User Guide

09/05/2023

Table of contents

1 Description of the Software Package 33
2 Installing the Axxon One Software Package 33
3 Licensing of the software product 33
4 Launching and Closing the Axxon One Software Package 34
5 Configuration of the Axxon One Software Package 34
6 Working with the Axxon One Software Package 34
7 Description of utilities 35
8 Appendices 35
9 User Guide. Introduction 36
9.1 General Information 36
9.2 Purpose of the Document 36
9.3 Purpose and functionality of Axxon One 36
10 Software Lifecycle Policy 38
10.1 Software Lifecycle Phases 38
10.2 Software Technical Support 38
10.3 Standard Period for Release of Software Updates 38
10.4 Licensing Policy with Regard to Software Updates 38
11 Description of the Software Package 40
11.1 Basic principles of building a security system based on the Axxon One software package 40
11.2 Axxon One features: reference information 40
11.2.1 Micromodule architecture 41
11.2.2 Support for IP devices 41
11.2.3 Support for analog cameras in Axxon One 41
11.2.4 Video and Audio Detection Tools 42
11.2.5 Video archive 42
11.2.6 Interactive 3D Map 43
11.2.7 User Interface 43
11.2.8 Face Recognition 43
11.2.9 Number Plate Recognition 43
11.2.10 Receiving Events from External Systems 43
11.3 Functions of the Distributed Security System 44

11.4 Network Topologies of the Axxon One Software Package ... 44
11.5 Specifications of the Axxon One software package ... 45
11.6 Implementation requirements for the Axxon One software package ... 46
11.6.1 Limitations of Axxon One ... 46
11.6.2 Operating system requirements ... 47
11.6.2.1 Windows OS ... 48
11.6.2.2 Windows Server OS ... 48
11.6.2.3 Linux OS ... 48
11.6.3 Disk storage subsystem requirements ... 48
11.6.3.1 General requirements ... 49
11.6.3.2 Storage requirements ... 50
11.6.3.2.1 Minimum requirements ... 50
11.6.3.2.2 Size of the archive ... 50
11.6.3.2.3 System log database ... 51
11.6.3.2.4 Metadata database ... 51
11.6.3.2.5 The system logs ... 51
11.6.3.2.6 Self-diagnostics service ... 51
11.6.4 Hardware requirements ... 51
11.6.4.1 General hardware requirements ... 51
11.6.4.1.1 Minimum RAM requirements ... 52
11.6.4.1.2 Minimum and recommended requirements for graphics cards ... 52
11.6.4.2 Hardware requirements for neural analytics operation ... 52
11.6.4.3 Hardware requirements for GPU based video decoding ... 54
11.6.4.4 Hardware requirements for License plate recognition (RR) ... 54
11.6.4.5 Hardware requirements for face detection ... 54
11.6.4.6 Hardware requirements for Face detection (VL) ... 54
11.6.4.7 Hardware requirements for License plate recognition (VT) ... 55
11.6.4.8 Hardware requirements for License plate recognition (IV) ... 55
11.6.5 TCP/IP Network Bandwidth Requirements ... 55
11.6.6 BIOS configuration requirements ... 56
11.6.7 Running Axxon One VMS in Virtual Machines ... 56
11.7 Interface of the Axxon One Software Package ... 56
11.8 Ports used by the Axxon One Software Package ... 57
11.9 Requirements for Personnel Quantity and Qualifications ... 58
12 Installing the Axxon One Software Package ... 60

12.1 Installing equipment ... 60
12.1.1 Types of Devices Used ... 60
12.1.2 Connecting IP Devices ... 60
12.1.3 Configuring IP Devices in Windows ... 61
12.1.4 Video capture cards pins ... 61
12.1.4.1 WS-216 video capture card pins ... 61
12.2 Installation the Axxon One Software Package ... 62
12.2.1 Installation ... 62
12.2.2 Installing DetectorPack add-ons ... 74
12.2.3 Repairing Installation ... 76
12.2.4 Removal ... 78
12.2.5 Silent install (Quiet Mode) ... 81
12.2.6 Updating Drivers Pack ... 84
12.2.7 Update ... 84
12.2.8 Automatic update of a remote Client ... 85
13 Licensing of the software product ... 86
13.1 Axxon One license types ... 86
13.1.1 Disclaimer ... 90
13.2 Licensing methods ... 90
13.3 Product activation utility ... 91
13.4 License Activation ... 93
14 Launching and closing the Axxon One software package ... 94
14.1 Startup ... 94
14.1.1 Starting a Server ... 94
14.1.2 Starting an Axxon One Client ... 94
14.1.3 Running multiple Axxon One Clients ... 97
14.1.4 Axxon One in demo mode ... 98
14.1.5 Automatic Start of the Client ... 99
14.2 Shutdown ... 99
14.2.1 Shutting down an Axxon One Client ... 99
14.2.2 Shutting down a Server ... 100
14.3 Automatic Server restart ... 100
14.4 Switching Users Quickly ... 101
14.5 Cross-System Client ... 101

14.6 Connecting LDAP users ... 102
14.7 Connecting to Another Server Quickly ... 102
15 Configuration of the Axxon One Software Package ... 104
15.1 General information on system configuration ... 104
15.1.1 System configuration: stages ... 104
15.1.2 Applying and resetting settings ... 104
15.1.3 Display of parameters in interface ... 105
15.1.4 System objects ... 105
15.1.5 Object search ... 106
15.2 Hardware configuration ... 107
15.2.1 Configuring Axxon domains ... 107
15.2.1.1 Axxon-domain object ... 108
15.2.1.2 Axxon Domain operations ... 108
15.2.1.2.1 Creating a new domain ... 108
15.2.1.2.2 Adding a Server to an existing Axxon-domain ... 109
15.2.1.2.3 Removing a Server from an domain ... 110
15.2.1.3 Cases of Axxon Domain configuration ... 111
15.2.2 Adding and removing IP devices ... 112
15.2.2.1 Bulk creation of IP devices ... 117
15.2.3 Configuring system objects for devices ... 118
15.2.3.1 The Server Object ... 118
15.2.3.1.1 Configuring the Web-Server ... 119
15.2.3.1.2 Configuring an RTSP Server ... 120
15.2.3.1.3 Configuring the ONVIF Server ... 121
15.2.3.2 The Camera object ... 122
15.2.3.2.1 Configuring the camera settings ... 122
15.2.3.2.2 Configuring video stream settings ... 125
15.2.3.2.3 Camera preview window ... 126
15.2.3.2.4 Restoring default camera settings ... 127
15.2.3.2.5 Mass configuration ... 127
15.2.3.2.6 Configuring fish-eye cameras ... 127
15.2.3.2.7 Connecting and configuring cameras over standard protocols ... 129
15.2.3.2.7.1 Notes on configuring video cameras connected via ONVIF ... 129
15.2.3.2.7.2 Configuring connection of devices via RTSP ... 131
15.2.3.2.7.3 Generic Drivers (General device, generic) ... 134

15.2.3.2.7.4 Connecting cameras via the GB/T28181 protocol ... 135
15.2.3.2.8 Configuring connection of video cameras with dynamic IP addresses ... 156
15.2.3.2.9 Configuring virtual video cameras ... 156
15.2.3.2.10 Privacy mask settings ... 157
15.2.3.2.11 Putting a text over the camera window ... 159
15.2.3.3 The IP Server Object ... 161
15.2.3.3.1 Configuring Virtual IP Servers ... 162
15.2.3.4 The Microphone Object ... 163
15.2.3.5 The PTZ Object ... 164
15.2.3.5.1 Configure HTTP-CGI commands to control Wash&Wiper ... 165
15.2.3.6 The Channel object ... 166
15.2.3.7 The Input Object ... 166
15.2.3.7.1 Configure virtual inputs ... 167
15.2.3.7.1.1 Creating and configuring virtual inputs ... 168
15.2.3.7.1.2 Switching virtual inputs ... 168
15.2.3.7.1.3 Virtual inputs' status on map ... 169
15.2.3.8 The Output Object ... 169
15.2.3.9 The Speaker Object ... 170
15.2.3.9.1 Creating and Configuring an Object ... 171
15.2.3.9.2 Configuring a Speaker Object ... 172
15.2.3.9.3 Checking Audio Notification ... 173
15.2.3.10 The Embedded storage object ... 174
15.2.4 Particulars of Configuration of Devices ... 174
15.2.4.1 AGRG-IO-16/8-WD-DS Sensor-Relay cards ... 174
15.2.4.1.1 Connecting AGRG-IO-16/8-WD-DS Sensor-Relay cards ... 174
15.2.4.1.2 Electrical and technical specifications of AGRG-IO-16/8-WD-DS devices ... 176
15.2.4.1.3 Special features of configuring AGRG-IO-16/8-WD-DS card in Axxon One ... 177
15.2.4.2 Axis IP Devices ... 177
15.2.4.2.1 Serial number check ... 177
15.2.4.2.2 Bonjour function ... 178
15.2.4.2.3 Video streams ... 178
15.2.4.3 CCTV Keyboards ... 178
15.2.4.3.1 General Information about CCTV Keyboards ... 178
15.2.4.3.2 Axis T8310 specific configuration features ... 179
15.2.4.3.2.1 Setting up on a Server ... 179
15.2.4.3.2.2 Setting up on a Client ... 179

15.2.4.3.3 Hikvision DS-1100KI specific configuration features ... 180
15.2.4.3.4 UNIVIEW KB-1100 specific configuration features ... 180
15.2.4.3.4.1 General description of the UNIVIEW KB-1100 PTZ control device ... 180
15.2.4.3.4.2 Configuring a remote control before adding it to Axxon One ... 181
15.2.4.3.4.3 Configuring UNIVIEW KB-1100 in Axxon One ... 181
15.2.4.3.5 Hikvision DS-1200KI specific configuration features ... 182
15.2.4.3.5.1 Configuring the Hikvision DS-1200KI control device before adding it to Axxon One ... 182
15.2.4.3.5.2 Features of the Hikvision DS-1200KI control device operation in Axxon One ... 184
15.2.4.3.6 Dahua DH-NKB1000 specific configuration features ... 184
15.2.4.3.6.1 Keyboard operating modes ... 184
15.2.4.3.6.2 Specific OS settings ... 184
15.2.4.3.6.3 Specific Axxon One settings ... 184
15.2.4.4 CH VM-Desktop USB multifunction controller ... 184
15.2.4.5 Configuring Vivotek Panoramic PTZ ... 184
15.2.4.6 Video capture cards ... 185
15.2.4.6.1 WS-216 video capture cards ... 185
15.2.4.6.2 YUAN PD652 cards ... 186
15.2.4.7 Joysticks ... 186
15.2.4.8 Sony IP Devices ... 186
15.2.4.9 Setting up Tibbo relay/loop boards ... 187
15.2.5 Configuring Tracking objects ... 189
15.2.5.1 Configuring Tag&Track Lite ... 189
15.2.5.2 Configuring Tag & Track Pro ... 189
15.2.5.2.1 Camera requirements for Tag&Track Pro ... 190
15.2.5.2.2 Configuring Smooth Motion for PTZ cameras ... 190
15.2.5.2.3 Linking panoramic cameras to a PTZ camera ... 190
15.2.5.2.4 Matching the telemetry device positions with the overview cameras frame points (calibration) ... 191
15.2.5.2.5 Setting PTZ mode for Tag & Track Pro ... 192
15.2.6 Receiving Events from External Systems ... 192
15.2.6.1 Event source object ... 192
15.2.6.2 Configuring POS devices ... 193
15.2.6.2.1 Connecting POS devices ... 193
15.2.6.2.2 Configuring titles view ... 194
15.2.6.2.3 Configuring receipt beginning/end ... 195
15.2.6.2.4 Configuring keywords ... 196
15.2.6.2.5 Importing parcers ... 197

15.2.6.3 Receiving Axxon PSIM Events ... 198
15.2.6.4 Configuring Receiving Events from CommaxComplexServer ... 198
15.2.6.4.1 Configuring Commax Complex Server via Event Source ... 199
15.2.6.4.2 Configuring Commax Complex Server via virtual IP server ... 199
15.2.7 Configuring video camera groups ... 200
15.2.7.1 Procedure for configuring video camera groups ... 201
15.2.7.2 Creating a Group object ... 201
15.2.7.3 Adding video cameras created in the system to Group objects ... 202
15.2.7.4 Creating a system of groups and subgroups ... 203
15.2.7.5 Managing Group and Video camera objects ... 203
15.2.8 Autocopy data from local to centralized servers ... 205
15.3 Configuring archives ... 206
15.3.1 General information about configuring archives ... 206
15.3.2 General information of SolidStore file system ... 208
15.3.3 General information about the cloud archive ... 208
15.3.3.1 General information about the Round-robin algorithm ... 209
15.3.4 Creating archives ... 209
15.3.4.1 Creating a local archive ... 209
15.3.4.2 Creating a remote archive ... 211
15.3.4.3 Creating an archive based on existing archive volumes ... 213
15.3.4.4 Creating a cloud archive ... 214
15.3.4.4.1 Configuring an archive volume based on the Microsoft Azure solution ... 216
15.3.4.4.2 Configuring an archive volume based on the Amazon solution ... 217
15.3.4.4.3 Configuring an archive volume based on the Huawei Cloud solution ... 219
15.3.4.4.4 Configuring an archive volume based on the Seagate Lyve Cloud solution ... 220
15.3.4.4.5 Configuring an archive volume based on the Wasabi solution ... 221
15.3.4.4.6 Configuring an archive volume based on the MinIO solution ... 222
15.3.5 Configuring recording to an archive ... 224
15.3.6 Setting the default archive ... 225
15.3.7 Configuring data replication ... 226
15.3.8 Configuring access restrictions to archive ... 227
15.3.9 Editing archives ... 228
15.3.10 Configuring a write limit on the archive volume ... 228
15.3.11 Protecting video footage from FIFO overwriting ... 228
15.3.11.1 Setting up a macro for automatic copying of protected records ... 229

15.3.11.2 Setting up record protection 230
15.3.12 Increasing capacity of an archive volume 231
15.3.12.1 Increasing capacity of an archive volume as a partition 231
15.3.12.2 Increasing capacity of an archive volume as a file 231
15.3.12.3 Increasing capacity of an object archive volume 231
15.3.13 Removing archive volumes 231
15.3.14 Removing archives 232
15.3.15 View information about the size of archives and Server disk space 232
15.3.16 Saving the archive when replacing the video signal device 233
15.4 Configuring detection tools 234
15.4.1 General Information on Configuring Detection 234
15.4.2 General information on metadata 237
15.4.3 General information on Neural Analytics 238
15.4.3.1 Data collection requirements for neural network training 239
15.4.3.2 Optimizing the operation of neural analytics on GPU 240
15.4.4 Processors used for detection tools operation 242
15.4.5 Creating detection tools 243
15.4.6 Mass configuration of detections tools 247
15.4.6.1 Mass creation of detection tools 247
15.4.6.2 Mass configure detection tools 248
15.4.6.3 Mass removal of tools 249
15.4.7 VMD (video motion detection) 249
15.4.7.1 Video requirements for VMD 249
15.4.7.2 VMD features and specifications 250
15.4.7.3 Configuring VMD 250
15.4.8 Tampering Detection 251
15.4.8.1 Functions of tampering detection 251
15.4.8.2 Video requirements for tampering detection 252
15.4.8.3 Configuring tampering detection 252
15.4.9 Service Audio Detection Tools 254
15.4.9.1 Functions of Service Audio Detection Tools 254
15.4.9.2 Set Parameters of Audio Detection 254
15.4.10 Scene Analytics detection tools 254
15.4.10.1 General information on Scene Analytics detection tools 254
15.4.10.2 Functions of Scene Analytics detection tools 255

