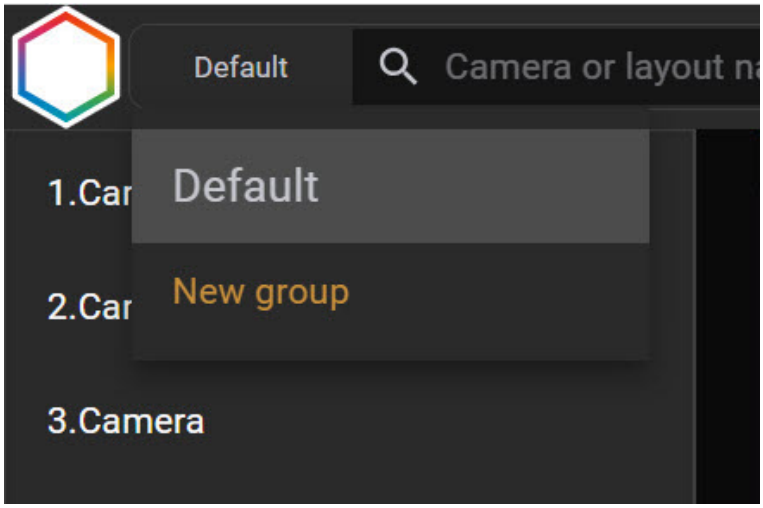
To search for a camera, enter the full or partial device name in the **Camera name** field. The cameras panel will display only the devices that meet the search criteria. All matching devices will be highlighted.



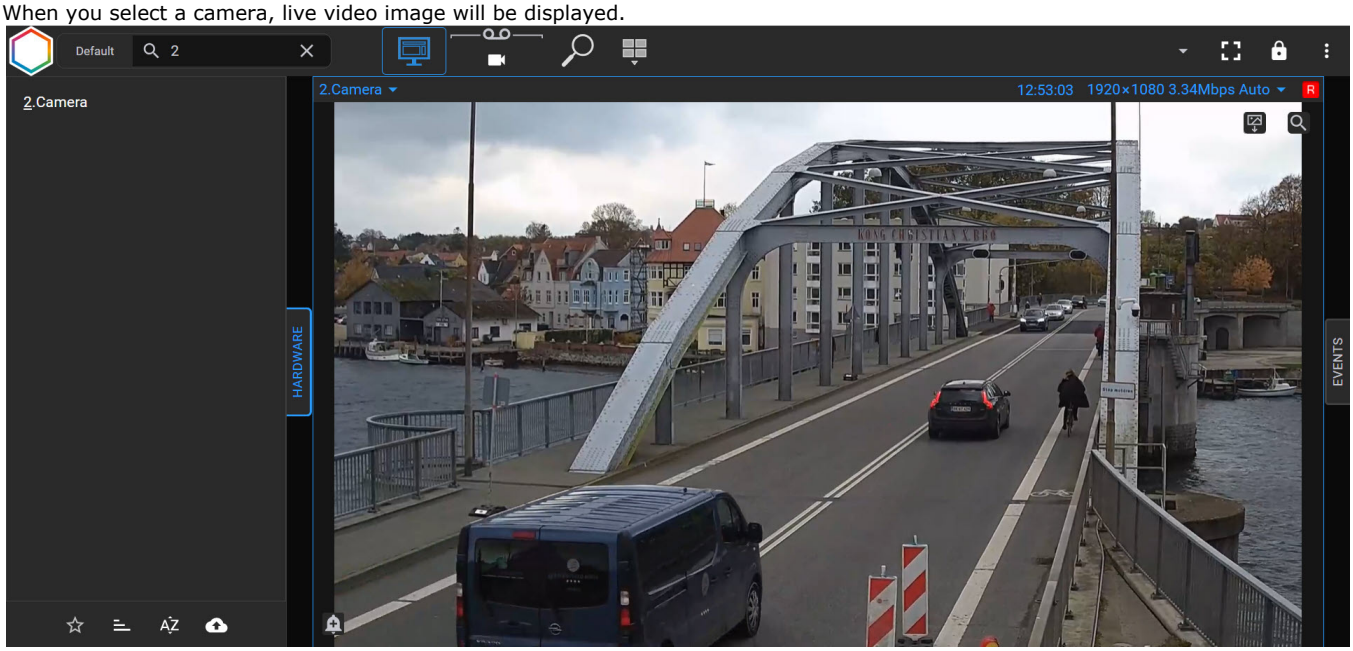
Note

- The search result includes both the list of cameras and the list of layouts.
- When you add new cameras to the Server configuration, they appear in the Web-Client dynamically without page reload.

To display a camera group (see Configuring video camera groups), click the **Default** button and select the required group.



When you select a camera, live video image will be displayed.



Each surveillance window in the upper right corner contains:

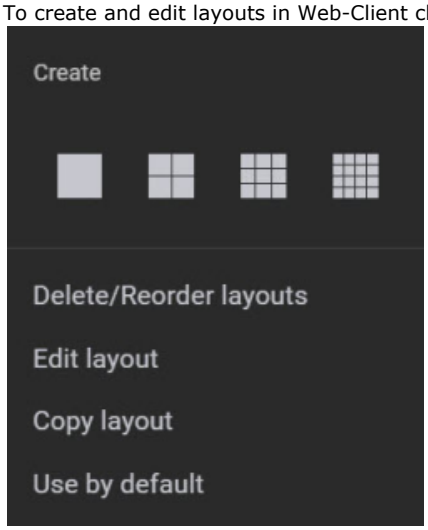
- time display (see Time Display in the main Client);
- video stream parameters;
- archive recording indicator.

Working with layouts in Web-Client

Summary of how to work with layouts in Web-Client

Configuring layouts

To create and edit layouts in Web-Client click  to access the corresponding menu.



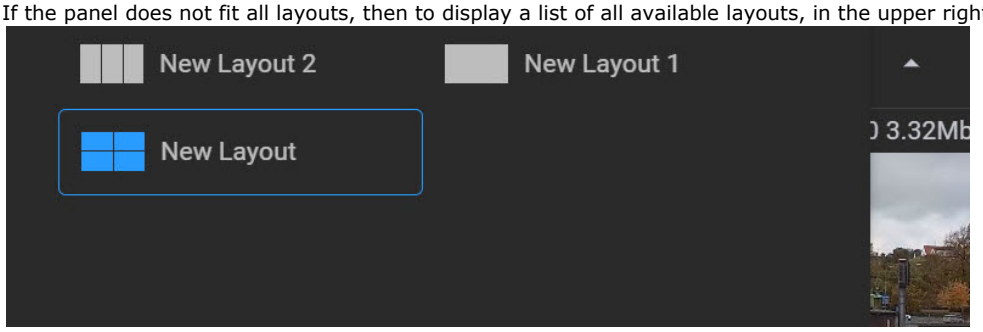
There are a number of things you need to consider when dealing with layouts in Web-Client:

1. In Web-Client, you cannot edit/share/delete layouts created in the main Client. You can only copy layouts or use them by default.
2. Layouts created in Web-Client will not be available in the main Client.

Selecting and searching for a layout

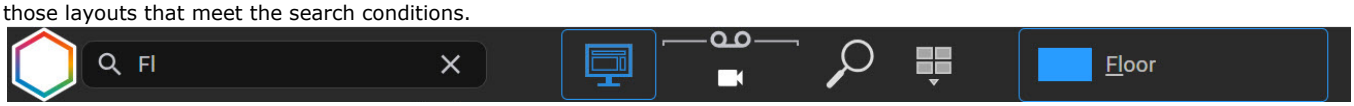
To go to the layout, click it on the panel.

If the panel does not fit all layouts, then to display a list of all available layouts, in the upper right corner click  .



To close the layout list, you need to press a button  .

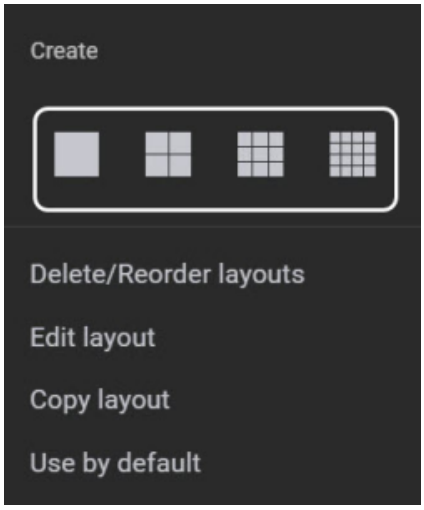
You can also search layouts in the search bar for video cameras. To do this, enter the layout name in part or in full. This will show only those layouts that meet the search conditions.



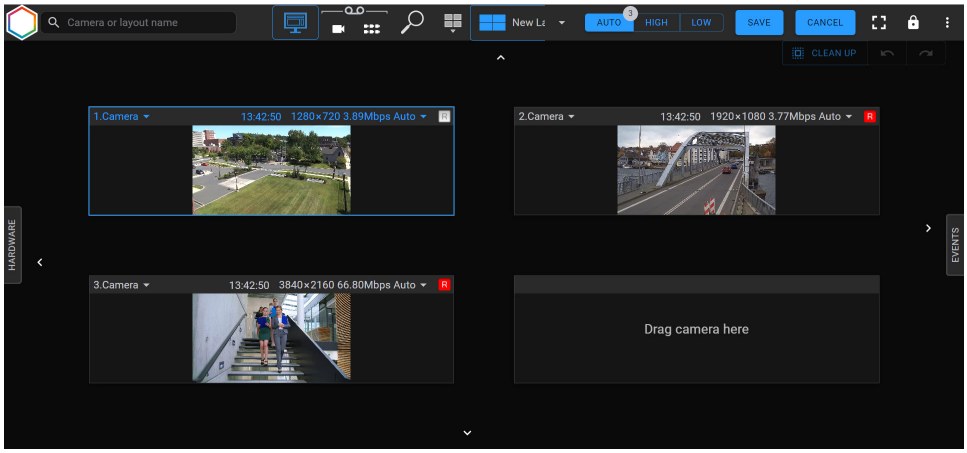
Creating a new layout in the Web-Client

To create a new layout in the Web-Client, do as follows:

1. Click the  button and select one of the standard layout types.



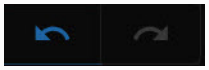
A layout will be created, displaying the video images from the cameras in real time from the list of the Cameras panel.



By default, the layouts display only active cameras. If you want the layout to display all available cameras, including inactive, disable the **Show only live cameras** parameter in the Web-Client settings (see Web-Client configuration).
After this, in the **Hardware** panel, video cameras will be highlighted in the following colors:

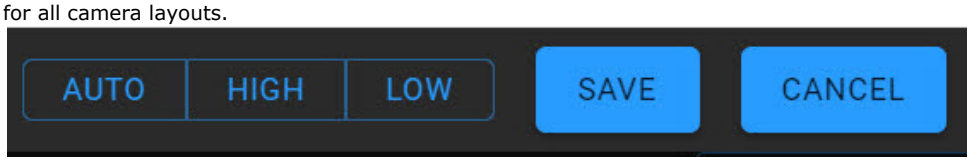
- white if they are active;
- orange if they are inactive (turned off in the *Axxon One* configuration);
- red if they are active, but with no signal.

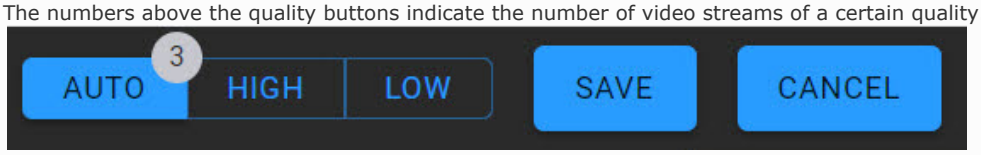
2. You can add new columns or rows of cells using arrows on the layout boundaries (similar to the main Client, see Adding new cells to a layout).

> **Note**
>
> - To delete a column or a row of empty cells, click the **Clean Up** button.
> - When editing a layout, the buttons to undo and redo the last action are available  .

3. You can resize the cells using arrows on the cell boundaries (similar to the main Client, see Resizing cells).
4. Add video cameras to the cells. To do this, drag & drop a camera from the Cameras panel (see Searching for video cameras in the Web-Client).

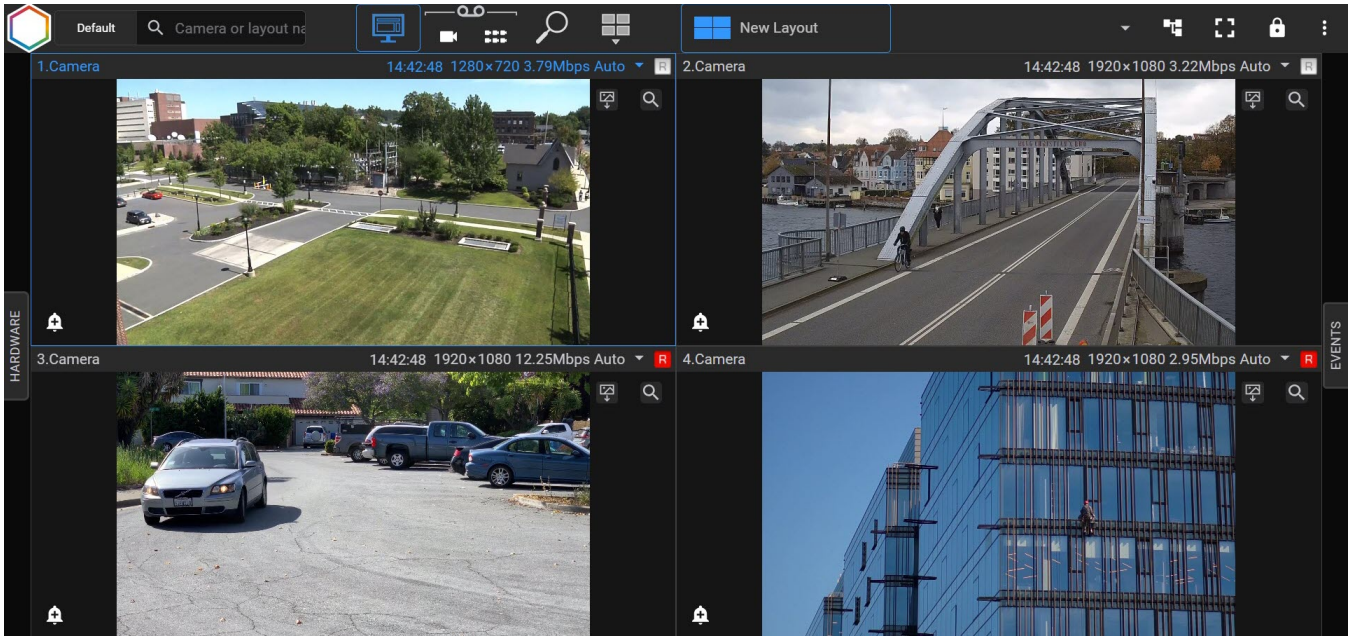
5. Select the default stream for each video camera from the **Quality** list. Use the buttons at the top of the screen to select quality for all camera layouts.



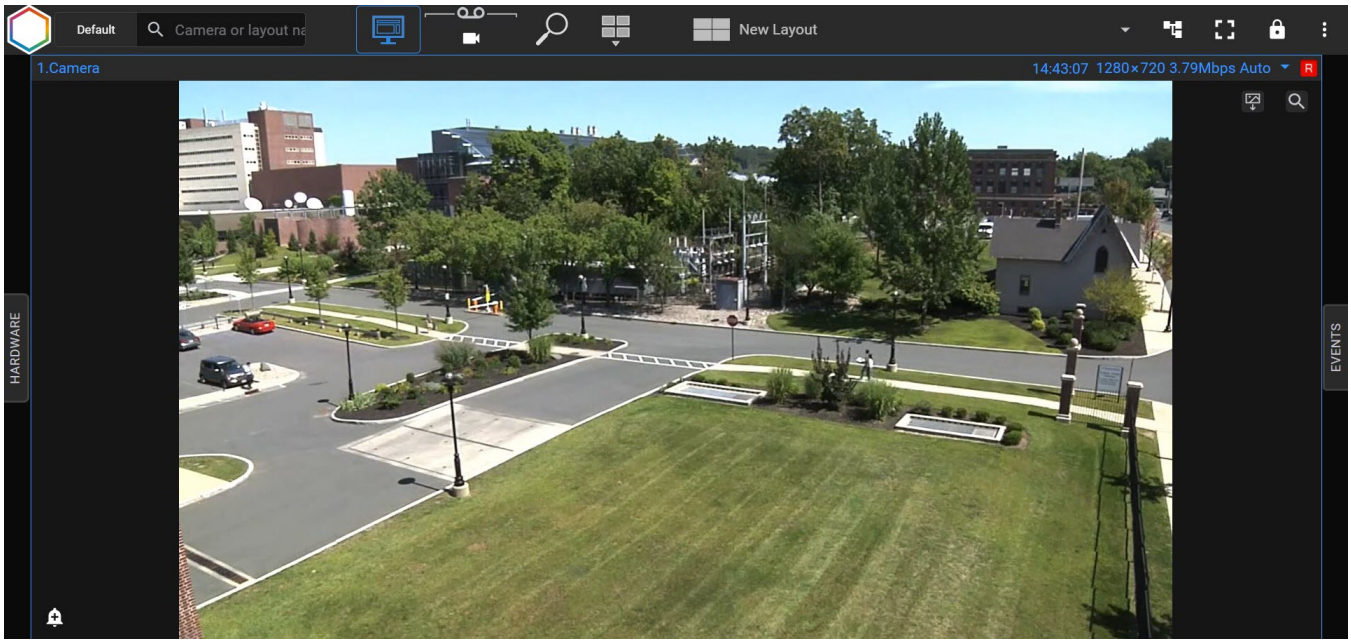
> **Note**
>
> The numbers above the quality buttons indicate the number of video streams of a certain quality.
>
> 
>
>
> In this example, there are three **Surveillance windows** on the layout: the stream quality is automatically selected in two windows (see Selecting video stream quality in a Surveillance window (GreenStream)), one window displays a high-quality video stream, and another window displays a low-quality video stream.

6. Click the **Save** button. To undo the layout creation, click the **Cancel** button.

The layout is created.



Double left-click the **Surveillance window** to open a temporary layout with this **Surveillance window**:

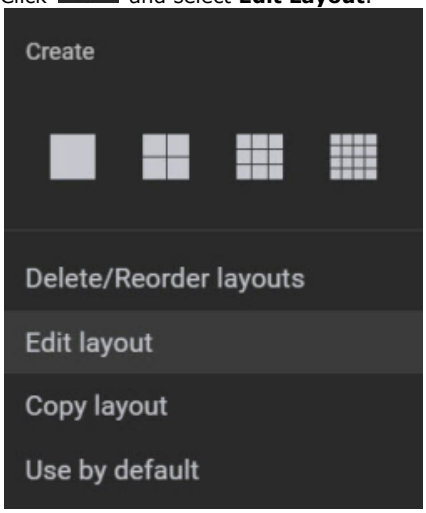


To return to the original view of the layout, double-click the **Surveillance window** again.

Editing and deleting layouts in Web-Client

To edit a layout in Web-Client, do as follows:

1. Select the layout.
2. Click  and select **Edit Layout**.



3. Make changes.
4. Click **Save**.

To rename a layout, do as follows:

1. Double left-click and enter a new name.



2. Click **Save**.

To rearrange the layouts, do as follows:

1. Click  and select **Delete/Reorder Layouts**.
2. Drag & drop layouts wherever you want.
3. Click **Save**.

To delete a layout, do as follows:

1. Click  and select **Delete/Reorder Layouts**.
2. Click to the right of the layout  .

Selecting the default layout in Web-Client

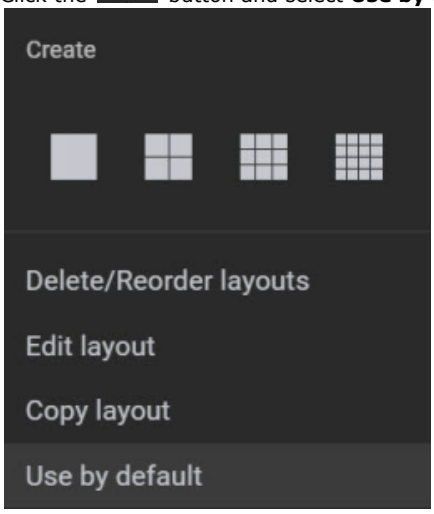
You can select the default layout for each user to be displayed after they launch Web-Client. If you don't set this layout, they'll see a blank screen.

If no layouts have been created before, the video cameras panel opens on the left and displays the video image from the first video camera in order.

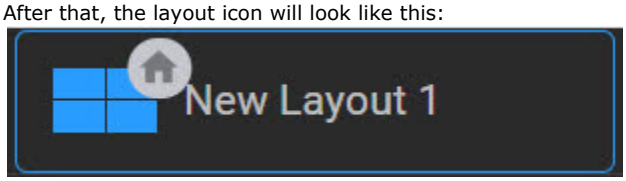
If some layouts have been created previously, the first layout in order will be displayed by default.

To set the default layout, do as follows:

1. Go to the required layout.
2. Click the  button and select **Use by default.**



After that, the layout icon will look like this:



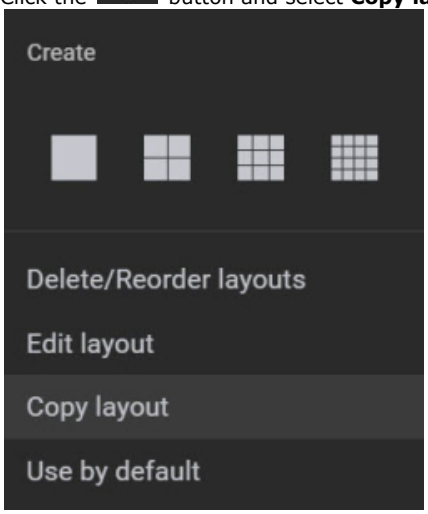
To remove the default layout, click the  button and select **Do not use by default**.

Copying layouts in the Web-Client

Layout copying

To copy a layout in the Web-Client, do the following:

1. Select the layout.
2. Click the  button and select **Copy layout**.



3. If necessary, you can make changes to the layout.
4. Click the **Save** button.

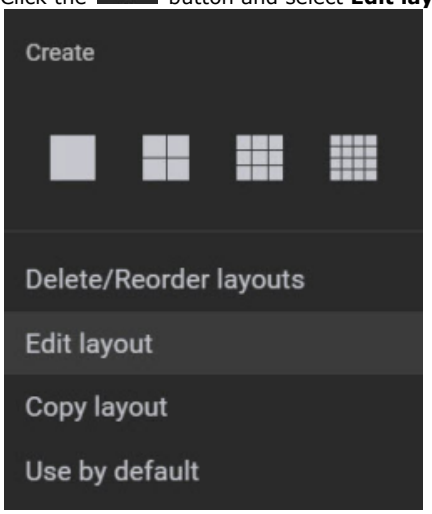
An identical layout will be created with the word "Copy" added to its name. All subsequent copies will have a copy number added to the name of the layout.

Sharing layouts in the Web-Client

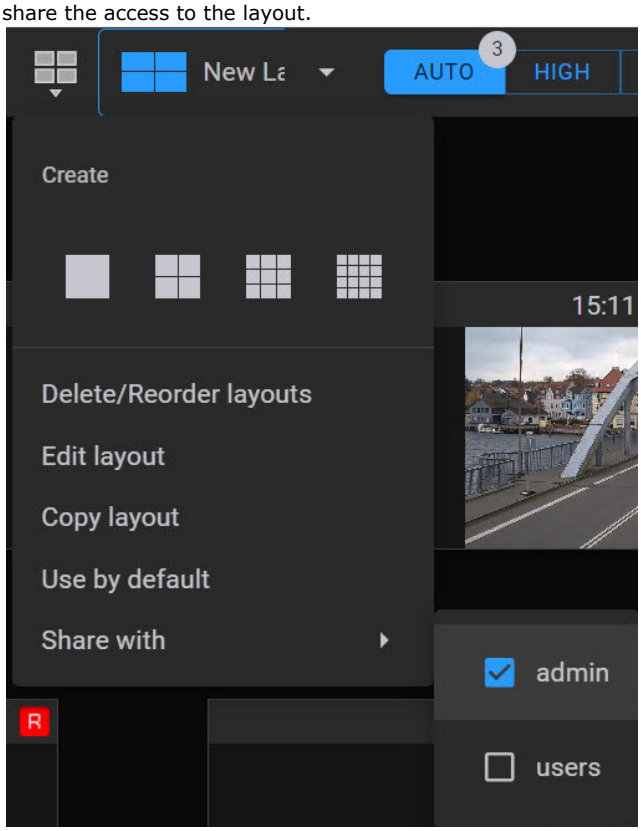
Share Layouts

To share a layout in the Web-Client, do the following:

1. Select a layout.
2. Click the button and select **Edit layout**.

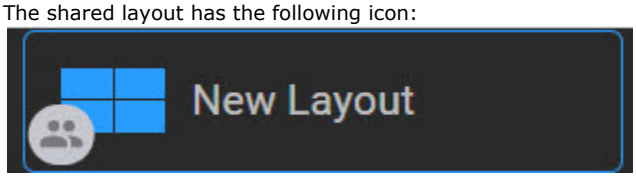


3. Click the button and in the **Share with** menu item, select one or several roles with the users of which you want to share the access to the layout.



4. Click **Save**.

The shared layout has the following icon:



Note

Only the user who created the layout can completely delete it in the Web-Client (see Editing and deleting layouts in Web-Client). If the layout was deleted by a user with whom the access to the layout was shared, the layout will be deleted only for this user.

After the layout is deleted, it will become unavailable to all users. If this layout was opened on the monitor of the user with whom the access to the layout was shared, then it will be available until the browser page is reloaded.

Creating a temporary layout in the Web-Client

Using the Web-Client, you can create and open temporary layouts with cameras via the browser address bar. To do this, you can use the following query:

```
http://<server IP>/?cams=CAM_1,...,CAM_N&[mode=live|arch|search]&[hideTopBar=true|false]&[resolution=0,1,auto]
```

Parameter name	Required	Description
server IP	Yes	Server IP address
cams		Name of the camera that is present on the layout
mode	No	Layout view mode: • **live**—real time mode (default); • **arch**—archive mode; • **search**—search mode
hideTopBar		Top panel of the Web-Client: • **true**—hidden; • **false**—displayed
resolution		Videostream: • **0**—high quality; • **1**—low quality; • **auto**—auto (GreenStream, used by default)

An example request for creating and opening a temporary layout with two cameras in real time without displaying the top panel:

```
http://127.0.0.1/?mode=live&hideTopBar=true&cams=hosts/DESKTOP-O123/DeviceIpint.1/SourceEndpoint.video:0:0,hosts
/DESKTOP-O123/DeviceIpint.2/SourceEndpoint.video:0:0
```

An example request for creating and opening a temporary layout with three cameras in real time, where:

- the first camera has a high quality video stream;
- the second camera has an auto video stream;
- the third camera has a low quality video stream.

```
http://127.0.0.1/?mode=live&hideTopBar=false&cams=hosts/DESKTOP-O123/DeviceIpint.1/SourceEndpoint.video:0:0,
hosts/DESKTOP-O123/DeviceIpint.2/SourceEndpoint.video:0:0,hosts/DESKTOP-O123/DeviceIpint.3/SourceEndpoint.video:
0:0&resolution=0,auto,1
```

You can also create and open a layout via the *AxxonNet* service. To do this, it is necessary to first connect the *Axxon One* domain to *AxxonNet* (see Configuring a domain in AxxonNet):

```
https://<webClientURL in cloud>/?authToken=<accessToken>&cams=CAM_1,...,CAM_N&[mode=live|arch|search]&
[hideTopBar=true|false]
```

Parameter name	Required	Description
webClientURL in cloud	Yes	Web-Client URL in the cloud service. To get the Web-Client URL, do the following: 1. Using the browser, open the Web-Client in *AxxonNet*. 2. Press the F12 key to open the developer console. 3. In the developer console, open the **Network** tab **groups** **Response**. 4. Find the **webClientURL** field. 5. Copy Web-Client URL

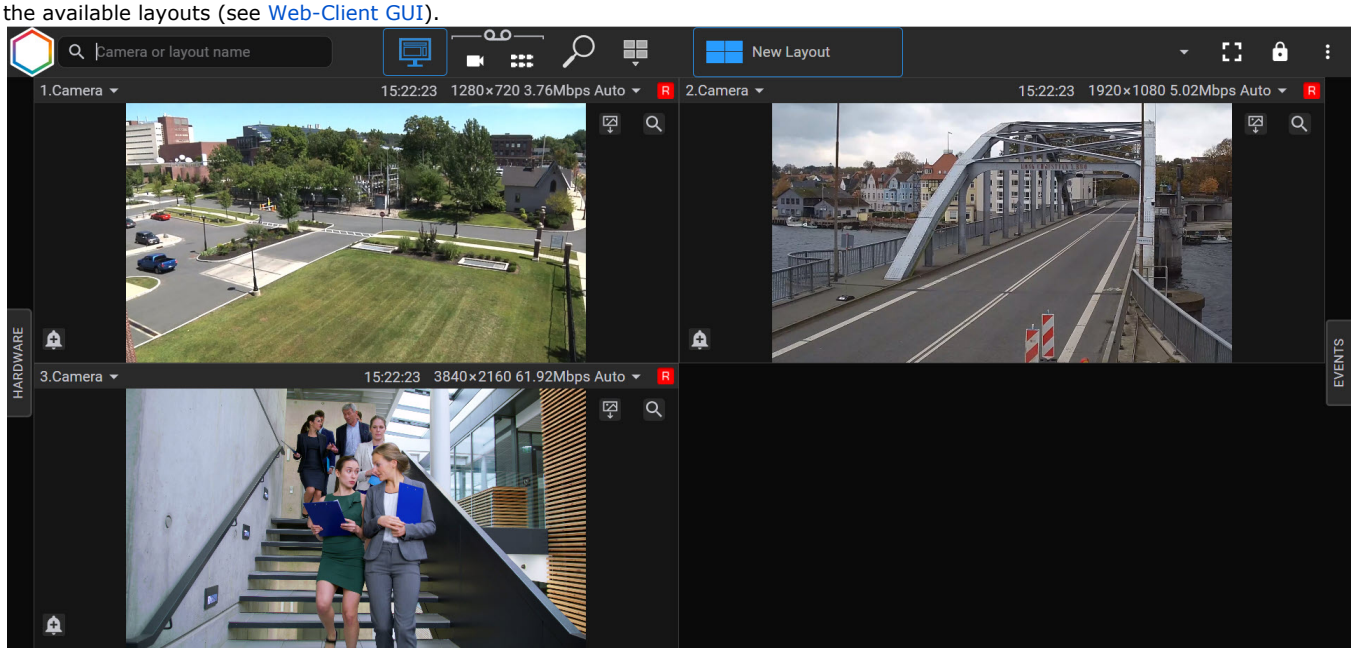
authToken		Authorization token. This parameter specifies the access token URL. To get the token, do the following: 1. Using the browser, open the Web-Client in *AxxonNet*. 2. Press the F12 key to open the developer console. 3. In the developer console, open the **Application** tab **Storage** **Local storage** https://axxonnet.com/. 4. Find the **accessToken** key. 5. Copy the key value

An example of creating and opening a layout via *AxxonNet* with two cameras in the archive mode:

```
https://axxonnet.com/minio/35436_0_co1ri88u45045635cs5g/webclient/?mode=arch&cams=hosts/DESKTOP-O123
/DeviceIpint.1/SourceEndpoint.video:0:0,hosts/DESKTOP-0OFNEM9/DeviceIpint.2/SourceEndpoint.video:0:
0&authToken=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJVc2VySUQiOjIxNTI1LCJVc2VyTmFtZSI6ImFsZXhmb25vdjUwQGdtYWlsLmNvbSIsIkNsaWVudElEIjoiY2M5YjQ4MzQwOWZkNTdhMWVlNjA4
ZjE5MWRiZDkxOWIiLCJUeXBlIjoiYWNjZXNzVG9rZW4iLCJWZXJzaW9uIjoidjIiLCJDcmVhdGVkQXQiOiIyMDI0LTAzLTI3VDEwOjQyOjM4LjIz
MjMwOTc5N1oiLCJleHAiOjE3MTE2MjI1NTgsImlhdCI6MTcxMTUzNjE1OCwiaXNzIjoiQ2xvdWQifQ.Sl5uhUWB7FDc-
EtgzPaOIU082iD2PCtROr9JhbEM7CQ
```

Real-time video surveillance in the Web-Client

To view a video image, you should select either a camera on the panel (see Searching for video cameras in the Web-Client), or one of the available layouts (see Web-Client GUI).



The Web-Client supports video playback in the following video formats: MJPEG, H.264, H.265. All other formats are trans-coded to MJPEG on the Server.

Attention!

H.265 video playback is possible in the following browsers: Safari, Microsoft Edge with HEVC video extension installed, Google Chrome version 107 and higher, if:

- hardware acceleration is enabled in the browser settings;
- the video card has hardware support for the H.265 codec.

You can playback a video in the Web-Client with two players: JPEG and MP4. If your browser supports the MP4 format, the MP4 player is used. Otherwise, your videos will be played back with the JPEG player.

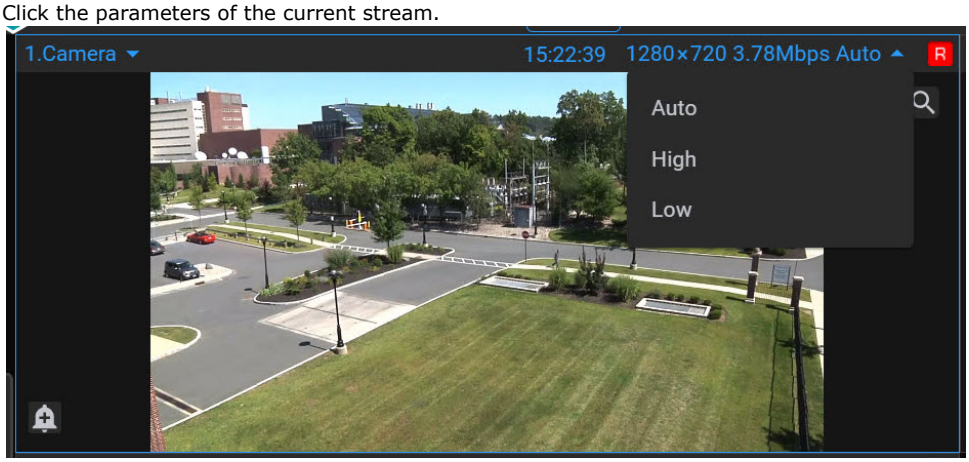
Attention!

- If your layout contains several video cameras, only the key frames may be displayed in the H.264 format video cameras, depending on the settings (see Web-Client configuration). If you select a specific camera, all frames will be displayed. In the MJPEG video format each frame is displayed.
- Video records containing b-frames will play choppy.

The Web-Client supports displaying panoramic views for fisheye video cameras. To enable such a display, select **Yes** for **Activate** parameter in **Panomorph** parameters group in the video camera settings in a common Client (see Configuring fisheye cameras).

To select a displayed stream in the Web-Client manually (see The Camera object), do the following:

1. Click the parameters of the current stream.



2. Select a stream to be displayed:

Menu item	Description
Auto (GreenStream, default)	If a stream was selected based on the maximum bitrate, then another stream will be selected only if its bitrate is more than 5% higher than the current one (in order to eliminate frequent switching if the indicators are approximately equal) (see The Camera object). When you enlarge the surveillance window, the video stream switches to a high quality video stream
High quality	A high quality video stream is used in the video surveillance window (see The Camera object)
Low quality	A low quality video stream is used in the video surveillance window (see The Camera object)

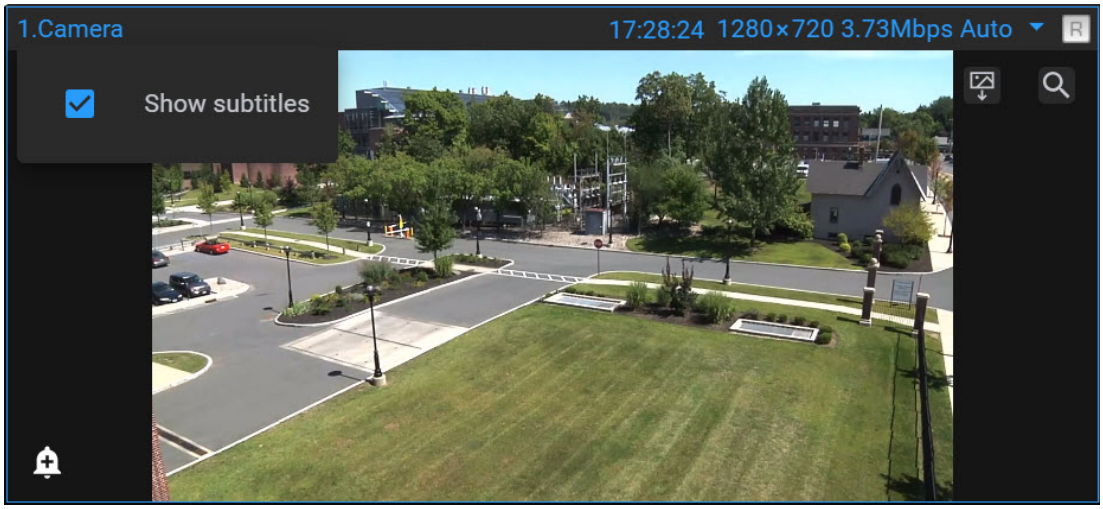
Note

A selected video stream is saved when switching between the layouts, but after the page reloads, the video stream that was specified when creating the layout will be automatically selected.