15.4.10.3 Video requirements for scene analytics detection tools ... 256
15.4.10.3.1 Video requirements for object tracker-based scene analytics detection tools ... 256
15.4.10.3.2 Video requirements for object tracker (with neural filter)-based scene analytics detection tools ... 257
15.4.10.3.3 Video requirements for VMD-based scene analytics detection tools ... 257
15.4.10.3.4 Video stream and scene requirements for neural tracker operation ... 258
15.4.10.3.5 Objects image requirements for neural tracker ... 258
15.4.10.3.6 Camera requirements for abandoned objects detection ... 259
15.4.10.3.7 Camera requirements for neural filter operation ... 259
15.4.10.4 Configuring Scene Analytics Detection Tools ... 260
15.4.10.4.1 Setting up Tracker-based Scene Analytics detection tools ... 260
15.4.10.4.1.1 Setting general parameters of Tracker-based Scene Analytics detection tools ... 260
15.4.10.4.1.2 Settings specific to Cross Line Detection ... 268
15.4.10.4.1.3 Settings specific to Abandoned object detection ... 270
15.4.10.4.1.4 Settings specific to Loitering Detection ... 272
15.4.10.4.1.5 Settings specific to Multiple objects ... 272
15.4.10.4.1.6 Settings specific to Stop in area detection ... 273
15.4.10.4.1.7 Settings specific to Move from area to area detection tool ... 273
15.4.10.4.2 Setting up Neural Tracker-based Scene Analytics detection tools ... 274
15.4.10.4.3 Setting up VMD-based Scene Analytics detection tools ... 277
15.4.10.4.4 Examples of configuring neural tracker for solving typical tasks ... 278
15.4.11 Face detection tools ... 278
15.4.11.1 Functions of face detection tools ... 279
15.4.11.2 Requirements for face detection tools ... 279
15.4.11.3 Configuring Face detection ... 280
15.4.11.3.1 Fine-tuning the Face detection tool ... 282
15.4.11.3.2 Optimizing the operation of Face detection on GPU ... 284
15.4.11.4 Configuring Face detection (VL) ... 285
15.4.11.4.1 Fine-tuning the face detection (VL) ... 286
15.4.11.4.2 License activation for Face detection (VL) ... 287
15.4.11.5 Configuring additional face detection tools ... 291
15.4.11.5.1 Configuring Masks Detection ... 291
15.4.11.5.2 Configuring Appearance in area and Loitering in area detection ... 292
15.4.11.5.2.1 Appearance in area detection ... 292
15.4.11.5.2.2 Loitering in area detection ... 293
15.4.11.5.3 Face Detection and Temperature Control with Mobotix M16 TR cameras ... 293
15.4.11.5.3.1 Functional parameters of the Face Detection and Temperature Control ... 293

15.4.11.5.3.2 Camera requirements for face detection and temperature control ... 294
15.4.11.5.3.3 Temperature screening protocol ... 294
15.4.11.5.3.4 Pre-configuration of the Mobotix M16 TR camera ... 295
15.4.11.5.3.5 Configuring Face Detection and Temperature Control ... 298
15.4.11.6 Configuring real-time face recognition ... 301
15.4.11.6.1 Configuring macros when working with face lists ... 301
15.4.11.6.1.1 Presence of the recognized face in the selected face list ... 301
15.4.11.6.1.2 Absence of the recognized face in the selected face list ... 301
15.4.11.6.1.3 Recognition of the presence of a specific face from the face list ... 302
15.4.11.6.1.4 Absence of the recognized face in all created face lists ... 302
15.4.11.6.1.5 Examples of macros used for working with face lists ... 302
15.4.11.6.2 Configuring FaceCube integration ... 307
15.4.12 Automatic Number Plate Recognition (LPR/ANPR) tools ... 308
15.4.12.1 License plate recognition (VT) ... 308
15.4.12.1.1 License plate recognition (VT) features and specifications ... 308
15.4.12.1.2 Camera and image requirements for License plate recognition (VT) ... 310
15.4.12.1.2.1 General requirements ... 310
15.4.12.1.2.2 Video camera requirements ... 310
15.4.12.1.2.3 Camera installation requirements ... 312
15.4.12.1.2.4 License plate image requirements ... 313
15.4.12.1.2.5 Recommendations for highways ... 314
15.4.12.1.3 Configuring License plate recognition (VT) ... 314
15.4.12.1.4 Fine-tuning the VT number plate detection tool ... 317
15.4.12.1.5 Licensing of the software module for License plate recognition (VT) ... 320
15.4.12.1.5.1 Installing the license key environment ... 320
15.4.12.1.5.2 Installing a demo license ... 320
15.4.12.1.5.3 Installing a hardware key ... 321
15.4.12.1.5.4 Installing a software key ... 321
15.4.12.1.5.5 Activating and updating the license ... 323
15.4.12.1.5.6 Removing a license ... 324
15.4.12.1.5.7 Checking a license ... 324
15.4.12.2 License plate recognition (IV) ... 324
15.4.12.2.1 License plate recognition (IV) features and specifications ... 324
15.4.12.2.2 Camera requirements for License plate recognition (IV) ... 325
15.4.12.2.2.1 Camera requirements ... 325
15.4.12.2.2.2 Video requirements ... 325
15.4.12.2.2.3 Camera installation requirements ... 325

15.4.12.2.2.4 Examples of correct and incorrect video images ... 325
15.4.12.2.3 Configuring License plate recognition (IV) ... 326
15.4.12.3 License plate recognition (RR) ... 329
15.4.12.3.1 License plate recognition (RR) features and specifications ... 329
15.4.12.3.2 Camera requirements for License plate recognition (RR) ... 330
15.4.12.3.3 Configuring License plate recognition (RR) ... 330
15.4.12.4 Optimizing the operation of the License plate (RR) and RR vehicles recognition on GPU ... 333
15.4.12.5 License plate recognition (BRS) ... 334
15.4.12.5.1 Camera requirements for License plate recognition (BRS) ... 334
15.4.12.5.1.1 Camera requirements ... 334
15.4.12.5.1.2 Video image requirements ... 334
15.4.12.5.1.3 Camera installation requirements ... 335
15.4.12.5.2 License plate recognition (BRS) features and specifications ... 335
15.4.12.5.3 Configuring License plate recognition (BRS) ... 335
15.4.12.6 Configuring real-time vehicle license plate recognition ... 337
15.4.12.6.1 Configuring macros when working with vehicles lists ... 338
15.4.12.6.1.1 Presence of the recognized license plate in the selected list ... 338
15.4.12.6.1.2 Absence of the recognized license plate in the selected list ... 338
15.4.12.6.1.3 Presence of the specific license plate from the selected list ... 338
15.4.12.6.1.4 Absence of the recognized license plate in all created lists ... 339
15.4.12.6.1.5 Examples of macros used when working with vehicles lists ... 339
15.4.13 Neural Counter ... 344
15.4.13.1 Video stream and scene requirements for neural counter operation ... 344
15.4.13.2 Functions of the neural counter ... 345
15.4.13.3 Configuring a Neurocounter ... 345
15.4.13.4 Example of configuring neural counter for solving typical task ... 349
15.4.13.5 Objects image requirements for neural counter ... 349
15.4.14 Fire and Smoke Detection Tools ... 349
15.4.14.1 Functions of Fire and Smoke detection ... 349
15.4.14.2 Camera requirements for Fire and Smoke Detection ... 350
15.4.14.3 Configuring Fire and Smoke Detection Tools ... 350
15.4.15 Object presence detection tool ... 352
15.4.15.1 Functions of the object presence detection tool ... 352
15.4.15.2 Camera requirements for the object presence detection tool ... 353
15.4.15.3 Configuring the object presence detection tool ... 353
15.4.16 Personal protective equipment detection tools ... 355

15.4.16.1 PPE detection (VL) 355
15.4.16.1.1 Functions of the PPE detection tool (VL) 355
15.4.16.1.2 Video stream and scene requirements for PPE detection tool (VL) operation 355
15.4.16.1.3 Objects image requirements for PPE detection tool (VL) 356
15.4.16.1.4 Configuring PPE detection tool (VL) 357
15.4.16.2 Equipment detection tool (PPE) 358
15.4.16.2.1 Functions of the Equipment detection tool (PPE) 358
15.4.16.2.2 Video stream and scene requirements for Equipment detection tool (PPE) operation 358
15.4.16.2.3 Objects image requirements for Equipment detection tool (PPE) 359
15.4.16.2.4 Configuring equipment detection tool (PPE) 359
15.4.16.2.5 Examples of configuring Equipment detection tool (PPE) for solving typical tasks 362
15.4.16.3 Example of providing a list of valid equipment at the facility 363
15.4.17 Person-based privacy masking 366
15.4.17.1 Person-based privacy mask functions 366
15.4.17.2 Camera requirements for person-based privacy masking 367
15.4.17.3 Person-based privacy masking configuration 367
15.4.18 Privacy masking detection tool 368
15.4.18.1 Functions of the Privacy masking detection tool 368
15.4.18.2 Camera requirements for the Privacy masking detection tool 369
15.4.18.3 Configuring the Privacy masking detection tool 369
15.4.19 Pose detection tools 371
15.4.19.1 Functions of Pose detection tool 371
15.4.19.2 Video stream and scene requirements for Pose detection tools 372
15.4.19.3 Objects image requirements for Pose detection tool 372
15.4.19.4 Configure Pose detection tools 373
15.4.19.4.1 Setting up common parameters for Pose detection tools 373
15.4.19.4.2 Specific settings for the Sitting person detection tool 375
15.4.19.4.3 Specific settings for the Man down detection tool 376
15.4.19.4.4 Specific settings for Hands up detection tool 378
15.4.19.4.5 Specific settings for Handrail holding detection tool 378
15.4.19.4.6 Specific settings for People counter detection tool 379
15.4.19.4.7 Specific settings for Close-standing people detection tool 381
15.4.19.4.8 Specific settings for People masking detection tool 382
15.4.20 Retail Analytics 383
15.4.20.1 Functions of retail analytics 383

15.4.20.2 Camera requirements for Queue detection ... 383
15.4.20.3 Camera requirements for Visitors counter operation ... 384
15.4.20.3.1 Requirements for the person size in the frame ... 385
15.4.20.4 Configuring retail analytics detection tools ... 386
15.4.20.4.1 Configuring the Queue detection tool ... 386
15.4.20.4.2 Configuring the Visitors counter detection tool ... 388
15.4.21 Water Level Detection ... 390
15.4.21.1 Camera requirements for Water level detection ... 390
15.4.21.2 Configuring Water level detection ... 390
15.4.22 Embedded Detection Tools ... 393
15.4.22.1 Embedded Temperature Detection Tool ... 393
15.4.22.2 Obtaining metadata ... 394
15.4.22.3 ANPR ... 394
15.4.22.4 AxxonSoft tracking in Axis devices ... 394
15.4.23 Configuring Inputs ... 397
15.4.24 Checking the Triggering of a Detection Tool ... 398
15.4.25 Automatic Rules ... 399
15.5 Configuring macros and counters ... 400
15.5.1 General information about the macros ... 400
15.5.1.1 Types of macros ... 400
15.5.1.2 Configuring macros ... 401
15.5.2 General information about the counters ... 401
15.5.3 Create Macros ... 403
15.5.4 Creating and configuring counters ... 405
15.5.5 Configuring filters for event-driven macros ... 407
15.5.5.1 Specific parameters for triggering a face recognition macro ... 411
15.5.5.2 Triggering macros by statistical data ... 412
15.5.6 Settings specific to actions ... 413
15.5.6.1 Wait for event ... 413
15.5.6.2 Wait for timeout ... 414
15.5.6.3 Wait till previous action finishes ... 415
15.5.6.4 Record to archive ... 418
15.5.6.5 Initiating an alarm in the system ... 420
15.5.6.6 Stopping alarm ... 421
15.5.6.7 Switch output ... 422

15.5.6.8 Switching to a PTZ camera preset ... 422
15.5.6.9 Arm /disarm a camera ... 422
15.5.6.10 Checking whether the camera is in armed mode ... 423
15.5.6.11 View camera ... 424
15.5.6.12 Open layout ... 425
15.5.6.13 Show map ... 426
15.5.6.14 Starting export ... 427
15.5.6.15 Start replication ... 429
15.5.6.16 Notifications ... 431
15.5.6.16.1 Audio notification on Client ... 431
15.5.6.16.2 Voice notification from Client ... 432
15.5.6.16.3 Play audio on Server ... 432
15.5.6.16.4 E-mail notification ... 433
15.5.6.16.4.1 The E-mail notifier object ... 435
15.5.6.16.5 Push notification ... 437
15.5.6.16.6 Telegram bot notification ... 438
15.5.6.17 Starting an external program on Clients ... 439
15.5.6.18 Starting an external program on Servers ... 439
15.5.6.19 Start/stop slideshows of layouts ... 441
15.5.6.20 Enable/disable a component ... 442
15.5.6.21 Checking for archive video recordings ... 442
15.5.6.22 Switching to MomentQuest2 search results in archive ... 444
15.5.6.23 Executing a macro ... 444
15.5.6.24 Checking protected video records in the archive ... 444
15.5.6.25 Executing a web query ... 444
15.5.6.26 Text templates in macros ... 445
15.5.6.27 Managing the counter ... 447
15.5.7 Cyclical macros ... 448
15.6 Configuring user permissions ... 450
15.6.1 Types of user permissions to hardware, archives and macros ... 451
15.6.2 Creating and configuring roles ... 452
15.6.3 Connecting to an LDAP catalog ... 462
15.6.4 Working with users ... 464
15.6.4.1 Creating local users ... 464
15.6.4.1.1 Registering local users ... 464

15.6.4.1.2 Adding users to a role ... 466
15.6.4.2 Locking a user account ... 467
15.6.4.3 Creating LDAP connections ... 468
15.6.4.4 Synchronize LDAP users ... 469
15.6.4.5 Deleting users ... 469
15.6.5 Configuring the user security policy ... 469
15.7 Configuring layouts ... 471
15.7.1 Creating and deleting layouts ... 471
15.7.2 Rename Layouts ... 472
15.7.3 Reorder Layouts ... 473
15.7.4 Layout copying ... 473
15.7.5 Editing layouts ... 473
15.7.5.1 Switching to layout editing mode ... 474
15.7.5.2 Selecting a layout for editing ... 475
15.7.5.3 Configuring layout cells ... 475
15.7.5.3.1 Adding new cells to a layout ... 475
15.7.5.3.2 Resizing cells ... 478
15.7.5.3.3 Moving cells ... 479
15.7.5.3.4 Adding cameras to cells ... 479
15.7.5.3.5 Adding information boards to cells ... 481
15.7.5.3.6 Linking cells ... 481
15.7.5.3.7 Merging videos from adjacent cameras (FrameMerge) ... 482
15.7.5.3.8 Clearing cells ... 484
15.7.5.4 Configuring viewing tiles ... 484
15.7.5.4.1 Selecting default functions for viewing tiles ... 484
15.7.5.4.2 Selecting the default video stream for all cameras on the layout ... 484
15.7.5.4.3 Selecting the default video mode for a camera ... 484
15.7.5.4.4 Moving input and output icons in a viewing tile ... 485
15.7.5.4.5 Configuring default zoom levels (the Fit screen function) ... 485
15.7.5.4.6 Configuring pan/tilt angle for video cameras with Immervision lenses in 180o Panorama display format ... 486
15.7.5.4.7 Configuring display of water level detection ... 487
15.7.5.4.8 Adding links to other cameras to the Camera Window ... 488
15.7.5.5 Configuring information boards ... 489
15.7.5.5.1 Configuring information board templates ... 489