Click the  button to open the window in full screen. To exit the full screen mode, click the  button again, or press the **Esc** key.

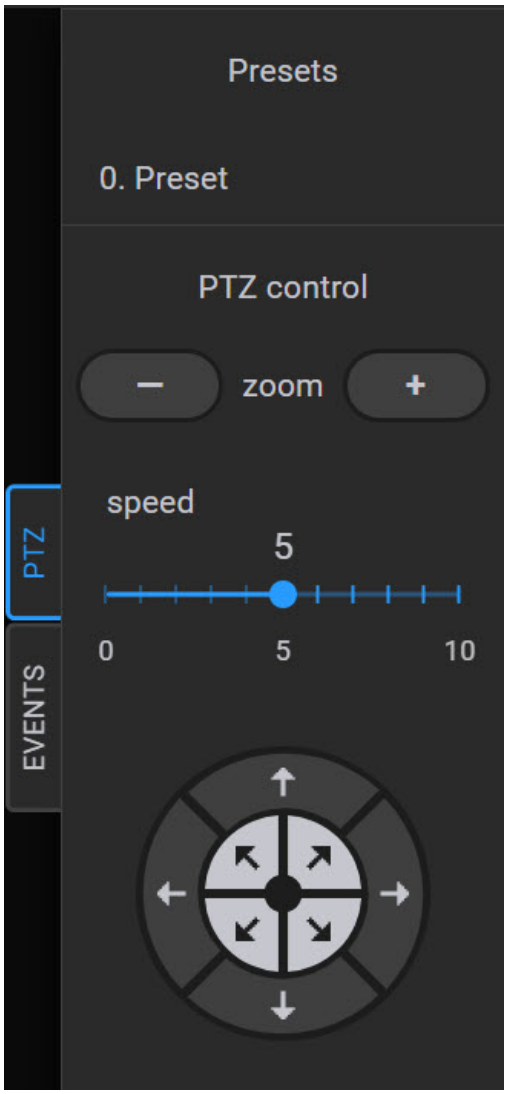
To open a temporary layout from a certain camera on the layout, double right-click the camera video image. To return to the layout, double-click the video image again.

You can enable the display of captions in the video camera viewing window. To do this, click on the name of the camera and set the **Show subtitles** checkbox.



Controlling PTZ cameras through the Web-Client

A PTZ video camera is controlled through the PTZ device control panel. To open the panel, click on the video surveillance window that contains a live video camera which supports a PTZ control interface. As a result, the **PTZ** tab will open on the right side panel. Clicking on the **PTZ** tab to control the PTZ camera.

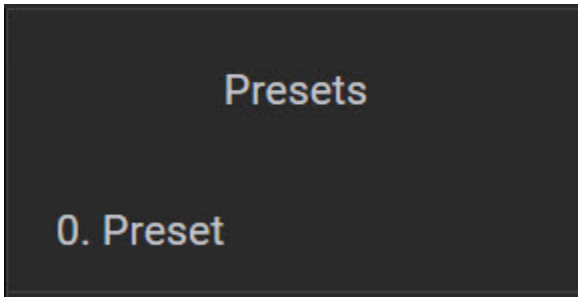


The following actions can be performed using the PTZ device control panel:

1. Use presets.
2. Adjust optical zoom and positioning speed of the video camera.
3. Modify the horizontal and vertical tilt angle of the video camera.

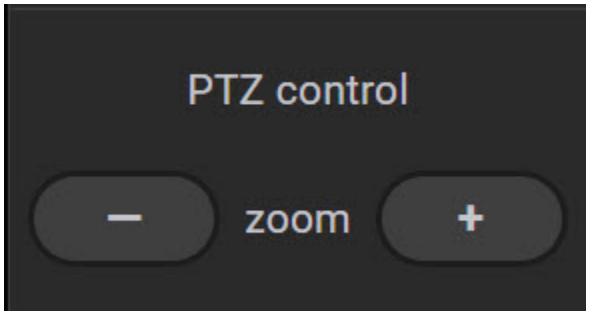
Controlling a PTZ camera through the Web-Client by using presets

To go to a preset, select the relevant item in the list of presets.



Changing the optical zoom of a PTZ camera in the Web-Client

You can change the optical zoom of the PTZ camera using the buttons of the **zoom** group.

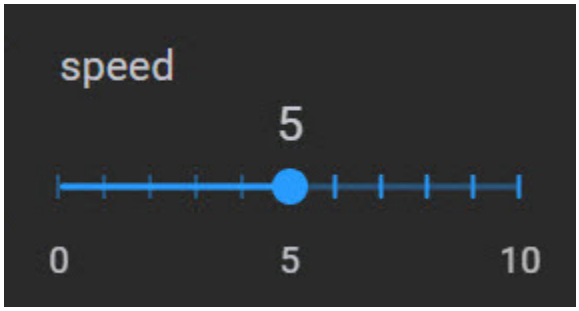



—zoom in.


—zoom out.

Changing the positioning speed of a PTZ camera in the Web-Client

You can change the positioning speed of a PTZ camera using the slider in the **speed** group.



Move the slider:

- to the right—to increase the positioning speed;
- to the left—to reduce the positioning speed;

The value of the current positioning speed is displayed above the slider.

Changing the tilt of a PTZ camera in the Web-Client

You can change the tilt of a PTZ camera using the arrows in the **PTZ control** group.



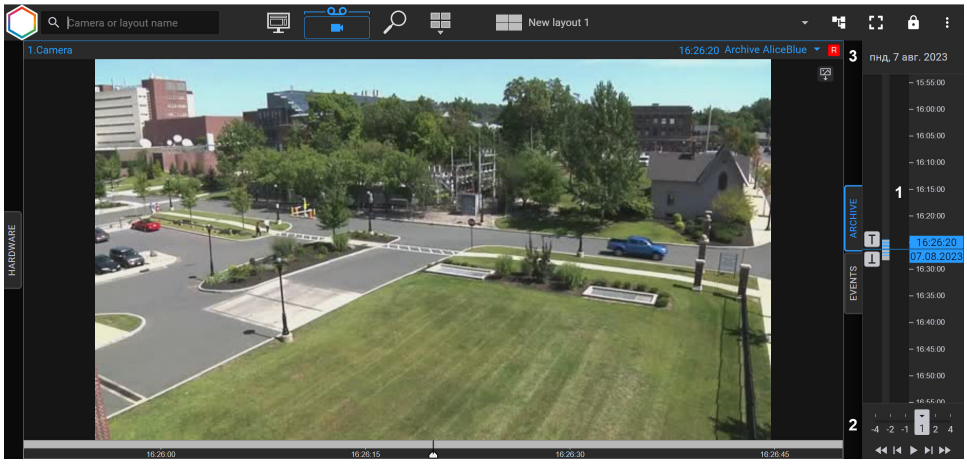
The arrow direction indicates the direction in which the camera lens will be moved when the arrow is clicked.

Viewing video archives through the Web-Client

Single-camera archive view mode

To view a single camera archive, do the following:

1. Select the required camera on the cameras panel or on the layout.
2. Click the  button.



> **Note**
>
> By default, the archive that is set as a default archive will open (see Setting the default archive).

3. The archive panel will be displayed with the following interface elements:
   a. Timeline (**1**). Archive navigation using the timeline in the Web-Client is similar to the video surveillance in the *Axxon One* Client (see Navigating Using the Timeline).

> **Note**
>
> Similar to the Client (see The Timeline), alarm flags and comment icons are displayed on the timeline.

b. Playback control panel (**2**). The following operations are available for navigating in the archive using the playback panel in the Web-Client:

 —recording playback;

 —stop recording playback;

 —jump to the previous frame;

 —jump to the next frame;

 —jump to the previous recording;

 —jump to the next recording;

The playback can be fast. You can also change the playback direction (forward/reverse) by dragging the slider on the panel or by clicking the digits. The digits indicate a fold increase of the playback speed. Minus indicates the reverse playback.

Example of a forward playback with two-fold increase in playback speed:



Example of a reverse playback with two-fold increase in playback speed:



Attention!

- Reverse fast-forward playback of H.264 video is based on key frames, so it will not be smooth.
- Audio is unavailable during fast forward and reverse playback of the archive video.

c. Archive position selection panel (**3**). The archive position selection panel is opened by left-clicking the date above the timeline (see Archive position selection panel for the Web-Client).

Note

You can also navigate in the archive using the time indicator similar to the Client (see Navigation via the time indicator).

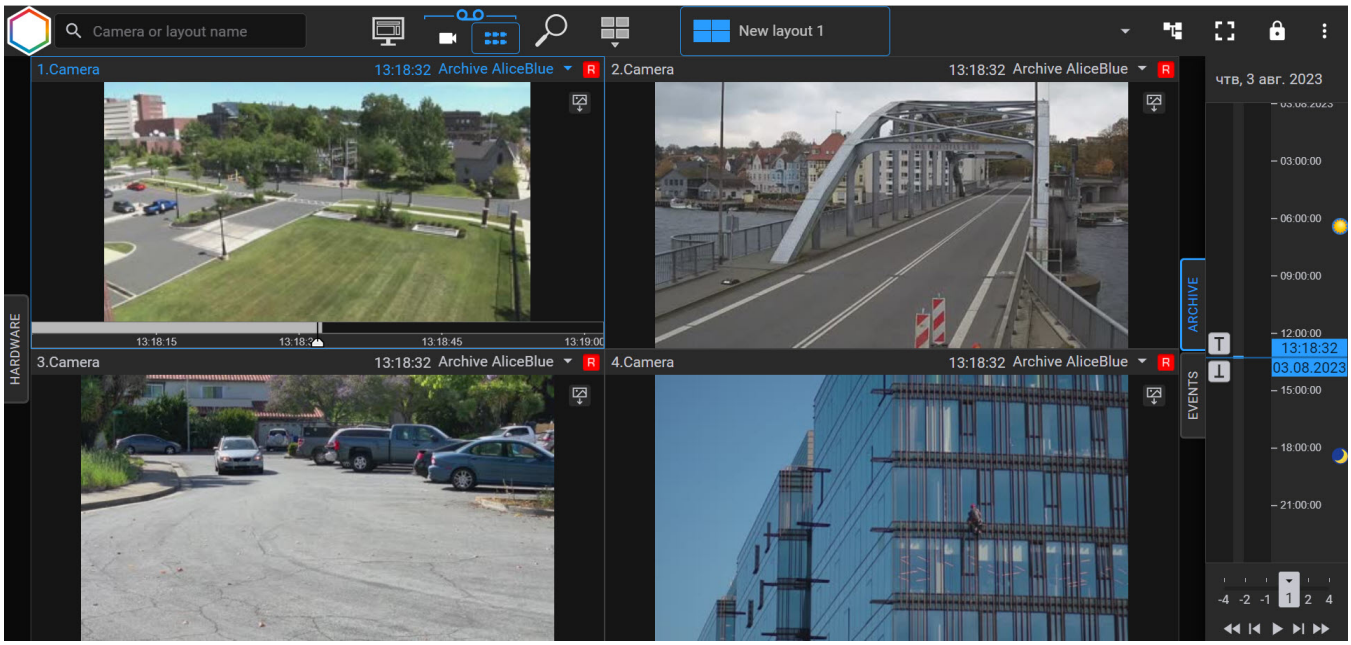
4. To select an archive, do the following:
   a. click the name of the current archive;



   b. select the required archive.

Multi-camera archive view mode

You can switch all cameras on the layout to the archive mode. To do this, click the  button.

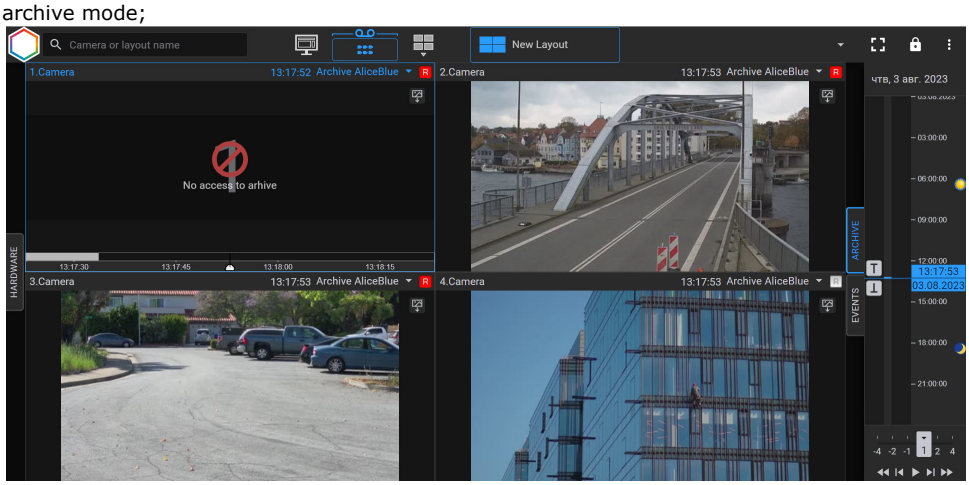


You can control the archive viewing using the playback control panel, the same as when viewing the archive of a single video camera.

When all cameras on the layout are in the archive mode, there is no audio playback. To play back the audio, you need to go to the archive of a single camera.

Access to viewing the archive of a camera depends on the settings of user access permissions to the camera (see Creating and configuring roles). If the user permissions are limited, then:

- if there are several cameras with limited access to the archive on the layout, you can view the archive only in the multi-camera archive mode;
- if you click a camera with limited access to the archive in the multi-camera archive mode, you won't go to the single-camera archive mode;

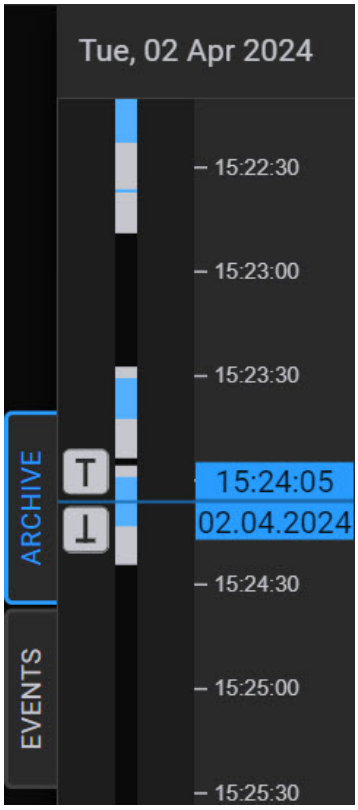


- if there is only one camera with limited access to the archive on the layout, the buttons for changing the mode (archive, search) won't be displayed;
- if the user is already in the archive mode or in the search in a single camera mode, and selects a camera with limited access to the archive, the user will automatically go to the live view mode for this camera, and the archive/search buttons won't be displayed.

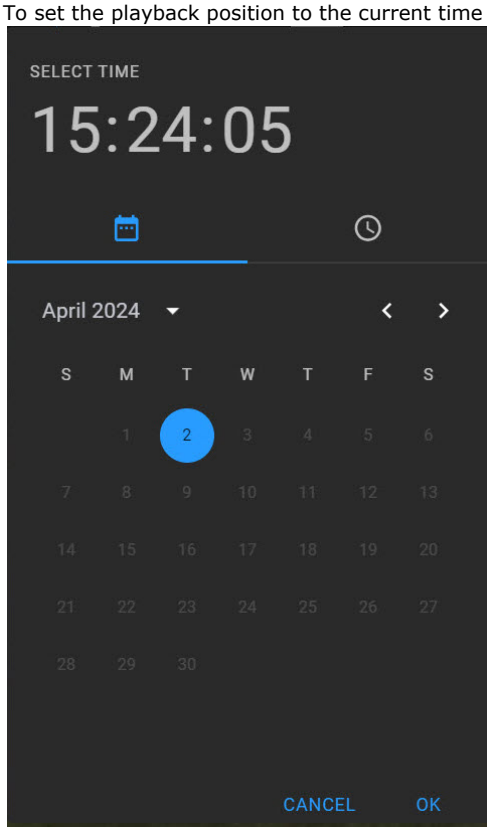
Archive position selection panel for the Web-Client

To choose a time position in the archive by using the archive position selection panel:

1. Click the date above the timeline to open the position selection panel.



2. To set the playback position to the current time and date, go to step 6.

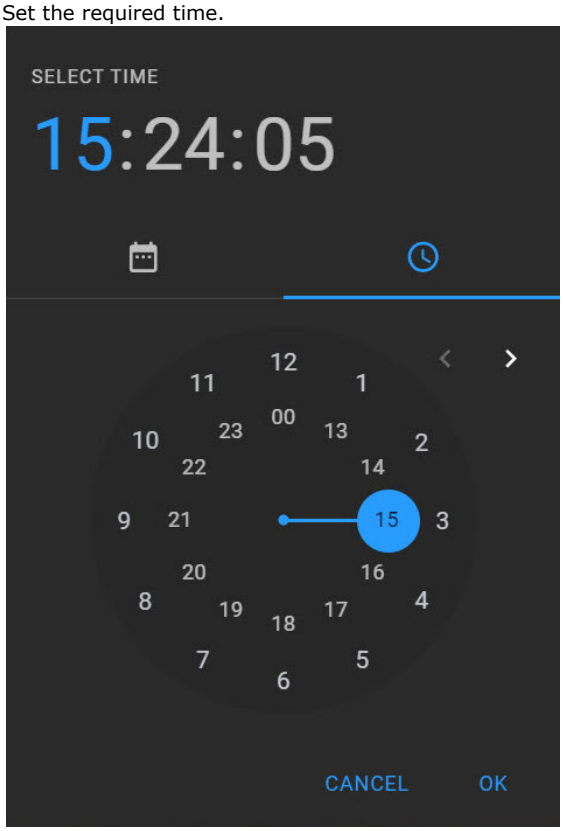


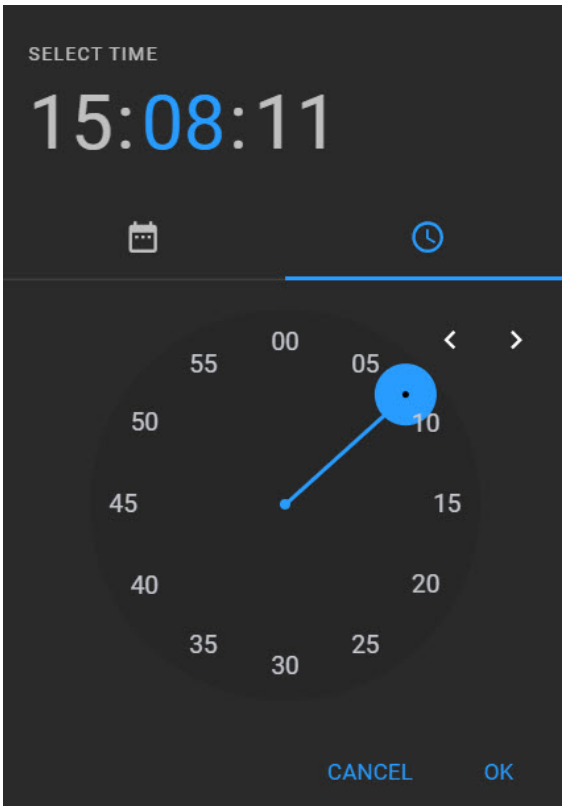
3. Use the  and  buttons to select a month.

4. Click the necessary date on the calendar to select a day.

> **Note**
>
> The days, for which there is video footage are in light shade.

5. Set the required time.





6. To set the playback position, click the **OK** button.

The time position in the archive is now chosen.

Archive search in the Web-Client

There are two ways to search the archive in the Web-Client:

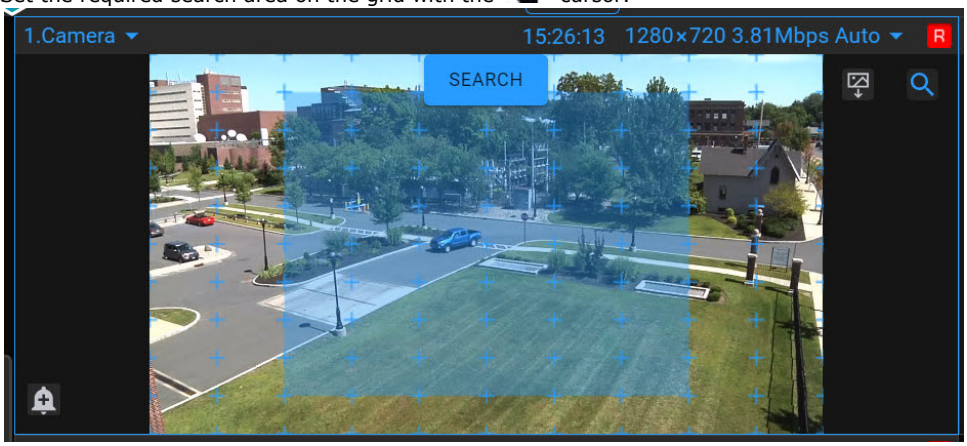
- **Standard search**. To go to the search in the archive, do the following:
  1. Select the required camera on the cameras panel or on the layout.
  2. Click the  button.

The interface of the archive search in the Web-Client will open. It is similar to the interface of the Client (see Archive Search mode interface).

- **Quick search**. To go to the quick search in the archive, do the following
  1. Select the required camera on the cameras panel or on the layout.
  2. Click the  button on the camera fold.

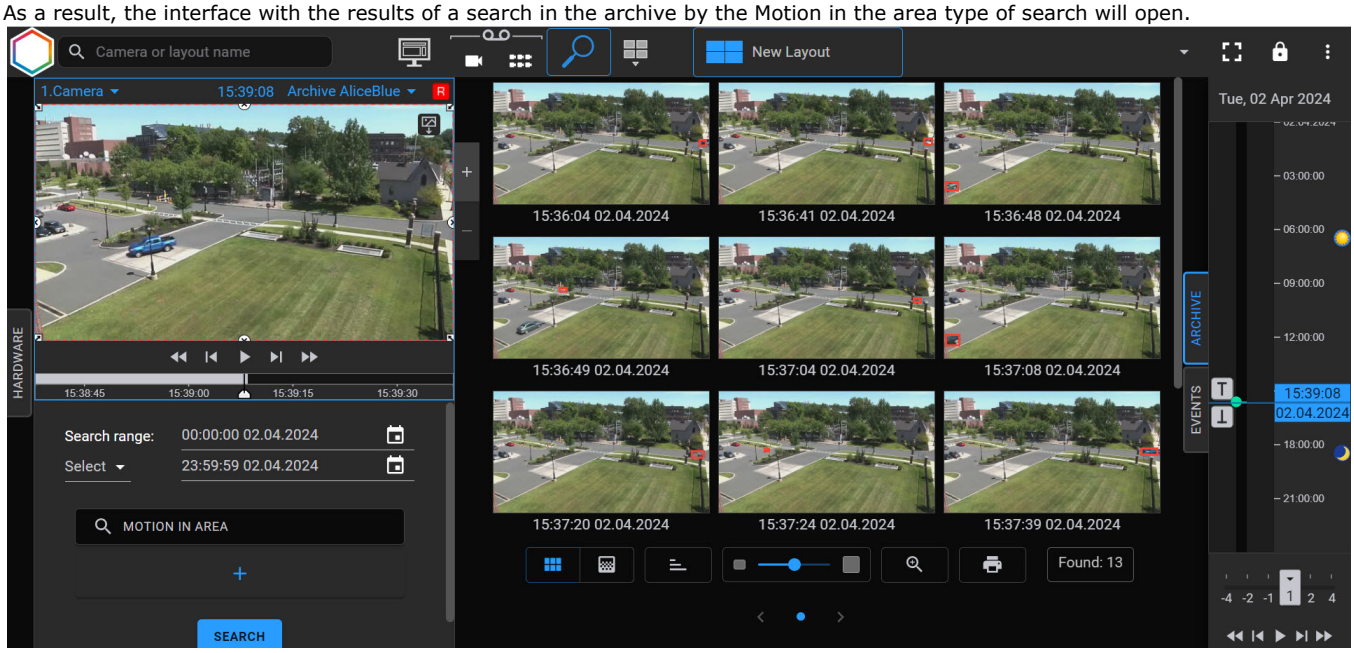
> **Note**
>
> The quick search button is displayed on the fold of the cameras, on the basis of which the detection tools with the ability to track objects are created (see Tracking objects).

  3. Set the required search area on the grid with the  cursor.



  4. Click the **SEARCH** button.

As a result, the interface with the results of a search in the archive by the Motion in the area type of search will open.



The search in the archive is similar to the search in the Client (see Search in an archive of a single video camera). The search results are the video archive frames that match the specified search criteria.

Attention!

- The previews of the search results are downloaded gradually and displayed when you scroll the screen.
- In addition to the type of the search, the number of the search results depends on how long the timeline covers (the timeline of the Web-Client is similar to the timeline of the Client, see The Timeline). The more time the timeline covers, the more extensive the search will be.
- Depending on the search type and the time period, it may take some time for the search results to load. Search results loading process is indicated by the  icon in the middle of the screen.

You can resize the found frames using the  slider or the following buttons:  (zoom out),  (zoom in).

You can change the size of the Surveillance window using the  buttons.

Attention!

If you select a device on the cameras panel (see Searching for video cameras in the Web-Client), the following conditions exist:

- If you switch to the camera that was searched previously, the search conditions will be from the previous search.
- If you switch to the camera that was not searched previously, the search conditions will be from the camera from which the transition was made.

If you searched several times on the same camera and didn't leave the search tab, you can navigate between the search results:



If you change the camera inside the search, the previous results will be deleted.

Search results can be displayed as:

- tiles ( , default mode)—found frames are displayed;
- heat map ()—found frame of the video image on which the heat map is built is displayed.

You can build a report based on search results using the  button (see Reporting the search results).

Types of archive search in the Web-Client

The following types of search are available in the Web-Client:

1. Motion in area.
2. Line crossing.
3. Motion from one area to another.
4. Multiple objects.
5. Loitering.
6. Face search.

> **Attention!**
>
> You can upload only jpeg images.

7. LPN search.
8. TimeSlice.

> **Note**
>
> The default interval is set in the Web-Client settings (see Web-Client configuration).

9. Events search.

The available search types depend on the detection tools that were created on the basis of the video camera. If no detection tools are created on the basis of the video camera, only the Event search and TimeSlice search types will be available in the archive of the selected video camera in the Web-Client.

The interface of the archive search and the parameters of the search in the Web-Client are similar to the Client (see Video surveillance in archive search mode).

You can also build a Heat Map in the Web-Client (see Building a Heat Map).

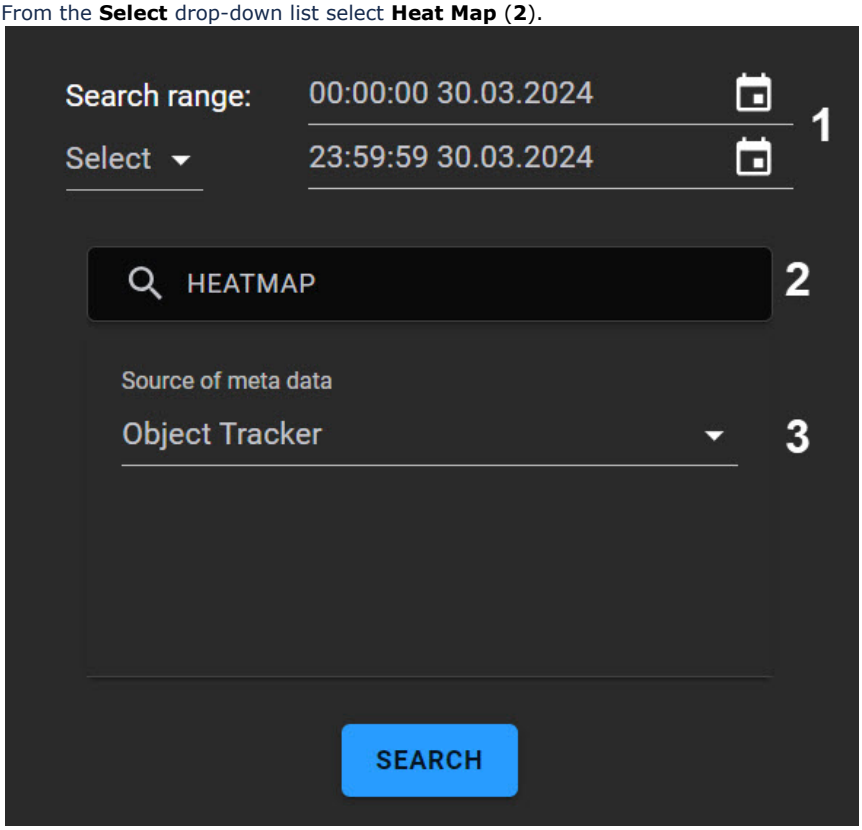
Building a Heat Map

> **Attention!**
>
> To build a Heat Map, you need at least one source of metadata (for example, an Object Tracker).

Heat Maps are useful for evaluation of motion intensity within the scene and determining common trajectories of moving objects.

How to build a Heat Map:

1. Proceed to the Archive search (see Archive search in the Web-Client).
2. Specify time period to build the Heat Map for (**1**).
3. From the **Select** drop-down list select **Heat Map** (**2**).



4. Select the source of metadata (**3**).
5. Click the **SEARCH** button.

The Heat Map appears in the search results window.



Use the dedicated slider to adjust the transparency of the heat map.

Click  to download the heat map.

You can build a report based on the received data (see Reporting the search results).

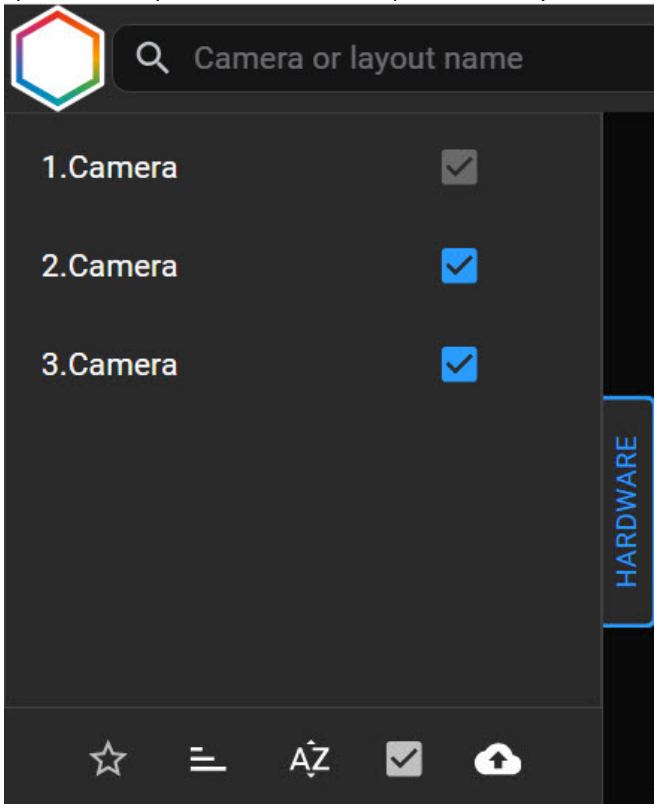
Simultaneous search in multiple camera Video Footage via the Web-Client

You can use the Web-Client for multiple camera Video Footage searching by:

- facial recognition events;
- ANPR events;
- detection tool triggering events;
- TimeSlice.

To simultaneously search multiple camera's Video Footage, do the following:

1. Proceed to the Video Footage search (see Archive search in the Web-Client).
2. Set the search criteria.
3. Open Cameras panel and select the required devices (see Searching for video cameras in the Web-Client).



> **Note**
>
> To select all cameras, select the appropriate box on the bottom of the page.

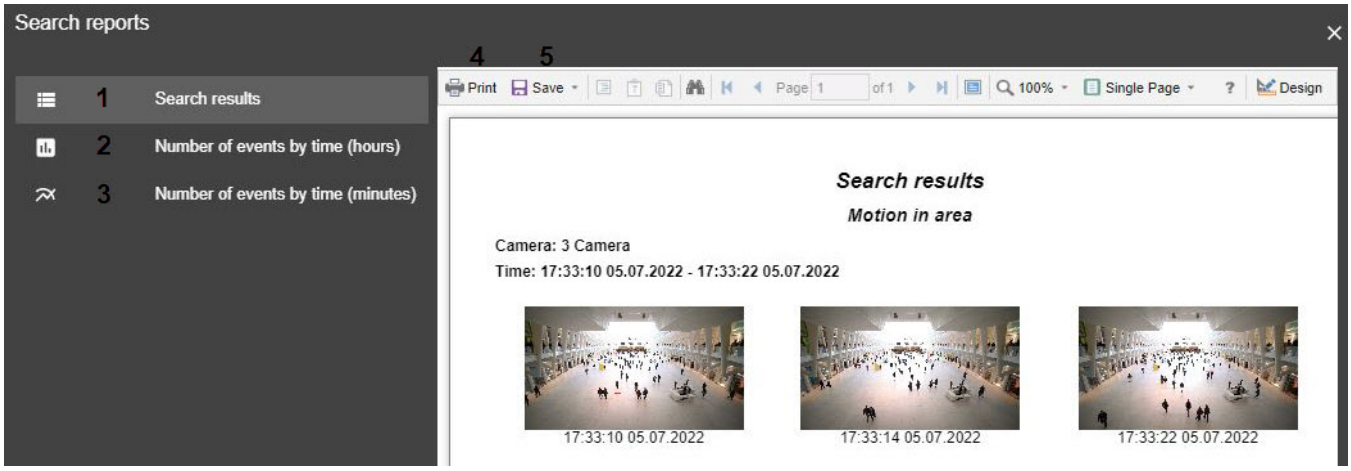
4. Click the **Search** button.

Reporting the search results

The Web-Client also includes the Stimulsoft report editor for building reports on retrieved video fragments.

To build a report after you finished searching, click  in the bottom part of the screen.

> **Attention!**
>
> The report is limited to first 60 retrieved videos.



There are 3 types of reports available:

1. Retrieved fragments (**1**).
2. Retrieved fragments (number/per hours) (**2**).
3. Retrieved fragments (number/per minutes) (**3**).

Click Print (**4**) to hardcopy a report, or **Save** (**5**) to export into an appropriate format.

Viewing video camera detection tool triggerings in the Web-Client

You can view the detection tool triggerings of the selected video camera on any layout. To do this:

1. Select a video camera on the layout.
2. On the right edge of the screen, click the **Events** button.
   The event panel will open, which will display only the triggerings of detection tools that were created for the selected video camera.



> **Note**
>
> If no video camera is selected on the layout, then when you click the **Events** button, the panel will display detection tool triggerings for all video cameras.

If you click on the detection tool triggering, you will be switched to the archive mode at the time the detection tool was triggered.

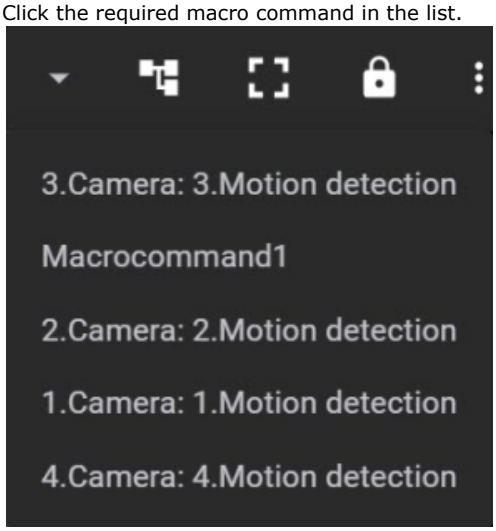
To close the panel, click the **Events** button again.

Running macros in Web-Client

In Web-Client, you can run macro commands that were previously created in the regular *Axxon One* Client (see Create Macros).

To run a macro in Web-Client, do the following:

1. Click on the  button on the top panel.
2. Click the required macro command in the list.



As a result, the selected macro will be launched in Web-Client.

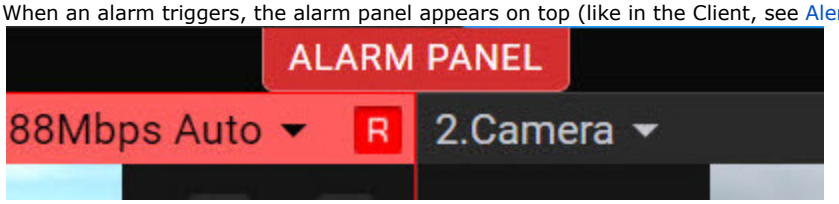
Viewing and processing alarms in Web-Client

You can use the Web-Client to view active alarms across the entire Axxon-domain.

To make the Web-Client display active alarms, select any camera or a layout (see Searching for video cameras in the Web-Client, Web-Client GUI).

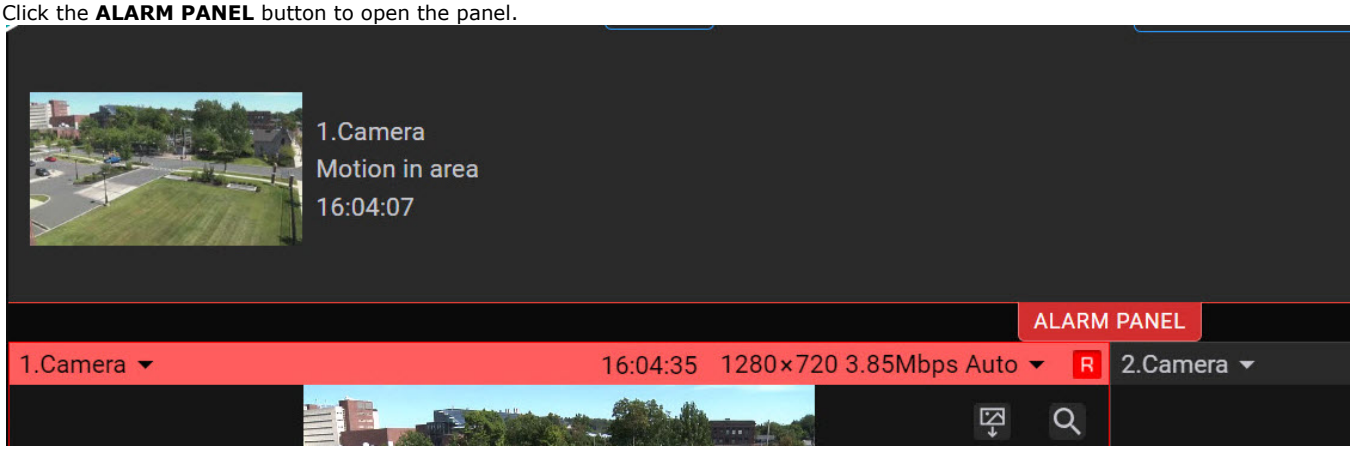
> **Note**
>
> The alarms that were triggered before selecting a camera or a layout are only displayed if the user is in the workspace. After you reload the page, go to the open statistics or bookmarks sections, the panel with the current alarms will disappear.

When an alarm triggers, the alarm panel appears on top (like in the Client, see Alert panel).



> **Note**
>
> The browser tab will indicate the number of current alarms in the Web-Client.
>
> 
>

Click the **ALARM PANEL** button to open the panel.

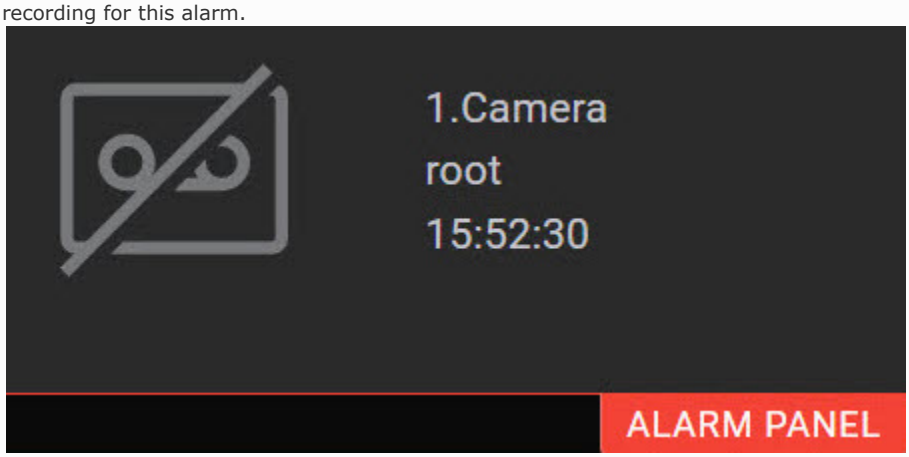


The panel will display the alarm thumbnails with the name of the camera in which the alarm occurred, the initiator of the alarm and the time of the alarm.

If you click the alarm thumbnail on the panel, you will go to the archive mode to view the event.

Note

If the first frame of an alarm is not received within 15 seconds, then an icon will be displayed indicating that there is no video recording for this alarm.



You can change the size of the alarm panel in the Web-Client. To do this, hover the mouse cursor over the panel and expand it with the cursor.



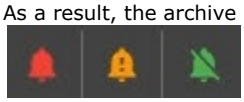
Alarm processing in the Web-Client

In the Web-Client, it is possible to manage and take into processing the active alarms of the entire Axxon-domain.

To go into the alarm event management mode and take the alarm into processing, do the following:

1. Initiate an alarm by clicking the  button (like in the Client, see Switch to Alarm Management mode).
2. Click the  button to go into the alarm event management mode.

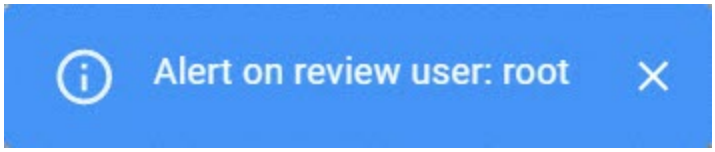
As a result, the archive mode will open, and the panel for managing an alarm event will appear (see Assessing an alarm event).



Note

Only one operator can take an alarm into processing (like in the Client, see Limitations when working with alarm events in case of multi-user processing).

If another operator took an alarm into processing, the current operator won't be able to take the alarm into processing and will see the notification:



Listening to a camera's microphone via the Web-Client

> **Attention!**
>
> You can play back audio in mp4 format only.

To listen to a camera's microphone, click the  button in the camera window.

> **Note**
>
> Audio playback in Web browsers is supported in Windows 8 and higher OS versions.

After you complete this action, a volume slider appears.



> **Note**
>
> You cannot play back audio from multiple cameras simultaneously.

The higher is the slider position, the higher is the volume.

To mute audio, click the  button.

Digital video zoom in the Web-Client

Digital zoom of video occurs in a viewing tile during viewing of live video as well as when viewing archive video. To increase the zoom level, use the mouse scroll wheel.

The image cannot be made smaller than the source size. The maximum video zoom is 8x.

To select the viewed portion of the frame at a changed scale, drag the mouse outside of the video viewing area.

> **Note**
>
> For PTZ units, you can zoom in by using the buttons in the **ZOOM** group.

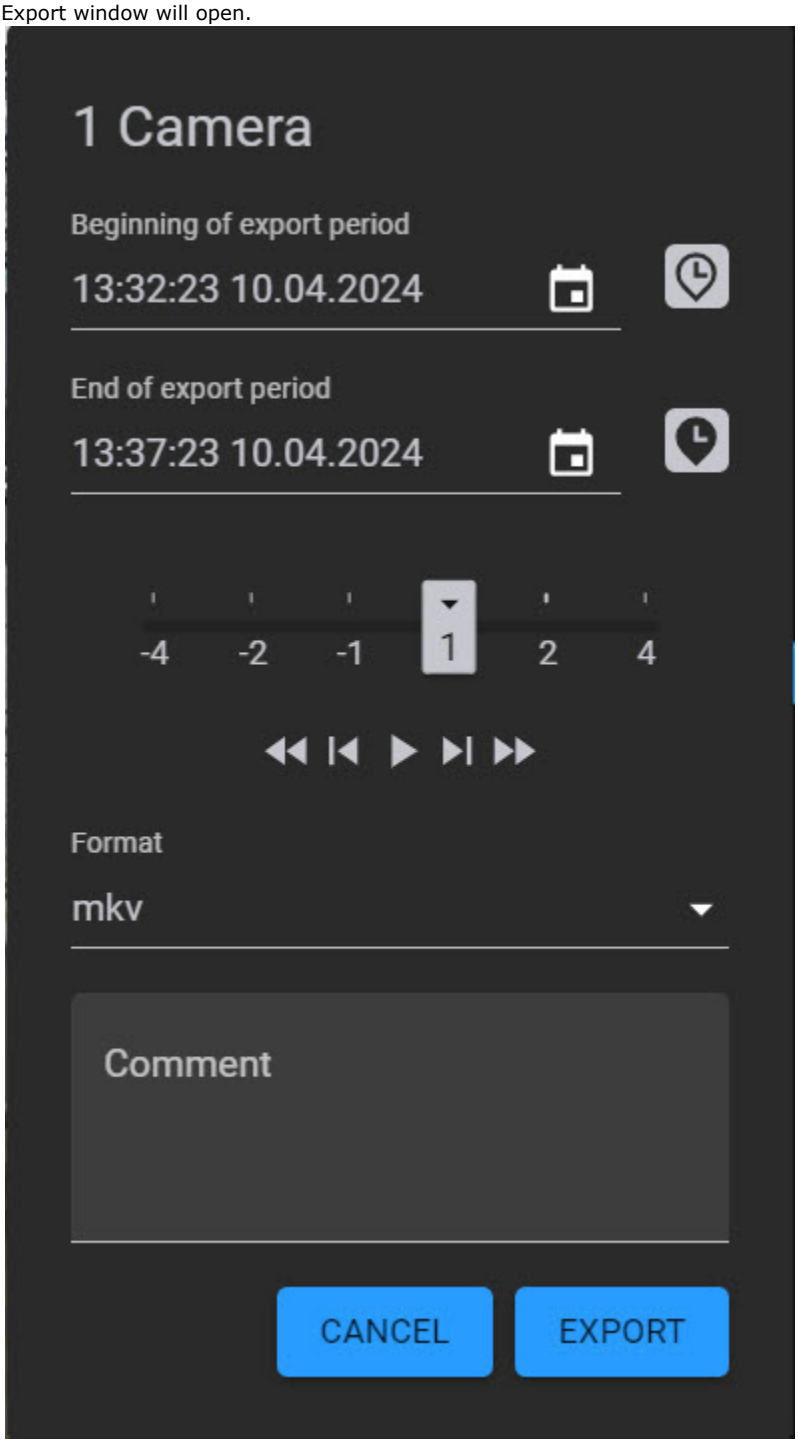
Export in the Web-Client

> **Note**
>
> Users without export permissions won't have the access to the  icon, as well as to the possibility of selecting the export period on the timeline (see Creating and configuring roles).

To export a video, do the following:

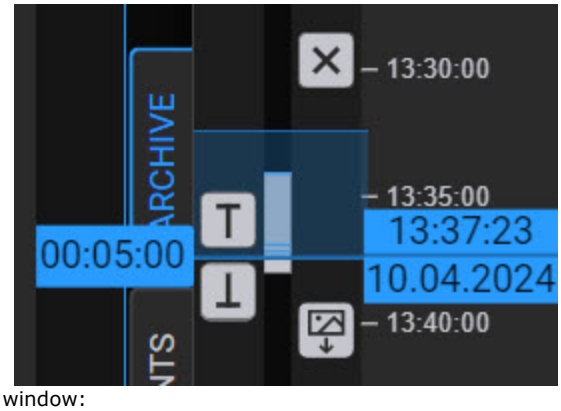
1. In the live mode (see Real-time video surveillance in the Web-Client) or in the archive mode (see Viewing video archives through the Web-Client), click the  icon in the **Surveillance window** of a camera.

2. Export window will open.



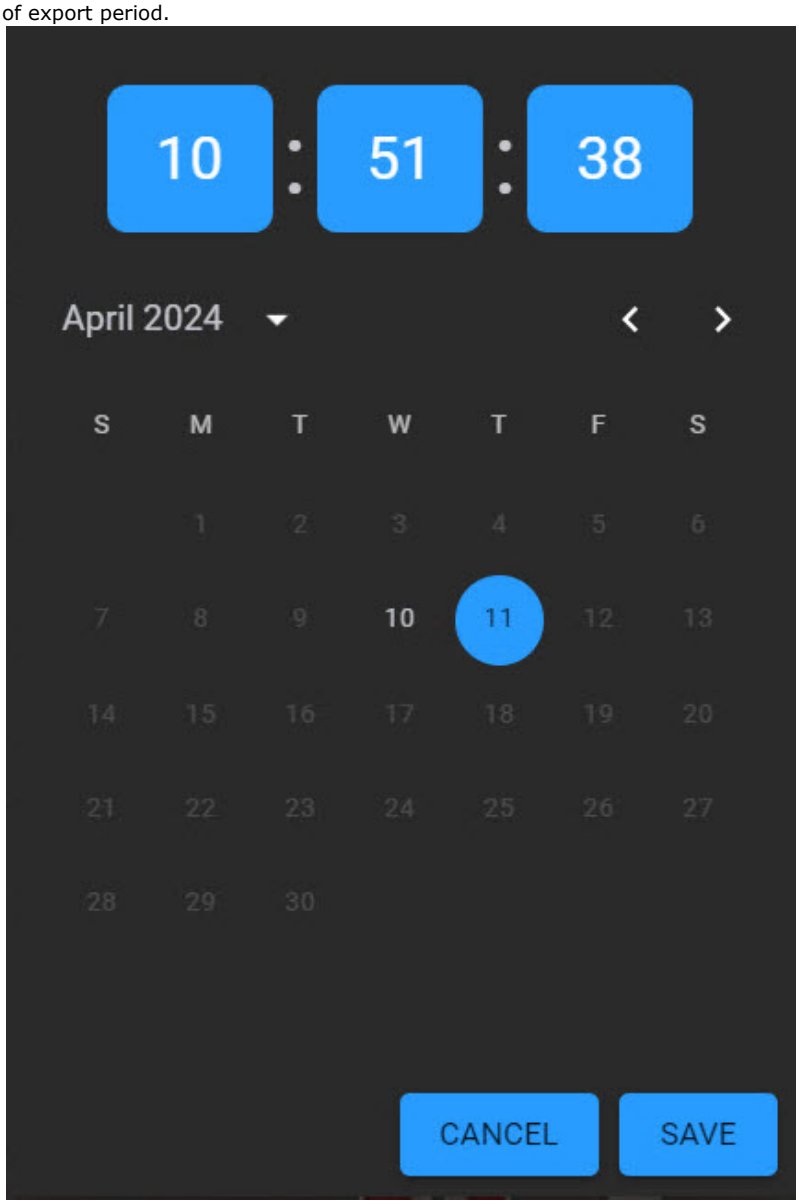
3. By default, the export period is the last five minutes of the archive. To specify the export period, you can use:
    a. The timeline:
        i. Set the pointer to the position corresponding to the beginning of the export period and click the T button.
        ii. Set the pointer to the position corresponding to the end of the export period and click the ⊥ button.

> **Note**
>
> To delete a period, click the ✕ button.



b. Export window:
   i. Specify the beginning and end of export period by entering the time and date in the **Beginning of export period** and **End of export period** fields. If you want the video to start from the moment where the pointer is set on the timeline, click the  button next to the **Beginning of export period** field. As a result, the moment of video start will move to the pointer position. Click the  button next to the **End of export period** field to set the end of video at the pointer position.

ii. Or click the button and in the window that will open, specify the time and date of the beginning and end of export period.



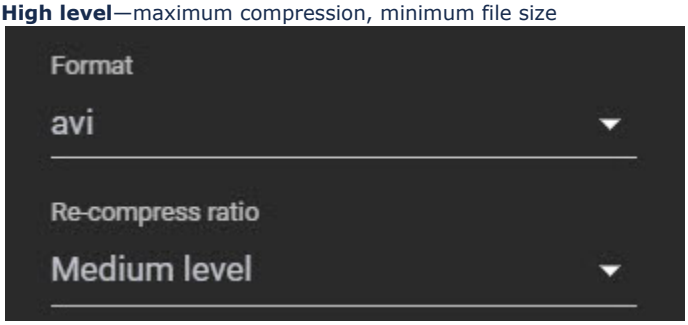
> **Note**
>
> You can select only the days on which the archive was recorded. The days on which the archive wasn't recorded aren't available for selection.

4. Select the speed and direction of video playback for export.
5. From the **Format** drop-down list, select a video export format. If necessary, enter a comment for the export. The comment will be displayed as captions when you playback the exported video.

> **Note**
>
> - In Windows OS and Linux OS, you can export to **AVI**, **MKV**, **MP4**, **JPG**, and **EXE** formats.
> - In macOS, you can export to **AVI**, **MKV**, **MP4**, and **JPG** formats. **EXE** files are not supported in this OS.

6. If you export to **AVI** or **MP4** format, select the **Re-compression ratio** of a video:
   - **Low level**—minimum compression, maximum file size;
   - **Medium level** (default)—medium compression, medium file size;

- **High level**—maximum compression, minimum file size



7. To export a frame, select **JPG** format. On the timeline or in the export window, select the time to export the frame similar to specifying an export period for a video.
8. Click the **EXPORT** button. Click the **CANCEL** button to cancel export.

The export progress is displayed on the drop-down panel as in the Client (see Viewing export progress).



When the export is complete, the panel color changes to green. To download an exported file, click its name on the panel.



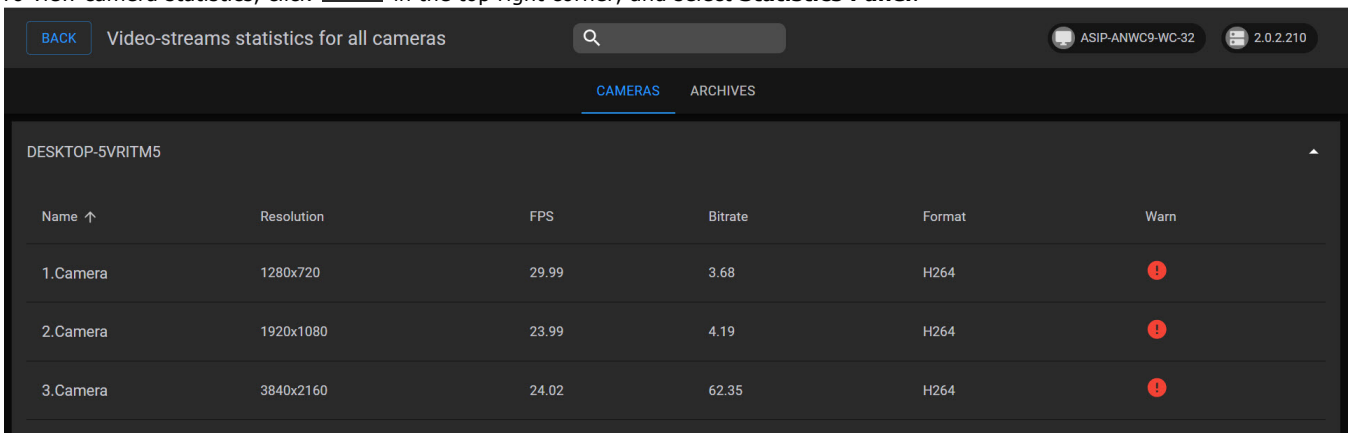
Note

The text of the timestamp in the exported video will depend on the language selected in the browser.



Viewing Camera and Archive Statistics

To view camera statistics, click  in the top right corner, and select **Statistics Panel**.



On the **CAMERAS** tab, the following parameters are displayed for each video stream of each camera:

- resolution;
- frame rate;
- bit rate;
- compression format.

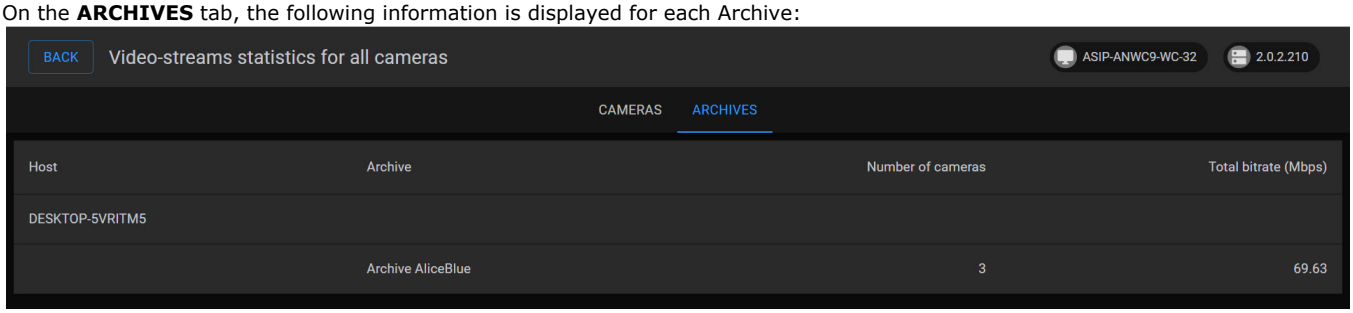
If the bit rate exceeds the expected value, and there is more than 1 Mbit per megapixel, the stream is marked with  .

If the bit rate exceeds the expected value, and there is more than 2 Mbit per megapixel, the stream is marked with  .

By default, the cameras on the **CAMERAS** tab are sorted by name, but you can also sort them by resolution, frame rate, bit rate, format, or warning in ascending or descending order. To sort cameras by a certain parameter, hover over the name of the parameter and click the up arrow  . If the cameras are sorted in ascending order, an up arrow  is displayed; in descending order—a down arrow is displayed  .

> **Note**
>
> The indicator in the upper right corner displays the *Axxon One* Web-Client and Server version numbers.

On the **ARCHIVES** tab, the following information is displayed for each Archive:



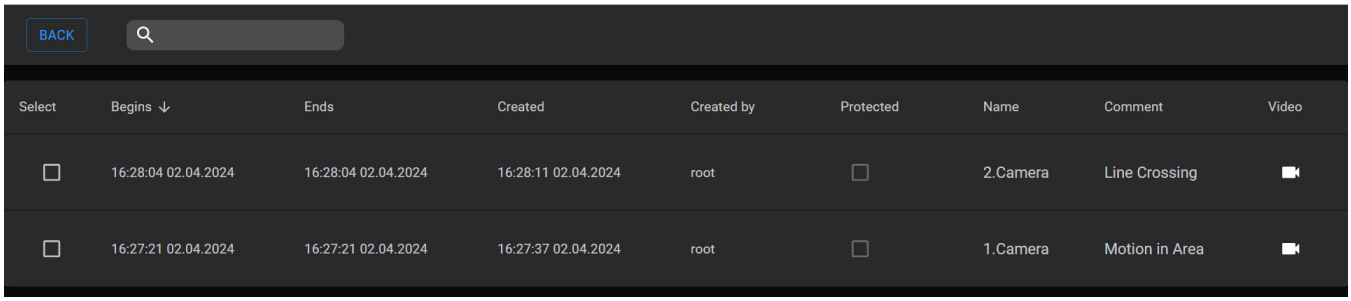
- name;
- number of linked cameras;
- cumulative bit rate of linked cameras.

To return to the previous page, click **BACK** in the left upper corner of the screen.

Working with bookmarks in the Web-Client

A bookmark represents either a comment in the archive (see Operator comments), or a protected video recording (see Protecting video footage from FIFO overwriting).

To work with bookmarks, click the  button in the top right corner of the Web-Client window, and select the **Archive Bookmarks** option.



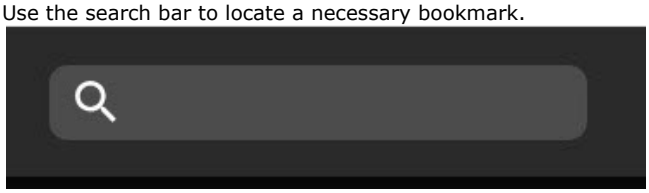
Attention!

- You can access only the bookmarks on the visible part of the archive (see Configuring access restrictions to archive).
- The bookmarks belonging to the archive fragment that was overwritten in a loop will not be displayed.

You can:

1. Edit a bookmark.
2. Delete a bookmark.
3. Un-protect a protected video.
4. Delete a protected video.

Use the search bar to locate a necessary bookmark.



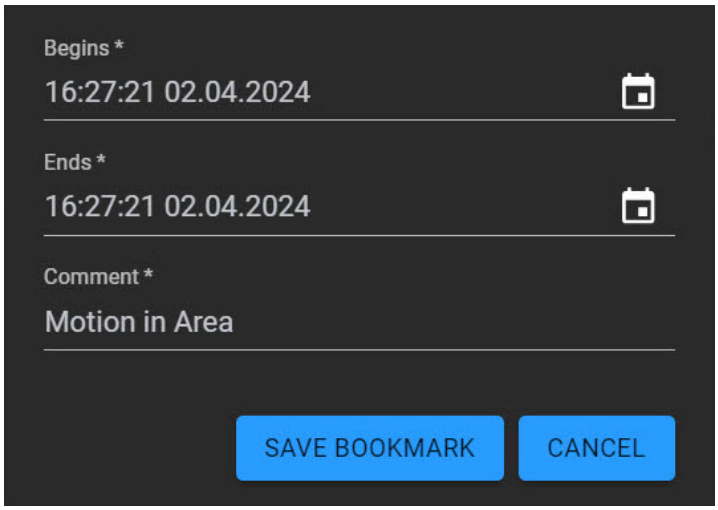
To proceed to a particular video, click the  button in the **Video** column. To return to a main page, click the **BACK** button.

Editing a bookmark

To edit a bookmark, do the following:

1. Select the required bookmark in the table.

2. Click the **EDIT BOOKMARK** button.



3. If necessary, you can change the time interval and/or a text comment.
4. Click the **SAVE BOOKMARK** button.

Deleting a bookmark

To delete a bookmark, select it in the table and click the **DELETE BOOKMARK** button.

You can delete several bookmarks. To do this, set the checkboxes next to the required bookmarks and click the **DELETE BOOKMARK** b utton.

Un-protecting a video

To un-protect a video, clear the **Protected** checkbox next the bookmark.

Deleting a protected video

To delete a protected video, select a protected bookmark and click the **DELETE RECORD** button.

Working with interactive map via the Web-Client

You can create and configure an interactive map using the regular *Axxon One* Client (see Configuring the interactive map, Working with the interactive map). In the Web-Client, you can only view the created maps.

There are three modes of viewing an interactive map in the Web-Client:

1. Both map and layout.
2. Map only.
3. Layout only.

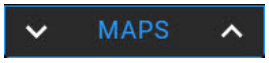
The markers displayed in the Web-Client indicate video cameras and transitions to other maps that were previously added in the regular *Axxon One* Client (see Adding video cameras, Adding switches to another map).



In the Web-Client, You can disable the display of the names of video cameras and transitions to other maps that are displayed near the markers. To do this, you need to disable the **Show marker names** option in the user preferences (see Web-Client configuration).

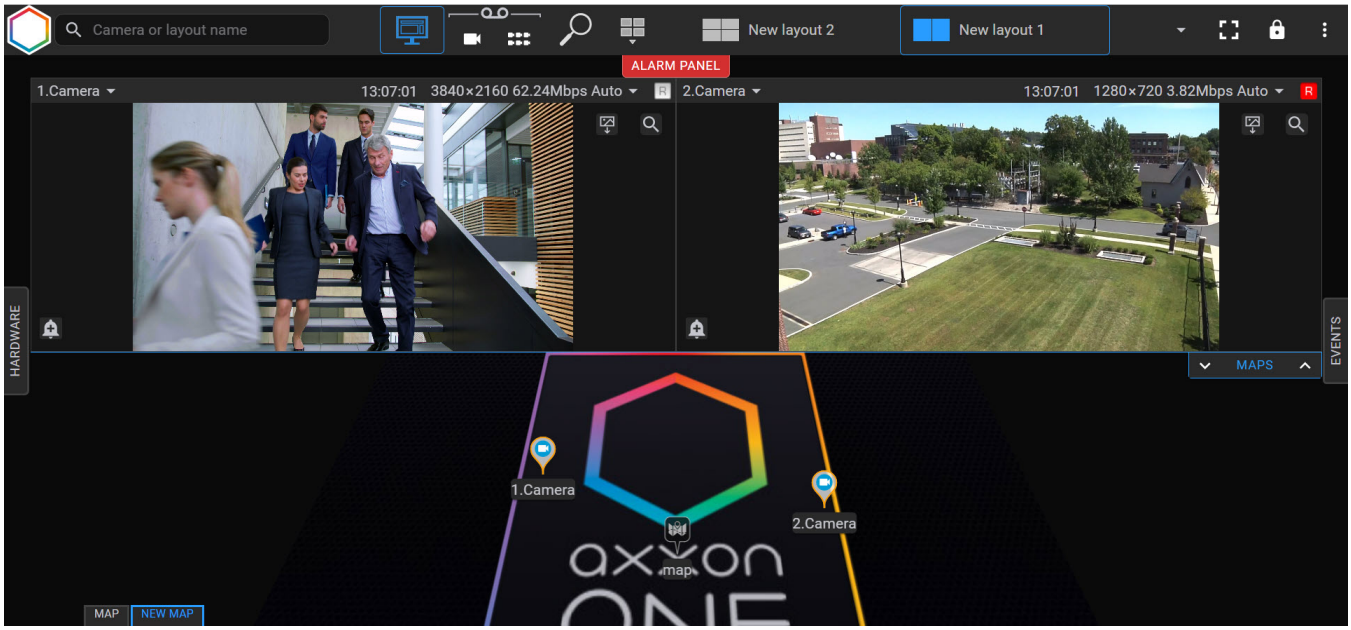
Displaying an interactive map in the Web-Client

You can switch to the map viewing mode from any video surveillance mode, except the archive search mode.

To switch to the map viewing mode, click the **Maps** button in the lower right corner of the screen 

.

The map will be displayed in a 3D projection, and the layout will move to the top of the screen, decreasing in size.



To switch to full screen mode, click on the  button to the right of the **Maps** button. To exit the map viewing mode, click the  button to the left of the **Maps** button.

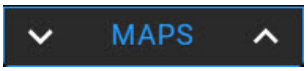
When using the full-screen map display mode, after clicking on the video camera marker, a window with a video image from this camera will appear. When you click on the video window, the map will be minimized to half the screen and a layout will open containing the selected video camera. In order to open only the cell with the selected video camera, you need to disable the **Open selected camera on layout** option in the user preferences (see Web-Client configuration).

If the map is open in half the screen, then when you click on the camera marker, if this camera is already present in the current viewing layout, this camera will either be activated or opened in single view mode, depending on the **Open selected camera on layout** setting. If the selected camera is not on the current layout, a window with a player will appear in the place of the marker.

Changing the display of the map on a layout via the Web-Client

By default, maps are displayed as they were attached to layouts in the Client (see Attaching a map to a layout).

To change the display of the map on a layout via the Web-Client, do the following:

1. Click the  button and select **Edit layout**.
2. Using the 

buttons, change the display of the map to one of three options:
    a. both map and layout are displayed.
    b. only map is displayed.
    c. only layout is displayed.
3. Click the **Save** 

button.

As a result, when you switch to this layout, the map will always be displayed in the way that you selected when editing the layout.

Zooming and moving the map in the Web-Client

You can manually zoom the map by scrolling the mouse wheel (the mouse cursor should be hovered over the map).



After zooming in, you can drag the map (while pressing and holding the left mouse button) in any direction.

Working with Axxon One Through the Mobile Clients

Axxon One clients are available on the iOS, and Android operating systems.

For more information on configuring and using the mobile client apps, refer to the corresponding documentation.

Changing user password

You can change user passwords in *Axxon One* with a few clicks.

Please follow the steps below:

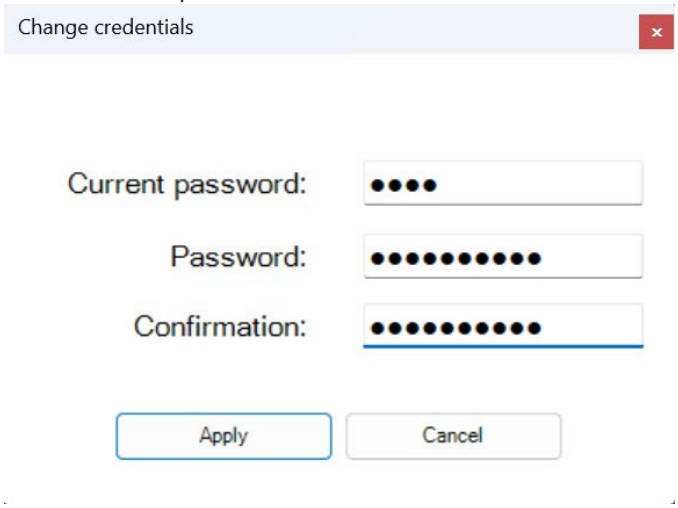
1. Go to the Settings tab  .
2. In the upper-right corner, click the user name.



3. Click **Change password**.



4. Enter the current password.



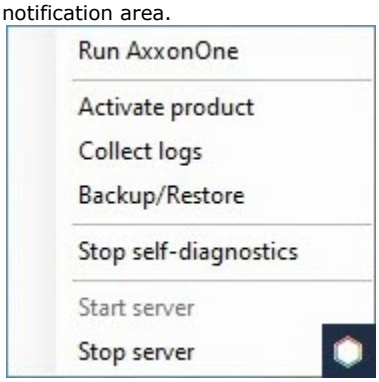
5. Enter a new password and confirm it.
6. Click **Apply**.

The next time log in with a new password.

Description of utilities

Axxon One Tray Tool

The *Axxon One* Tray Tool launches automatically during system startup and displays an icon in the Microsoft Windows taskbar notification area.



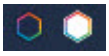
Note.

The executable TrayTool.exe is located at <*Axxon One* installation folder>\Axxon One\bin.

With the *Axxon One* Tray Tool utility, you can quickly start the following applications from the notification area:

- Client,
- Activation Utility,
- Axxon Support Tool,
- Configuration Backup and Restore utility,
- Self-checking Service,
- Server rebooting.

Color indication of the *Axxon One Tray Tool* utility reflects the state of the Server.

Icon color	Icon type	State of the Server
Multicolored		Server is on
Orange white	 (flashing)	Starting/stopping of the Server
Orange		Server is off
Grey		Server is inactive

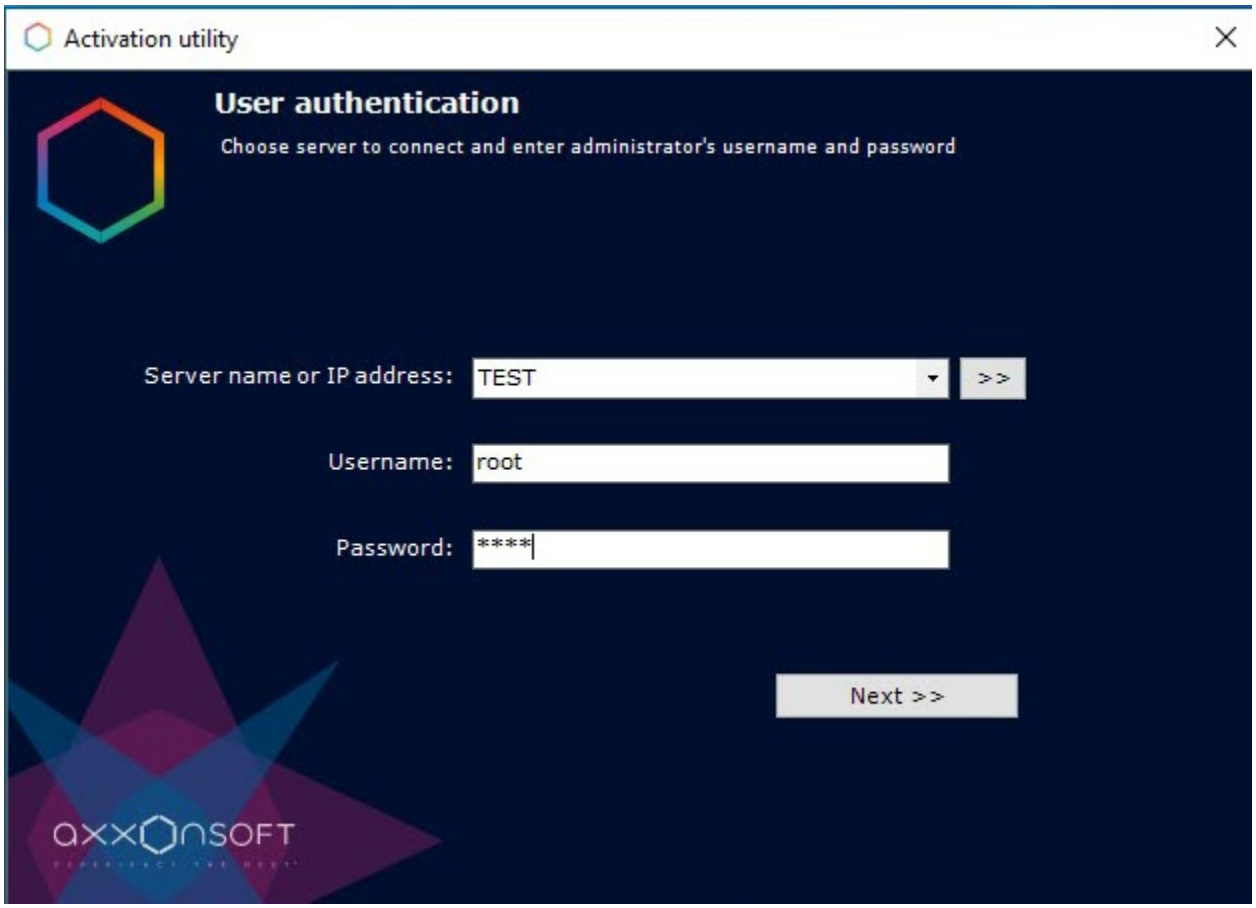
Activation utility

License activation for the *Axxon One* software package is carried out through the product activation utility.