15.7.5.5.2 Configuring an Event Board ... 490
15.7.5.5.3 Configuring a Health Board ... 491
15.7.5.5.4 Configuring a Statistics Board ... 492
15.7.5.5.5 Configuring a Web Board ... 493
15.7.5.5.6 Configuring a Dialog Board ... 495
15.7.5.5.7 Configuring an Alarm Board ... 498
15.7.5.6 Configuring Alarms Panel on a layout ... 499
15.7.5.7 Exiting Layout Editing mode ... 499
15.7.6 Share Layouts ... 499
15.7.7 Configuring special layouts ... 501
15.7.7.1 Creating special layouts ... 501
15.7.7.2 Configuring Alarmed cameras layout ... 502
15.7.7.3 Configuring Marked cameras layout ... 504
15.7.8 Configuring user-defined slide shows ... 506
15.7.9 Setting the default layout ... 507
15.7.10 Setting a layout ID ... 507
15.8 Configuring Videowall ... 508
15.9 Configuring the interactive map ... 510
15.9.1 Adding a new map ... 510
15.9.2 Adding system objects to the map ... 512
15.9.2.1 Adding video cameras and changing size of their icons on the map ... 512
15.9.2.2 Adding inputs and outputs ... 512
15.9.2.3 Adding switches to another map ... 513
15.9.2.4 Adding counters ... 513
15.9.2.5 Adding macros ... 514
15.9.3 Configuring cameras on the map ... 515
15.9.3.1 Configuring a camera in standard map viewing mode ... 515
15.9.3.2 Configuring cameras with an embedded GPS tracker ... 517
15.9.3.3 Configuring cameras in immersion mode ... 517
15.9.4 Attaching a map to a layout ... 518
15.9.5 Configuring the floors ... 519
15.9.5.1 Creating a new floor ... 519
15.9.5.1.1 Adding child map ... 519
15.9.5.1.2 Adding as child map ... 520
15.9.5.2 Configuring floor location on the map ... 522

15.9.5.3 Editing a floor ... 522
15.9.5.4 Removing a floor ... 523
15.9.6 Removing objects from the map ... 523
15.9.7 Setting keywords for geo map search ... 523
15.9.8 Changing map type and display ... 524
15.9.9 Renaming the map ... 524
15.9.10 Sorting of map lists ... 524
15.9.11 Deleting a map ... 524
15.10 System preferences ... 525
15.10.1 Server settings ... 525
15.10.1.1 Configuring Forensic Search MomentQuest in Archive ... 525
15.10.1.1.1 Turning on the video stream metadata recording ... 525
15.10.1.1.2 Configuring user permissions for Forensic Search in archive ... 526
15.10.1.1.3 Video suitability for Forensic Search of recorded video (requirements) ... 526
15.10.1.2 Setting up privacy masking ... 526
15.10.1.2.1 Masking faces ... 526
15.10.1.2.2 Setting up privacy masking in Video Footage ... 527
15.10.1.3 Analyzing video from external systems (Offline Analytics) ... 531
15.10.1.3.1 Importing video to Axxon One ... 531
15.10.1.3.2 Indexing video from external sources ... 533
15.10.1.3.3 How to set a folder to import videos from ... 534
15.10.1.4 Configuring hardware video decoding for display on the Client ... 535
15.10.1.4.1 Hardware-based decoding with Intel Quick Sync Video ... 535
15.10.1.4.2 Hardware-based decoding with NVIDIA NVDEC chips ... 537
15.10.1.4.3 Simultaneous decoding with Intel Quick Sync Video and NVIDIA NVDEC chips ... 538
15.10.1.5 Configuring automatic response when Axxon One VMS PC integrity check fails ... 538
15.10.1.6 Configuring storage of the system log and metadata ... 539
15.10.1.7 Configuring Alarm processing ... 540
15.10.1.8 Configuring PTZ control ... 540
15.10.1.9 Configuring schedules ... 541
15.10.1.9.1 Creating schedules ... 541
15.10.1.9.2 Deleting a schedule ... 542
15.10.1.10 Configuring the Server ports ... 543
15.10.1.10.1 Changing the gRPC API port ... 543
15.10.1.10.2 Changing the port range of the Server ... 543

15.10.1.11 Configuring Server logging ... 543
15.10.1.12 Configuring NTP synchronization ... 544
15.10.1.13 Vector maps in Axxon One ... 545
15.10.1.13.1 Raster or vector image ... 546
15.10.1.13.2 Google ... 546
15.10.1.13.3 OpenStreetMap ... 550
15.10.2 Client settings ... 551
15.10.2.1 Configuring the user interface ... 551
15.10.2.1.1 Selecting the interface language ... 551
15.10.2.1.2 Selecting the calendar type ... 553
15.10.2.1.3 Configuring the slideshow parameters ... 554
15.10.2.1.4 Hiding prompts ... 554
15.10.2.1.5 Configuring smooth motion ... 555
15.10.2.1.6 Configuring display of video statistics ... 555
15.10.2.1.7 Configuring preview of alarm events ... 556
15.10.2.1.8 Configuring map auto zoom ... 557
15.10.2.1.9 Configuring the Client screen mode (full screen or window) ... 557
15.10.2.1.10 Configuring the display of the surveillance window ... 558
15.10.2.1.11 Configuring time display ... 559
15.10.2.1.12 Configuring the display of the camera short name ... 560
15.10.2.1.13 Optimizing video image on the layout ... 560
15.10.2.1.14 Configuring video display on the layout ... 562
15.10.2.1.15 Configuring camera sorting on Objects Panel ... 564
15.10.2.1.16 Configuring the videowall mode ... 565
15.10.2.1.17 Configuring cell maximization on double click ... 565
15.10.2.2 Configuring how Axxon One starts ... 567
15.10.2.2.1 Configuring Axxon One instead of the standard Windows OS shell ... 567
15.10.2.2.2 Configuring Cross-System Client and autologon ... 568
15.10.2.2.3 Configuring automatic exiting and locking of the Client ... 570
15.10.2.2.4 IP address filtering configuration ... 571
15.10.2.2.5 Selecting Preferred Servers ... 571
15.10.2.3 Configuring export ... 572
15.10.2.3.1 Configuring export options ... 572
15.10.2.3.2 Configuring Export agent ... 576
15.10.2.4 Configuring audio on the Client ... 577

15.10.2.5 Configuring hot keys ... 578
15.10.2.5.1 Introduction to hot keys in Axxon One ... 578
15.10.2.5.2 Assigning hot keys ... 578
15.10.2.5.3 Exporting and importing hot keys ... 579
15.10.2.5.4 Notes regarding hot key actions ... 579
15.10.2.5.5 Joystick Configuration ... 581
15.10.2.6 Configuring video capturing on operator monitor ... 583
15.10.2.7 Configuring Client logging ... 586
15.11 Configuring Failover VMS ... 587
15.11.1 General information about a failover system ... 587
15.11.2 Ports used by the failover system ... 588
15.11.3 Supervisor Web-Interface ... 589
15.11.4 Creating a cluster ... 590
15.11.5 Failover Database ... 594
15.11.6 Configure a Failover System Cluster ... 595
15.11.6.1 Setting up basic configuration ... 595
15.11.6.2 Setting up a configuration with the backup Server ... 599
15.11.6.3 Creating and configuring independent nodes ... 602
15.11.6.4 1+1 cluster configuration ... 604
15.11.6.4.1 Setting up 1+1 configuration ... 604
15.11.6.4.2 Converting to 1+1 configuration ... 605
15.11.6.4.3 Editing the configuration ... 606
15.11.6.4.4 Setting up archive replication ... 607
15.11.6.4.5 How replication will run ... 608
15.11.6.5 Suspending a Server within a cluster ... 608
15.11.6.6 Disbanding a cluster ... 608
15.11.7 Set up access to a supervisor ... 609
15.11.8 Configuration backup and restore for failover VMS ... 610
15.11.9 Cluster Monitoring ... 612
15.11.10 Connecting to a Node and Configuring of an Axxon domain ... 613
15.11.11 Configuring automatic connections to nodes ... 614
15.11.12 Updating Servers within a cluster ... 614
15.11.13 Setting network interfaces for system nodes operation ... 616
15.11.14 Connecting the Client to the Failover Server behind NAT ... 616
15.11.15 Changing logging levels for the Consul and Nomad processes in a failover system ... 618

15.11.15.1 Changing the logging level for Consul ... 618
15.11.15.2 Changing the logging level for Nomad ... 618
15.12 Self-diagnostics service ... 619
15.12.1 General information about the self-diagnostics service ... 619
15.12.2 Starting and stopping the self-diagnostics service ... 619
15.12.3 Viewing metrics in the self-diagnostics service ... 620
15.12.4 Viewing self-diagnostics metrics using third-party Grafana | Prometheus software ... 624
16 Working with the Axxon One Software Package ... 628
16.1 Main Elements of the User Interface ... 628
16.1.1 Surveillance window ... 628
16.1.1.1 Color Coding of Frames ... 630
16.1.1.2 Viewing Tile Context Menu ... 630
16.1.1.3 Time Display ... 631
16.1.1.4 Display of Video Statistics ... 632
16.1.1.5 Video Surveillance Mode Selection Tabs ... 633
16.1.1.6 Advanced Archive Navigation Panel ... 633
16.1.2 Information boards ... 635
16.1.3 The Archive Navigation Panel ... 636
16.1.3.1 Show and Hide the Archive Navigation Panel ... 636
16.1.3.2 The Structure and Function of the Archive Navigation Panel ... 637
16.1.3.3 Events filter ... 638
16.1.3.4 The Timeline ... 639
16.1.3.5 Events List ... 641
16.1.3.6 The Playback Panel ... 643
16.1.4 Video Wall Panel ... 643
16.1.5 Monitor Panel ... 644
16.1.6 The Layouts panel ... 644
16.1.7 Interactive Map ... 645
16.1.8 Camera Search Panel ... 646
16.1.9 Alert panel ... 646
16.1.10 Objects Panel ... 648
16.1.11 The PTZ Control Panel ... 650
16.1.12 Story board ... 652
16.2 Video Surveillance ... 653
16.2.1 Video Surveillance Modes ... 653

16.2.2 Functions Available in All Video Surveillance Modes 654
16.2.2.1 Scaling the surveillance window 654
16.2.2.2 Digitally Zooming Video Images 655
16.2.2.2.1 Enlarging a video image using the digital zoom scale 655
16.2.2.2.2 Enlarging a video image through area selection 656
16.2.2.2.3 Enlarging a video image using the mouse scroll wheel 657
16.2.2.3 Video image processing 657
16.2.2.3.1 Changing the Contrast Level 658
16.2.2.3.2 Setting the Sharpness Level 659
16.2.2.3.3 Using Deinterlacing 660
16.2.2.4 Rotate Video Image 661
16.2.2.5 Tracking objects 663
16.2.2.6 Operator comments 667
16.2.2.6.1 Adding comments in different surveillance modes 668
16.2.2.6.2 Adding a comment 668
16.2.2.7 Switching to other camera via a link in the Camera window 670
16.2.2.8 Viewing titles from POS terminals 670
16.2.2.9 Partial decoding of video 672
16.2.2.10 Displaying information from a detection tool (mask) 672
16.2.3 Real-time video surveillance 673
16.2.3.1 Switching to Live Video Mode 673
16.2.3.2 Video Surveillance Functions Available in Live Video Mode 674
16.2.3.3 Arming and Disarming a Video Camera 674
16.2.3.4 Controlling a PTZ Camera 675
16.2.3.4.1 Presets 678
16.2.3.4.1.1 Creating and editing presets 678
16.2.3.4.1.2 Selecting a preset 679
16.2.3.4.2 PTZ Tours 680
16.2.3.4.2.1 Creating and editing PTZ tours 680
16.2.3.4.2.2 Launching a PTZ tour 681
16.2.3.4.3 Control using step buttons and virtual joystick 681
16.2.3.4.4 Patrolling 682
16.2.3.4.5 Controlling Focus, Iris and Optical Zoom 683
16.2.3.4.6 Controlling a PTZ Video Camera in the OnScreen PTZ Mode 683
16.2.3.4.7 Control using Point&Click 684

16.2.3.4.8 Control using Areazoom 684
16.2.3.5 Functions for tracking of moving objects 685
16.2.3.5.1 Tag&Track Pro 685
16.2.3.5.2 Tag & Track Lite 686
16.2.3.5.3 Simultaneously using Tag & Track Pro and Tag & Track Lite 687
16.2.3.6 Managing Outputs 687
16.2.3.7 Displaying the input status 689
16.2.3.8 Selecting video stream quality in a Surveillance window (GreenStream) 690
16.2.3.9 Autozoom 691
16.2.3.10 Autoreplace Offline Cameras on Layouts 693
16.2.3.11 Snapshot 693
16.2.3.12 Viewing selected camera's detection tool triggering events 693
16.2.3.13 Removing a camera from a layout 694
16.2.4 Video surveillance in archive mode 695
16.2.4.1 Switching to Archive Mode 695
16.2.4.2 Video Surveillance Functions Available in Archive Mode 697
16.2.4.3 Selecting an Archive 697
16.2.4.4 Viewing a combined Archive 698
16.2.4.5 Synchronized playback of archives 698
16.2.4.6 Compressed playback of archives (TimeCompressor) 699
16.2.4.6.1 Switching to TimeCompressor mode 699
16.2.4.6.2 Playback control 700
16.2.4.6.3 Switching back to the original recording of an object 701
16.2.4.7 Viewing recorded video with operator comments 702
16.2.4.8 Viewing External Archives 703
16.2.4.9 Delete a part of an archive 704
16.2.4.10 Navigating in the Archive 705
16.2.4.10.1 Navigating Using the Timeline 705
16.2.4.10.2 Navigation using the advanced panel 706
16.2.4.10.3 Navigating Using the Events list 708
16.2.4.10.4 Navigating using the Playback Panel 708
16.2.4.10.5 Navigation via the time indicator 709
16.2.4.10.6 Keyboard navigation 709
16.2.4.11 Displaying the causes of triggered Scene Analytics detection tools 710
16.2.4.12 Viewing the results of a saved search query 710

16.2.4.13 Manual Archive Replication ... 712
16.2.4.14 Tag & Track Lite in Archive mode ... 713
16.2.5 Video surveillance in alarm management mode ... 714
16.2.5.1 Video surveillance functions available in Alarm Management mode ... 714
16.2.5.2 Switch to Alarm Management mode ... 714
16.2.5.3 Initiating an alarm event ... 715
16.2.5.3.1 Manual initiation ... 715
16.2.5.3.2 Automatic Initiation ... 716
16.2.5.4 Working with an assessment of an alarm event ... 716
16.2.5.4.1 Displaying and viewing alarm events ... 716
16.2.5.4.2 Outlining an object that triggered an alarm event ... 717
16.2.5.4.3 Selecting an alarm event for Alarm Management ... 717
16.2.5.5 Working with the Alarm Management window ... 718
16.2.5.5.1 Interface elements of the Alarm Management window ... 718
16.2.5.5.2 Alarm event playback ... 718
16.2.5.5.3 Assessing an alarm event ... 719
16.2.5.6 Limitations when working with alarm events in case of multi-user processing ... 720
16.2.6 Video surveillance in archive search mode ... 721
16.2.6.1 Switching to Archive Search mode ... 721
16.2.6.2 Archive Search mode interface ... 722
16.2.6.3 Video surveillance functions available in Archive Search mode ... 724
16.2.6.4 Search in an archive of a single video camera ... 725
16.2.6.4.1 Selecting the search type ... 725
16.2.6.4.2 Setting a search interval ... 725
16.2.6.4.3 Events search ... 727
16.2.6.4.4 Time search for video fragments (TimeSlice) ... 728
16.2.6.4.5 Searching comments ... 729
16.2.6.4.6 Forensic Search for Fragments (MomentQuest) ... 730
16.2.6.4.6.1 Motion in Area ... 730
16.2.6.4.6.2 Loitering of an object in a specific area ... 732
16.2.6.4.6.3 Simultaneous presence of a large number of objects in a specific area ... 732
16.2.6.4.6.4 Motion from one area to another ... 733
16.2.6.4.6.5 Crossing of a virtual line by an object's trajectory ... 734
16.2.6.4.6.6 Configure the search parameters ... 735
16.2.6.4.7 Titles search ... 740
16.2.6.4.8 LPR search ... 741