The activation utility is accessible at **Start** -> **All Programs** -> **Axxon One** -> **Utilities** -> **Program Activation**, or from the tray menu (see the Axxon One Tray Tool section).

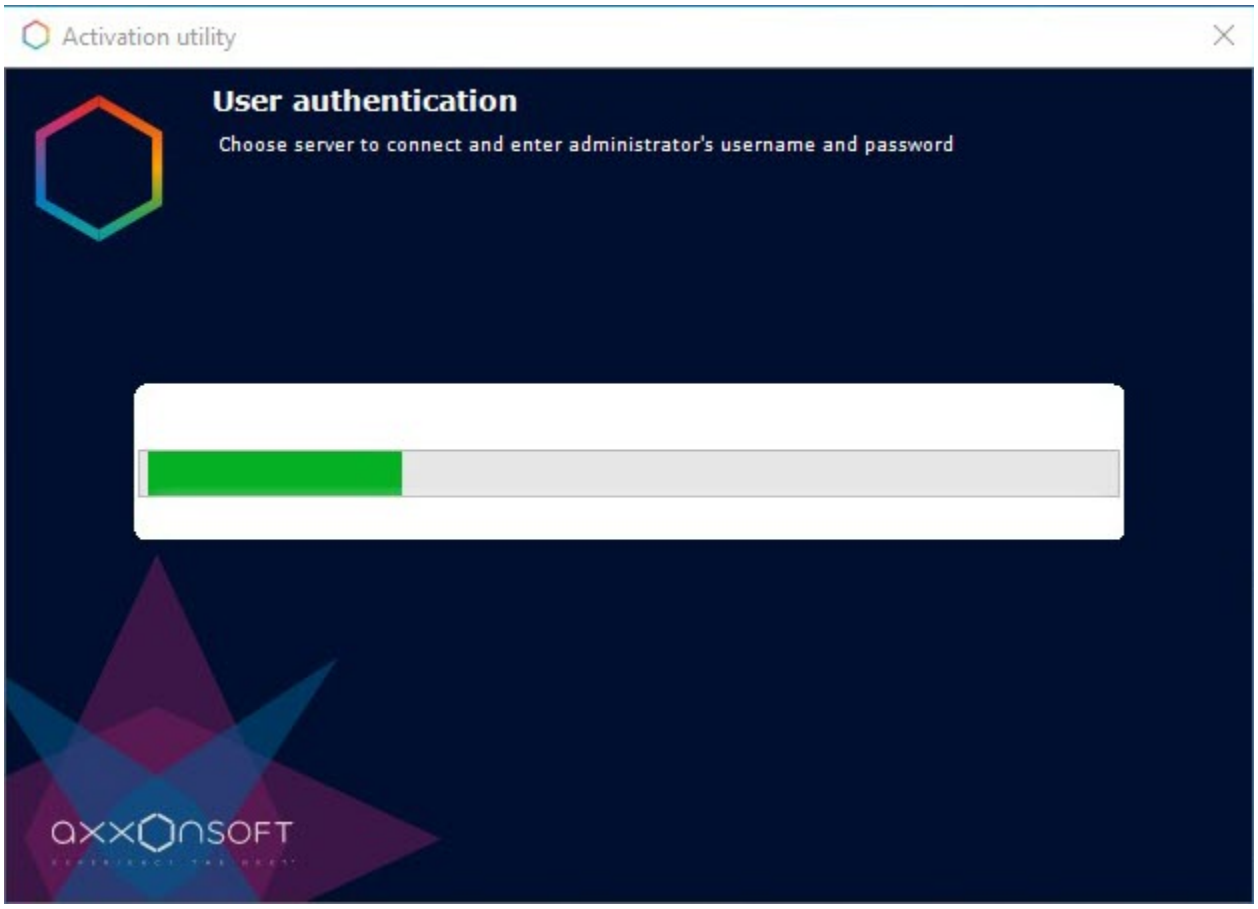
> **Note**
>
> The product activation utility program file LicenseTool.exe is located in the folder <Directory where *Axxon One* is installed>\AxxonSoft\Axxon Smart\bin\

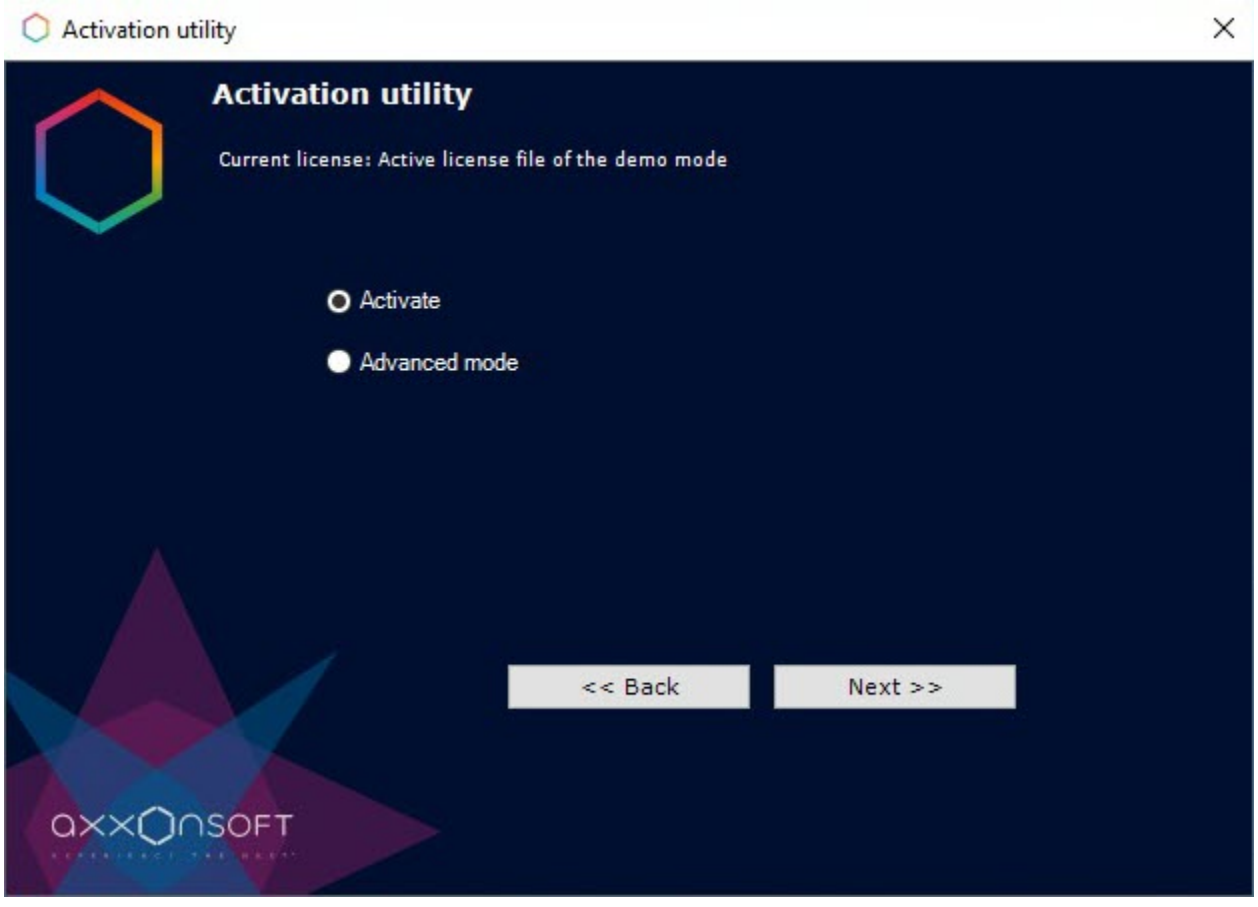
Then you must select the name of one of the Axxon Domain servers to which the license file will be applied (the file is applied to all Axxon Domain servers launched at the moment of activation) and connect to the system, under an administrator's user name and password, to continue the activation process.



After the download is complete the main window of license utility will be displayed.

> **Note**
>
> To activate *Axxon One*, connect to a Server in the Axxon domain. Otherwise, an error message appears.


Activation utility
User authentication
Choose server to connect and enter administrator's username and password
axxonsoft


Activation utility
Activation utility
Current license: Active license file of the demo mode
Activate
Advanced mode
<< Back
Next >>
axxonsoft

To activate *Axxon One*, please refer to the document titled Activation Guide*,* which presents step-by-step instructions on activating, updating and upgrading *Axxon One*.

It is also recommended that you use the prompts displayed in the product activation utility's dialog boxes.

Axxon Support Tool

Purpose of the Support.exe Utility

The Support.exe utility is designed to collect information about the configuration and operating status of hardware, the Windows operating system, and the *Axxon One* software. The utility generates an archive that can be used by the company's technical support department. In case of malfunctions or errors in the *Axxon One* software package, please visit our technical support server at https://support.axxonsoft.com/ and compose a message containing a description of the problem and attach the archive that was generated by the Support.exe utility.

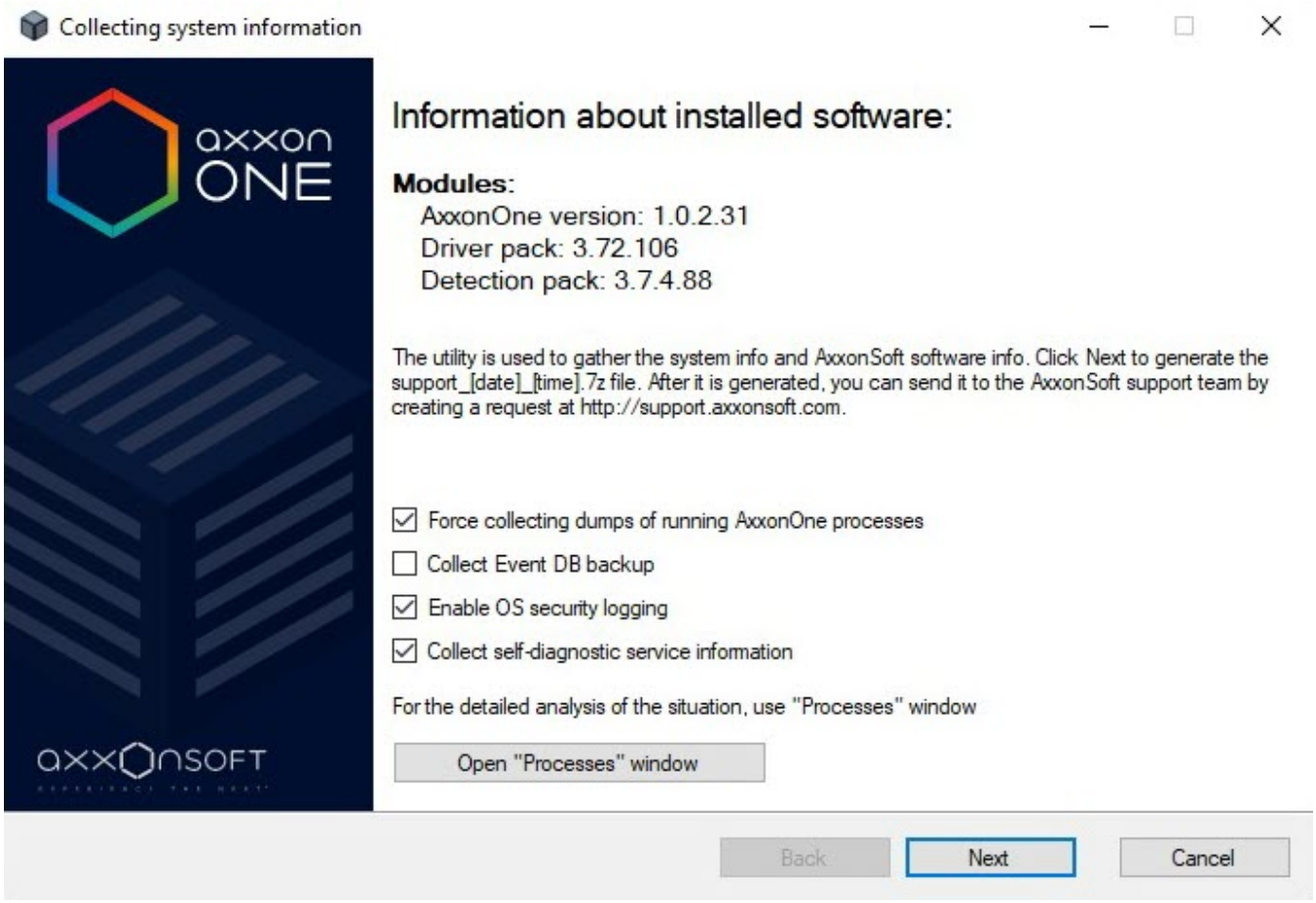
Launching and Closing the Utility

The Support.exe utility is launched using the **Start** menu, which is intended for launching user programs in Windows. Go to **Start All Programs Axxon One Gathering system information.**

Note

- The Support.exe utility is located in the folder <*Axxon One* installation directory>\Axxon One\bin
- The Support.exe utility requires administrator rights to run.

The Support.exe utility dialog box will then be displayed.

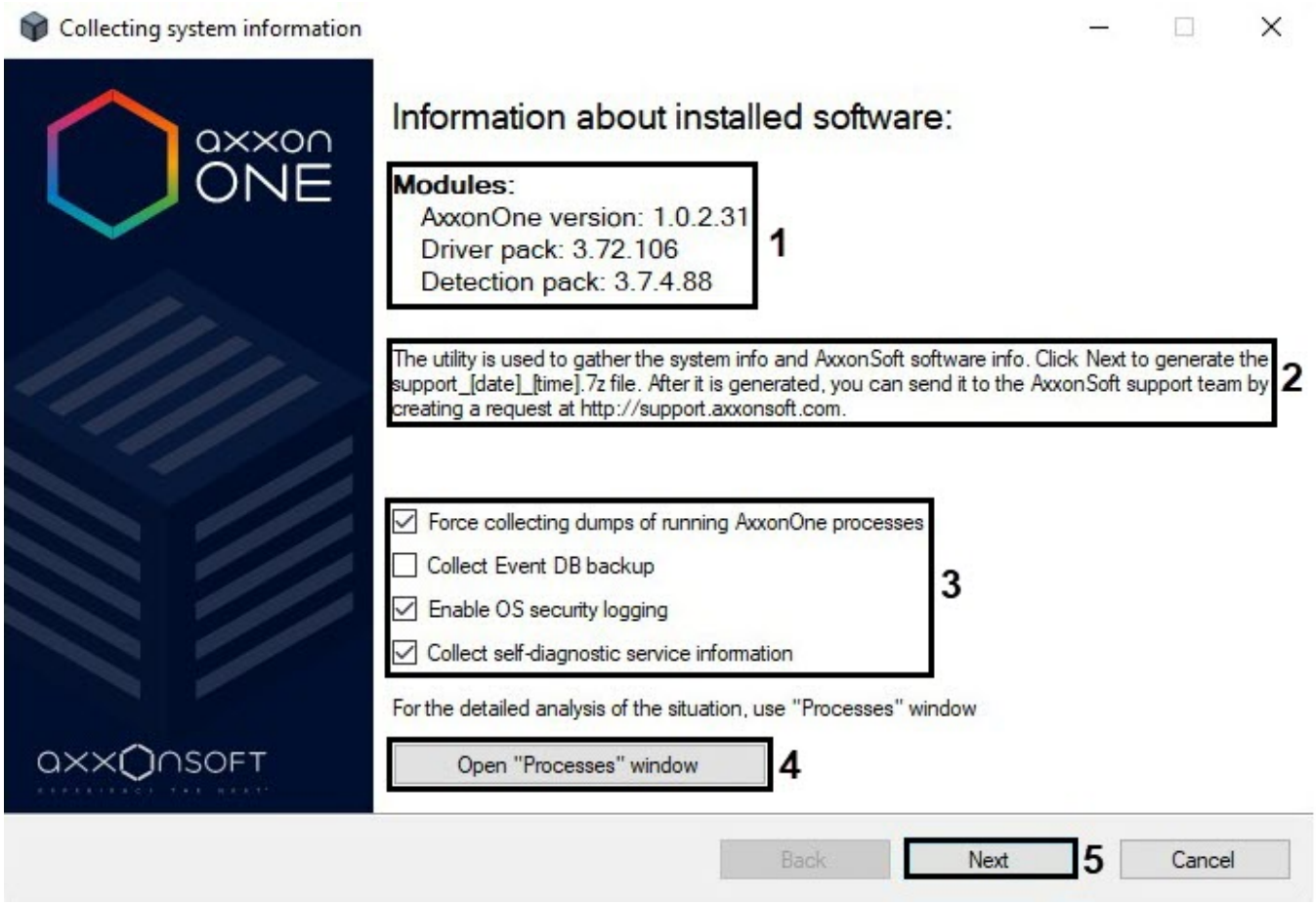


To close the Support.exe utility, click the **Cancel** button or .

Description of the Support.exe utility interface

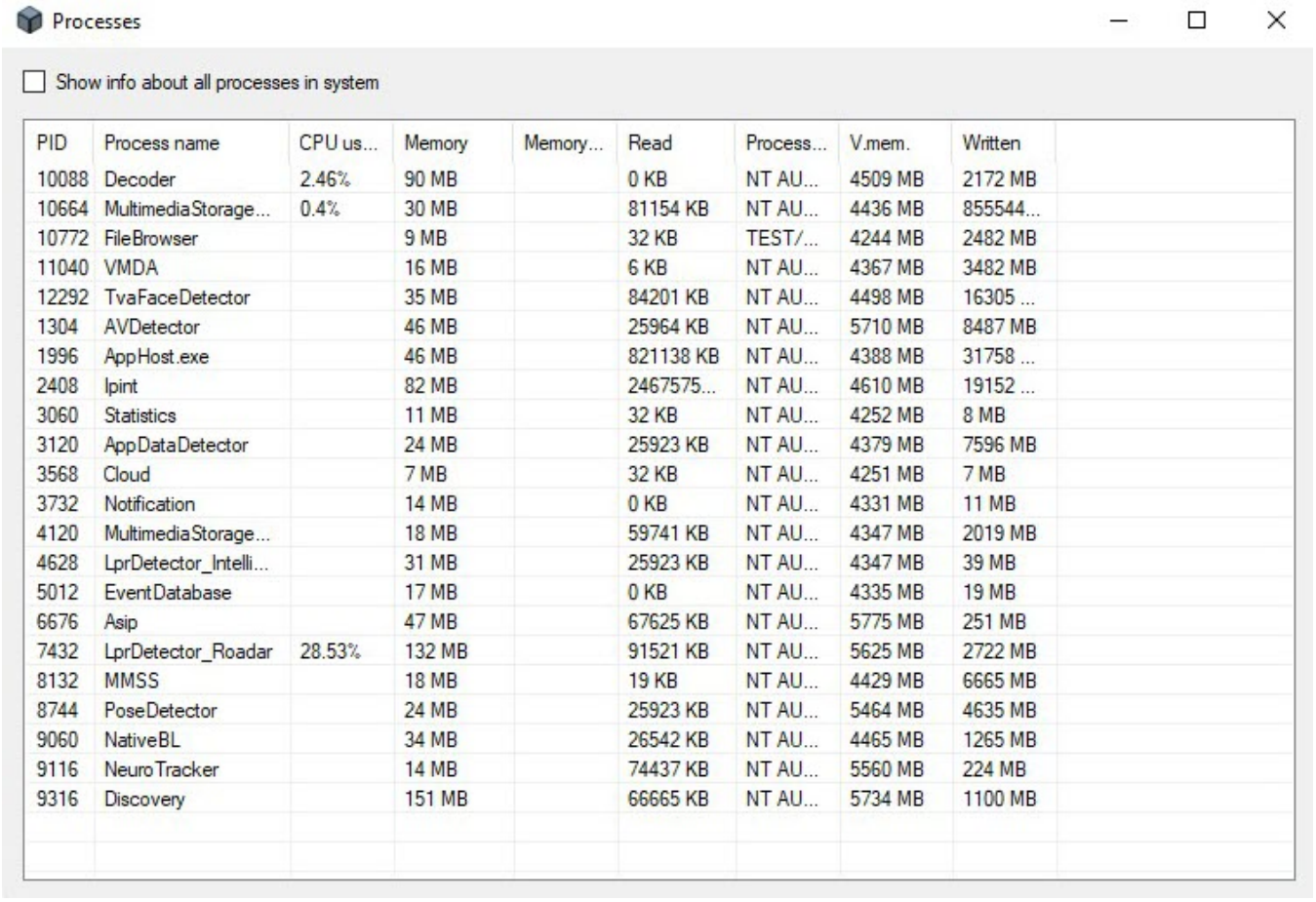
The Support.exe user interface includes the following elements:

1. Summary of installed software (**1**).
2. Short instructions on how to use the Support.exe utility (**2**).
3. Check boxes for configuring data collection (**3**).
4. A button for launching the **Processes** service, which offers an in-depth situation analysis (**4**).
5. A button for starting the information gathering process (**5**).



The Processes Service

The **Processes** service is used for detailed analysis of a situation. To launch it, click the **Open "Processes" window** button; the **Processes** window will then appear, displaying information about processes running on the computer initiated by the Support.exe utility.



PID	Process name	CPU us...	Memory	Memory...	Read	Process...	V.mem.	Written
10088	Decoder	2.46%	90 MB		0 KB	NT AU...	4509 MB	2172 MB
10664	MultimediaStorage...	0.4%	30 MB		81154 KB	NT AU...	4436 MB	855544...
10772	FileBrowser		9 MB		32 KB	TEST/...	4244 MB	2482 MB
11040	VMDA		16 MB		6 KB	NT AU...	4367 MB	3482 MB
12292	TvaFaceDetector		35 MB		84201 KB	NT AU...	4498 MB	16305 ...
1304	AVDetector		46 MB		25964 KB	NT AU...	5710 MB	8487 MB
1996	AppHost.exe		46 MB		821138 KB	NT AU...	4388 MB	31758 ...
2408	Ipint		82 MB		2467575...	NT AU...	4610 MB	19152 ...
3060	Statistics		11 MB		32 KB	NT AU...	4252 MB	8 MB
3120	AppDataDetector		24 MB		25923 KB	NT AU...	4379 MB	7596 MB
3568	Cloud		7 MB		32 KB	NT AU...	4251 MB	7 MB
3732	Notification		14 MB		0 KB	NT AU...	4331 MB	11 MB
4120	MultimediaStorage...		18 MB		59741 KB	NT AU...	4347 MB	2019 MB
4628	LprDetector_Intelli...		31 MB		25923 KB	NT AU...	4347 MB	39 MB
5012	EventDatabase		17 MB		0 KB	NT AU...	4335 MB	19 MB
6676	Asip		47 MB		67625 KB	NT AU...	5775 MB	251 MB
7432	LprDetector_Roadar	28.53%	132 MB		91521 KB	NT AU...	5625 MB	2722 MB
8132	MMSS		18 MB		19 KB	NT AU...	4429 MB	6665 MB
8744	PoseDetector		24 MB		25923 KB	NT AU...	5464 MB	4635 MB
9060	NativeBL		34 MB		26542 KB	NT AU...	4465 MB	1265 MB
9116	NeuroTracker		14 MB		74437 KB	NT AU...	5560 MB	224 MB
9316	Discovery		151 MB		66665 KB	NT AU...	5734 MB	1100 MB

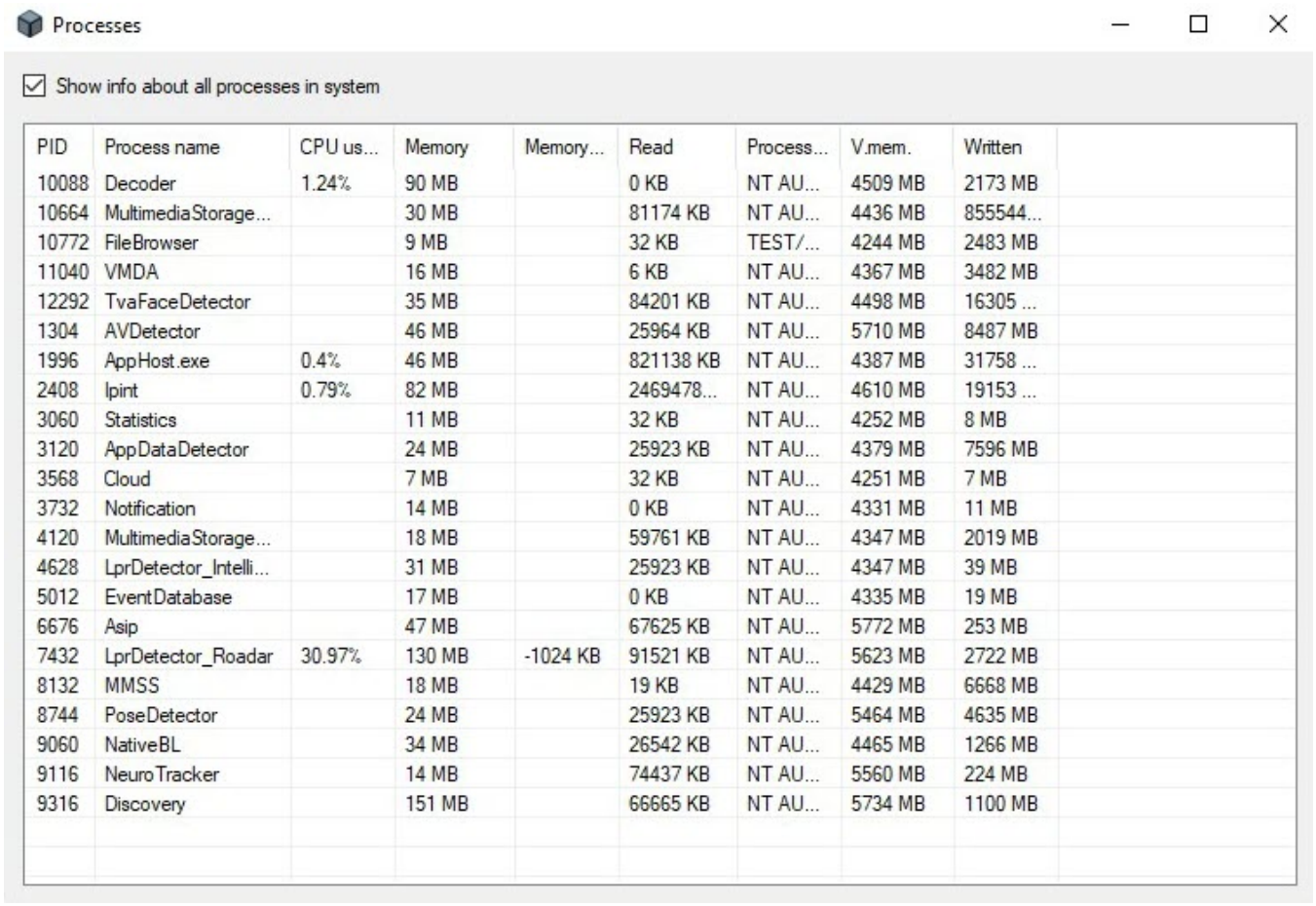
A list of all possible *Axxon One* processes is given in the table.

Process	**Description**
Axxon.Discovery	Process that searches for peripheral devices (video cameras, analog video cards, devices connected to a serial port, etc.).
Axxon.VMDA	Process responsible for the metadata database, writes metadata and searches in the archive.
Axxon.MMSS	Web server process.
Axxon.Notification	Process for managing events in the system and creating a database of these events.
Axxon.Axxon One	GUI process.
Axxon.Bootstrap	Main process responsible for configuration, licensing, storing settings, and starting other processes.
Axxon. FileBrowser	Process that provides access to the file system and information about server files.
Axxon.NVR	Logic module responsible for alarms and automatic rules.
Axxon.InfraServer	Process responsible for interaction between *Axxon One* modules.
Axxon.Decoder	Process that performs decoding of multimedia streams.
Axxon.Detector	Process that performs detection.
Axxon.Proxy	Process that performs buffering and grooming of multimedia streams.

Axxon. NVR_Archive	Process that writes multimedia data to the archive.
Axxon.Ipint	Process that interfaces with the Drivers Pack.
Axxon.MiscMMSS	Process that plays back audio on the server audio card.

Note

Selecting the **Show info about all processes in system** check box enables viewing of all processes running on the computer.



PID	Process name	CPU us...	Memory	Memory...	Read	Process...	V.mem.	Written
10088	Decoder	1.24%	90 MB		0 KB	NT AU...	4509 MB	2173 MB
10664	MultimediaStorage...		30 MB		81174 KB	NT AU...	4436 MB	855544...
10772	FileBrowser		9 MB		32 KB	TEST/...	4244 MB	2483 MB
11040	VMDA		16 MB		6 KB	NT AU...	4367 MB	3482 MB
12292	TvaFaceDetector		35 MB		84201 KB	NT AU...	4498 MB	16305 ...
1304	AVDetector		46 MB		25964 KB	NT AU...	5710 MB	8487 MB
1996	AppHost.exe	0.4%	46 MB		821138 KB	NT AU...	4387 MB	31758 ...
2408	Ipint	0.79%	82 MB		2469478...	NT AU...	4610 MB	19153 ...
3060	Statistics		11 MB		32 KB	NT AU...	4252 MB	8 MB
3120	AppDataDetector		24 MB		25923 KB	NT AU...	4379 MB	7596 MB
3568	Cloud		7 MB		32 KB	NT AU...	4251 MB	7 MB
3732	Notification		14 MB		0 KB	NT AU...	4331 MB	11 MB
4120	MultimediaStorage...		18 MB		59761 KB	NT AU...	4347 MB	2019 MB
4628	LprDetector_Intelli...		31 MB		25923 KB	NT AU...	4347 MB	39 MB
5012	EventDatabase		17 MB		0 KB	NT AU...	4335 MB	19 MB
6676	Asip		47 MB		67625 KB	NT AU...	5772 MB	253 MB
7432	LprDetector_Roadar	30.97%	130 MB	-1024 KB	91521 KB	NT AU...	5623 MB	2722 MB
8132	MMSS		18 MB		19 KB	NT AU...	4429 MB	6668 MB
8744	PoseDetector		24 MB		25923 KB	NT AU...	5464 MB	4635 MB
9060	NativeBL		34 MB		26542 KB	NT AU...	4465 MB	1266 MB
9116	NeuroTracker		14 MB		74437 KB	NT AU...	5560 MB	224 MB
9316	Discovery		151 MB		66665 KB	NT AU...	5734 MB	1100 MB

Click the button to close the **Processes** window.

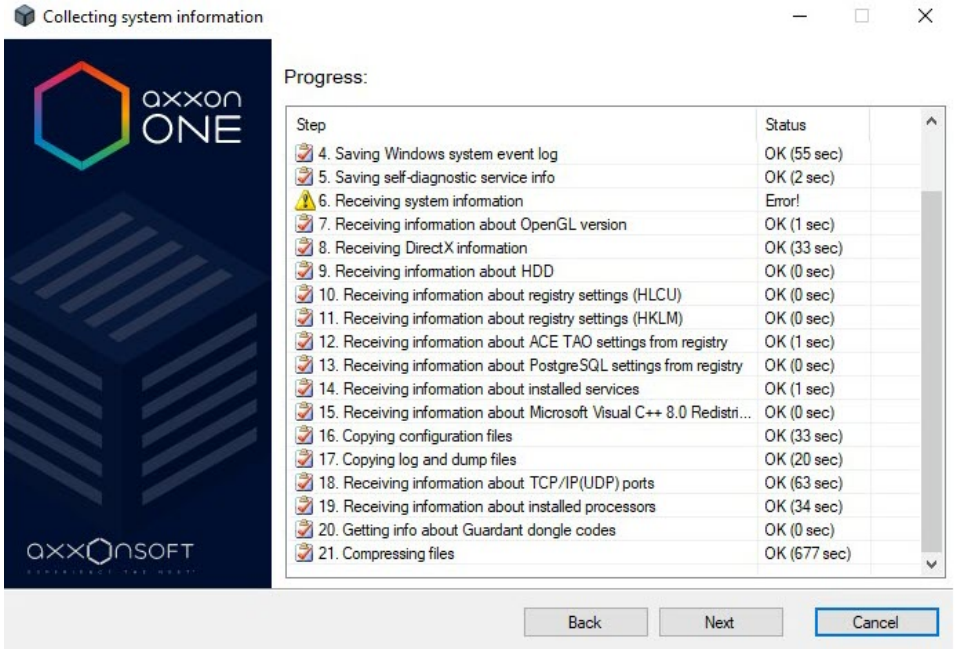
Collecting Data on the Configuration of Servers and Clients Using the Support

To collect data using the Support.exe utility, perform the following:

1. Launch the Support.exe utility (see the section Launching and Closing the Utility).



2. By default, a report includes data about already launched *Axxon One* processes. To exclude this data from reports, deselect the checkbox (**1**).
3. Select the corresponding checkbox to include a backup copy of events database in reports (**2**).
4. By default, a report includes information about Windows security system. To exclude this data from reports, deselect the checkbox (**3**).
5. Select the corresponding checkbox to include a self-diagnostic service (see Self-diagnostics service) information in reports (**4**).
6. Click the **Next** button (**5**).
   The data collection process will begin. The table that displays the progress of data collection includes two columns: **Step** and **St atus**. In the **Step** column, a brief description of the stage of information collection is displayed. In the **Status** column, a progress indicator and the time spent on executing the stage are displayed.



7. When information collection is complete, click the **Next** button.

8. A window containing information about the generated archive **support_[date]_[time].7z** will then appear. You can access the folder containing this archive by clicking the **Open directory with file** button.

> **Note**
>
> The archive is located in the folder <System disk>:\Documents and Settings\<Current User>\My Documents if you're using Windows XP, or in the folder <System disk>:\Users\<Current User>\Documents if you're using Windows Vista.



9. Send an email with the attached **support_[date]_[time].7z archive** to the AxxonSoft technical support department.

Log Management Utility

By default, information about all system events is recorded in the *Axxon One* system log, which is stored in a local database of the server. It is possible to record information about desired events in external logs, which are log files stored in local directories of a server. Log data is archived at set intervals and moved to the log archive. Configuration of these capabilities is carried out through the log management utility.

Axxon One component	**Log storage directory**
Server	<*Axxon One* installation folder>\logs
Client	<Letter of system disk>:\Users\<User>\Appdata\Local\AxxonSoft\Axxon One\logs (for Windows Vista, and Windows 7 and higher) <Letter of system disk>:\Documents and Settings\User\Local Settings\Application Data\AxxonSoft\Axxon One\Logs (for Windows XP)

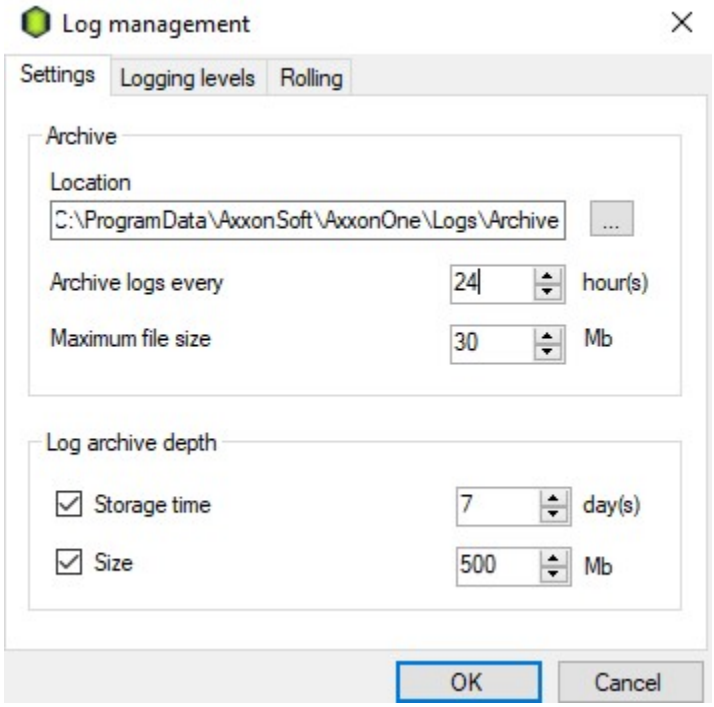
The log management utility is used to configure the following parameters:

1. Parameters for the archive of external logs containing information about system events.
2. Loging levels for the *Axxon One* Client and Server.

Starting and closing the utility

The log management utility can be launched using the **Start** menu, which is intended for launching user programs in Windows. **Start All Programs Axxon One Utilities Logs Archiving**.

The log management utility dialog box will then appear.