16.2.6.4.9 Face search ... 744
16.2.6.4.9.1 Search for similar face ... 744
16.2.6.4.9.2 Search for all recognized faces ... 746
16.2.6.4.9.3 Search for face contacts ... 747
16.2.6.4.9.4 Identifying "friend" or "foe" from a photo ... 748
16.2.6.4.10 Saving search queries ... 749
16.2.6.4.11 Switching between search results ... 749
16.2.6.4.12 Working with search results ... 750
16.2.6.4.12.1 Viewing search results ... 750
16.2.6.4.12.2 Viewing Search Results In TimeCompressor ... 751
16.2.6.4.12.3 Playback of video fragments ... 752
16.2.6.4.12.4 Enlargement of found moments ... 754
16.2.6.4.12.5 Exporting the video fragments and repeated search ... 755
16.2.6.4.13 Heat map ... 755
16.2.6.4.14 Image Search ... 756
16.2.6.5 Simultaneous search in an archive of several video cameras ... 759
16.2.7 Working with fisheye cameras ... 761
16.2.7.1 Viewing modes for video from fisheye cameras ... 761
16.2.7.1.1 Selecting viewing mode for videos from a fisheye camera ... 761
16.2.7.1.2 360 degree Panorama and Regional view (virtual PTZ) ... 761
16.2.7.1.3 180 degree Panorama ... 763
16.2.7.2 Fisheye cameras on an interactive map ... 764
16.2.7.2.1 Viewing video and controlling a fisheye camera from the map ... 764
16.2.7.2.2 Fish-eye cameras in immersive mode ... 765
16.2.8 Face recognition and search ... 765
16.2.9 Vehicle number plate recognition and search ... 768
16.2.10 Temperature screening ... 769
16.3 Working with information boards ... 771
16.3.1 Resizing information boards ... 771
16.3.2 Hiding information boards ... 771
16.3.3 Automatically switching to layouts with information boards ... 772
16.3.4 Working with Event Boards ... 772
16.3.4.1 Options for displaying information on Events Boards ... 772
16.3.4.2 Switching a camera linked to an Event Board to the archives ... 774
16.3.5 Working with System Health Boards ... 774
16.3.5.1 Viewing server status ... 775

16.3.5.2 Viewing camera status ... 777
16.3.6 Working with Statistics Boards ... 779
16.3.7 Working with Web Boards ... 781
16.3.8 Working with Dialog Board ... 782
16.3.9 Working with an Alarm Board ... 784
16.4 Layouts management ... 786
16.4.1 Changing cameras on a layout ... 786
16.4.2 Selection and Slideshow of Layouts ... 786
16.4.3 Working with Special layouts ... 788
16.5 Monitor management ... 790
16.5.1 Managing monitors on a local Client ... 790
16.5.1.1 Displaying layouts on monitors ... 790
16.5.1.2 Editing layouts ... 791
16.5.1.3 Selecting cameras to display on the layout ... 791
16.5.1.4 Closing the layout of the additional monitor ... 792
16.5.2 Managing monitors on remote Clients within the Axxon-domain ... 792
16.6 Audio Monitoring ... 793
16.6.1 General Information ... 793
16.6.2 Listening on the Client to sound from a camera microphone ... 793
16.6.3 Playing back sound from Client microphone on camera speakers ... 794
16.7 Working with the interactive map ... 795
16.7.1 Opening and closing the map ... 796
16.7.2 Geo map search ... 797
16.7.3 Changing the map tilt ... 798
16.7.4 Scaling and focusing of map ... 800
16.7.5 Customizing an Interactive Map ... 801
16.7.6 Switching between maps ... 801
16.7.7 Immersion mode ... 802
16.7.8 Controlling devices from the map ... 803
16.7.9 Displaying device status ... 805
16.7.10 Displaying the counters ... 806
16.7.11 Selecting Cameras for a Temporary Layout ... 807
16.8 Exporting frames and video recordings ... 808
16.8.1 Frame export ... 808
16.8.2 Exporting Video Recordings ... 809

16.8.2.1 Standard video recordings export ... 809
16.8.2.2 Instant video export ... 812
16.8.2.3 Simultaneous export of video from multiple cameras ... 813
16.8.2.4 Exporting all event videos ... 814
16.8.3 Configuring export area and masks ... 816
16.8.4 Viewing export progress ... 817
16.9 Macros control ... 817
16.10 Event control ... 818
16.10.1 Control in Live Video mode ... 818
16.10.2 The System Log ... 819
16.10.2.1 Setting Event Search Filters ... 819
16.10.2.2 Event search procedure ... 820
16.10.2.3 Refreshing Event Search Results ... 820
16.10.2.4 Viewing Event Search Results ... 821
16.10.2.5 Exporting Event Search Results ... 822
16.10.2.6 Switching to archive video of specific events ... 822
16.11 Working with Axxon One through the Web-Client ... 823
16.11.1 Web-Client overview ... 823
16.11.2 Hardware and software requirements for the Web-Client operation ... 823
16.11.3 Starting and logging in to the Web-Client ... 823
16.11.3.1 Changing the user in the Web-Client ... 825
16.11.4 Web-Client GUI ... 826
16.11.5 Web-Client configuration ... 827
16.11.5.1 Changing the user password in the Web-Client ... 829
16.11.6 Searching for video cameras in the Web-Client ... 830
16.11.7 Working with layouts in Web-Client ... 832
16.11.7.1 Summary of how to work with layouts in Web-Client ... 832
16.11.7.2 Selecting and searching for a layout ... 833
16.11.7.3 Creating a new layout in the Web-Client ... 833
16.11.7.4 Editing and deleting layouts in Web-Client ... 835
16.11.7.5 Selecting the default layout in Web-Client ... 836
16.11.7.6 Copying layouts in the Web-Client ... 837
16.11.7.7 Sharing layouts in the Web-Client ... 837
16.11.8 Real-time video surveillance in the Web-Client ... 838
16.11.9 Controlling PTZ cameras through the Web-Client ... 841

16.11.9.1 Controlling a PTZ camera through the Web-Client by using presets ... 841
16.11.9.2 Changing the optical zoom of a PTZ camera in the Web-Client ... 842
16.11.9.3 Changing the positioning speed of a PTZ camera in the Web-Client ... 842
16.11.9.4 Changing the tilt of a PTZ camera in the Web-Client ... 842
16.11.10 Viewing video archives through the Web-Client ... 843
16.11.10.1 Single-camera archive view mode ... 843
16.11.10.2 Multi-camera archive view mode ... 844
16.11.11 Archive position selection panel for the Web-Client ... 846
16.11.12 Archive search in the Web-Client ... 847
16.11.12.1 Types of archive search in the Web-Client ... 849
16.11.12.2 Building a Heat Map ... 849
16.11.12.3 Simultaneous search in multiple camera Video Footage via the Web-Client ... 851
16.11.12.4 Reporting the search results ... 851
16.11.13 Viewing and processing alarms in Web-Client ... 852
16.11.13.1 Alarm processing in the Web-Client ... 853
16.11.14 Listening to a camera's microphone via the Web-Client ... 854
16.11.15 Digital video zoom in the Web-Client ... 854
16.11.16 Export in the Web-Client ... 854
16.11.17 Viewing Camera and Archive Statistics ... 856
16.11.18 Working with bookmarks in the Web-Client ... 857
16.11.18.1 Editing a bookmark ... 858
16.11.18.2 Deleting a bookmark ... 858
16.11.18.3 Un-protecting a video ... 858
16.11.18.4 Deleting a protected video ... 858
16.12 Working with Axxon One Through the Mobile Clients ... 858
16.13 Changing user password ... 858
17 Description of utilities ... 860
17.1 Axxon One Tray Tool ... 860
17.2 Activation utility ... 860
17.3 Axxon Support Tool ... 863
17.3.1 Purpose of the Support.exe Utility ... 863
17.3.2 Launching and Closing the Utility ... 863
17.3.3 Description of the Support.exe utility interface ... 864
17.3.4 The Processes Service ... 865
17.3.5 Collecting Data on the Configuration of Servers and Clients Using the Support ... 867

17.4 Log Management Utility ... 870
17.4.1 Starting and closing the utility ... 870
17.4.2 Configuring a Log archive ... 871
17.4.3 Configuring Logging levels ... 872
17.4.4 Set the size and maximum number of logs ... 873
17.4.5 Configuring Client RAM usage logging ... 874
17.5 Digital signature verification utility ... 875
17.6 Backup and Restore Utility ... 877
17.6.1 Purpose of BackupTool.exe ... 877
17.6.2 Starting and quitting BackupTool.exe ... 877
17.6.3 Roll back the local configuration to a selected restore point ... 880
17.6.4 Roll back the global configuration to a selected restore point ... 884
17.6.5 Configuration backup ... 885
17.6.6 Configuration restore ... 889
17.6.7 Changing the Server name ... 893
17.7 POS-terminal log collection utilit ... 895
17.8 Console utility for working with archives ... 897
17.9 Network settings utility ... 899
18 Appendices ... 901
18.1 Appendix 1. Glossary ... 901
18.2 Appendix 2. Known issues in the Axxon One Software Package ... 903
18.2.1 Possible errors during installation ... 903
18.2.1.1 Error connecting to the Postgres Database ... 904
18.2.1.2 Error installing Drivers Pack ... 904
18.2.1.3 Window 10 OS installation error ... 904
18.2.1.4 Server error on Windows 11 OS and Windows Server 2019 OS ... 904
18.2.1.5 An error occurred when installing on Windows with the language pack Norsk (bokmål) ... 905
18.2.1.6 Error uninstalling Axxon One on systems with Videoinspector installed ... 905
18.2.2 Possible Errors During Start-Up ... 905
18.2.2.1 The Client cannot be connected to the Server ... 905
18.2.3 Possible Errors During Operation ... 905
18.2.3.1 All video channels or archives stop working once the license maximum is reached ... 906
18.2.3.2 No signal from video cameras and failure to connect to other Servers ... 906
18.2.3.3 Incorrect display of Client interface elements ... 906

18.2.3.4 Server error on Windows Server 2012 ... 906
18.2.3.5 Emergency shutdown of the Client on Windows 8.1 ... 906
18.2.3.6 Error creating new archives even when license restriction on total capacity is observed ... 906
18.2.3.7 Axxon One VMS operation with Windows Defender software ... 907
18.2.3.8 Upper panel display problem ... 907
18.2.3.9 High CPU load during OpenGL software emulation ... 907
18.2.3.10 Axxon One operation with NetLimiter 2 ... 907
18.2.3.11 Exported videos' playback in Movies and TV application ... 907
18.2.3.12 Axxon One operation on Windows N and KN editions ... 907
18.3 Appendix 3. Assigning of the domain takes place when the Axxon One server is installed ... 907
18.4 Appendix 4. Using Axxon One with antivirus software ... 908
18.4.1 ESET NOD32 ... 909
18.4.2 ESET NOD32 Internet Security ... 909
18.4.3 ESET Smart Security ... 909
18.4.4 AVG ... 909
18.4.5 DrWeb ... 909
18.5 Appendix 5. Using CH VM-Desktop USB multifunction controllers with Axxon One ... 909
18.6 Appendix 6. Hotkeys in Axxon One ... 912
18.7 Appendix 7. Automated configuration backup and restore ... 914
18.8 Appendix 8. Configuring and operating Axxon One in Linux OS ... 916
18.8.1 Linux OS supported versions ... 916
18.8.2 Axxon One limitations in Linux OS ... 916
18.8.3 Features and potential problems with Linux OS ... 917
18.8.3.1 Problem with displaying a dialog box or a drop-down list ... 917
18.8.3.2 Peculiarities of detection tools operation on NVIDIA GPUs in Linux OS ... 917
18.8.3.3 Problem with incorrect CPU load when decoding on Intel GPU in detection tool configuration ... 918
18.8.3.4 Peculiarities of database operation when the PostgreSQL service is stopped ... 918
18.8.4 Installing Axxon One in Linux OS ... 918
18.8.4.1 Installing the Axxon One Server in Linux OS ... 918
18.8.4.1.1 Installing from repository ... 918
18.8.4.1.2 Manual installation ... 919
18.8.4.1.3 Installing add-ons to the basic DetectorPack in Linux OS ... 921
18.8.4.2 Installing the Axxon One Client in Linux OS ... 922
18.8.5 Starting and stopping the Axxon One Server in Linux OS ... 924
18.8.6 Updating Axxon One on Linux OS ... 925

18.8.7 Uninstalling the Axxon One software in Linux OS ... 926
18.8.8 Configuration and log folders ... 926
18.8.9 Configuring the Axxon One Client logging parameters on Linux OS ... 926
18.8.10 System data collection in Linux OS ... 927
18.8.11 Configuring the metadata storage in NAS on Linux OS ... 928
18.8.12 Axxon One Server configuration change on Linux OS ... 928
18.8.13 Moving the Axxon One configuration from Windows OS to Linux OS ... 931
18.8.14 Starting and stopping the Axxon One self-diagnostics service in Linux OS ... 932
18.8.15 Archive creation features in Linux OS ... 933
18.8.15.1 Archive as a disk creation features in Linux OS ... 933
18.8.15.2 Archive as a file creation features in Linux OS ... 934
18.8.15.3 Features of archives with ext and xfs file systems ... 935
18.8.15.4 Features of NAS archives ... 935
18.8.16 Axxon One Server launch using Docker ... 935
18.8.16.1 Working with the Axxon One container ... 938
18.8.17 Licensing of the software module for License plate recognition (VT) on Linux OS ... 939
18.8.17.1 General information ... 939
18.8.17.2 Installing the Sentinel LDK Run-time environment ... 939
18.8.17.3 Installing a hardware key ... 940
18.8.17.4 Installing a software key ... 940
18.8.17.5 Updating the license ... 941
18.8.17.6 Removing a license ... 942
18.8.17.7 Checking a license ... 943
18.8.18 License activation of License plate recognition IV on Linux OS ... 943
18.9 Appendix 9. Using Axxon One with NAT ... 944
18.9.1 Consolidating the Servers from different networks into Axxon domain ... 944
18.9.2 Connecting the Client to the Server behind NAT ... 946
18.9.3 Connecting the Web and Mobile Clients to the Server behind NAT ... 948
18.9.4 Audio transmission from the Client's microphone behind NAT to the Server's or camera's loudspeaker ... 950
18.10 Appendix 10. Creating system variable ... 951

User Guide. Introduction(see page 36)
Software Lifecycle Policy(see page 38)

1 Description of the Software Package

Basic principles of building a security system based on the Axxon One software package(see page 40)

Axxon One features: reference information(see page 40)

Functions of the Distributed Security System(see page 44)

Network Topologies of the Axxon One Software Package(see page 44)

Specifications of the Axxon One Software Package(see page 45)

Implementation Requirements for the Axxon One Software Package(see page 46)

Interface of the Axxon One Software Package(see page 56)

Ports used by the Axxon One Software Package(see page 57)

Requirements for Personnel Quantity and Qualifications(see page 58)

2 Installing the Axxon One Software Package

Installing equipment(see page 60)

Installation the Axxon One Software Package(see page 62)

3 Licensing of the software product

Axxon One license types(see page 86)

Licensing methods(see page 90)

Product activation utility(see page 91)

License Activation(see page 93)

4 Launching and Closing the Axxon One Software Package

Startup(see page 94)

Shutdown(see page 99)

Automatic Server restart(see page 100)

Switching Users Quickly(see page 101)

Cross-System Client(see page 101)

Connecting LDAP users(see page 102)

Connecting to Another Server Quickly(see page 102)

5 Configuration of the Axxon One Software Package

General information on system configuration(see page 104)