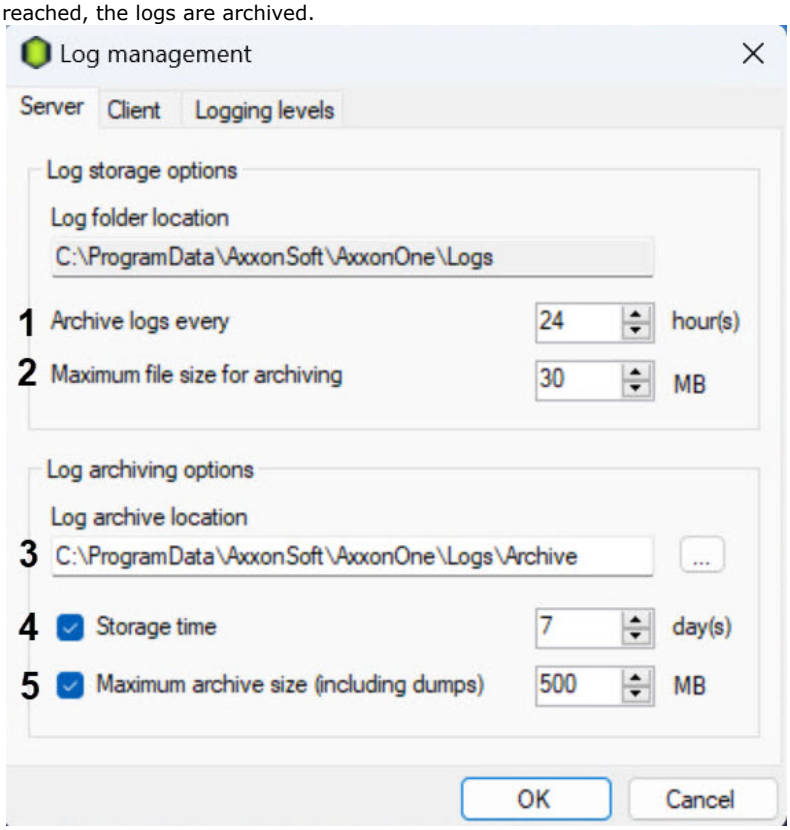
To close the log management utility, click the **Cancel** button or  (accessible in all tabs of the utility).

Configuring the Server log storage and archiving options

You can configure the log storage and archiving options on the **Server** tab of the Log management utility.

To configure log storage options, do the following:

1. In the **Archive logs every** field (**1**), enter the interval for system log archiving in hours.
2. In the **Maximum file size for archiving** field (**2**), set the size of the log file in megabytes (**3**). When the specified size is reached, the logs are archived.



3. In the **Log archive location** field (**3**), enter the full path to the directory in which you want to place the log archives. To set the path using standard Windows methods, click the ... button.
4. In the **Storage time** field (**4**), set the maximum time of storing a log in the archive in days, after which the log is deleted.
5. In the **Maximum archive size (including dumps)** field (**5**), set the maximum size of the archive, above which the earliest logs are deleted from the archive.

> **Note**
>
> Archive size limitations take priority over log storage time limitations. For example, the earliest logs will be automatically deleted even if their storage time hasn't expired, if the archive size has exceeded the maximum value. If it is not necessary to impose any limitations on log storage time and/or archive size, clear the corresponding checkboxes in the **Log archiving options** group.

6. Click the **OK** button to save the changes.

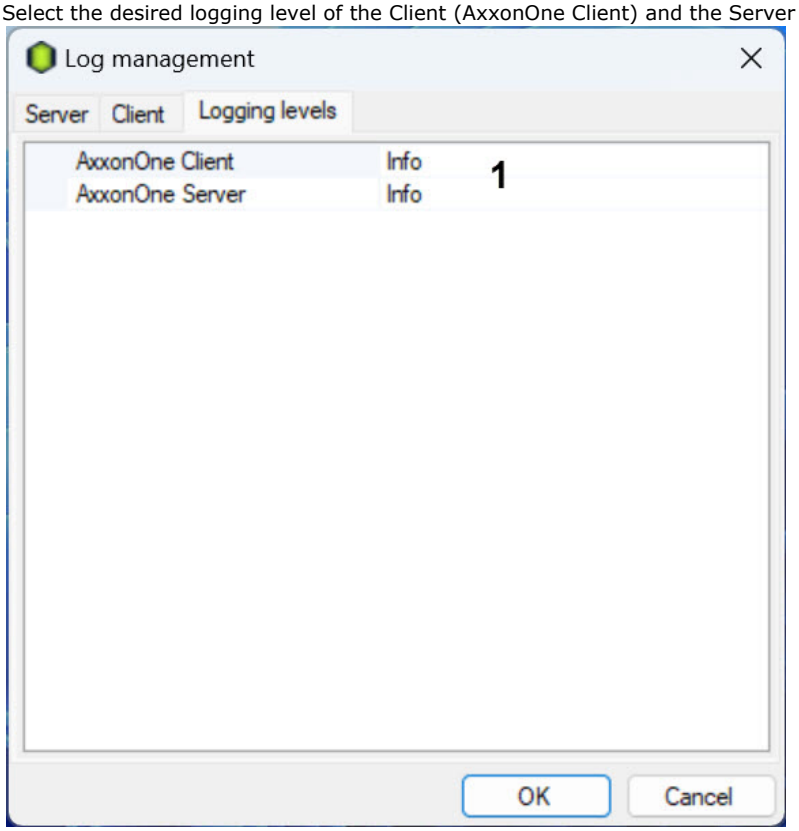
The Server log storage and archiving options are now configured.

Configuring the logging levels

Logging levels differ in the list of events to be recorded in external logs, as well as the level of event specification (low, medium, high). Levels are configured in the **Logging levels** tab of the log management utility.

To configure the logging level, do the following:

1. Select the desired logging level of the Client (AxxonOne Client) and the Server (AxxonOne Server) (**1**).



> **Note**
>
> - If you change the logging level of a Server, the server will be restarted.
> - If the *Axxon One* VMS is installed in the **Failover Server and Client** configuration (see Installation), you can log in as either a Client or a Supervisor (see Configuring Failover VMS).

Logging level	Logging level description
None	Event logging disabled
Error	Low specification level—only system errors are logged
Warning	Low level of detail—only system warnings and system errors are logged
Info	Low level of detail—logs informational messages, system warnings, and system errors
Debug	Medium level of detail—logs debugging events, informational messages, system warnings, and system errors
Trace	High specification level—all system events are logged

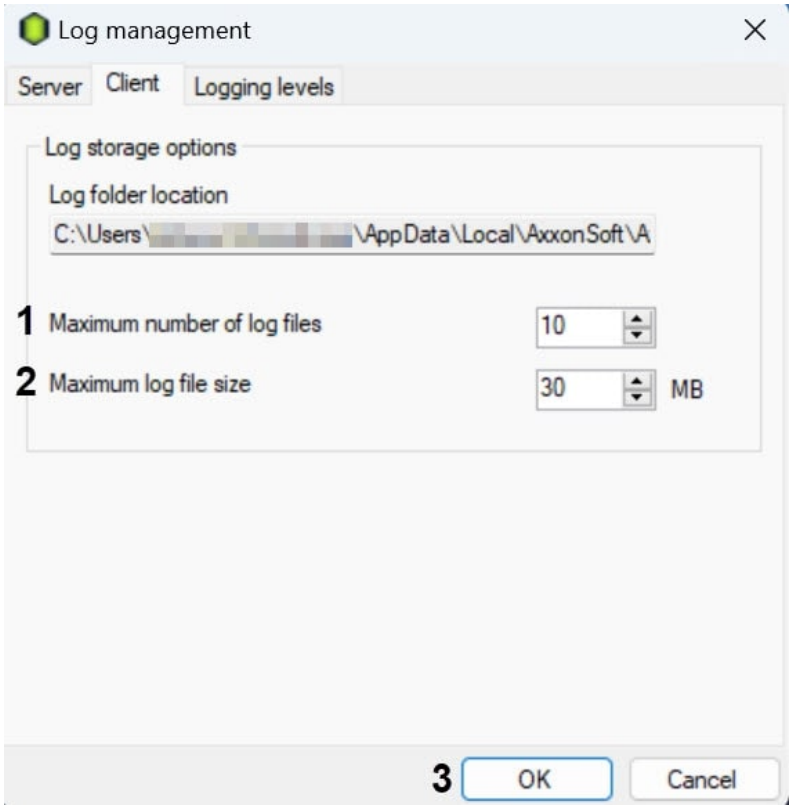
2. Click the **OK** button to save the changes.

Configuration of logging levels is complete.

Configuring the Client log storage options

To configure the Client log storage options, do the following:

1. Go to the **Client** tab.



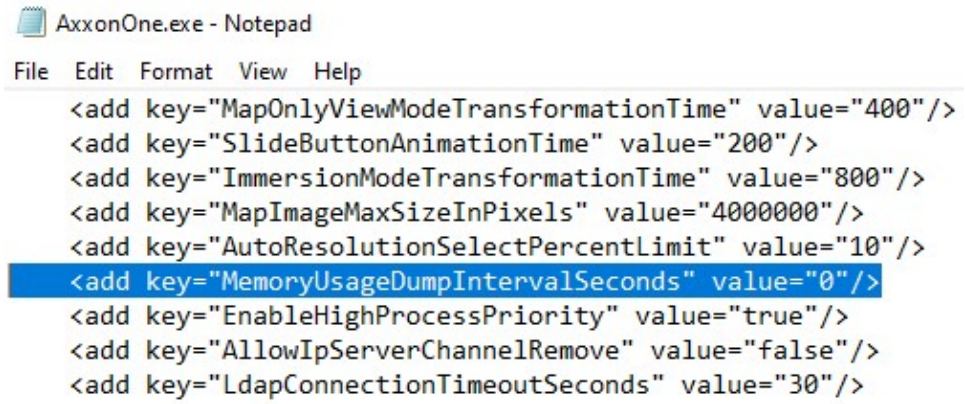
2. In the **Maximum number of log files** field (**1**), set the maximum number of log files.
3. In the **Maximum log file size** field (**2**), set the maximum log size in megabytes. When the specified size is reached, a new log file is created.
4. Click the **OK** button to save the changes.

The Client log storage options are now configured.

Configuring Client RAM usage logging

You can log Client RAM usage at specified intervals (AxxonOne.exe process). To do this:

1. Quit Client (see Shutting down an Axxon One Client).
2. Open the AxxonOne.exe configuration file, located in the <System disk>:\Program Files\AxxonSoft\AxxonOne\bin, in a text editor.
3. Find the **MemoryUsageDumpIntervalSeconds** option and set a value for it, corresponding to the period of adding the information to the log in seconds.



> **Note**
>
> Value **0** – no information is logged.

4. Save the changes to the file.
5. Run client (see Starting the Axxon One Client).

Here is an example of the Client RAM usage information in the log:

```
*** Memory usage: ***
    Private size  425 MB
    Working set   404 MB
```

Private size – the amount of reserved memory.

Working set – memory footprint.

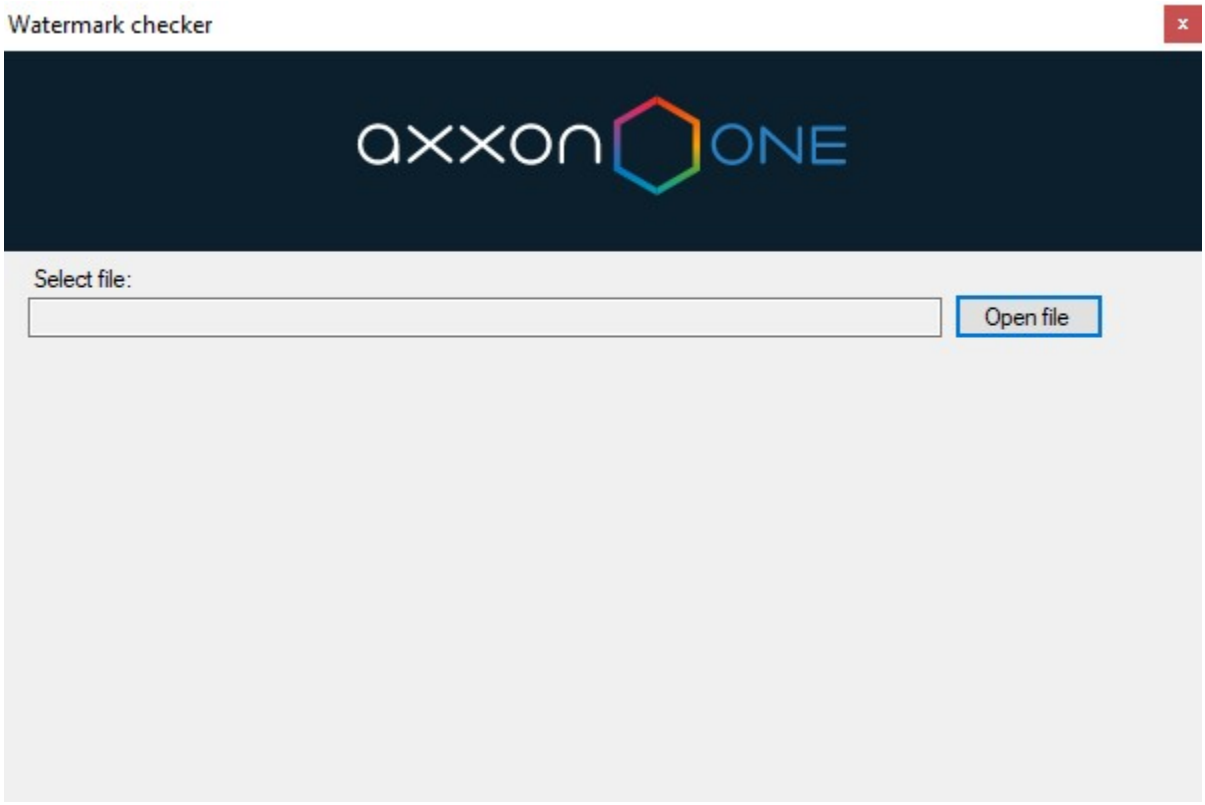
Digital signature verification utility

This utility verifies the digital signature that is added during export of video and snapshots from *Axxon One*.

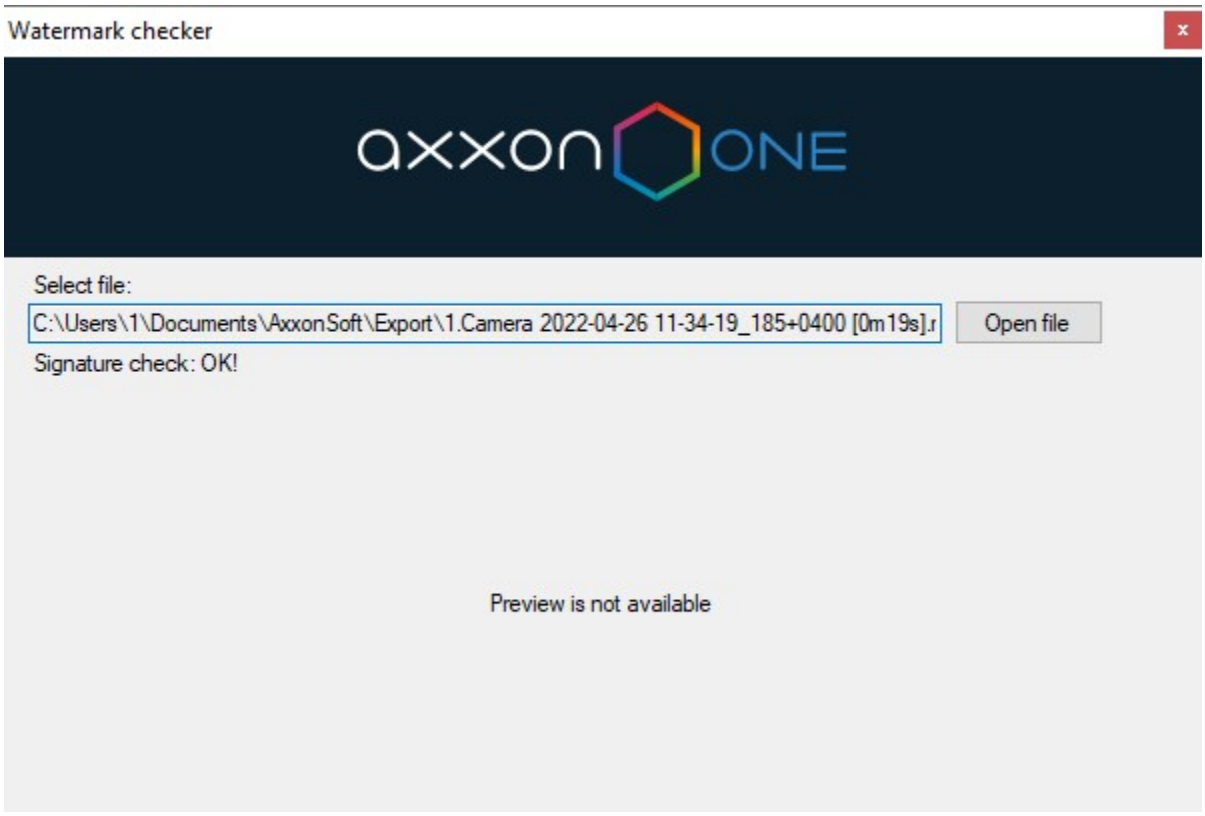
To start the utility, open the standard **Start** menu in Windows: **Start > Programs > Axxon One > Utilities > Watermark checker**.

> **Note**
>
> The utility executable file WatermarkCheck.exe is also located in the folder <System disk>:\Program Files\AxxonSoft\AxxonOne\bin\.

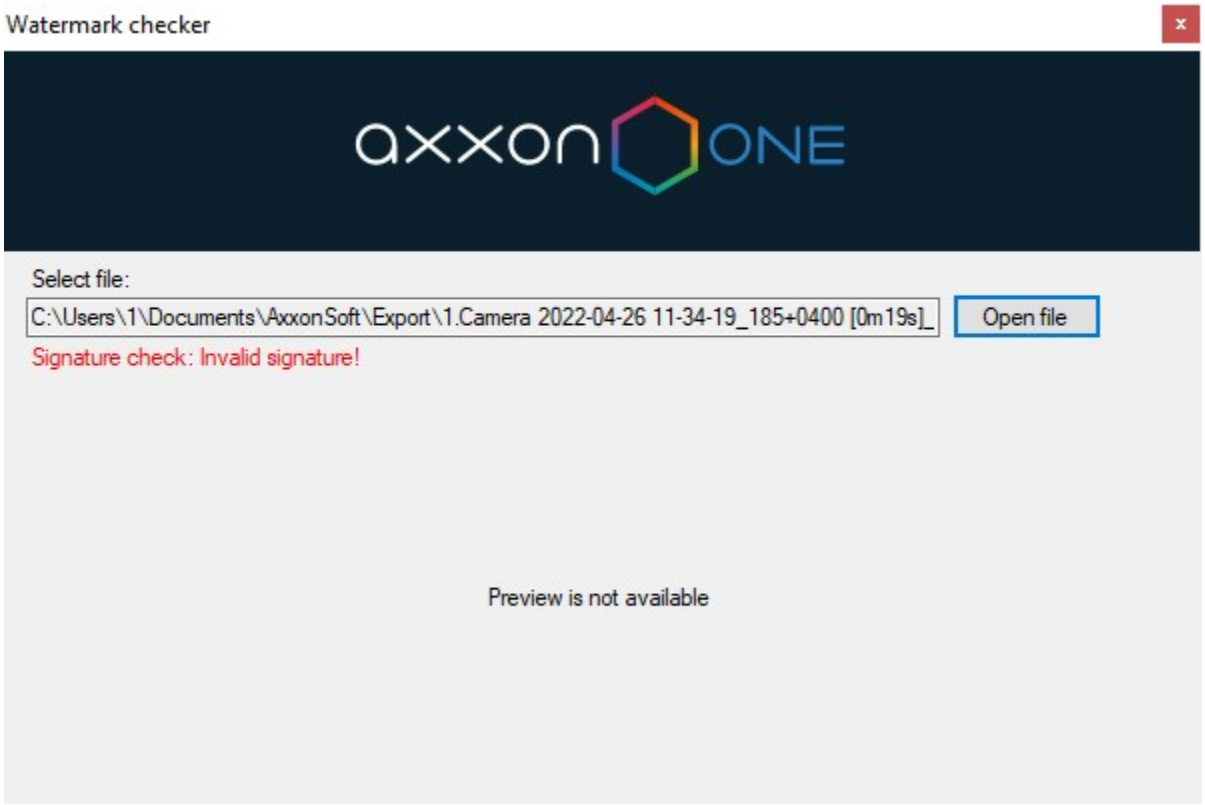
To check a digital signature, click the **Open file** button and select the file of the exported snapshot or video.



If the digital signature is valid, the utility will show the message: **Signature check: OK!**



If it is not valid, the utility will show the message: **Signature check: Invalid signature!**



Note

During verification of a digital signature, the thumbnail of a snapshot is shown in the utility window. Videos cannot be previewed during the verification process.

Digital signature verification is now complete.

To quit the utility, click the  button.

Backup and Restore Utility

Purpose of BackupTool.exe

BackupTool.exe allows system users to save a copy of the system configuration, roll back the configuration to a previous version, and restore the system configuration from a previously created copy.

> ⚠ **Attention!**
>
> The backup and restore utility may be applied to both the local configuration of a selected Server (including video cameras, archives, detection tools, event sources, logging levels) and the global configuration of the Axxon domain (users, maps, layouts, etc.).

This utility can also be used to change the name of the local Server.

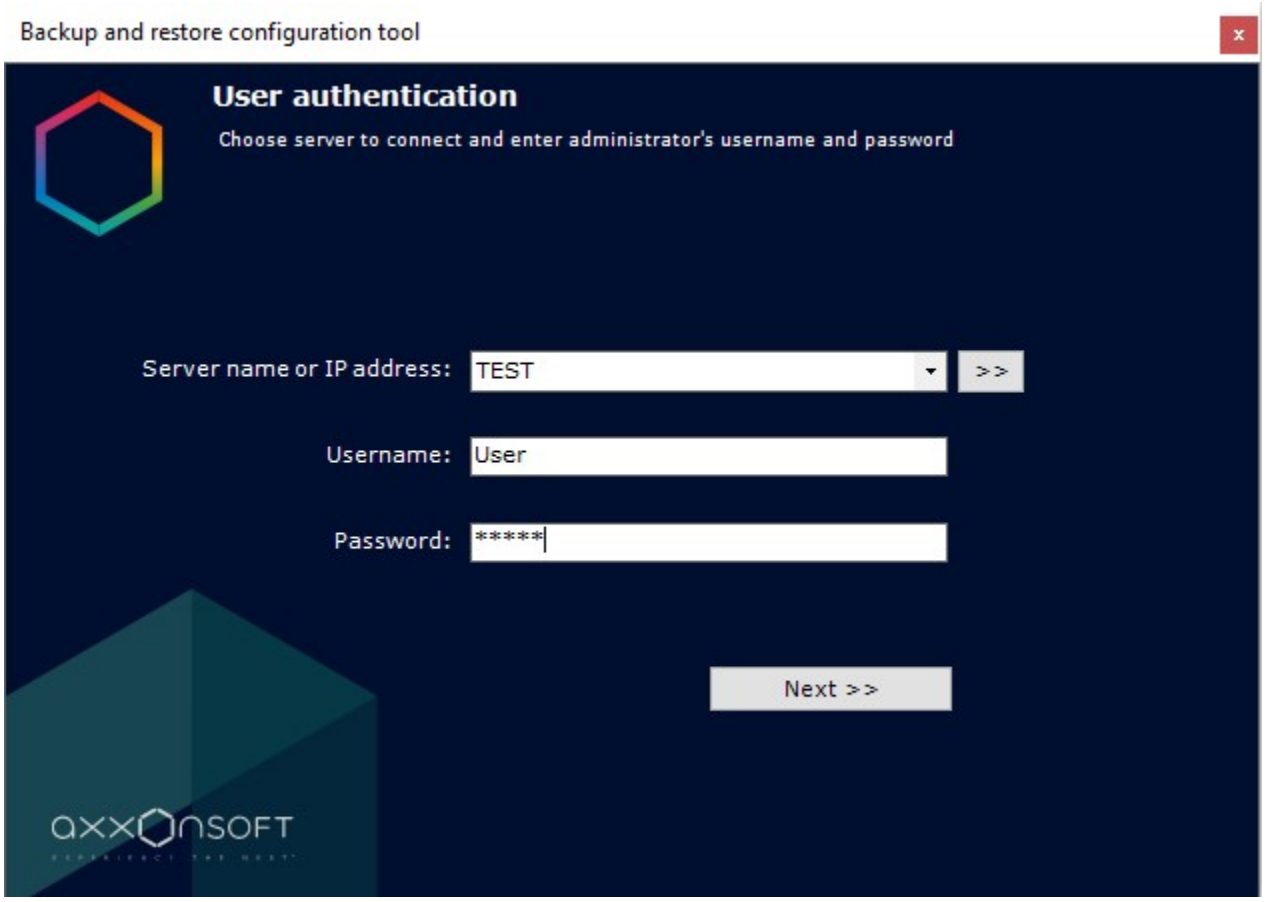
Starting and quitting BackupTool.exe

Start BackupTool.exe from **Start** -> **All Programs** -> **Axxon One** -> **Utilities** -> **Backup and restore**, or from the tray menu (see the Axxon One Tray Tool section).

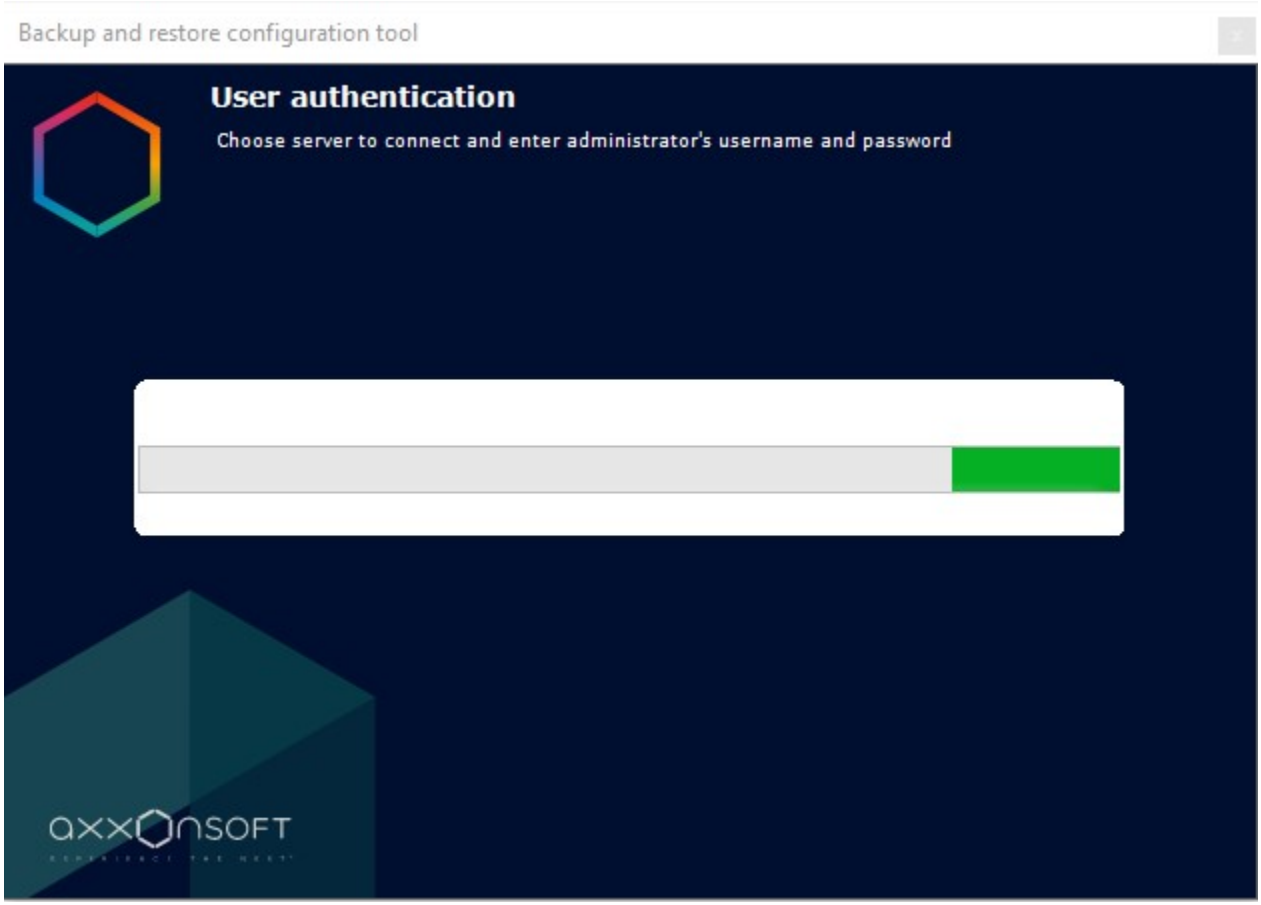
> **Note.**
>
> The BackupTool.exe executable is located at <*Axxon One* installation folder>\Axxon One\bin\.

After you perform this action, BackupTool.exe displays a dialog box.

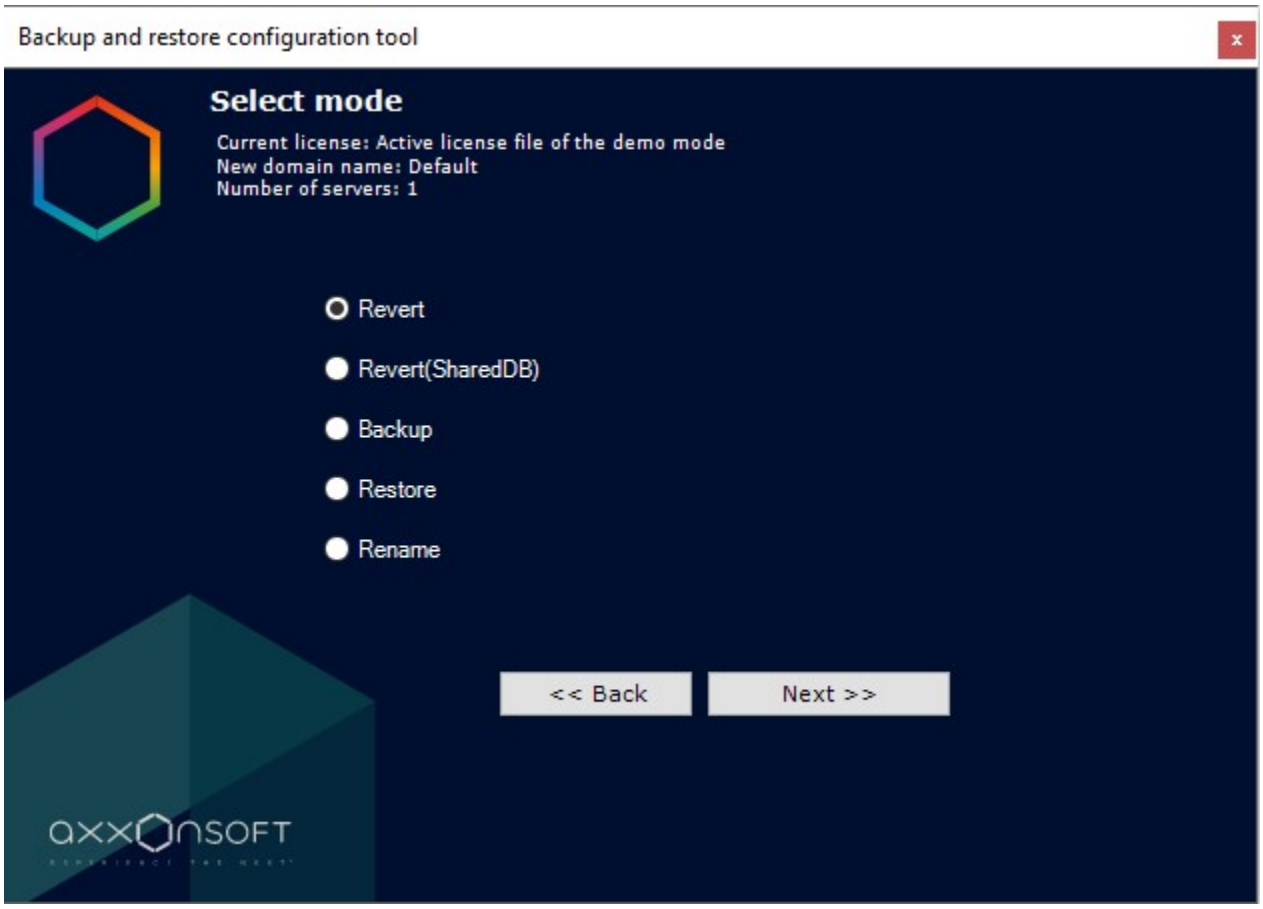
Then select the name of an Axxon-domain Server whose configuration you want to use and log in to it, using the name and password of an *Axxon One* administrator.



A progress indicator is displayed.



After loading is complete, the main page of the Backup and restore utility is shown.

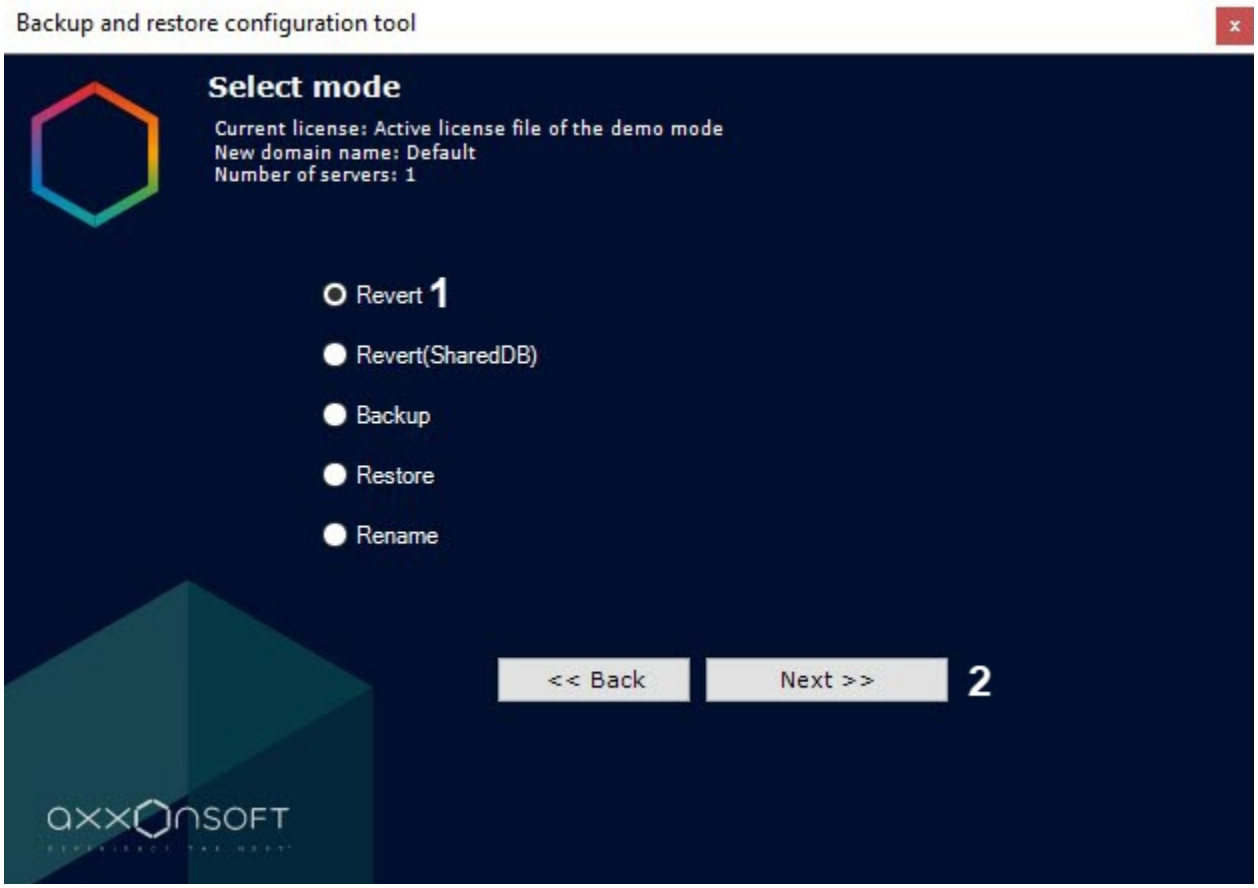


To quit BackupTool.exe, click the x button.

Roll back the local configuration to a selected restore point

The system creates a restore point when the local configuration of the Server is changed (creation/deletion/changing settings of any objects, linking cameras to different archives, etc.). You can roll back your configuration to any available restore point at any time.

To roll back, on the main page of the Backup and restore utility, set the switch to the **Revert** position (**1**). To continue, click the **Next >>** button (**2**).