Hardware configuration(see page 107)

Configuring Archives(see page 206)

Configuring detection tools(see page 234)

Configuring Macros[1]

Configuring user permissions(see page 450)

Configuring Layouts(see page 471)

Configuring Videowall(see page 508)

Configuring the Interactive Map(see page 510)

System preferences(see page 525)

Configuring Failover VMS(see page 587)

Self-diagnostics service(see page 619)

6 Working with the Axxon One Software Package

Main Elements of the User Interface(see page 628)

Video Surveillance(see page 653)

Working with information boards(see page 771)

Layouts Management(see page 786)

Monitor Management(see page 790)

Audio Monitoring(see page 793)

Working with the Interactive Map(see page 795)

Exporting Frames and Video Recordings(see page 808)

Macros control(see page 817)

Event Control(see page 818)

Working with Axxon One Through the Web-Client(see page 823)

1 https://docs.axxonsoft.com/confluence/display/one20en/Configuring+Macros

7 Description of utilities

Axxon One Tray Tool(see page 860)

Activation Utility(see page 860)

Axxon Support Tool(see page 863)

Log Management Utility(see page 870)

Digital signature verification utility(see page 875)

Backup and Restore Utility(see page 877)

POS-terminal log collection utility[2]

Console utility for working with archives(see page 897)

Network settings utility(see page 899)

8 Appendices

Appendix 1. Glossary(see page 901)

Appendix 2. Known issues in the Axxon One Software Package(see page 903)

Appendix 3. Assigning of the domain takes place when the Axxon One server is installed(see page 907)

Appendix 4. Using Axxon One with antivirus software(see page 908)

Appendix 5. Using CH VM-Desktop USB multifunction controllers with Axxon One(see page 909)

Appendix 6. Hotkeys in Axxon One(see page 912)

Appendix 7. Automated configuration backup and restore(see page 914)

Appendix 8. Configuring and operating Axxon One in Linux OS(see page 916)

Appendix 9. Using Axxon One with NAT(see page 944)

Appendix 10. Creating system variable(see page 951)

2 https://docs.axxonsoft.com/confluence/display/one20en/POS-terminal+log+collection+utility

9 User Guide. Introduction

On page:

- General Information(see page 36)
- Purpose of the Document(see page 36)
- Purpose and functionality of Axxon One(see page 36)

9.1 General Information

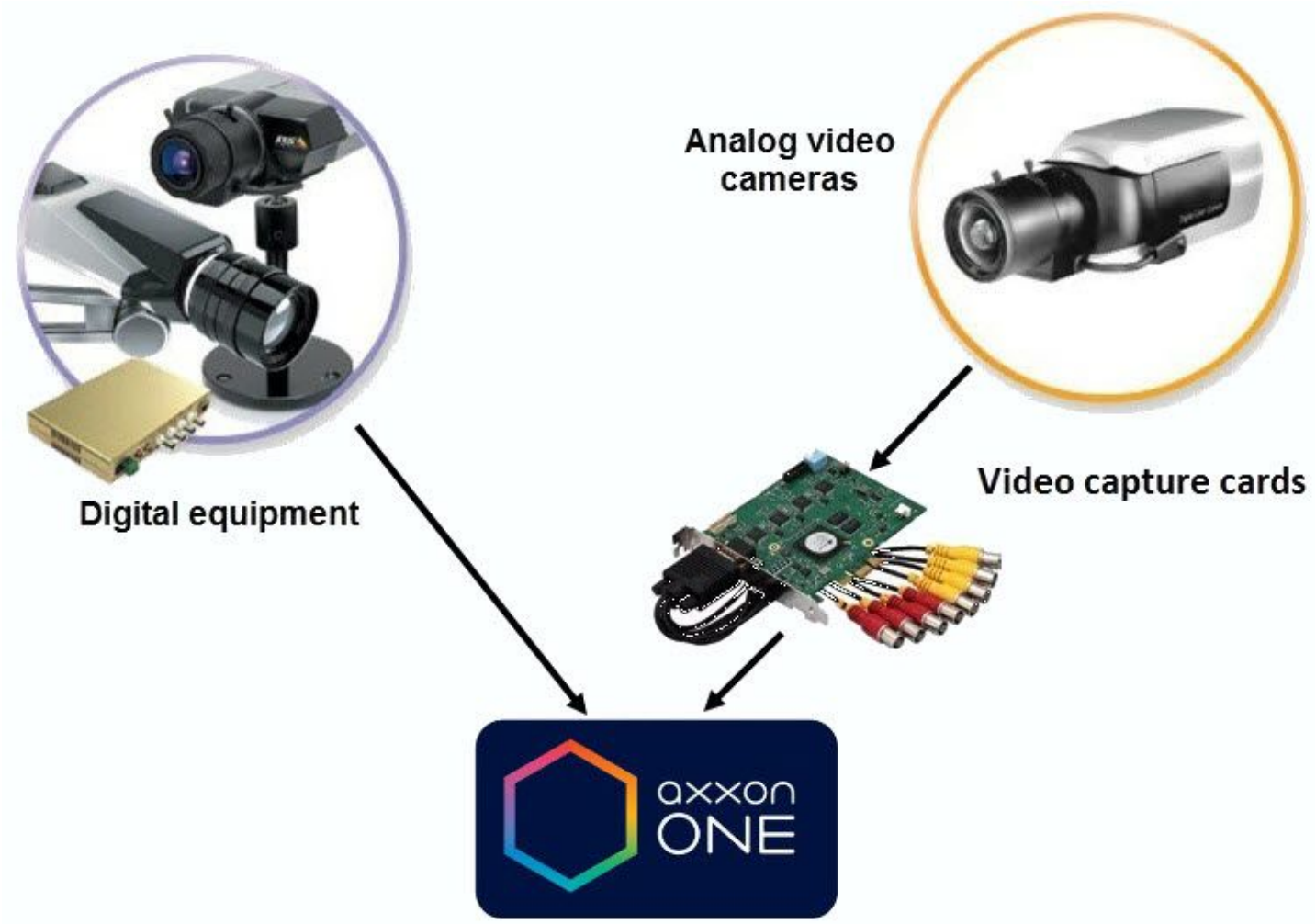
No part of this document may be reproduced or transmitted in any form or by any means without the prior written permission of AxxonSoft.
The *Axxon One* trademark is the property of AxxonSoft. All other trademarks included in this document are the property of their respective owners.
All information 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.

9.2 Purpose of the Document

This document, titled User guide(see page 32) contains the information necessary for building, implementing, and operating a security system based on *Axxon One*.
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 more detailed study. The chapters in this guide, whether they are informative or serve as a reference, have their own internal structure.
The chapters Introduction(see page 36) and Description of the Software Package(see page 40) are intended to generally acquaint the user with the technical features and functionality of the *Axxon One* software package, 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 equipment are presented in detail in the chapter Installing the Axxon One Software Package(see page 60). The chapter Licensing of the software product(see page 86) contains instructions on how to register a license to use the *Axxon One* software package.
Startup and shutdown of the software package are described in the chapter Launching and closing the Axxon One software package(see page 94).
The chapter Configuration of the Axxon One Software Package(see page 104) 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 the *Axxon One* software package are presented in chapter Working with the Axxon One Software Package(see page 628).
Chapter Description of utilities(see page 860) contains a description of additional software utilities employed when working with the software package.
The Appendices(see page 901) 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*.

9.3 Purpose and functionality of Axxon One

The *Axxon One* software package is a next-generation open-platform video management software (VMS). Security systems based on *Axxon One* range from home security systems (for an apartment or house) to Proffesional large-scale distributed security systems for small and mid-size businesses (hotels, automotive service centers, shops, parking structures, etc.).
Video and audio surveillance of guarded locations, video analysis, 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.
The *Axxon One* software package enables the user to accomplish a wide spectrum of tasks, as it works both with digital equipment and with analog video cameras (through video capture cards), and also makes it possible to create a hybrid security system containing both kinds of equipment.



The modern and constantly expanding feature set of *Axxon One* allows implementing new video surveillance functionality that increases the convenience and precision of protection at end-user sites.

10 Software Lifecycle Policy

On page:

- Software Lifecycle Phases(see page 38)
- Software Technical Support(see page 38)
- Standard Period for Release of Software Updates(see page 38)
- Licensing Policy with Regard to Software Updates(see page 38)

10.1 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.

10.2 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.

10.3 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[3]. Releases with bug and security fixes can be requested from technical support[4].

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

10.4 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.

3 https://www.axxonsoft.com/
4 https://support.axxonsoft.com/jira/secure/Dashboard.jspa

- New software features that are subject to licensing will not be available until the license key is updated.

11 Description of the Software Package

11.1 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(see page 46), Operating system requirements(see page 47))
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(see page 58)).

11.2 Axxon One features: reference information

On the page:

- Micromodule architecture(see page 41)
- Support for IP devices(see page 41)
- Support for analog cameras in Axxon One(see page 41)
- Video and Audio Detection Tools(see page 42)
- Video archive(see page 42)
- Interactive 3D Map(see page 43)
- User Interface(see page 43)
- Face Recognition(see page 43)
- Number Plate Recognition(see page 43)
- Receiving Events from External Systems(see page 43)

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 1500 models of IP cameras is included, as well as remote access from mobile devices and a web interface. The *Axxon One* software package supports touchscreens.

11.2.1 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.

11.2.2 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.

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.

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.

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.

360 degree camera support

360 degree camera support allows dewarping video from a fish-eye 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 unit.

ONVIF

AxxonSoft is a member of ONVIF[5] (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*.

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.

11.2.3 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.

5 http://www.onvif.org/

11.2.4 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 in area detection.
3. Neural tracker.
4. Object tracker.
5. Pose detection.
6. Equipment detection (PPE).
7. Person-based privacy masking.
8. Fire detection and smoke detection.
9. Water level detection.
10. Neurocounter.
11. Queue detection.
12. Visitors counter.

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

1. Noise detection.
2. Silence 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(see page 243).

11.2.5 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[6], the reliability of using an object archive is up to 99.999999999%.

See Configuring archives(see page 206).

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.

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).

6 https://aws.amazon.com/s3/faqs/?nc1=h_ls#Durability_.26_Data_Protection

11.2.6 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 viewing tile on the map; fixed objects in the field of view (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[7] license.

Virtual PTZ cameras on the map

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

11.2.7 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 viewing tiles 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 fish-eye camera footage.

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.

11.2.8 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.

11.2.9 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.

11.2.10 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.

---

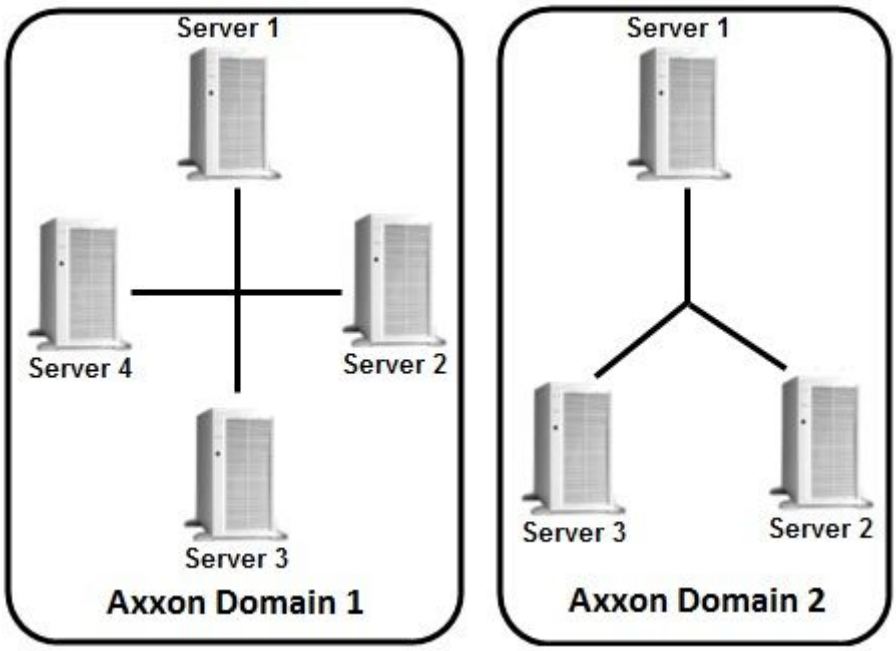
7 https://www.openstreetmap.org/copyright/en

11.3 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[8]. Detailed information on OpenVPN and examples of virtual private network configuration are given in the official documentation[9].
> Suppose, the Server relies on a defined port range (see Installation(see page 62)), 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 Axxon domains(see page 107).

11.4 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.

8 http://openvpn.net/
9 http://openvpn.net/index.php/access-server/docs.html

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(see page 587)) 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).

11.5 Specifications of the Axxon One software package

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

Characteristics	Value
Number of servers in the distributed system	Unlimited
Number of clients which support simultaneous connection to the server	Unlimited
Number of servers which simultaneously transmit video images 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, etc.)	depends on the sound card used for 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(see page 254)	up to 25
Number of license plate recognition channels	Is determined by the license; there is no upper limit
Number of face recognition channels	Is determined by the license; there is no upper limit
Number of mobile clients or Web clients connections	Unlimited
Number of video walls	Unlimited
Number of maps	Unlimited
Analog video camera support	yes (through video capture cards)
IP device support	IP cameras and IP video servers This list is continuously expanding: support for new hardware is added through updates to Axxon Driver Pack
CPU support	64-bit (x64)

Characteristics	Value
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 video camera analytics	yes
Support for touchscreens	yes

11.6 Implementation requirements for the Axxon One software package

11.6.1 Limitations of Axxon One

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 should be met: 1. Version 2.0 and higher. 2. The following extensions should be available: **ARB_vertex_program**, **GL_EXT_blend_func_separate**, **GL_ARB_framebuffer_object**. Extensions availability can be checked with the *OpenGL Extension Viewer* program (download[10]). 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%. You may have issues with *Axxon One* VMS if the screen resolution is set lower than 1280*960 pixels
3	The Server and the Client must be of the same version. If not, the correct operation of *Axxon One* VMS isn't guaranteed
4	For the correct operation of *Axxon One* VMS, the OS should 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
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 should be no spaces at the beginning of the name of the folder which contains the installer

10 http://realtech-vr.com/home/glview

No.	Limitation
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(see page 62), certain ports were specified, the access to these ports via the TCP and UDP protocols should be enabled. Otherwise, access to all ports should 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(see page 899))
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(see page 899)). 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(see page 174)). 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(see page 62)). 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(see page 100))

11.6.2 Operating system requirements

On the page:

- Windows OS(see page 48)
- Windows Server OS(see page 48)
- Linux OS(see page 48)

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.

11.6.2.1 Windows OS

- **Windows 11** [5]: Home, Pro, Education, Pro Education, Pro for Workstations, Enterprise;
- **Windows 10**: Pro, Enterprise, Education, Home Edition;
- **Windows 10 IoT** [4]: Enterprise, Enterprise LTSB 2016, Enterprise LTSC 2019;
- **Windows 8** [1]: Core, Pro, Enterprise;
- **Windows 7 SP1** [1]: Home Basic [2], Home Premium [2], Professional, Enterprise, Ultimate.

11.6.2.2 Windows Server OS

- **Windows Server 2022** [5]: Standard, Essentials, Datacenter, Azure Datacenter;
- **Windows Server 2019** [5]: Essentials [3], Standard, Datacenter;
- **Windows Server IoT 2019** [5];
- **Windows Server 2016** [1, 5]: Essentials [3], Standard, Datacenter;
- **Windows Server 2012** [1, 5]: Foundation [2], Essentials [3], Standard, Datacenter;
- **Windows Server 2012 R2** [1, 5]: Essentials [3], Standard, Datacenter.

11.6.2.3 Linux OS

- **Debian**: 11, 10, 9 [6];
- **Ubuntu**: 22, 20, 19, 18.

Appendix 8. Configuring and operating Axxon One in Linux OS(see page 916)
Axxon One limitations in Linux OS(see page 916)

Attention!

[1]—neural analytics is not applicable (see Hardware requirements for neural analytics operation(see page 52)).
[2]—there are restrictions, posed by OS edition (1 physical processor)—see http://www.microsoft.com[11].
[3]—there are restrictions, posed by OS edition (2 physical processors)—see http://www.microsoft.com[12].
[4]—Core edition is not supported.
[5]—Full Installation type is supported. Server Core Installation type is not supported (see Possible Errors During Operation(see page 905)).
[6]—the basic Face detection cannot work (see Configuring Face detection(see page 280)).

11.6.3 Disk storage subsystem requirements

On the page:

11 https://www.microsoft.com/en-us/?ql=3
12 https://www.microsoft.com/en-us/?ql=3

- General requirements(see page 49)
- Storage requirements(see page 50)
  - Minimum requirements(see page 50)
  - Size of the archive(see page 50)
  - System log database (see page 51)
  - Metadata database (see page 51)
  - The system logs(see page 51)
  - Self-diagnostics service(see page 51)

11.6.3.1 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(see page 897)).
   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.

11.6.3.2 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.

11.6.3.2.1 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.

11.6.3.2.2 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

Recording parameters	Calculating results
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

11.6.3.2.3 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.

11.6.3.2.4 **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(see page 237)),

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.

11.6.3.2.5 The system logs

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

11.6.3.2.6 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.

11.6.4 Hardware requirements

11.6.4.1 General hardware requirements

Axxon One is designed for use on computers.

The required hardware configuration (RAM, CPU, and hard disk) can be determined using the AxxonSoft calculator[13].

13 https://sale.axxonsoft.com/calc/calculator.jsf

Disk storage subsystem requirements(see page 48)
TCP/IP Network Bandwidth Requirements(see page 55)
Hardware requirements for neural analytics operation(see page 52)
Hardware requirements for face detection(see page 54)
Hardware requirements for GPU based video decoding[14]

Attention!

If *Axxon One* is installed on a computer with two processors, it is recommended to disable the Hyper-threading.

11.6.4.1.1 Minimum RAM requirements

At least 8 GB of RAM is recommended. For a specific calculation, use the platform calculator[15]. 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*.

11.6.4.1.2 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) 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 Extensions availability can be checked using the OpenGL Extension Viewer program (download[16]).

It is recommended to use 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.

11.6.4.2 Hardware requirements for neural analytics operation

The hardware requirements for the neural analytics (see General information on Neural Analytics(see page 238)) are:

1. Some NVIDIA SDK specific features allow the neural analytics to work only on Windows Server 2019 or Windows 10.
2. For neural analytics operation, you may use CPU, GPU NVIDIA, VPU (Intel NCS[17], Intel HDDL).

Attention!

14 https://docs.axxonsoft.com/confluence/display/next45en/Hardware+requirements+for+GPU+based+video+decoding
15 https://sale.axxonsoft.com/calc/calculator.jsf
16 http://realtech-vr.com/home/glview
17 https://software.intel.com/en-us/neural-compute-stick

- To connect Intel NCS[18], 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. Intel NCS[19] may be used with any PC that meets *Axxon One* hardware requirements (see Hardware requirements(see page 51)).
- We do not recommend using more than one Intel NCS[20] device per Server. You can use several Intel HDDL devices on the 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[21]).

3. If the detection tool uses CPU or Intel GPU resources, the following requirements should be met:
   a. Supported CPUs:
      i. 6th-10th Generation Intel® Core™ processors;

      Attention!

      When using a CPU lower than 6th Generation Intel® Core™ processors, the operation of the detection tool is not guaranteed.

      ii. Intel® Xeon® v5 family;
      iii. Intel® Xeon® v6 family;
      iv. Intel® Movidius™ Neural Compute Stick;
      v. Intel® Neural Compute Stick 2;
      vi. Intel® Vision Accelerator Design with Intel® Movidius™ VPUs.
   b. OpenVino should support the Intel CPU in use (see https://software.intel.com/content/www/us/en/develop/tools/openvino-toolkit/system-requirements.html).
   c. CPU should support the AVX2 or AVX512 instruction set (see https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-InstructionSetExtensions=3533&1_Filter-Family=595).
4. Video card: NVIDIA GeForce 1050 Ti or 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[22]).
   - You can check Compute Capability GPU version on the manufacturer's[23] website.
   - If you use NVIDIA graphics cards, make sure to download the latest drivers from the manufacturer's website[24].

When using a video card, a single neural network requires 500 MB of video memory, except for the neural network for face detection (see Hardware requirements for face detection(see page 54)) and license plate recognition (RR) (see Hardware requirements for License plate recognition (RR)(see page 54)). 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 video cards in your system.

Attention!

For correct operation of each detection tool, video image should match a specified set of requirements. The requirements for each detection tool are listed in the corresponding sections (see Configuring detection tools(see page 234)).

18 https://software.intel.com/en-us/neural-compute-stick
19 https://software.intel.com/en-us/neural-compute-stick
20 https://software.intel.com/en-us/neural-compute-stick
21 https://docs.openvino.ai/latest/openvino_docs_install_guides_overview.html#install-openvino
22 https://en.wikipedia.org/wiki/CUDA
23 https://developer.nvidia.com/cuda-gpus
24 https://www.nvidia.com/Download/index.aspx?lang=en-us

11.6.4.3 Hardware requirements for GPU based video decoding

If detection tools use GPU for video decoding (see Configuring detection tools(see page 234)), make sure the following hardware requirements are met:

1. For NVIDIA GPUs:
   a. CUDA 11.1–11.4.
   b. Support for the required codec in NVDEC (see here[25]).
   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[26]).
> - You can check Compute Capability GPU version on the manufacturer's[27] website.
> - When using NVIDIA GPUs, it is recommended to install the latest driver from the official website[28].
> - To decode video in *Axxon One*, you can use up to four NVIDIA GPUs installed on the Server (Nvidia GPU 0, Nvidia GPU 1, Nvidia GPU 2, Nvidia GPU 3).

2. For the integrated Intel GPUs:
   a. 6th generation CPU or higher.
   b. Support for the required codec in Quick Sync Video.

11.6.4.4 Hardware requirements for License plate recognition (RR)

If license plate recognition (RR) runs on GPU, make sure the following hardware requirements are met:

1. The GPU is an NVIDIA with at least 1.4 GB of video memory.
2. Compute Capability from 3.5 to 7.5 inclusive.

> **Note**
>
> You can check Compute Capability GPU version on the manufacturer's[29] website.

3. NVIDIA driver version 450.36.06 or higher.
4. CPUs with the AVX2 instruction set support, which are listed here[30].

11.6.4.5 Hardware requirements for face detection

The face detection tool requires a CPU supporting SSE4.2, FMA3 or AVX2.0 instruction set.

If face recognition runs on GPU, make sure the following hardware requirements are met:

1. The GPU is an NVIDIA with at least 6 GB of video memory.
2. Compute Capability 6.0 or higher.

> **Note**
>
> You can check Compute Capability GPU version on the manufacturer's[31] website.

3. NVIDIA driver version is 418.39 or higher.

11.6.4.6 Hardware requirements for Face detection (VL)

The face detection (VL) requires a CPU supporting AVX2.0 instruction set.

25 https://developer.nvidia.com/video-encode-and-decode-gpu-support-matrix-new
26 https://en.wikipedia.org/wiki/CUDA
27 https://developer.nvidia.com/cuda-gpus
28 https://www.nvidia.com/Download/index.aspx?lang=en-us
29 https://developer.nvidia.com/cuda-gpus
30 https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-InstructionSetExtensions=3532
31 https://developer.nvidia.com/cuda-gpus

If face detection (VL) runs on GPU, make sure the following hardware requirements are met:

1. Operation is only possible on NVIDIA devices with 6 GB of video memory or more. 8 GB of video memory or more is recommended.
2. NVIDIA driver version 452.39 and higher.
3. Compute Capability 6.1 and higher.

> **Note**
>
> You can check Compute Capability GPU version on the manufacturer's[32] website.

11.6.4.7 Hardware requirements for License plate recognition (VT)

The VT automatic number plate recognition tool runs on the following processors: CPU, Intel GPU, VPU (IntelNCS).

For NVIDIA GPUs:

> **Attention!**
>
> GPUs with NVIDIA Ampere architecture are not supported.

1. Compute Capability 3.5 and higher.

> **Note**
>
> You can check Compute Capability GPU version on the manufacturer's[33] website.

2. Support for CUDA 10.2 or higher.

You can find the list of supported devices on the OpenVINO™ toolkit[34] page.

11.6.4.8 Hardware requirements for License plate recognition (IV)

If License plate recognition (IV) runs on GPU, make sure the following hardware requirements are met:

1. TensorRT 7.2.1 is supported (see documentation[35]).
2. NVIDIA driver version 450.36.06 or higher.
3. CPUs that support the AVX2 instruction set, see the list[36].
4. Compute Capability 3.5 or higher, recommended 5.0 or higher.

> **Note**
>
> You can check Compute Capability GPU version on the manufacturer's[37] website.

11.6.5 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!**

32 https://developer.nvidia.com/cuda-gpus
33 https://developer.nvidia.com/cuda-gpus
34 https://docs.openvino.ai/latest/openvino_docs_OV_UG_supported_plugins_Supported_Devices.html
35 https://docs.nvidia.com/deeplearning/tensorrt/archives/tensorrt-721/support-matrix/index.html
36 https://ark.intel.com/content/www/us/en/ark/search/featurefilter.html?productType=873&1_Filter-InstructionSetExtensions=3532
37 https://developer.nvidia.com/cuda-gpus

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[38] (check the **Total bitrate from ip devices (Mbit/s)** parameter).

11.6.6 BIOS configuration requirements

Axxon One suite performance (namely, video decoding) is sensitive to CPU frequency. The higher the frequency, the better will be *Axxon One* performance on this platform.

Modern computers have the power saving mode enabled in BIOS by default. Using this mode in multiprocessor systems results in incomplete CPU core utilization and decreases the performance of an input/output subsystem.

To increase *Axxon One* suite performance, configure the computer BIOS as follows:

1. Disable all Enhanced Intel SpeedStep (EIST) technologies.
2. Disable power saving modes: select options providing maximum performance.
3. Disable green technologies such as Energy Saving, Turbo Boost, SmartThrottling.

Attention!

Different motherboard manufacturers use different names for these technologies. Therefore, for every particular motherboard model you must find the technology name in the documentation for this model.

11.6.7 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[39]) instead.

11.7 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

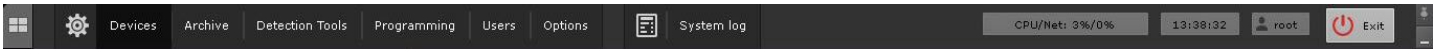
38 https://sale.axxonsoft.com/calc/calculator.jsf
39 http://www.net-usb.com/downloads/

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(see page 450)).

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.

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

1. Camera search panel(see page 646).
2. System time.
3. Context menu.
4. Video surveillance mode selection tabs.
5. Video wall management panel.(see page 643)
6. Monitor management panel(see page 644).
7. Layouts panel(see page 644).
8. Macro menu(see page 817).
9. Layout scaling buttons(see page 654).

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)(see page 557)), to collapse the client window, click the button.

11.8 Ports used by the Axxon One Software Package

Appendix 9. Using Axxon One with NAT(see page 944)

Ports	Changeable	Installation type	Process	Open the port*
20040 (Windows, Linux) 20041 (Windows, Linux) 20042 (Linux) 20108 (Windows, Linux)	No	Server and Client Failover Server and Client	Self-diagnostics service(see page 619)	Not required

Ports	Changeable	Installation type	Process	Open the port*
20109	Yes	Server and Client Failover Server and Client	gRPC API (see Configuring the Server ports(see page 543))	Required
20110	Yes	Server and Client Failover Server and Client	PostgreSQL database (see Configuring the Server ports(see page 543))	Required
20111–20210	Yes	Server and Client Failover Server and Client	Server (see Installation(see page 62), Network settings utility(see page 899))	Required
80 (Windows) 8000 (Linux)	Yes	Server and Client Failover Server and Client	Web server (see Configuring the Web-Server(see page 119))	If necessary + HTTPS port 443
554 (Windows) 50554 (Linux)	Yes	Server and Client Failover Server and Client	RTSP server (see Configuring an RTSP Server(see page 120))	Not required
8080	Yes	Server and Client Failover Server and Client	Virtual input (see Configure virtual inputs(see page 167))	Required
8888	No	Server and Client Failover Server and Client Client	Client HTTP API (see Client HTTP API[40])	Not required
4000 4646–4648 8300–8302 8500 8600	No	Failover Server and Client	Failover (see Ports used by the failover system(see page 588))	Required
27000–35000	Yes	Server and Client Failover Server and Client	Server (see Installation(see page 62), Network settings utility(see page 899))	Firewall is required, but port forwarding under NAT is not required (see Connecting the Client to the Server behind NAT(see page 946))

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

11.9 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.

40 https://docs.axxonsoft.com/confluence/display/one20en/Client+HTTP+API

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.

12 Installing the Axxon One Software Package

12.1 Installing equipment

12.1.1 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.

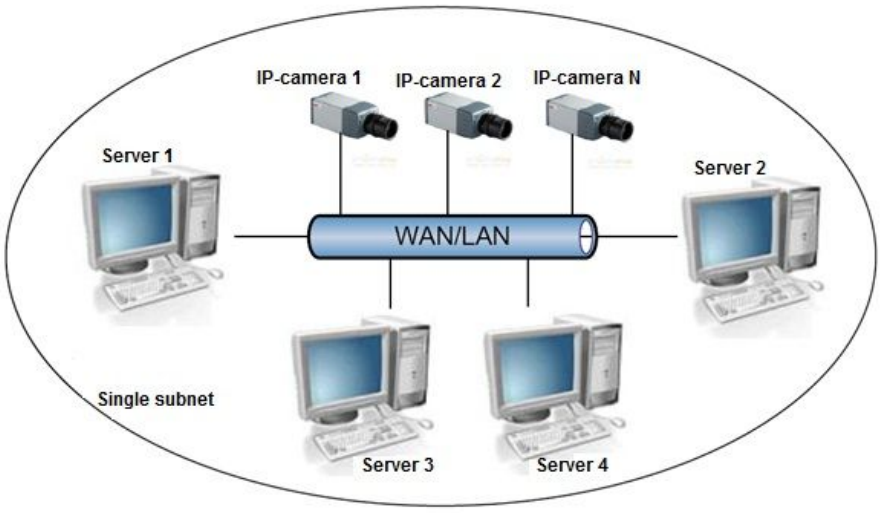
The following types of equipment are IP video and audio surveillance devices:

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.

12.1.2 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.

12.1.3 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.