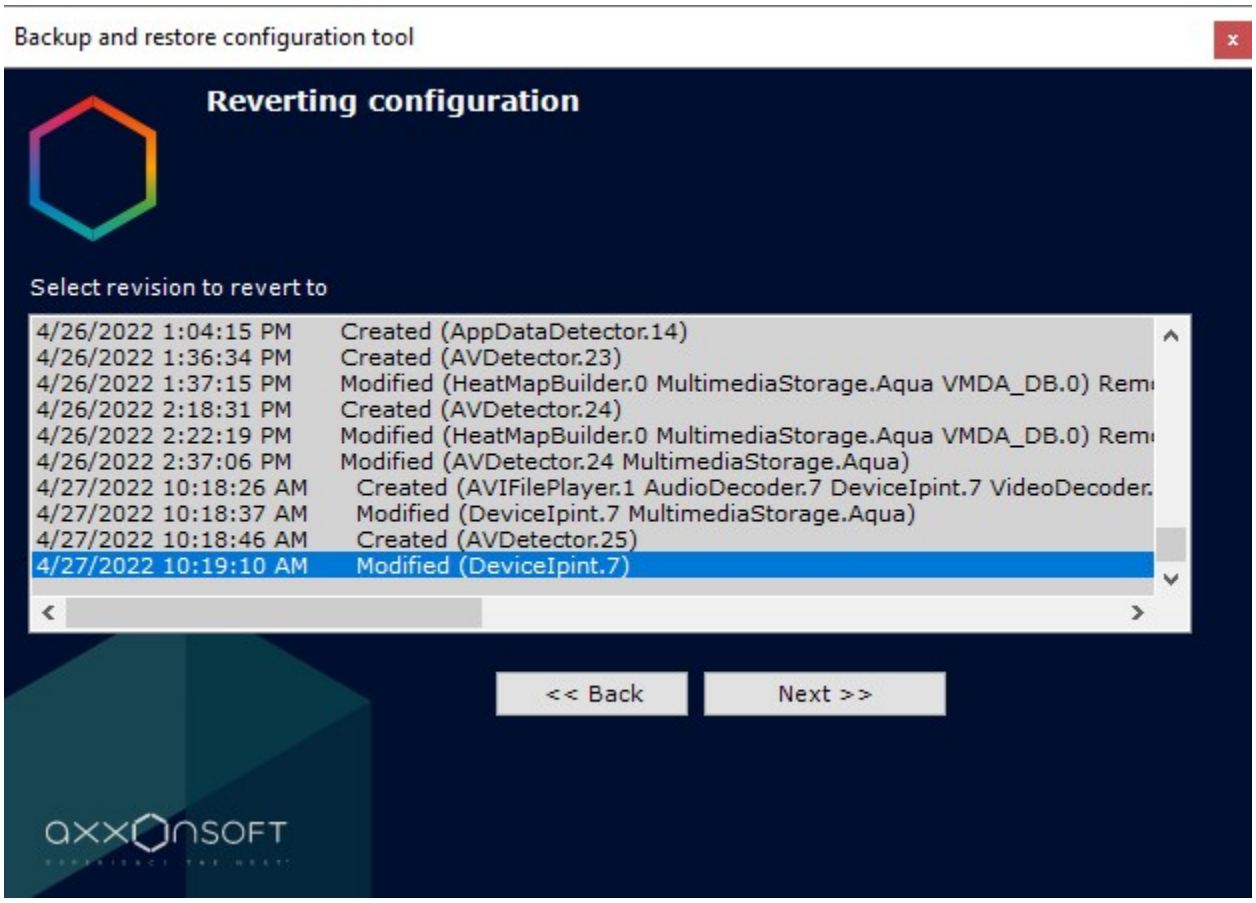


A window then opens, displaying a list of available restore points and their respective creation times, with a description of what was changed.

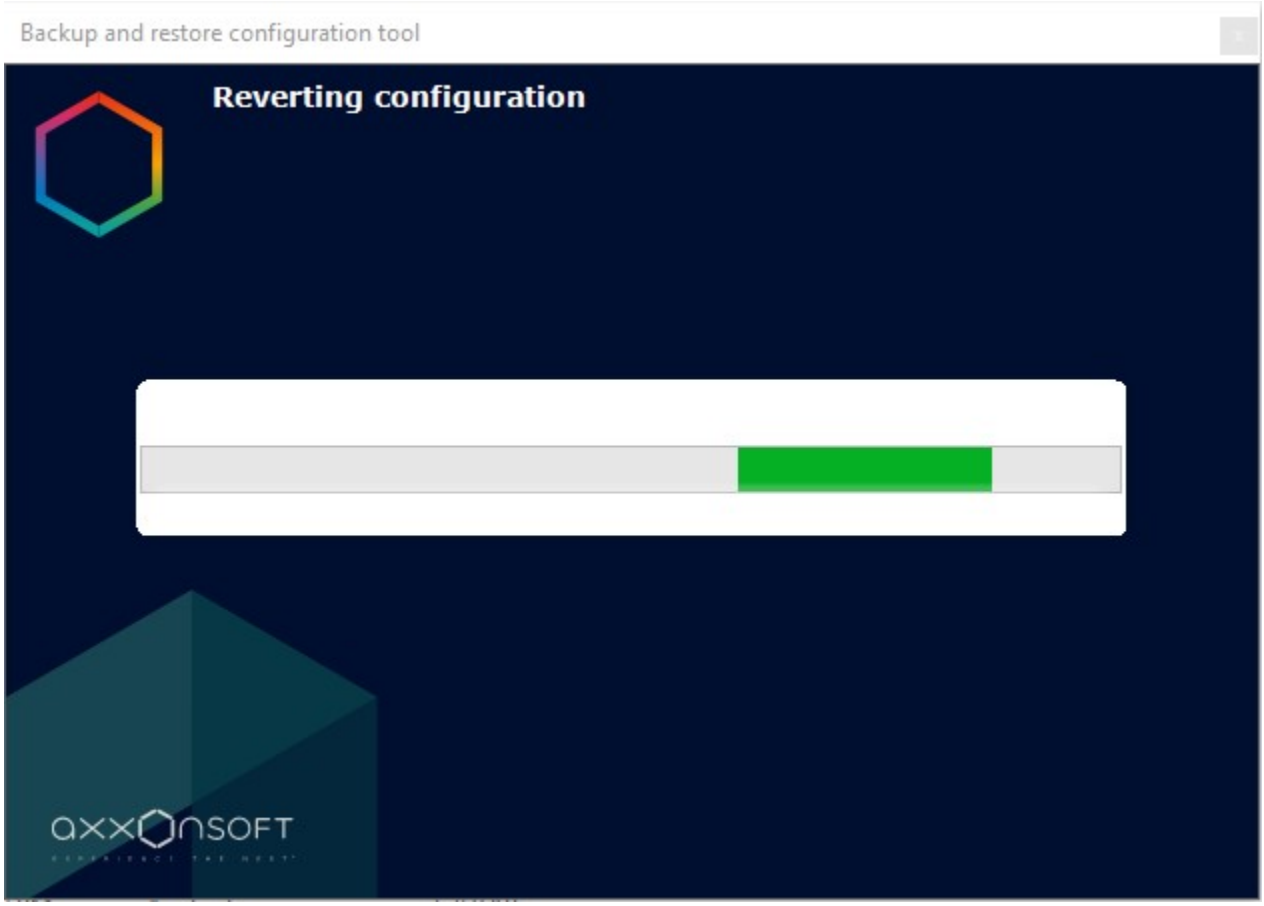
> **Note.**
>
> If multiple changes were made in a configuration but the **Apply** button was clicked only once, only one restore point is created in the list.

In the list, select the restore point to which you want to roll back. To continue, click the **Next** button.

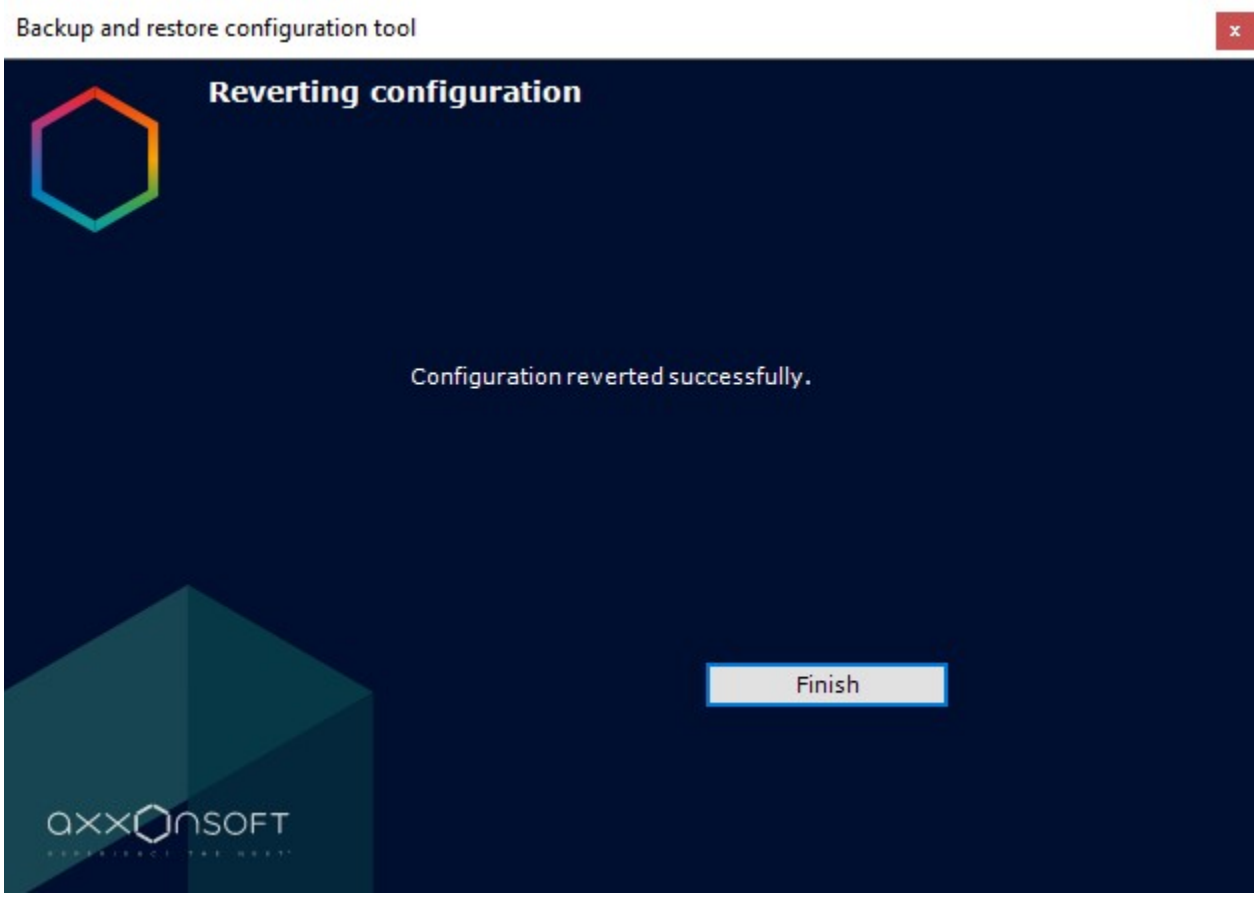
> **Note.**
>
> **Empty configuration** corresponds to when the system was first created.



Rollback of the configuration now begins.



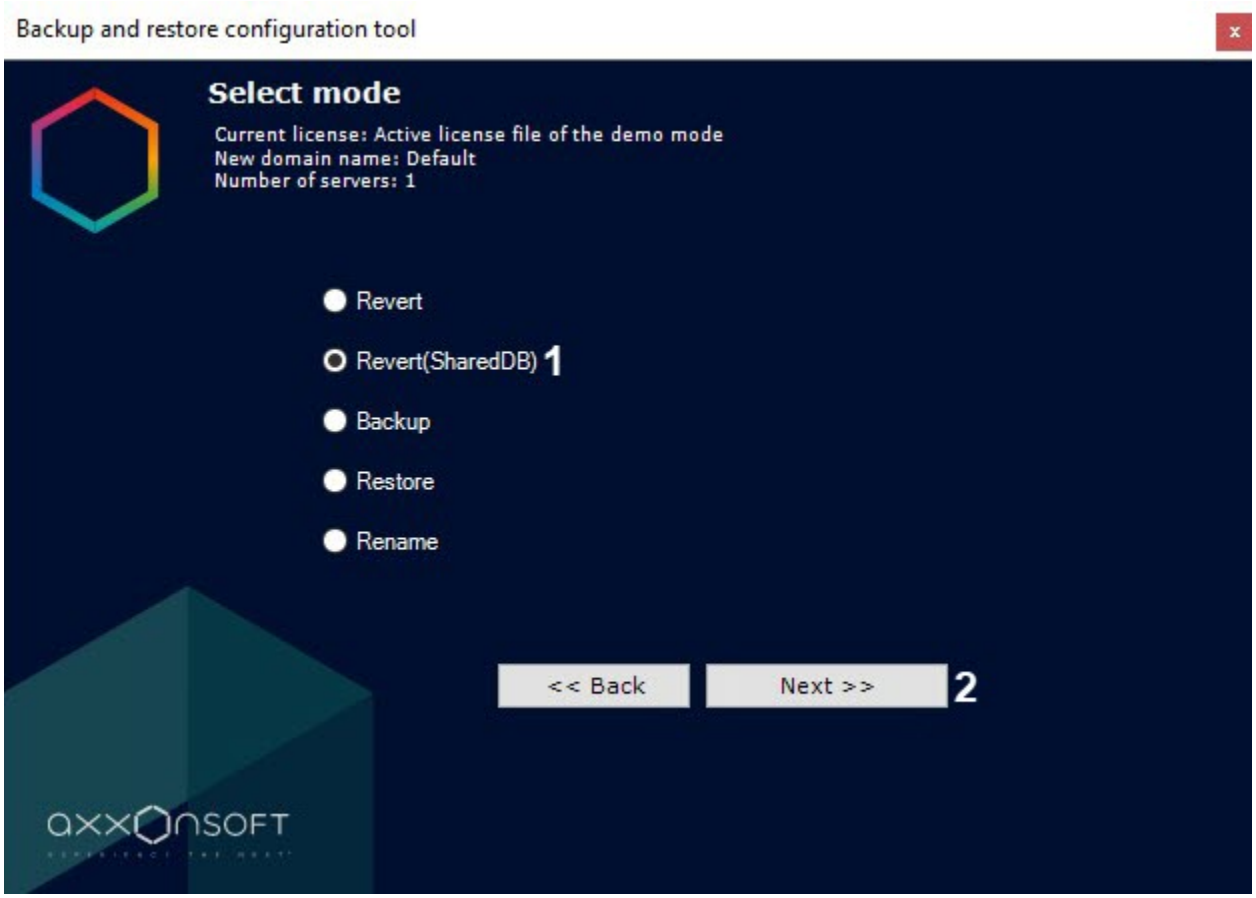
After the operation is completed, a message is shown to notify of successful rollback.



To close the window, click the **Finish** button.

Roll back the global configuration to a selected restore point

The system creates a restore point when the global configuration of the Axxon domain is changed (creation/deletion of roles, users, maps, layouts, etc.). You can roll back your configuration to any available restore point at any time. To launch the roll back process, go to the main page of Backup and restore utility (**1**) and set the switch to the **Revert (SharedDB)** position. To continue, click **Next >>** ( ).



Further steps are the same as for rolling back the local configuration (see Roll back the local configuration to a selected restore point).

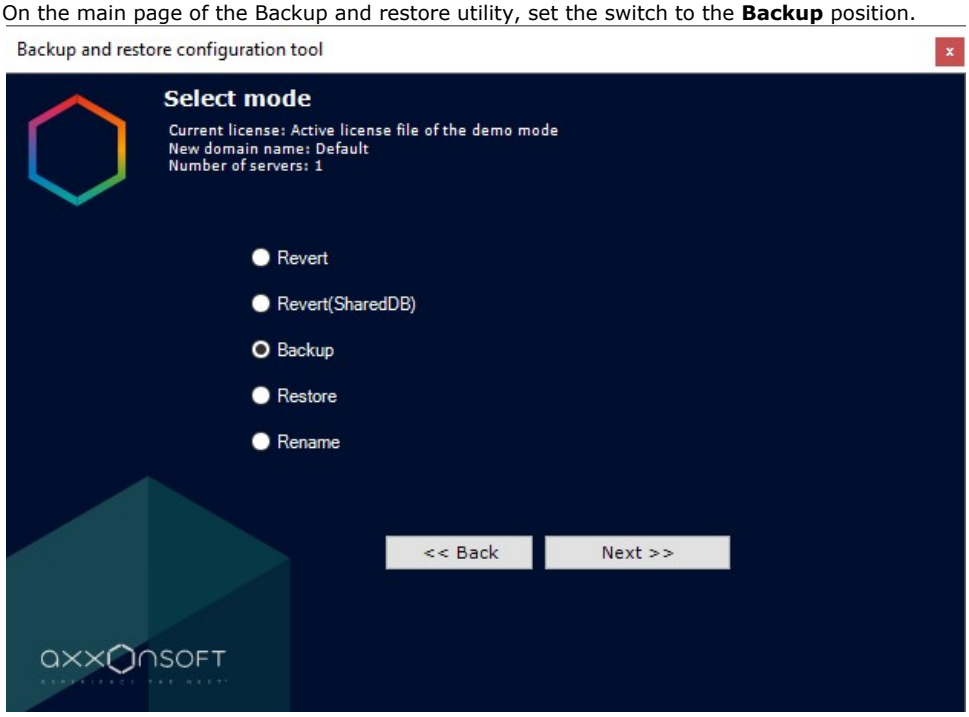
Configuration backup

Backing up a configuration involves creating and saving copies of the license key, domain structure, all created objects along with their parameters and relationships with history of changes, as well as database containing users, groups, passwords, and layouts.

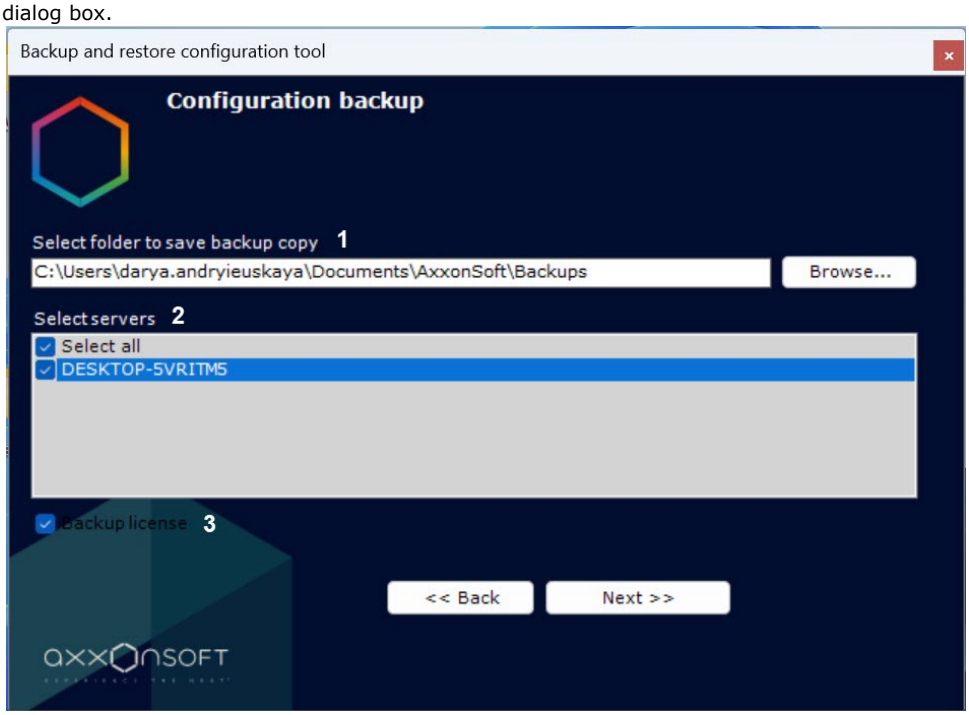
> **Attention!**
>
> We recommend you to back up your configuration after any major change in system configuration.

To create a backup of the system configuration:

1. On the main page of the Backup and restore utility, set the switch to the **Backup** position.

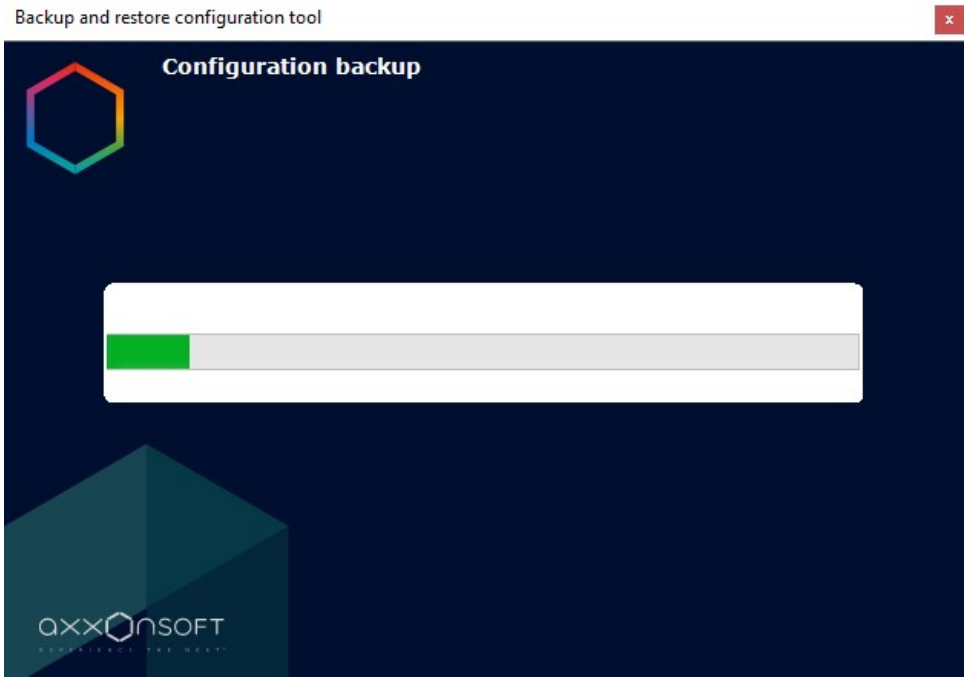


   A window then opens for configuring backup options.
2. In the field (**1**), specify a folder for saving the backup. The default folder is C:\Users\username\Documents\Axxonsoft\Backups\. To switch to a different folder, click **Browse** and select a folder in the dialog box.

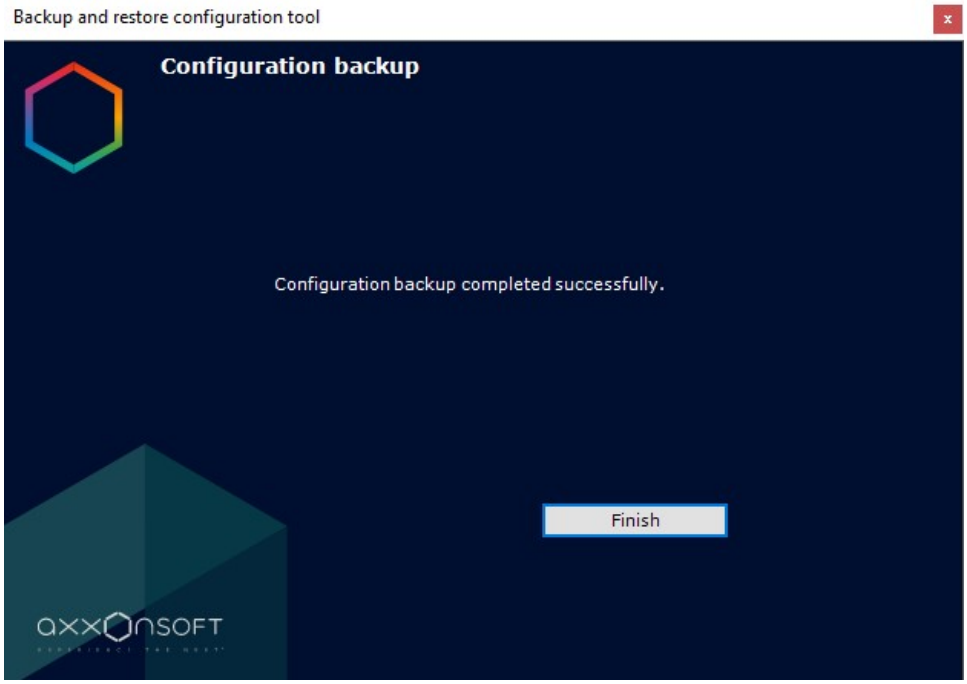


> **Note**
>
> For each copy of the backup configuration, a separate folder is created. The folder name contains the date and time of the backup copy and has the following format: YYYYMMDDHHMMSS. The default time zone is UTC + 0

3. In the **Select servers** field (**2**), select servers for creating the backup. You can select multiple servers. To select all servers, set the **Select all** checkbox.
4. Set the **Backup license** checkbox (**3**) to save the license key to a configuration backup. When restoring a copy of the configuration, it will be possible to restore the configuration with the license key. If you do not restore the configuration with the license key, the system will work in demo mode.
5. Start the backup process by clicking the **Next** button.
   Progress information is shown in the following window.



6. When the backup is complete, a window notifies of successful copying.



7. To close the window, click the **Finish** button.

A backup of the configuration has now been created.

Configuration restore

Attention!

If the backup copy does not match the current version of the product (including the build number), then critical errors may occur in the system during the configuration restore, and the configuration restoration process will be completed incorrectly.

Attention!

We can guarantee that your configuration will be fully recovered if:

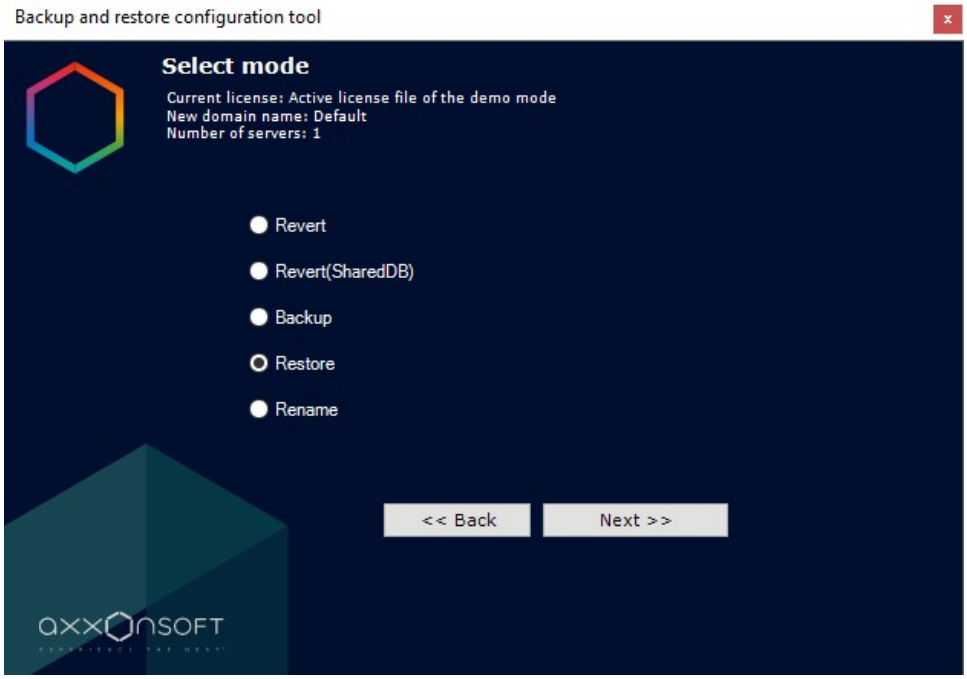
- the backup was created on the same software version (including the build number);
- the backup was created on the same PC, if licensing without the Guardant key was used (see Licensing methods).

The information about the product version and the PC's HID can be found in a JSON file in the saved configuration folder.

To successfully restore a configuration, please ensure that the current Server name is exactly the same as the Server name in the backup configuration.

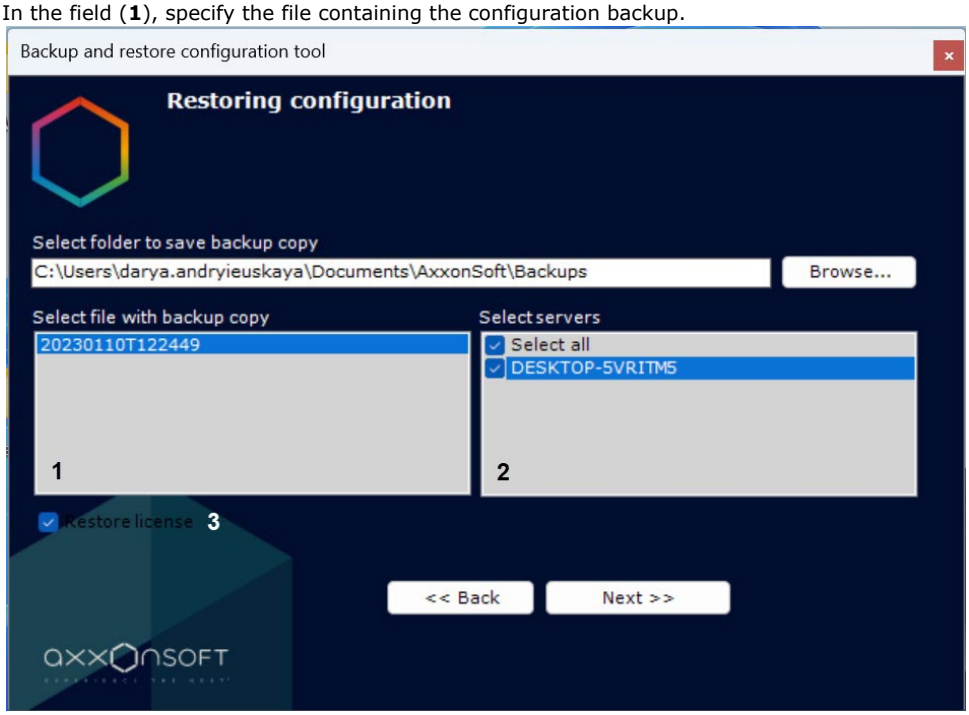
To restore a configuration:

1. On the main page of the Backup and restore utility, set the switch to the **Restore** position.

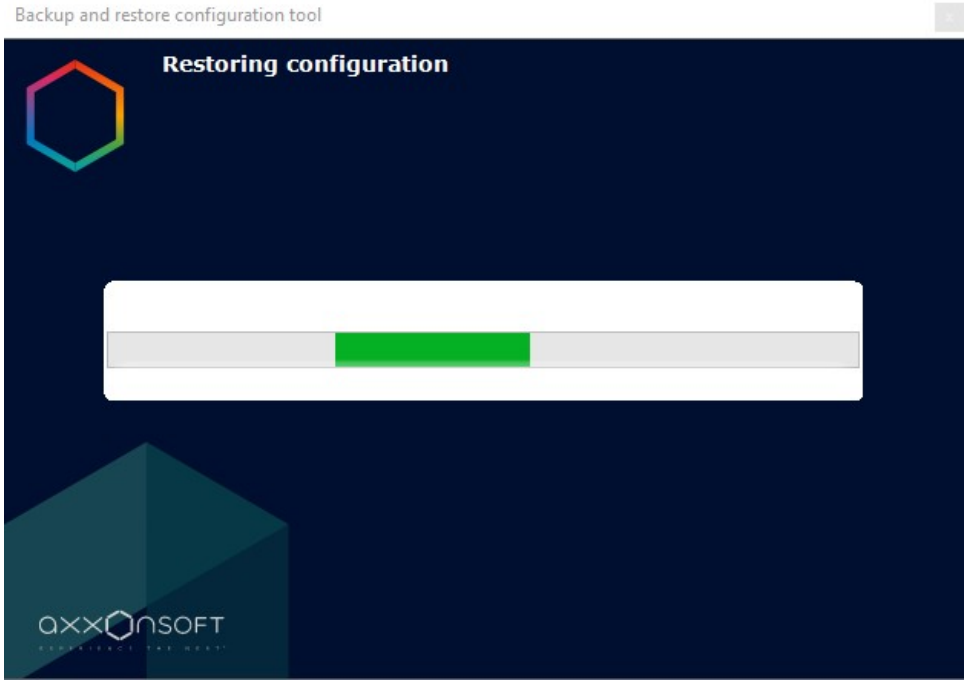


A window then opens for configuring restoration of the configuration.

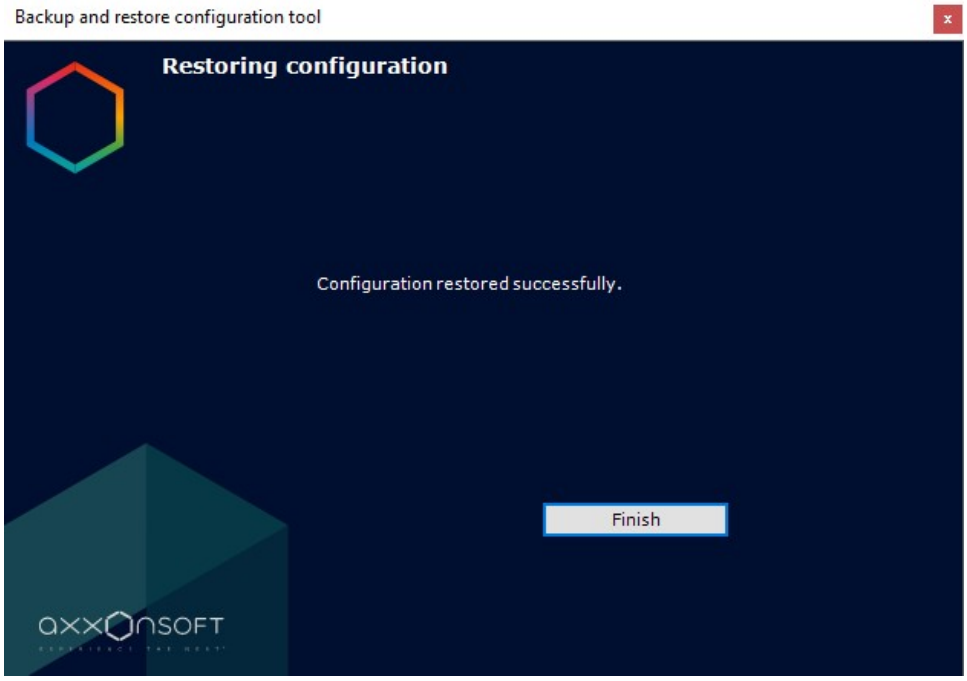
2. In the field (**1**), specify the file containing the configuration backup.



3. After the file is opened, the servers on the current domain are displayed in the other field (**2**). You can select a server in the list only if it is on the domain and the open file contains the corresponding backup.
4. Set the **Restore license** checkbox (**3**) to restore the license key that was saved at the configuration backup stage (see Configuration backup). If you do not restore the license, the system will work in demo mode
5. To start restore, click the **Next** button.
   Progress information is shown in the following window.



6. When restore is complete, a message informs of successful completion.



7. To close the window, click the **Finish** button.

Configuration restore is now complete.

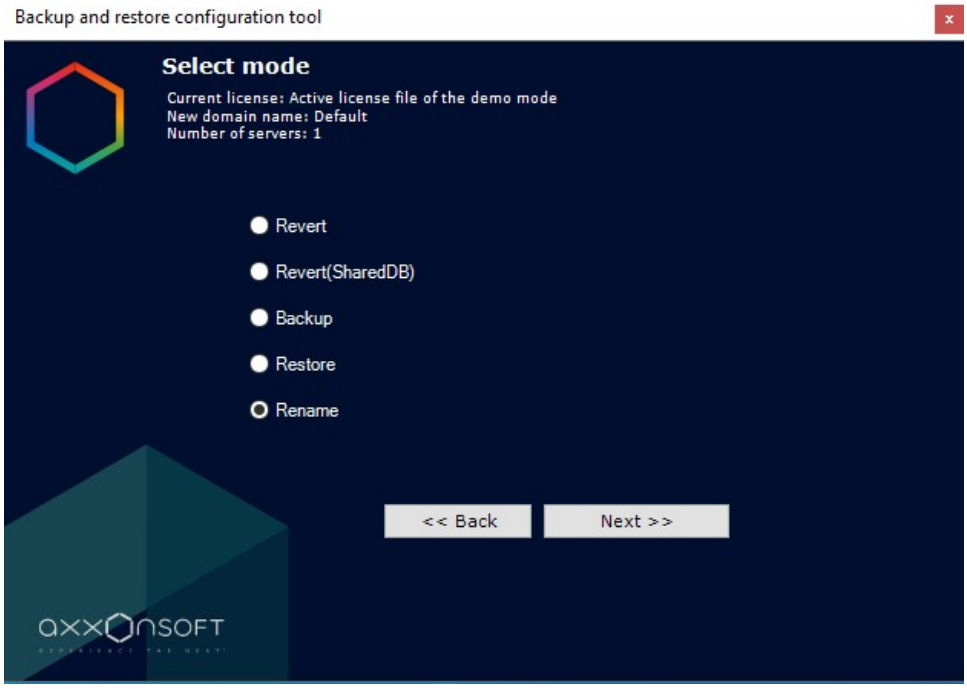
> **Attention!**
>
> The *Axxon One* Server must be restarted after restoring a configuration.