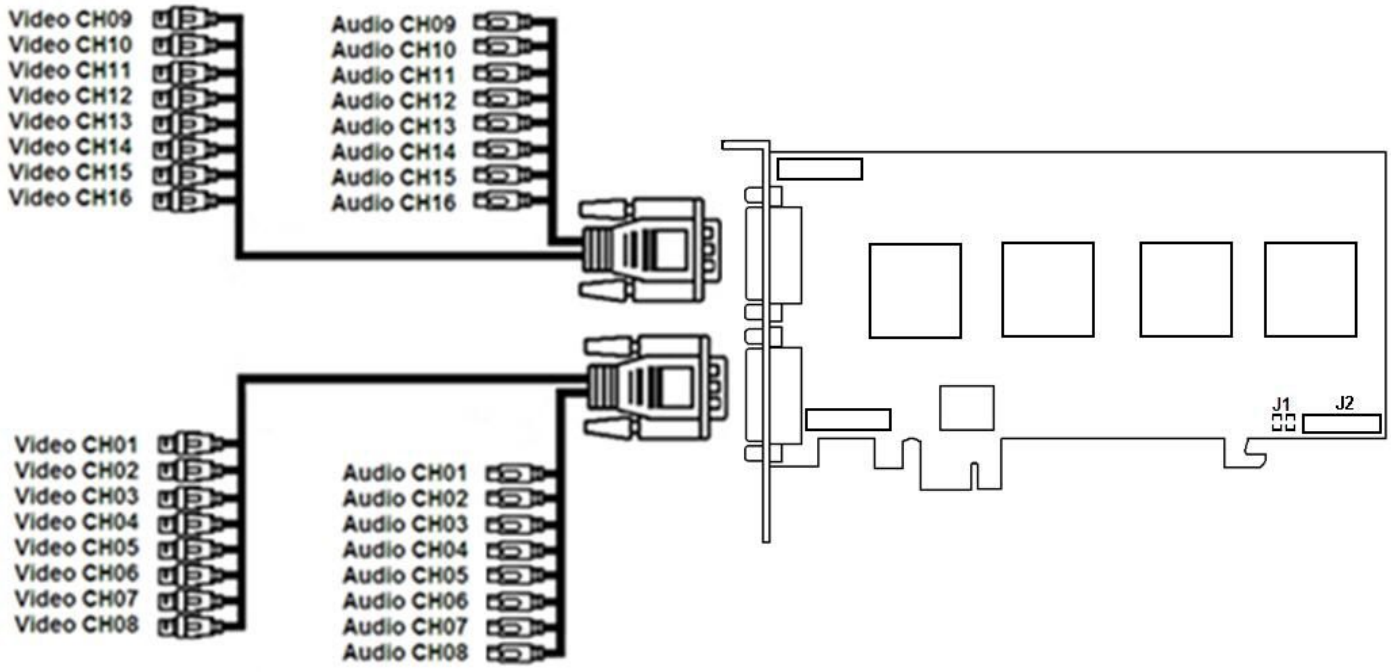
2. Web interface of the IP device. This interface is used to accomplish the following tasks:
   a. Configuring the IP devices with consideration for routing.
   b. Configuring modes for the IP devices to work with video and audio signals.
   c. Viewing video images coming in from IP devices in standard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

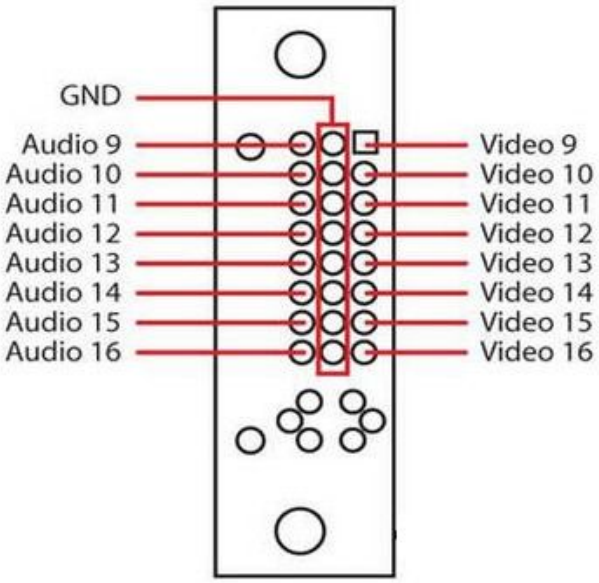
Configuration of IP devices in Windows is described in detail in the official reference documentation for the respective devices.

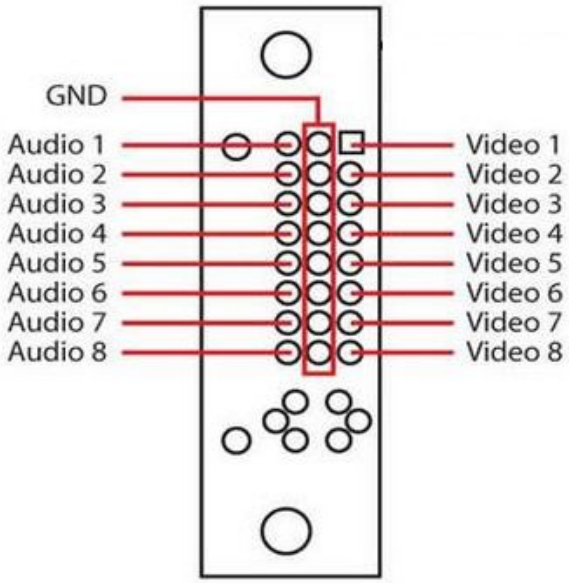
12.1.4 Video capture cards pins

12.1.4.1 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.





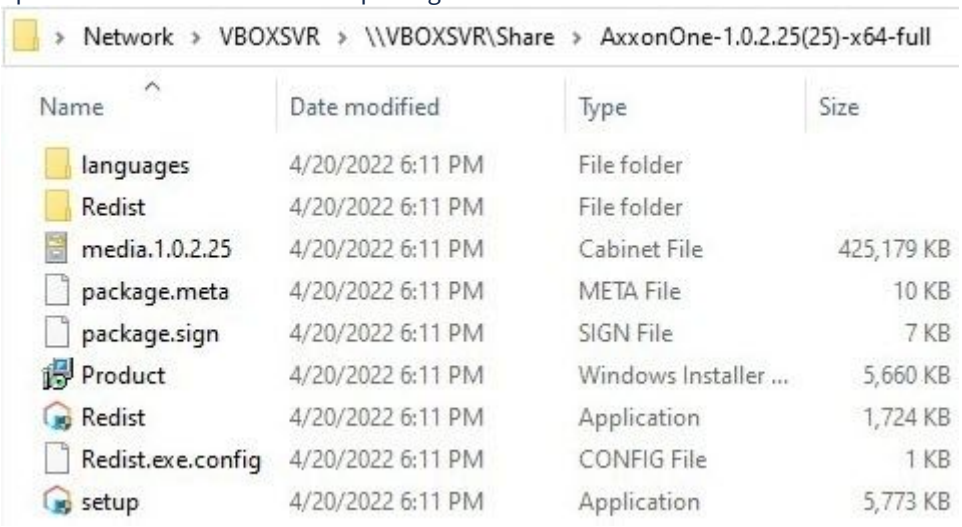


12.2 Installation the Axxon One Software Package

12.2.1 Installation

To install *Axxon One*, regardless of the type of installation, it is necessary to perform the following steps:

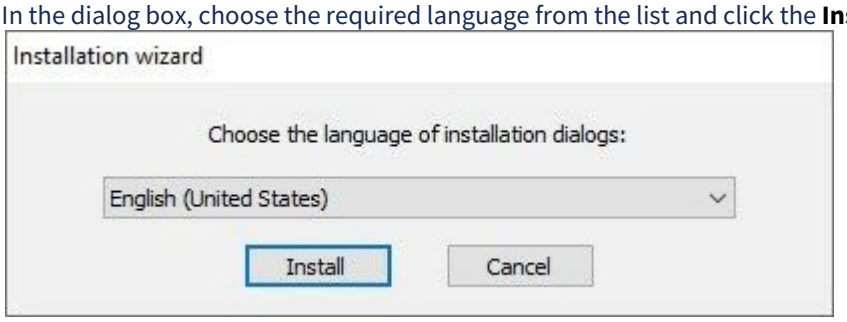
1. Open the *Axxon One* distribution package.



2. Run the Setup.exe file.

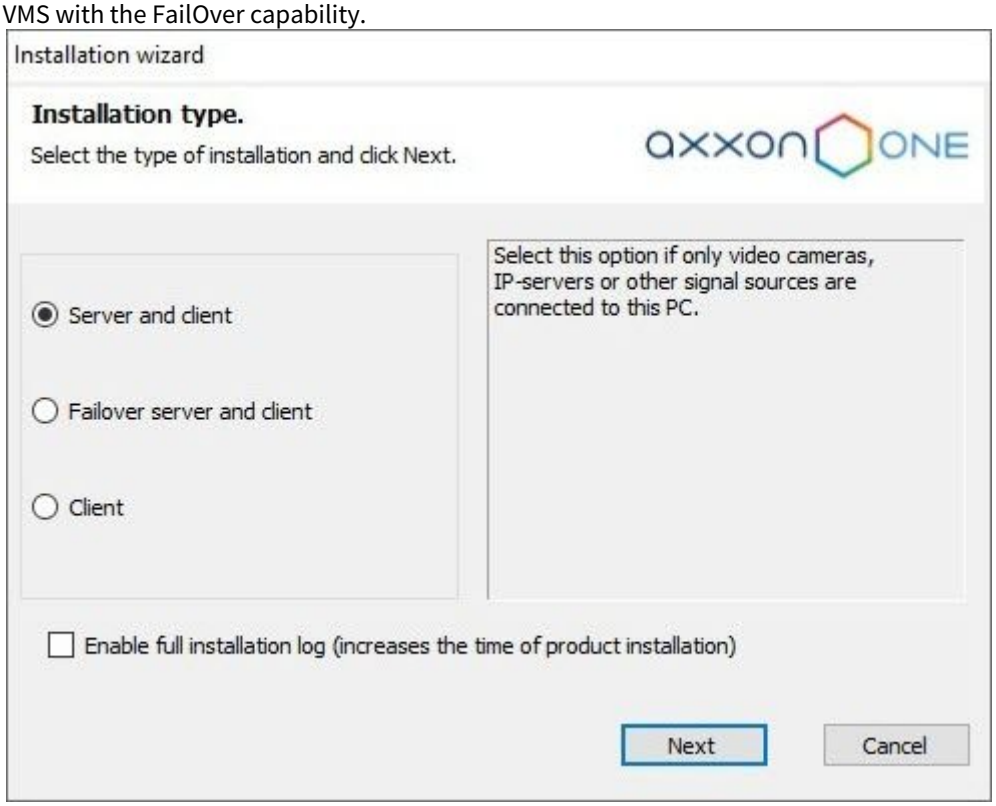
> **Note**
>
> If you cannot run the installation files downloaded from the Internet, do as follows: allow running programs and unsafe files in Windows OS.

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. **Client**—installs only a Client application that allows the user to connect to any Server and perform administration/management/monitoring operations with the protected object based on the permissions granted by the administrator.
   b. **Server and Client**—installs Client and Server services. *Axxon One* Server:
      i. Interacts with devices (cameras, microphones, inputs, outputs, etc.) that constitute a security system.
      ii. Writes video footage to archives on system disks; interacts with archives on NAS.
      iii. Hosts metadata database.
      iv. Employs detection tools to analyze live video.
      v. Keeps configurations of the security system, user settings, custom layouts, macros, etc.
   c. **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. Please refer to the section titled Configuring FailOver VMS(see page 587) for details on how to install

VMS with the FailOver capability.

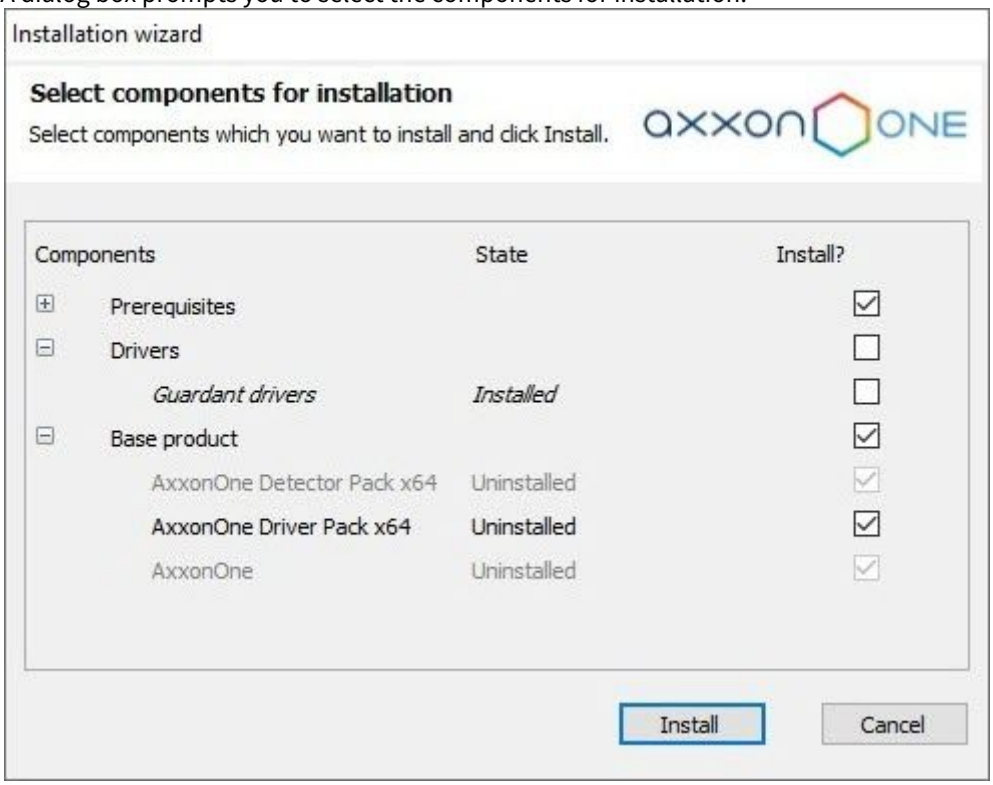


> **Note**
>
> We offer a separate installation package containing only the *Axxon One* Client. To obtain it, contact our technical support[41]. You can download additional packages from the official website[42].
> This installation package is intended only for Client updates. You cannot install it on a PC where *Axxon One* was not previously installed.

5. To record all installation-related events to a log file, select the **Enable full installation log** checkbox.
6. Click the **Next** button.

41 https://support.axxonsoft.com/
42 https://www.axxonsoft.com/support/downloads

A dialog box prompts you to select the components for installation.



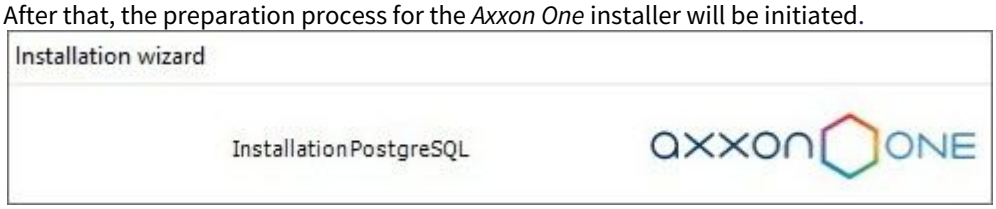
Note

To view the list of installed components, click ⊞.

Attention!

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.

7. Select checkboxes for the components that you want to install. We recommend installing all components.
8. Click the **Install** button. All selected components will be installed. The installation process may take considerable time. After that, the preparation process for the *Axxon One* installer will be initiated.



Attention!