Changing the Server name

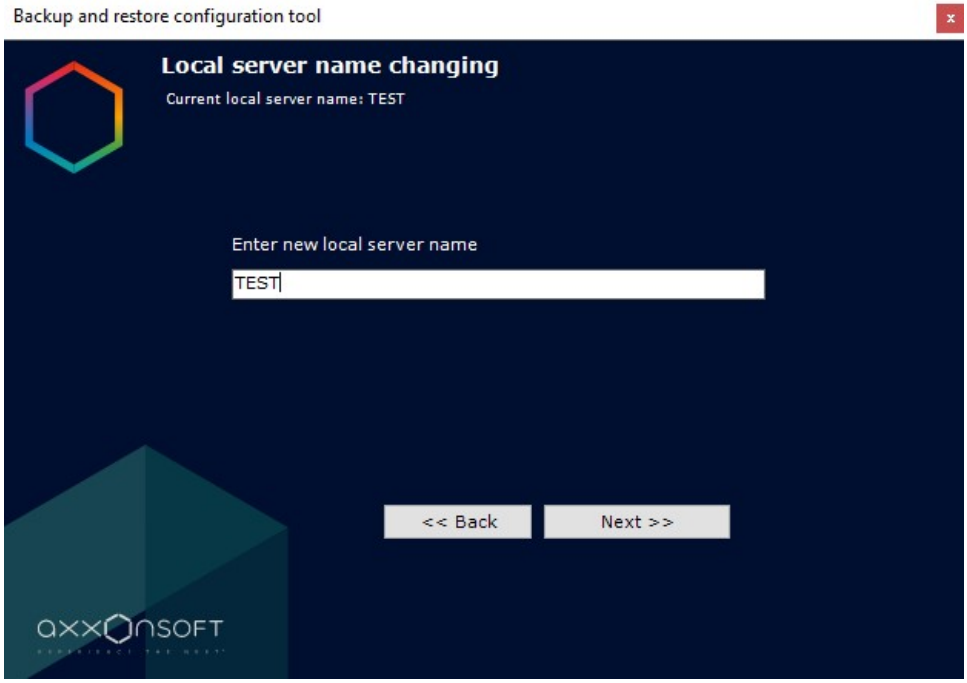
To change the local Server name using the Backup and Restore Utility, do the following:

> **Attention!**
>
> After this command is completed, the Server is excluded from Axxon-domain. You will not be able to access the archive. All maps, automatic rules and macros will be deleted. The cameras of the renamed Server will be deleted from the layouts.

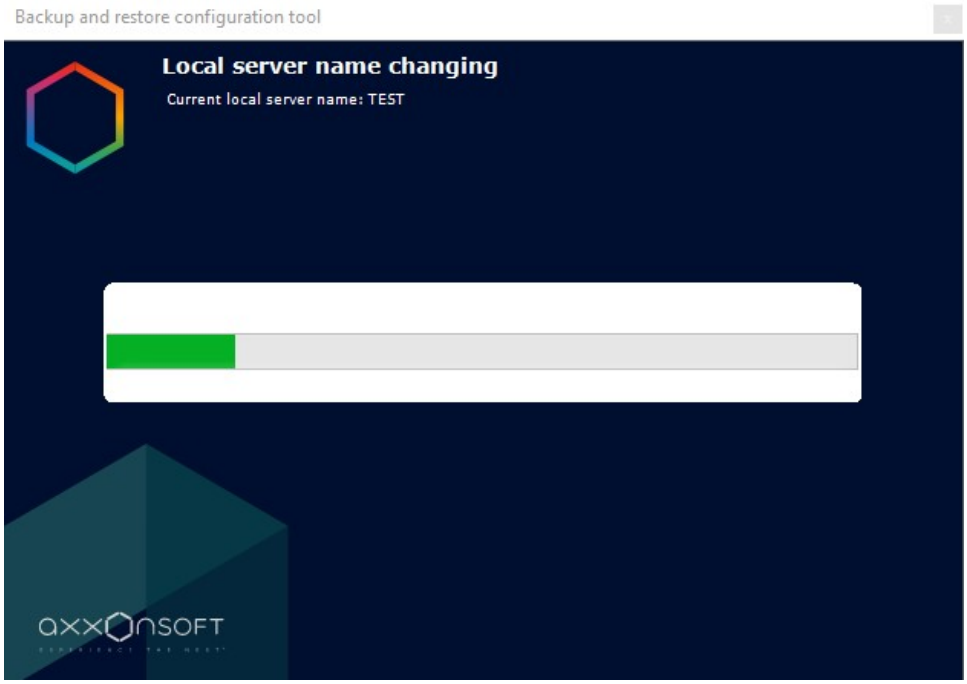
1. Connect to the Server that requires a name change (see Starting and quitting BackupTool.exe).
2. Select **Rename** and click the **Next** button on the Utility main page.



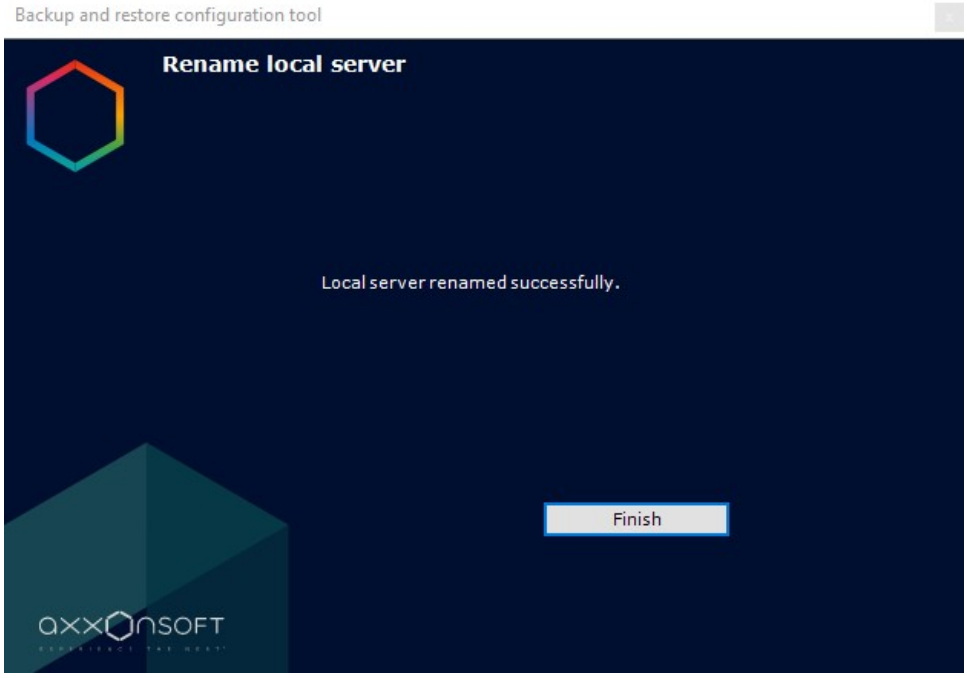
3. Enter the new Server name and click the **Next** button.



The Server name change process will start.



If the operation completes successfully, a notification message will appear.

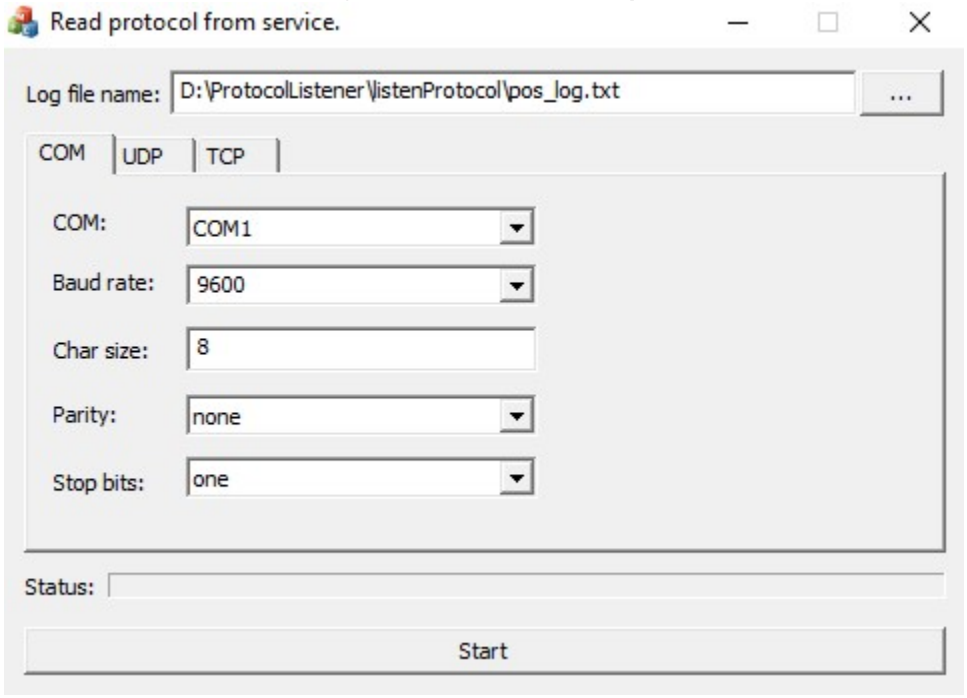


Server name change is complete.

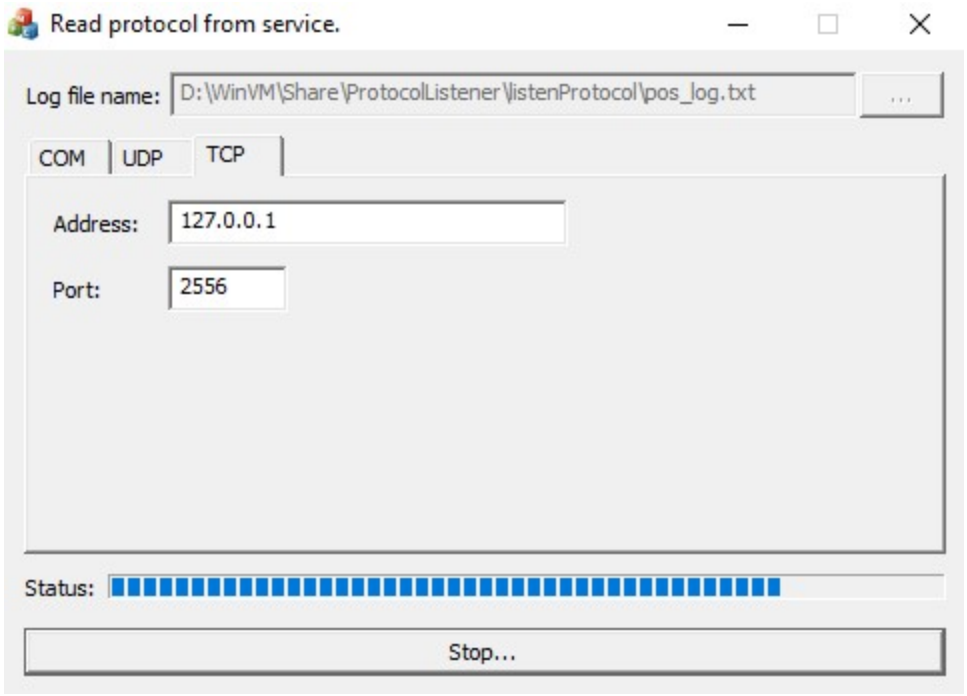
POS-terminal log collection utility

To collect information from the POS-terminal using a special utility, do the following:

1. Disable the Event Source object (see Configuring POS devices) and shutdown the Server (see Shutting down a Server).
2. If the POS-terminal supports data transmission via Ethernet or via the COM port, download the POS Terminal Data Collection Utility at the AxxonSoft website.
3. Unpack the archive.
4. Connect the POS-terminal to the computer.
5. Run the ProtocolLicenser.exe utility executable file. The **Read protocol from service** window opens.



6. In the **Log file name** field, specify a path to the folder where the file with the required information will be saved. By default, the file is saved in the same folder where the archive with the utility was unpacked.
7. If the POS-terminal is connected to the computer via the COM-port, specify the connection parameters in the **COM** tab.
8. If the POS-terminal is connected to the computer via Ethernet, specify the connection parameters for the TCP or UDP protocol in the corresponding tab.
9. Click the **Start** button to start log collection.
10. Start using the POS-terminal, i.e. issuing receipts. Execute all possible operations including Cancel, Return, etc. Process of log collection is displayed in the **Status** progress bar.



To finish log collection, click the **Stop** button.

After executing all possible operations on the POS-terminal, send the log file with copies of receipts to AxxonSoft.

Attention!

If the log file of the POS-terminal requires software processing, then provide AxxonSoft with the protocol description. The POS-terminal manufacturer can give you the protocol description.

Console utility for working with archives

vfs_format.exe is a console utility for working with *Axxon One* archives. The utility is located in the <*Axxon One* installation directory>\bin> folder.

Attention!

- For the correct operation of the utility, you must remove the corresponding archive volume in *Axxon One* without removing the archive files (see Removing archive volumes).
- Run the command line as Administrator.
- To run the utility on Linux OS, run the following command: ngprun start_app vfs_tools + arguments. To open the argument list, run the vfs_tools --help command.
- To log error messages, you must add the path for the log file at the end of each query.
  For example, vfs_format.exe --volume S:\FILEONE.afs --fill G:\ --log-level=100 > S:\log.txt.

The utility contains the following parameters:

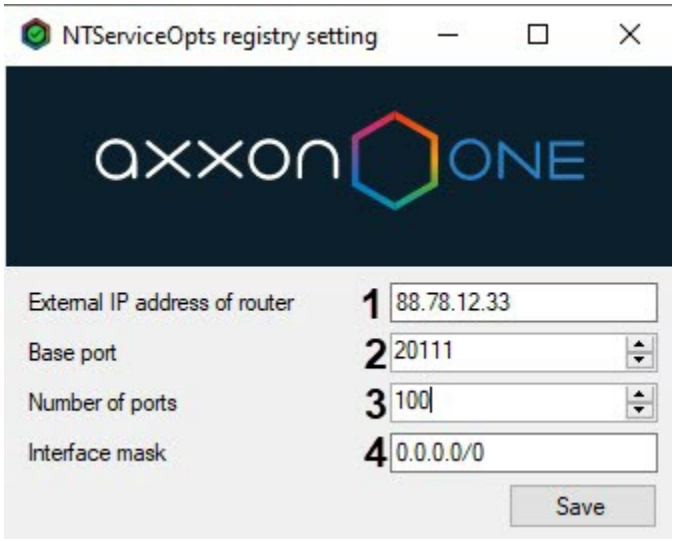
Parameter	Description
--help	Help window
--volume	Archive volume path. The basic parameter must always be present in the query. For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs (for the archive volume as a file) or vfs_format.exe --volume D:\ (for the archive volume as a disk).
--fill	Multiple filling of an archive with data from another archive. The system fills up a destination archive or a volume with multiple copies of a source archive or a volume. For easier timeline handling, each new copy is written with one minute offset. For example: vfs_format.exe --volume S:\FILEONE.afs --fill G:\
--cache-to-memory	Copy an archive to RAM and further copy to a destination archive. Use with the --fill parameter. This parameter is valid only for archives that could fit to RAM. For example: vfs_format.exe --volume S:\FILEONE.afs --fill G:\ --cache-to-memory
--dump	Collect service information about the archive volume in a TXT or XML file. For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs --dump C:\DumpArc.txt
--dump-meta	Collect service information about the archive volume metadata in a TXT file. For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs --dump-meta C:\DumpMetaArc.txt
--dump-fullness	Collect service information about the archive fullness in a TXT file. For example: vfs_format.exe --volume C:\archiveAliceBlue.afs --dump-fullness C:\DumpFullnessArc.txt
--expand	Specify the new size of the archive volume in blocks. By default, the size of one block is 4MB, if the --format parameter was not applied. This parameter is relevant only for the archive volume as a file. For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs --expand 128
--size	Specify the new size of the archive volume in megabytes. This parameter is relevant only for the archive volume as a file. For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs --size 4096 **Attention!** The value of the --size parameter must be a positive integer. The value of the parameter must not contain spaces, characters, or punctuation marks.

--format	Split the archive volume into blocks of the specified size (in megabytes). For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs --format 16
--copy	Copy archive volume. Specify the path and name of the new archive file. If the archive volume is copied as a disk, create a partition without formatting, larger than the copied volume. If you have a smaller partition, then only the most recent entries are copied. For example: vfs_format.exe --volume D:\archiveAntiqueWhite.afs --copy C:\NewArc.afs
--skip-bad-block	Skip the bad blocks when copying the archive volume. This parameter is used only together with --copy. For example: vfs_format.exe --volume D:\archiveAliceBlue.afs --copy C:\NewArc.afs --skip-bad-block
--modify-corrupted-flag	Enable/disable reindexing of the archive volume. **1**—enable reindexing, **0**—disable. For example: vfs_format.exe --volume D:\archiveAliceBlue.afs --modify-corrupted-flag 1
--build-meta	Launch the process of metadata generation of an archive volume (including timeline markers and video footage size per channel). For example: vfs-format.exe --volume D:\ --build-meta **Attention!** Processing large archives may take significant amount of time.
--clear-meta	Delete metadata of the archive volume. For example: vfs-format.exe --volume D:\ --clear-meta
--clear-data	Delete the archive volume service information (does not operate without the **from** and **to** arguments). For example: vfs_format.exe --volume C:\archiveAliceBlue.afs --clear-data --from 20220210T110000 --to 20220210T114000. --from and --to are used to set the UTC time intervals in the ISO YYYYMMDDThhmmss format. Then you must confirm the deletion
--log-level	Set the logging level for this action. Available values: • 0—OFF; • 10—ERROR; • 20—WARN; • 40—INFO (recommended); • 50—DEBUG; • 60—TRACE; • 100—ALL
--channel	Specify the archive channel. For example: vfs_format.exe --volume=Q:/archiveAliceBlue.afs --channel=E7C79FA3-E0D4-B6CD-9307-6C24E96C305E You can force masking of the blocks for certain archive channels. **Attention!** Masking of blocks is available only if the archive volume is disabled. For example: vfs_format.exe --volume=Q:/archiveAliceBlue.afs --channel=E7C79FA3-E0D4-B6CD-9307-6C24E96C305E --clear-from=20350101T000000 --clear-to=20370101T000000, where --clear-from—start interval in the YYYYMMDDThhmmss format, --clear-to—end interval in the YYYYMMDDThhmmss format

--recover	Recover the last recording layer after formatting the archive. This parameter is relevant only if there were records after the last formatting. For example: vfs_format.exe --volume E:\ --recover
--recover=2	Recover the last recording layer after formatting the archive. For example: vfs_format.exe --volume E:\ --recover=2 after the archive formatting, or vfs_format.exe --volume E:\archiveAliceBlue.afs --recover=2 after the disk formatting

Network settings utility

You can launch the network settings utility from the Windows Start menu: **Start All Programs Axxon One Utilities Network settings**.



The utility allows you to:

1. Set the external IP address or DNS name of the router if the Server is located behind the NAT (**1**).

   > **Note**
   >
   > You may set multiple interfaces using a comma separated list, such as: "IP Address1 or DNS Name1, IP address2 or DNS Name2".
   >
   > For example: 88.78.12.33, ExampleAxxon.ddns.net.

2. Set the port range for operation of the *Axxon One* Server (**2**-**3**). To do this, specify the beginning of the range and the number of ports. The number of ports should not be lower than 20.

   > **Attention!**
   >
   > Within an Axxon Domain, the port ranges of Servers should not overlap.

   > **Note**
   >
   > The number of ports that you select affects the scalability of the system. Keep the following in mind when specifying the number of ports:
   >
   > - **6 ports** is a minimum system requirement for machines with *Axxon One*.
   > - In a 64-bit configuration, for any number of cameras, **6 ports** are required.
   > - **2 ports** are required to write to the **archive**.
   > - To use the Object Tracking database (track recording), **1 port** is required.
   > - To use basic detection tools, **2 ports** are required.
   > - To use Scene Analytics, **2 ports** are required.
   > - To use E-mail- (through SMTP) or server audio notification **1 port** is required .

3. Restrict the visibility of Servers from various networks in the Servers list during the *Axxon One* setup (**4**). Possible values:
   a. "0.0.0.0/0" – servers from all networks will be visible.
   b. "10.0.1.23/32,192.168.0.7/32" – only Servers from specified networks will be visible.
   c. "127.0.0.1" – only Servers from the local network will be visible.

After you save the settings, the Server will be restarted.

Appendices

Appendix 1. Glossary

Active viewing tile – viewing tile currently in use by the user.

AWS (automated workstation) – security system user workstation, a minimally equipped personal computer with *Axxon One* software installed.

Archive – all audio/video files stored on a hard disk that can be played and exported to supported formats.

Default archive of a video camera – the archive to which images from a given video camera are recorded during user-initiated alarms.

Audio detection tool – a detection tool used to analyze the audio signal from a microphone.

Audio recording: 1. the process of recording a digitized audio signal on a hard disk; 2. audio data stored in a specific format on a hard disk.

The audio subsystem encompasses all the tools that provide for the collection of audio data, its processing, and its storage on media.

Video detection tool – a detection tool used to analyze the video image from a video camera.

Video recording: 1. the process of recording a digitized video signal on a hard disk; 2. video information stored in a specific format on a hard disk.

Video camera: 1. source of a video signal; 2. a system object displaying the properties of an installed video camera and controlling its operation.

The video subsystem encompasses all the tools that provide for the acquisition of video data, its processing, and its storage on media.

Timeline – an interface object used to search for video recordings and navigate an archive.

Input: 1. a physical device intended for receiving information on the status of an object; 2. a system object that displays the properties of an installed Input.

Scene Analytics detection tool – a detection tool used to analyze the situation in a camera's field of view according to set criteria.

Audio signal detection – a detection tool is triggered by an increase in the signal/noise ratio above a set level.

Loss of quality detection – a detection tool is triggered by a loss of quality in the video image from a camera.

Position change detection – a detection tool is triggered by a substantial change in the background of a video image indicating a change in the position of the camera in space.

Object disappearance detection – a detection tool is triggered by the disappearance of an object in a set area of a video camera's field of view.

Abandoned object detection – a detection tool is triggered when an object remains motionless in a detection zone for a prolonged period.

No Signal detection – a detection tool is triggered by the absence of an audio signal from an audio device.

Line Crossing detection – a detection tool is triggered when the trajectory of an object crosses a virtual line in a video camera's field of view.

Object appearance detection – a detection tool is triggered by the appearance of an object in a set area of a video camera's field of view.

Stopping detection – a detection tool is triggered by the cessation of motion in a set area of a video camera's field of view.

Noise detection – a detection tool is triggered by an decrease in the signal/noise ratio below a set level.

Axxon Domain – a selected group of computers on which the server configuration of the *Axxon One* software package is installed. Linking the servers in a group makes it possible to set up interaction between them, thus organizing a distributed system.

Detection zone – the area of a video image processed by a detection tool is triggered.

Interface cable – cable used to connect two or more devices together for data transfer.

Interface object – a system object used for interaction between the user and software (data input/output).

Client – designation for a personal computer on which *Axxon One* software is installed (or will be installed) as a Client. Designation for the graphical shell of the *Axxon One* software package.

Slideshow – automatic switching of user layouts, or of viewing tiles in a single layout if working with standard layouts.

Licensing – regulating and setting the terms for usage of AxxonSoft software modules.

Detection zone: 1. the area of a video image processed by a detection tool is triggered; 2. a tool which allows the user to mark out an area of the video image which is not to be processed by a detection tool is triggered.

Microphone: 1. a source of audio signals; 2. a system object used to manage the parameters of audio signal reception.

Video surveillance monitor – an interface object used to manage the user interfaces of the *Axxon One* software, e.g., layouts, viewing tiles, various panels and context menus, etc.

Viewing tile – interface object displaying the video stream coming from a certain video camera and enabling control of that video camera.

Dial panel – panel (part of the PTZ control panel) used to dial a preset.

Archive navigation panel – all interface objects used to work with an archive, e.g., timeline, list of alarm events, etc.

Control panel – panel made up of tabs accessible to the user, used to navigate from one group of interface objects to another.

Playback control panel – panel containing buttons to control playback of video recordings: Play, Pause, Go to next video recording, etc.

PTZ control panel – all interface objects used to control a certain PTZ device.

Layout control ribbon – panel containing tools to create, edit, and manage layouts.

PTZ device – a system object displaying the properties of an installed PTZ camera device.

> **Note**
>
> Also used to designate a physical device

The PTZ subsystem encompasses all the tools that provide for remote control of a PTZ device and the lens of a video camera.

The analytics subsystem encompasses all the tools that provide for automatic analysis of incoming video and audio data.

The Forensic Search in archive subsystem is a set of tools for searching video recordings in the archive by using video image metadata.

The Output subsystem encompasses all the tools that provide for the triggering of an execution device connected to the embedded Output port of a video camera or IP server when a detection tool is triggered (including one which processes the embedded Input of a video camera or IP server) is triggered.

The notification subsystem encompasses all the tools that provide for notification of the user about events which have occurred in the system.

Event registration subsystem – all the tools that provide for the collection of data about system events, processing, and its storage on media.

Pre-alarm recording is the period of pre-event recording that will be added to the beginning of an alarm event recording.

Preset – preprogrammed positioning of a PTZ device.

Software package – all software and hardware tools used together to build a security system.

Software module – a program or functionally complete component of a program used to perform a specific functional task (perform a user function).

Layout – preserved positioning of viewing tiles relative to each other.

Distributed system – a group consisting of several interacting *Axxon One* servers (up to four) and clients (unlimited number). *Axxon One* servers are linked within an Axxon Domain.

Output: 1. a physical device/electromechanical switch; 2. a system object that displays the properties of an installed Output.

Server – designation for a personal computer on which the Server configuration of *Axxon One* software is installed (or will be installed).

Security system – a set of devices used for video surveillance, audio surveillance, and object recognition, all controlled by the *Axxon One* software system.

The system log is a log containing system information on events, including system error entries.

Object tracking – a function which allows an operator to visually track the movement of objects in a camera's field of view.

Alarm flag – the flag symbol designating either the moment an alarm event began or a certain moment before the beginning of an alarm event.

Color coding – software-based graphical notification to a security system operator about the current status or operating mode of system objects (equipment, software modules).

Facial vector – mathematical representation of a facial image created upon face capture.

Captured faces – images detected on video by the facial detection tool.

Recognized faces – captured faces that reach a pre-defined degree of similarity against reference facial images.

Reference faces – pre-defined facial images to compare captured faces to.

Appendix 2. Known issues in the Axxon One Software Package

Possible errors during installation

On the page:

- Error connecting to the Postgres Database
- Error installing Drivers Pack
- Window 10 OS installation error
- Server error on Windows 11 OS and Windows Server 2019 OS
- Guardant drivers compatibility issue
- An error occurred when installing on Windows with the language pack Norsk (bokmål)
- Error uninstalling Axxon One on systems with Videoinspector installed

Error starting NGP Host Service

If port 20111 is busy during installation of *Axxon One* (for example, because of nethost.exe processes that have not been unloaded since removal of the previous version), an error message regarding the launch of NGP Host Service appears.

To continue installation, free up port 20111 and try again.

Error connecting to the Postgres Database

After installation of the Postgres database, the *Axxon One* installer may quit prematurely. This situation may be associated with the inability of the installer to connect to the Postgres database, if the firewall is enabled. To prevent this, disable your firewall during installation.

> **Note**
>
> Disabling the firewall during installation can cause another problem—see No signal from video cameras and failure to connect to other servers.

Error installing Drivers Pack

In some cases, you may encounter errors while installing *Drivers Pack*:

```
Installation failed because the Universal C Runtime is not installed. Please run Windows Update and install all
required Windows updates(KB2999226). You can download the UCRT separately from here: 'https://support.microsoft.
com/en-us/kb/2999226'.
```

This can be solved by installing the Windows update KB2999226.

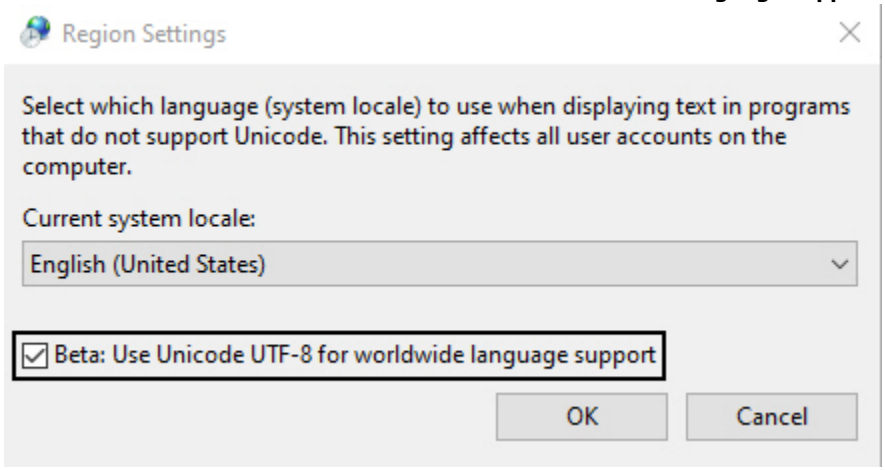
Window 10 OS installation error

When you install *Axxon One* on Windows 10.0.17763 and up you may see the Create Recovery Archive error message.

To fix the error, do as follows:

1. Go to Control Panel Clock and Region Region Administrative tab Change System Locale.

2. Deselect the checkbox **Beta: Use Unicode UTF-8 for worldwide language support**.



3. Reinstall *Axxon One*.

Server error on Windows 11 OS and Windows Server 2019 OS

On Windows 11 OS and Windows Server 2019 OS errors may occur in the Server operation when Guardant drivers are installed. It is recommended not to install Guardant drivers. Installation of Guardant drivers is disabled by default.

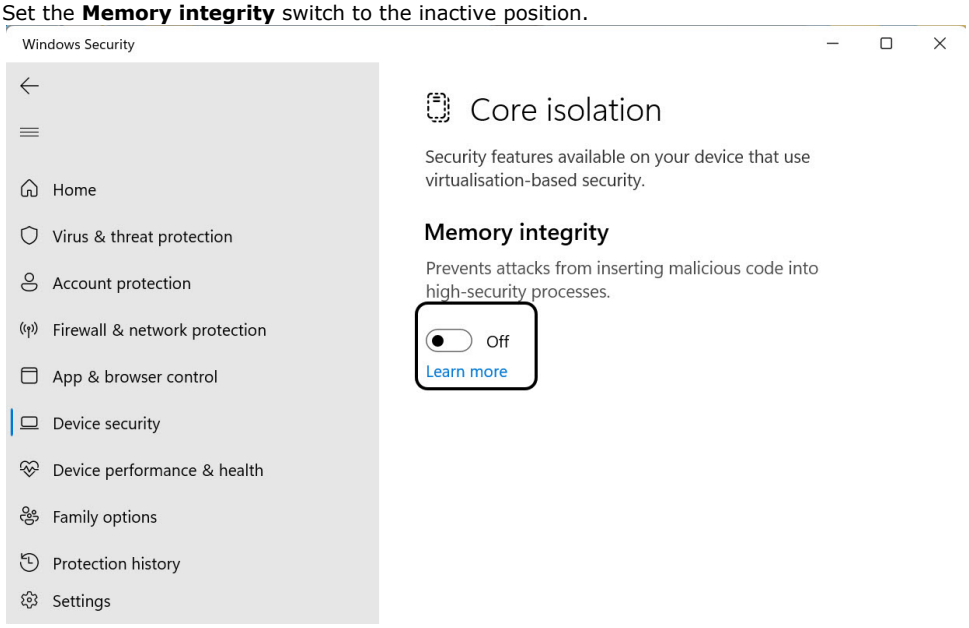
For the correct installation of Guardant drivers, it is necessary to disable the check of the drivers digital signature in the operating system and disable Secure Boot in BIOS.

Guardant drivers compatibility issue

When you install *Axxon One*, a Guardant driver compatibility issue may occur (**grdkey.sys** or **grdusb.sys** file error).

To fix the error, do as follows:

1. Disable **Memory integrity**:
   a. Open **Windows Security Center Device security**.
   b. In the **Core isolation** section, click the **Core isolation information** link.
   c. Set the **Memory integrity** switch to the inactive position.



   d. After you complete these steps, restart your computer to apply the changes.
2. Disable **Device Guard**:
   a. Using the command line, run the gpedit.msc command to launch the **Local Group Policy Editor**.
   b. Go to **Computer Configuration Administrative Templates System Device Guard** select **Enable virtualization-based security** on the right.
3. After you disable these options, restart your computer and reinstall the current version of Guardant drivers.

Attention!

If you use modern Guardant keys (Sign/Sign Net/Time/Code), you can contact the developer of the protected application and request to switch the key to driverless mode (see the official Guardant documentation). In this case, it will not be necessary to install the Guardant Driver on your computer to work with the key.

An error occurred when installing on Windows with the language pack Norsk (bokmål)

Installing the *Axxon One* Server on Windows with the language pack Norsk (bokmål) is not possible due to incompatibility with PostgreSQL.

You must install Norsk Language Pack (nynorsk).

Error uninstalling Axxon One on systems with Videoinspector installed

In some cases, uninstalling *Axxon One* may be impossible if *Videoinspector* is used.

To correctly uninstall *Axxon One*, first uninstall *Videoinspector.*

Possible Errors During Start-Up

The Client cannot be connected to the Server

If a "**Cannot find Server**" message appears after you connect to a Server, do the following:

1. Go to **Control Panel** -> **Regional Settings** -> **More**.
2. Change current language of non-Unicode applications to the one that is present in keyboard settings, and may appear in user name and folders.
3. Reboot the PC.

If a **Connection Error** message appears after you connect to a Server, do the following:

1. Go to **Local Security Policy interface**.
2. Select **Local Policies** -> **Security Settings**.
3. Turn off the following parameter: **System cryptography: use FIPS compliant algorithms for encryption, hashing, and signing**.

Launching the *Axxon One* software program with client logging enabled can take a long time when the ESET NOD32 Antivirus 4 **Real-time file system protection** mode is on.

To solve this problem, add the *Axxon One* installation folder and the folder with the client logs (<Letter of system disk>: \Users\<User>\Appdata\Local\AxxonSoft\Axxon One\logs) to the list of exceptions in ESET NOD32 Antivirus 4.

Possible Errors During Operation

On page:

- All video channels or archives stop working once the license maximum is reached
- No signal from video cameras and failure to connect to other Servers
- Incorrect display of Client interface elements
- Error creating new archives even when license restriction on total capacity is observed
- Axxon One VMS operation with Windows Defender software
- Upper panel display problem
- High CPU load during OpenGL software emulation
- Axxon One operation with NetLimiter 2
- Exported videos' playback in Movies and TV application
- Axxon One operation on Windows N and KN editions

All video channels or archives stop working once the license maximum is reached

If the activation key allows using fewer video channels than currently created in the system, it will not be possible to work with all video channels. To resume operation, remove the objects corresponding to the excess video channels and restart the Server.

Note

Restart the Server through the Start menu as follows:

1. **All Programs Axxon One Shut Down Server**
2. **All Programs Axxon One Start Server**

Similarly, if the activation key allows using archives with a total capacity less than the current one, you should adjust the capacity of the archives to the required amount and then restart the Server.

No signal from video cameras and failure to connect to other Servers

If the Windows Firewall (or firewall of other manufacturers) was disabled during installation of *Axxon One*, *Axxon One* services and applications will not be automatically added to the list of firewall exceptions.

After you turn on the firewall, you may see no signal from cameras in both main and Web-Client, and no possibility to connect to other Servers.

To solve this problem, add the following applications to the firewall exceptions: Apphost.exe, NetHost.exe, AxxonOne.exe, and LicenceTool.exe.

Incorrect display of Client interface elements

Client interface elements may be distorted on systems with some versions of GeForce drivers (such as 327.23, 337.88) installed.

In some cases this problem is solved by disabling stream optimization for the AxxonOne.exe process:

1. Run **Control panel NVIDIA control panel 3D parameters Software settings**.
2. Click the **Add** button and select the AxxonOne.exe file (<*Axxon One* installation directory >/bin).
3. Set the **Off** parameter for the **Threaded optimisation** function.
4. Click the **Apply** button.

If this solution does not eliminate the problem, then install an older driver for the graphics card.

Error creating new archives even when license restriction on total capacity is observed

If the user creates archives at the same time (in other words, without applying changes) while deleting some existing archives, creation of the archives may be forbidden even if the total archive capacity does not exceed the amount of the license restriction.

> **Note**
>
> This happens because when verifying the license restrictions, the size of created archives is calculated based on the total capacity at the time when changes were applied.

In such a situation, the user should first delete the unnecessary archives and apply changes, then create new archives.

Axxon One VMS operation with Windows Defender software

If you have Windows Defender software installed in your system, some problems may occur when accessing and saving data to the archive, as well as significant slowing down of MomentQuest searches.

As a workaround, you can either disable Windows Defender or add AppHost.exe, AppHostSvc.exe and vfs_format.exe files to the exceptions list.

Upper panel display problem

In some cases, the Client may have a problem displaying the upper panel.

In this case, it is recommended to install the most recent version of Intel graphics subsystem drivers.

High CPU load during OpenGL software emulation

If your computer's graphics card does not meet OpenGL requirements (see Limitations of Axxon One), OpenGL can be emulated in software.

But in this case the CPU load may be high.

Axxon One operation with NetLimiter 2

If *NetLimiter 2* is installed in the system, there may be a significantly increased load on the processor when working with *Axxon One*.

This problem is resolved by removing *NetLimiter 2.*

Exported videos' playback in Movies and TV application

Due to the lack of G.711 and G.726 codecs support in Windows 10's "Movies and TV" app, the app doesn not play audio in exported video.

You can use alternative video viewer applications to obtain the full playback.

Axxon One operation on Windows N and KN editions

Axxon One is not guaranteed to work on Windows N or KN editions. For correct operation, you need to install the Media Feature Pack.

Appendix 3. Assigning of the domain takes place when the Axxon One server is installed

The Windows OS will create two accounts when the *Axxon One* software package is installed using a **Client and Server** type of configuration.

1. An account with administrator rights which is used by the *Axxon One* file browser. The name of this account is set during installation of *Axxon One* (see Installation).

   For *Axxon One* to function correctly, this account must have Windows administrator rights. If the account is a domain user account, you must also add the account to the **Users** and **Power Users** groups.

   > **Note**
   >
   > The file browser helps to navigate through the Server's file system (such as when choosing disks for log volumes).

   The account can also be used for configuring access rights to the hard disk.
2. Axxonpostgres – an account under which the log data database service is started.

> **Note**
>
> A log database (Postgres) is used for storing system events.

Appendix 4. Using Axxon One with antivirus software

On the page:

- ESET NOD32
- ESET NOD32 Internet Security
- ESET Smart Security
- AVG
- DrWeb

To ensure the correct operation of *Axxon One*, it is recommended to configure the antivirus as follows:

1. Add the following processes to the exclusion list:
    a. consul.exe;
    b. nomad.exe;
    c. apphost.exe;
    d. postgres.exe.
2. Add the following folders to the exclusion list:
    a. C:\ProgramData\AxxonSoft\Axxon One;
    b. C:\Program Files\AxxonSoft\Axxon One;
    c. C:\Program Files\Common Files\AxxonSoft;
    d. Postgres and metadata folders if they were changed during installation.
3. Add the following ports to the exclusion list:
    a. 20109-20210;
    b. 4000 (only for the **Failover server and client** installation type);
    c. 4646-4648 (only for the **Failover server and client** installation type);
    d. 8300-8302 (only for the **Failover server and client** installation type);
    e. 8500 (only for the **Failover server and client** installation type);
    f. 8600 (only for the **Failover server and client** installation type).

Depending on the antivirus software that you use, when you install, start, and use *Axxon One*, your antivirus software may ask for permission for the software components to perform Internet access.

It is recommended that you allow these components to do so for proper functioning of the application.

Recommendations for the specific antivirus programs are given below.

ESET NOD32

If you use ESET NOD32 antivirus, it is strongly recommended to either disable the Web Access Protection service, or add the IP addresses of the IP cameras to the list of exclusions for antivirus scanning.

See also Possible Errors During Start-Up.

ESET NOD32 Internet Security

If you use ESET NOD32 Internet Security antivirus, if the SSL/TLS protocol filtering is enabled, it is strongly recommended to either add the certificate file to the list of known certificates, or add the Axxon One.exe app to the list of exclusions for antivirus scanning.

ESET Smart Security

If you use ESET Smart Security antivirus, select automatic mode with exclusions for Firewall and add the remote Servers to the exclusions by creating network rules (for help with creating these rules, refer to the official user guide for the antivirus software).

AVG

When you install *Axxon One*, allow the NetHost.exe and ngpsh.exe processes to run.

If you use AVG antivirus and a configuration with many video cameras, it is strongly recommended to add the IP addresses of the IP cameras to the list of exclusions. Otherwise, the avgsa.exe process may severely slow down the CPU.
This action can be performed only on the paid version of AVG.

DrWeb

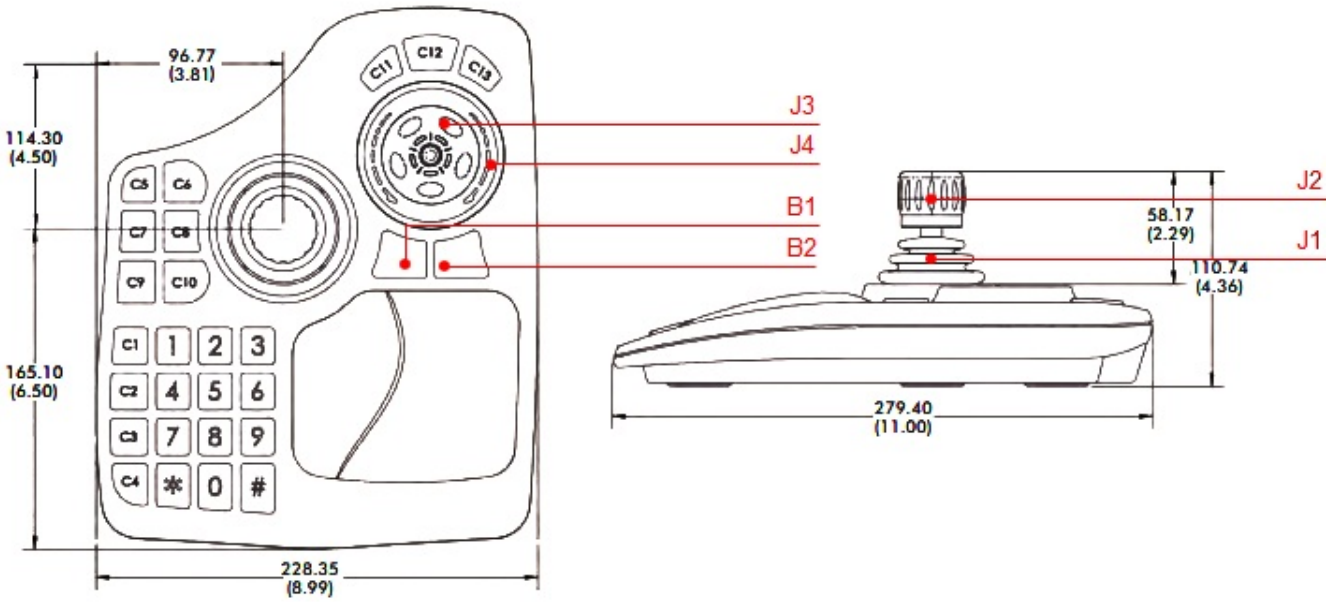
If you use DrWeb antivirus, do the following before installing *Axxon One*:

1. Disable the automatic start of the DrWeb firewall.
2. In the proactive protection settings, select the option to use custom settings and enable the following options:
    a. Allow low-level disk access
    b. Allow system services
    c. Allow loading drivers
    d. Allow User drivers
    e. Allow Winlogon shell parameters
3. In the SpiDer Gate settings, add the apphost.exe and Axxon One.exe processes to the list of exclusions for scanning of incoming traffic. If possible, it is recommended to disable scanning of incoming and outgoing traffic.

Appendix 5. Using CH VM-Desktop USB multifunction controllers with Axxon One

CH VM-Desktop USB multifunction controllers offer a range of input controls:

- Three-axis joystick for PTZ and digital zoom control (**J1** and **J2**)
- Jog/shuttle dial (**J3** and **J4**)
- 27 keys:
  - 10 number keys
  - * key
  - # key
  - Programmable keys **C1** to **C13** (keys cannot be remapped in *Axxon One*)
  - Two additional keys (**B1** and **B2**)



The multifunction controller can be used to operate *Axxon One* on the active monitor.

> **Note**
>
> The active monitor is either the main one (if all additional monitors are inactive or not connected) or an additional one, if the additional monitor is active (see Managing monitors on a local Client).
>
> The active monitor can be selected only by using the mouse. If no mouse is present, the multifunction controller will work on the main monitor only.

A description of key functions is given in the table.

Key	When available	Function
J1	Always	PTZ control for the selected camera. If the selected camera does not support PTZ control, the action is ignored.
J2	Always	Optical zoom control for the selected camera. If the selected camera does not support PTZ control, the action is ignored.
J3 (rotate counterclockwise)	Archive mode	Go to previous frame. If playback is active, the action is ignored.

J3 (rotate clockwise)	Archive mode	Go to next frame. If playback is active, the action is ignored.
J4 (rotate counterclockwise)	Archive mode	Go to previous video fragment.
J4 (rotate clockwise)	Archive mode	Go to next video fragment.
J4	Live Video mode	Iris control for the selected camera.
1	Live Video mode	Start/stop patrol mode.
2.3	Live Video mode	Focus control for the selected camera.
*** n #**	Always	Select a camera in a layout. **n** is the number of the camera to be activated via the number keys. If the camera with the relevant number is not in the current layout, a search is performed for the minimum layout containing the camera; the minimum layout is then displayed. If no such layout exists, a layout with one camera is created.
# n #	Always	Go to layout. n is the layout to be activated via the number keys; the number corresponds to the order in which the layout appears in the list.
C10	Always	Clear number. If the operator did not finish typing the number of a camera or layout (the # key was not pressed), pressing the C10 key clears the previously entered number.
C1	Alarm Management mode	Accept alarm with **False Alarm** resolution.
C2	Alarm Management mode	Accept alarm with **Non-Critical Alarm** resolution.
C3	Alarm Management mode	Accept alarm with **Critical Alarm** resolution.
C4	Always	Manually initiate an alarm and go to Alarm Management mode. Go to Alarm Management mode if an alarm has been previously initiated.
C5	Always	Increase size of layout cell.
C6	Always	Reduce size of layout cell.
C7	Always	Go to previous layout in the list.
C8	Always	Go to next layout in the list.
C11	Archive mode	Slow down playback.
C12	Archive mode	Start/pause video playback.
C13	Archive mode	Speed up playback.
B2	Archive mode, Alarm Management mode	Go to Live Video mode (without alarm classification).
B2	Live Video mode	Go to Archive Mode.
C9	Archive mode	Open/hide calendar.

B1, B2	Open calendar	Cycle through calendar elements (equivalent to pressing the tab key). **days of month - hours - minutes - seconds - am/pm** (**B2** key) and in reverse (by pressing the **B1** key).
J3	Open calendar	Navigate by days and set hours, minutes, seconds, and AM/PM.
J4	Open calendar	Navigate by months.

Appendix 6. Hotkeys in Axxon One

Axxon One comes with the following default hotkeys:

Function	Hotkey
Global General	
Activate panel of cameras	F4
Activate panel of configuration	F5
Activate panel of layouts	F2
Activate panel of video walls	F3
Select item of menu and panels, click Save, Apply, OK	Enter
Navigation. Down	Down
Navigation. Left	Left
Navigation. Right	Right
Navigation. Up	Up
Open comment panel	
Open menu of current layout	F1
Open panel with list of devices	F7
Open alarm panel	F6
Hide menu/panel, click Cancel	Esc
Lock application	Ctrl + Alt + L
Remove current value	Delete
Digit 1	D1
Digit 9	D9
Layouts	
Camera selection in current layout	Ctrl + N
Select monitor by number	Shift + N
Select layout by number	Alt + N
Select the previous* camera in current layout cell	
Select the next* camera in current layout cell	
Navigation the cameras, upward shift	Alt + Up
Navigation the cameras, left shift	Alt + Left
Navigation the cameras, downward shift	Alt + Down
Navigation the cameras, right shift	Alt + Right
Move to the previous layout	Shift + Left
Move to the next layout	Shift + Right
Increase layout cell	Ctrl + Add (+)
Decrease layout cell	Ctrl + Subtract (-)

* by short name	
Live Video display mode	
Videocamera	
Open menu of selected camera and select item	F9
Switch to archive mode	Ctrl + Tab
Switch to alarm classification mode	Ctrl + R
Switch to search in archive mode	Ctrl + F
Arm	Ctrl + A
Disarm	Ctrl + D
PTZ	
Move up	NumPad8
Move left	NumPad4
Move down	NumPad2
Move right	NumPad6
Close iris	Next
Focus far	End
Open iris	PageUp
Patrolling	Multiply (*)
Focus near	Home
Zoom in	NumPad9
Zoom out	NumPad3
Archive	
Open menu of selected camera and select item	Ctrl + E
Pause/Play	Ctrl + Space
Switch to Time Compressor mode	Ctrl + T
Go to the previous video clip	Ctrl + Shift + Left
Go to the previous frame	Ctrl + Left
Go to the next video clip	Ctrl + Shift + Right
Go to the next frame	Ctrl + Right
Show calendar	F8
Increase playback speed	Ctrl + Up
Reduce playback speed	Ctrl + Down
TimeCompressor	
Pause/Play	Ctrl + Space
Move home	Ctrl + B
Increase number of objects	Ctrl + Up
Decrease number of objects	Ctrl + Down
Alarms	

Go to the previous frame	Ctrl + Left
Go to the next frame	Ctrl + Right
Resolution False alarm	Ctrl + D3
Resolution Non-critical alarm	Ctrl + D2
Resolution Critical alarm	Ctrl + D1
Increase playback speed	Ctrl + Up
Reduce playback speed	Ctrl + Down

Appendix 7. Automated configuration backup and restore

You can use the ngpsh.exe utility and json commands to back up and restore your system configuration.

> **Attention!**
>
> These configuration backups are incompatible with those created with the Backup and configuration recovery utility, and vice versa.

To create a configuration backup:

1. Use Windows command line to access the <*Axxon One* installation directory>\Axxon One\bin folder.
2. Execute the following command:

```
ngpsh.exe backup backupJson [path_to_backup_folder] [node_name] [local] [shared] [license] [tickets]
```

Where

Parameter	Description
path_to_backup_folder	**Required parameter.** Specify a folder to save the configuration backup to. You have to use two "\" characters in the path.
node_name	**Required parameter.** Name of a Server whose configuration you want to save.
local	Add it, if you need to save the local configuration for this Server: all created objects along with their parameters, links and changes' histories.
shared	Add it, if you need to save the global configuration for an Axxon domain: users, layouts, etc.
license	Add it, if you need to save a license.
tickets	Add it, if you need to save the Axxon domain structure.

An example:

```
ngpsh.exe backup backupJson c:\\backups Server1 local
```

To restore a configuration from a backup:

```
ngpsh.exe backup restoreJson [path_to_backup_file] [node_name] [local] [shared] [license] [tickets]
[deleteLocal] [deleteShared]
```

Where

Parameter	Description
deleteLocal	Add it, if you need to clear the local configuration from objects not present in the backup copy.
deleteShared	Add it, if you need to clear the global configuration from objects not present in the backup copy.

An example:

```
ngpsh.exe backup restoreJson c:\\backups\Server1.json local
```

Appendix 8. Using Axxon One with NAT

Consolidating the Servers from different networks into Axxon domain

To consolidate the Servers from different networks separated by routers into Axxon domain, do the following:

1. Set the port range for operation and the router's public IP address on each Server that is to be included in the Axxon domain (see Network settings utility).

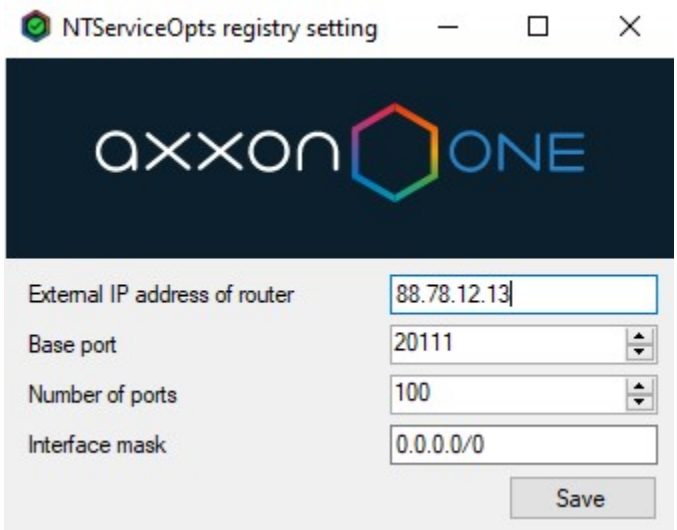
   Attention!

   The Server port ranges of Axxon Domain should not overlap within the same network.

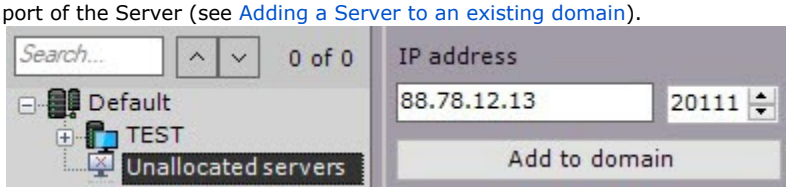
   By default, the base port is 20111, and the port range is 20111-20210. Hence, it is necessary to set and forward the port range 20211-20310 for the second Server, the port range 20311-20410 for the third Server, and so on (see Ports used by the Axxon One Software Package).

   Attention!

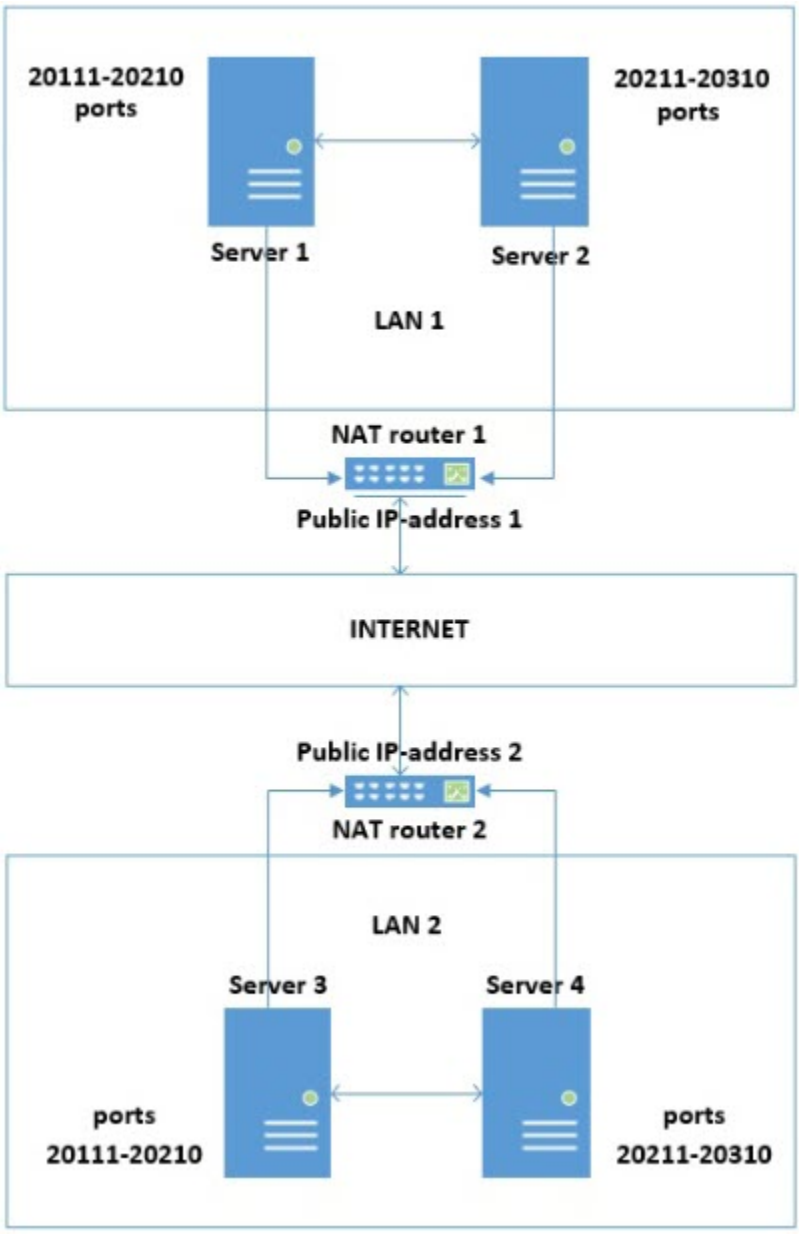
   The router's public IP address should be static.



2. For each router, forward the specified ports of the Server, which is located behind this switch, and the gRPC API 20109 port.
3. Connect the Client to the Server from any network (see Starting the Axxon One Client, Connecting the Client to the Server behind NAT).
4. Manually add other Servers to the Axxon domain using the public IP address of the corresponding router and the external base port of the Server (see Adding a Server to an existing domain).



Example:



To combine Servers into one Axxon domain in this configuration, do the following:

1. On Server 1, set the port range 20111-20210 and the public IP address of router 1.
2. On Server 2, set the port range 20211-20310 and the public IP address of router 1.
3. On Server 3, set the port range 20111-20210 and the public IP address of router 2.
4. On Server 4, set the port range 20211-20310 and the public IP address of router 2.
5. On router 1, configure the forwarding of:
    a. the router ports 20111-20210 to the internal IP address of Server 1 and ports 20111-20210;
    b. the router ports 20211-20310 to the internal IP address of Server 2 and ports 20211-20310;
    c. the gRPC API 20109 port (always static) to the internal IP address of Server 1 and the internal IP address of Server 2.
6. On router 2, configure the forwarding of:
    a. the router ports 20111-20210 to the internal IP address of Server 3 and ports 20111-20210;
    b. the router ports 20211-20310 to the internal IP address of Server 4 and ports 20211-20310;
    c. the gRPC API 20109 port (always static) to the internal IP address of Server 3 and the internal IP address of Server 4.
7. Connect to Server 1.
8. Manually add Server 2 to the Axxon domain using the local IP address of Server 2 and port 20211.
9. Manually add Server 3 to the Axxon domain using the public IP address of router 2 and port 20111.
10. Manually add Server 4 to the Axxon domain using the public IP address of router 2 and port 20211.

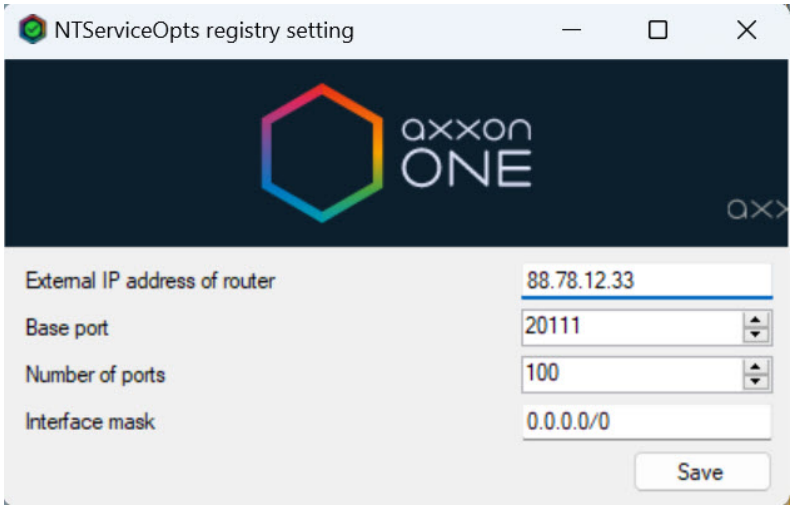
Connecting the Client to the Server behind NAT

To connect the Client to the Server behind NAT, do the following:

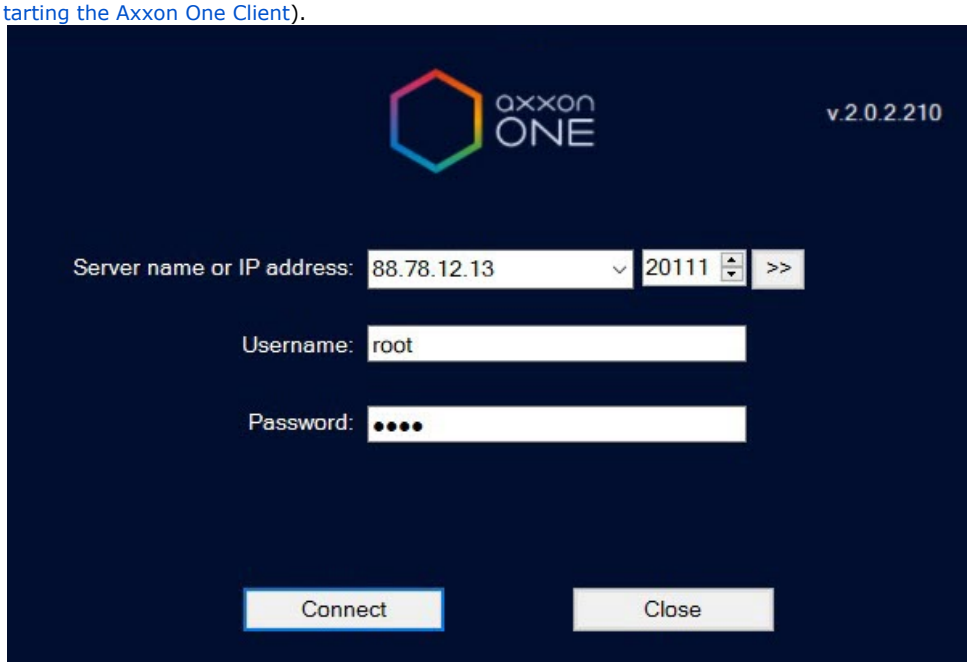
1. Set the router public IP address (see Network settings utility).

   Attention!

   The router public IP address should be static.



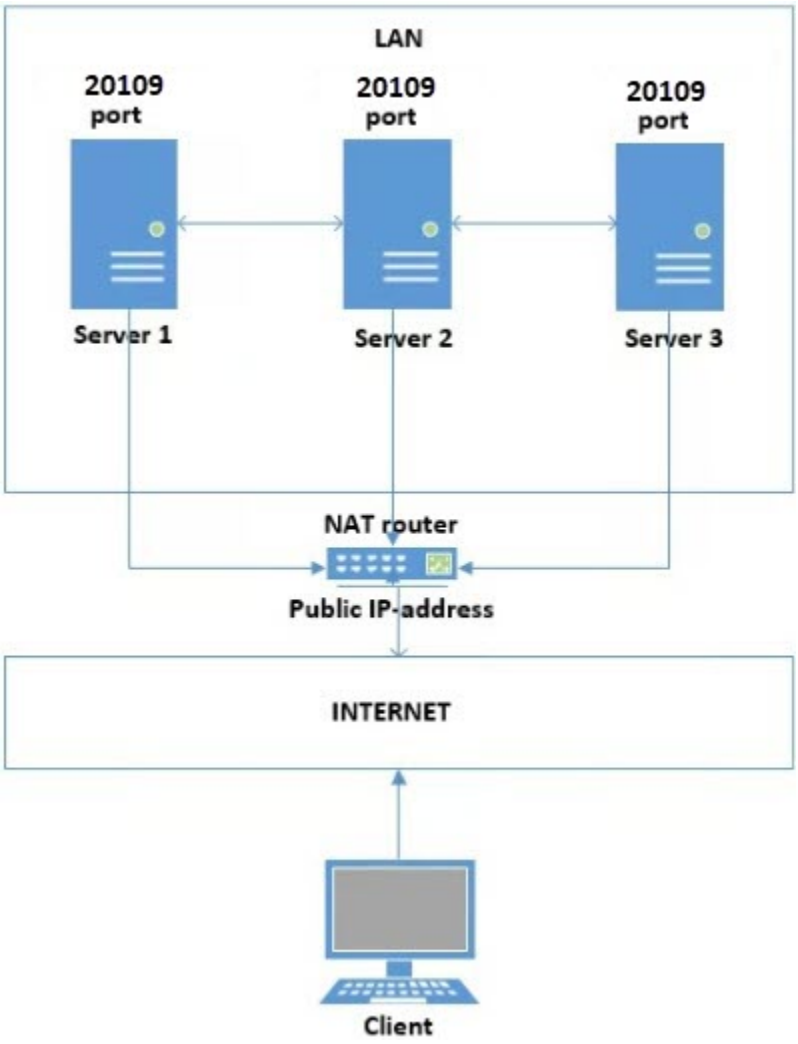
2. On the router, forward the gRPC API 20109 port to the internal IP address of the Server port 20109.
3. Launch the Client and specify the router external IP address and the Server external base port in the connection settings (see Starting the Axxon One Client).



   Attention!

   When connecting the Client from an external network, only those Servers that have access to the external network will be available in the Axxon-domain configuration (see Consolidating the Servers from different networks into Axxon-domain).

Example.



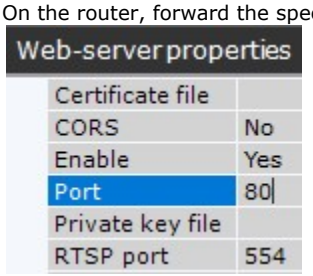
To connect the Client to the Servers behind NAT, do the following:

1. From one of the Servers, forward port 20109 to the router public IP address.
2. On the router, configure the forwarding of:
    a. The router port 20109 to the internal IP address of the Server port 20109.
3. When connecting the Client, enter the router public IP address and port 20109.

Connecting the Web and Mobile Clients to the Server behind NAT

To connect Web and Mobile Clients to the Server behind NAT, do the following:

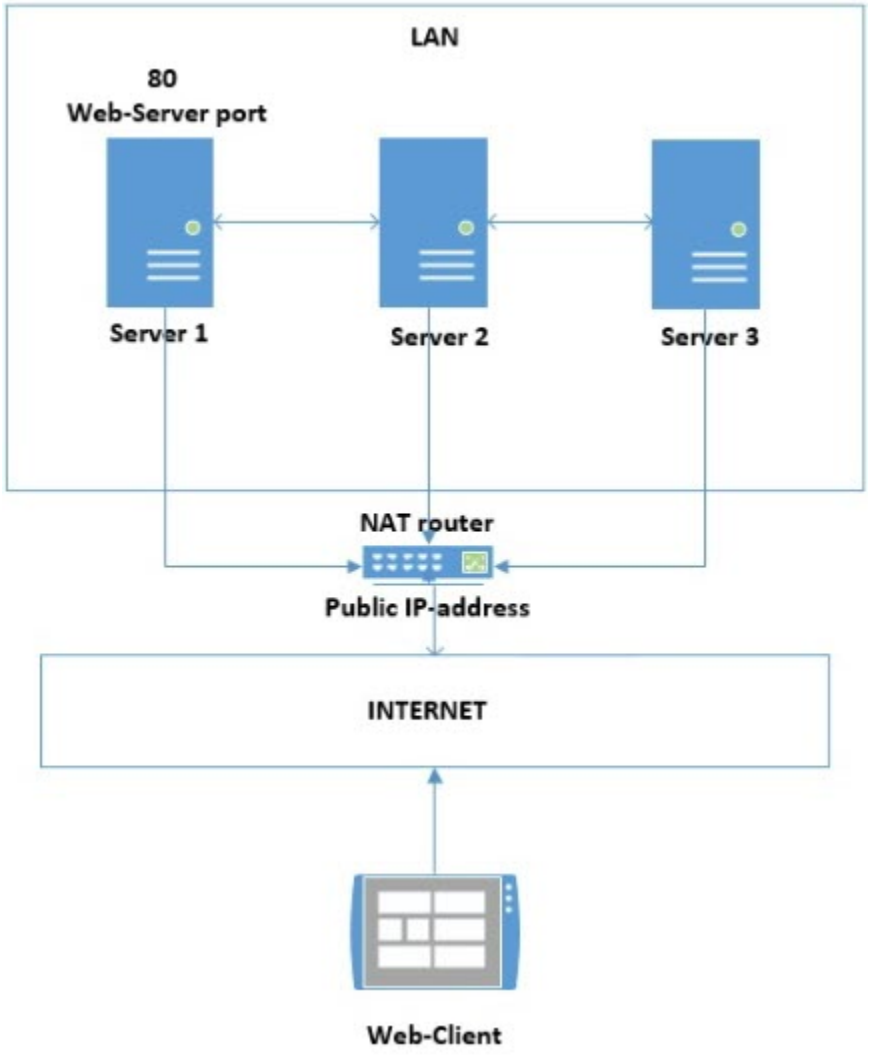
1. On the router, forward the specified port of the Web server (see Configuring the Web-Server). The default port is 80.



> **Note**
>
> To access all Servers of the Axxon domain, it is enough to forward any single port of the Web server.

2. When connecting using a Web browser or Mobile Client, use the Server's public IP address and the forwarded port of the Web server (see Starting and logging in to the Web-Client).

Example:



To connect the Web Client to the Axxon domain in this configuration, do the following:

1. On the router, forward the port 80 to the internal IP address of Server 1 and port 80.
2. When starting the Web Client, use the router's public IP address and port 80.

Audio transmission from the Client's microphone behind NAT to the Server's or camera's loudspeaker

Playing back sound from Client microphone on camera speakers

To transmit audio from the Client's microphone behind NAT to the Server's or camera's loudspeaker, do the following:

1. On the Client, specify a unique port range and an external router's public IP address. Follow the steps below:
   a. Add an NGP_CLIENT_PORT_BASE environmental variable and set its value to the first port number in the range (see Appendix 9. Creating system variable).
   b. Add an NGP_CLIENT_PORT_SPAN environmental variable and set its value to the number of ports in the range.

      Attention!

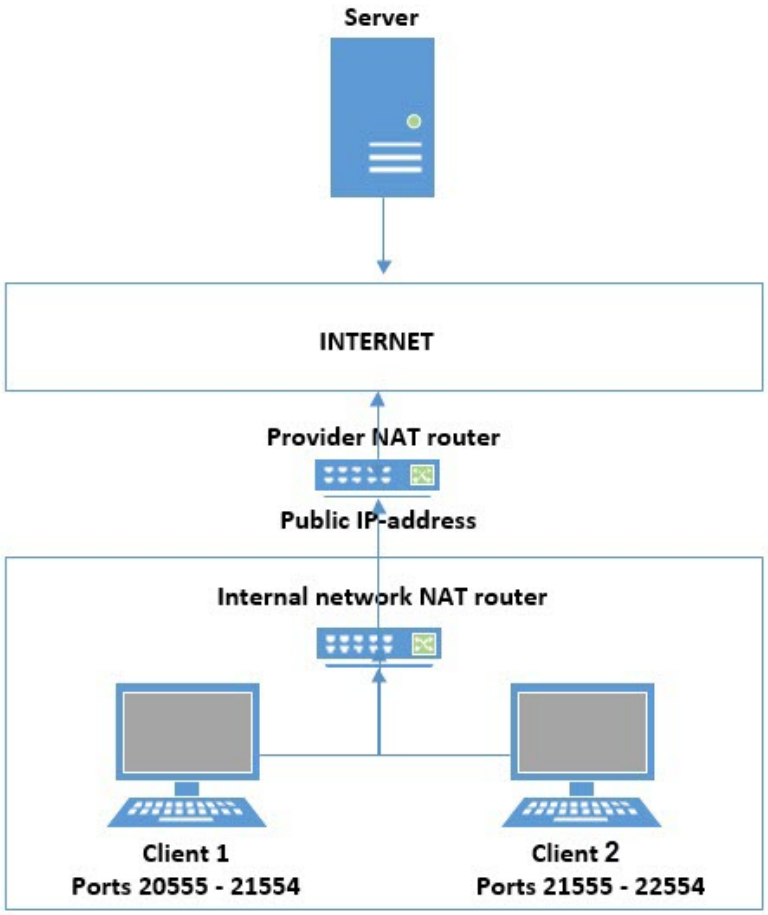
      We recommend you to use no less than 100 ports.

      Attention!

      If you have multiple Clients within your network, their port ranges must not overlap.

   c. Add an NGP_ALT_ADDR environmental variable and set its value to the public IP address of the externa router.
2. Configure forwarding of the specified ports on both external and internal router.

Example:



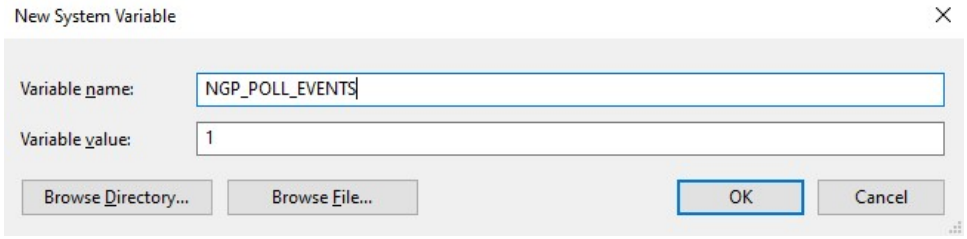
To transmit audio from microphones connected to Client 1 and Client 2 to the Server's or camera's loudspeaker, do the following:

1. On Client 1, set port range to 20555-21554, and the public IP address of your Internet provider's router.
2. On Client 2, set port range to 21555-22554, and the public IP address of your Internet provider's router.
3. Configure port forwarding on the internal router:
    a. ports 20555-21554 to the internal IP address of Client 1 and ports 20555-21554;
    b. ports 21555-22554 to the internal IP address of Client 2 and ports 21555-22554.
4. Configure port forwarding on the provider's router:
    a. router ports 20555-21554 to the IP address of the internal router and ports 20555-21554;
    b. router ports 21555-22554 to the IP address of the internal router and ports 21555-22554.

Appendix 9. Creating system variable

To add a new system variable:

1. Go to **Control panel System Advanced system settings**.
2. Click the **Environment Variables...** button.
3. Under **System variables** group, click the **New...** button.
4. Specify the name and value of variable.



5. Click the **OK** button.