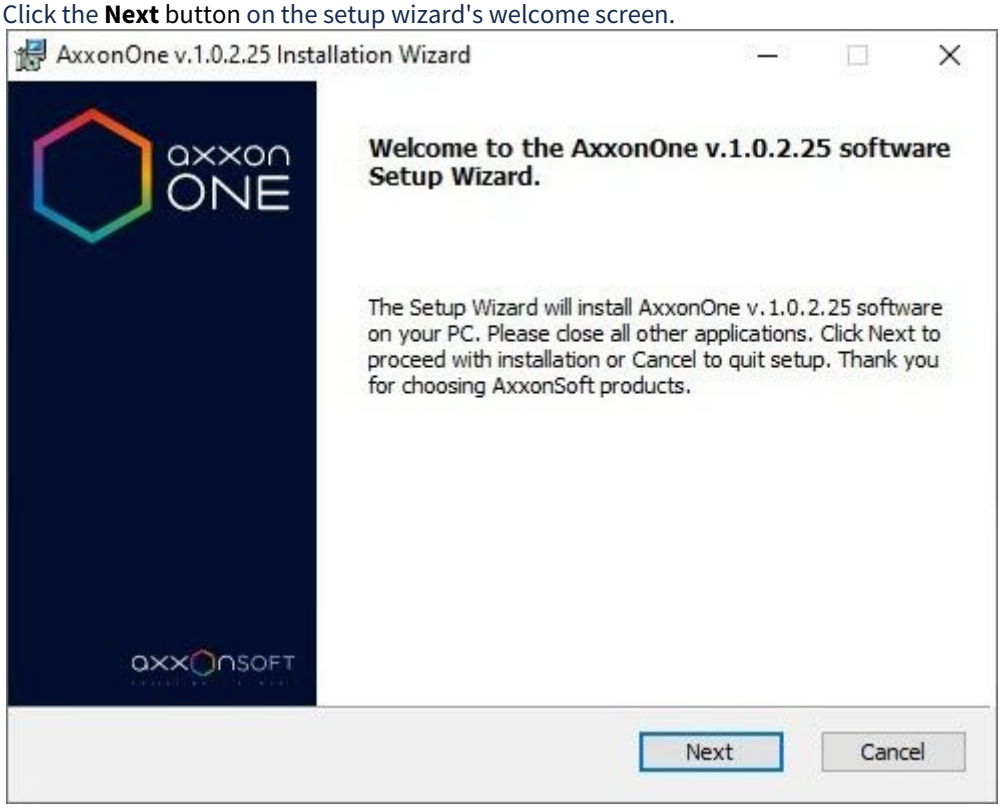
Starting from *Axxon Driver Pack* 3.51, this driver package requires the Windows update KB2999226 to be installed. If this update is missing, you will see a warning. To continue installation, download the upgrade from the official Microsoft website. When installing the upgrade, consider the bitness of your system.

Note

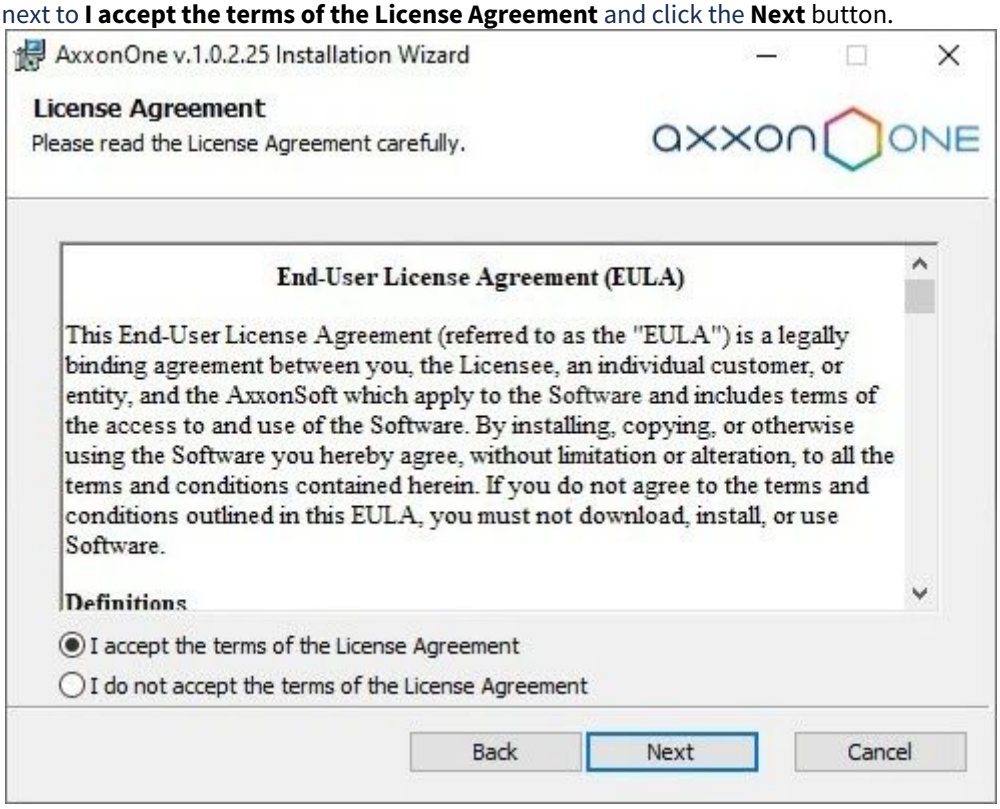
The following required software is installed, if necessary:

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)(see page 81)).
b. *NET Framework 2.0*, *.NET Framework 3.5 SP1* and *.NET Framework 4.0.*
c. Acrobat Reader, which is necessary for exporting in PDF format and printing freeze frames (see Frame export(see page 808)).

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



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*, and click the **Next** button.

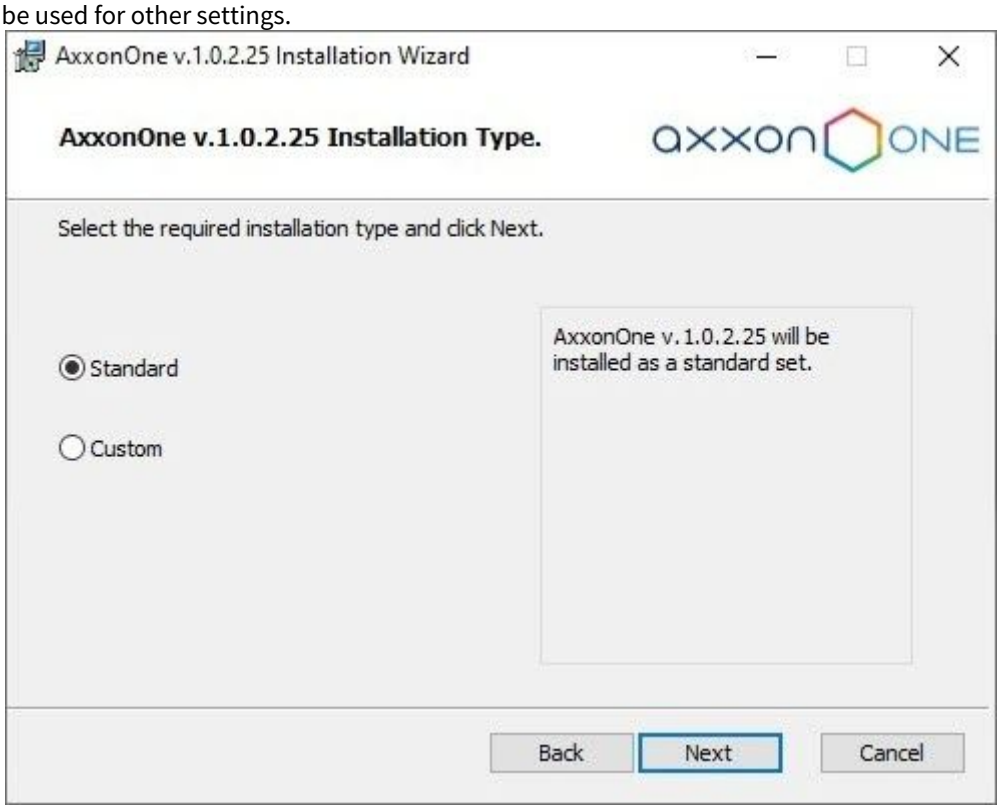
> **Attention!**
>
> The path to the folder for storing the log database and the metadata database should contain only Latin letters and numbers.

> **Attention!**
>
> To reduce the load on the system disk, it is recommended to store 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* software package, you can use the Disk storage subsystem requirements(see page 48) page.

> **Note**
>
> 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 the future, the metadata database can be placed in the network storage (see Configuring storage of the system log and metadata(see page 539)).

12. By default, shortcuts are added to both quick launch bar and desktop. De-select the corresponding checkboxes if it's not required.
13. By default, upon connecting to the Server, the Client may be automatically updated. If it's not required, clear the **Create an archive for automatic update** checkbox. In this case, you can save *Axxon One* VMS installation 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 PC name. If the PC name contains forbidden symbols, 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:

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

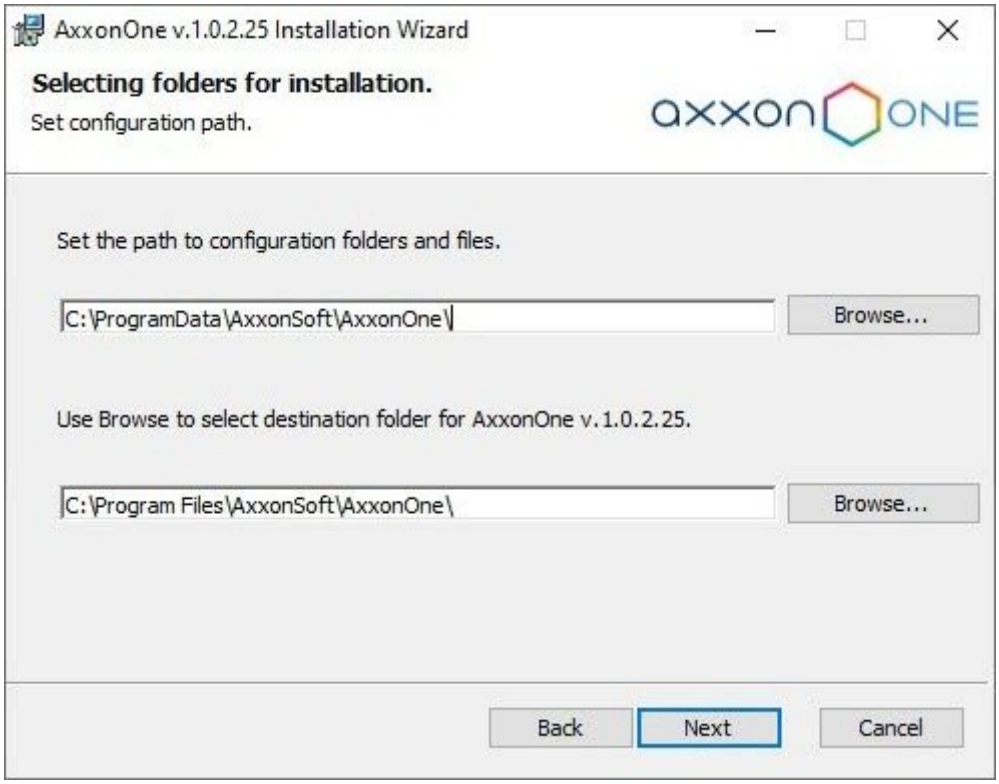
> **Attention!**
>
> After installation of *Axxon One*, make sure that a file browser account has been created in Windows and belongs to the Administrators group.

    a. Use default AxxonOne File Browser account.
    b. Use Local System account.

c. Specify username and password for new or already existing user.

18. Specify the path to *Axxon One* folders and configuration files.

> **Note**
>
> By default, the files and folders of the configuration are stored at the following path: C:\ProgramData\AxxonSoft\AxxonOne\.

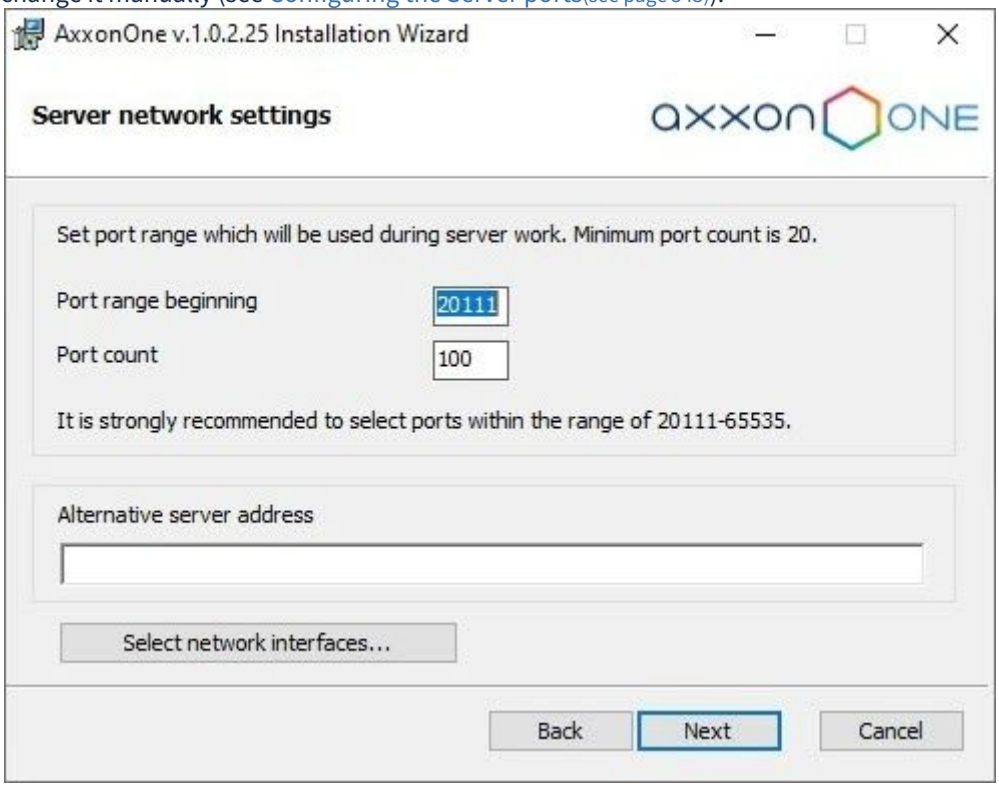


19. Specify the path to the folder for installing *Axxon One*.

> **Note**
>
> By default, *Axxon One* will be located in the C:\Program Files\AxxonSoft\AxxonOne\ folder.

> **Attention!**
>
> The installation path for *Axxon One* and its databases should contain only Latin letters and numbers.

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[43] 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(see page 57). After you install *Axxon One*, you can change it manually (see Configuring the Server ports(see page 543)).



> **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:
>
> - After the Server is installed, it occupies **10 ports**, including one for sending E-mails (via SMTP, see The E-mail notifier object(see page 435)).
>
> **Attention!** The FailOver Server and Client installation type uses 9 base ports and preset port ranges for each node (see Ports used by the FailOver system(see page 588));
> - 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 Video Footage through 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 loudspeakers in the system (see The Speaker Object(see page 170));
> - **1 port** is required for recording metadata into the DB;

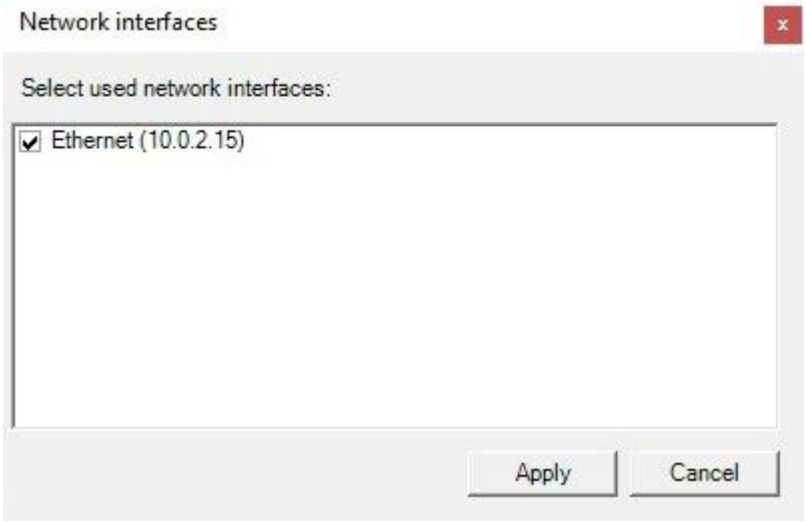
43 https://en.wikipedia.org/wiki/Port_forwarding

- **2 ports** are required for service detection tools operation;
- **2 ports** are required for scene analytics detection tools operation;
- **2 ports** are required for neuro tracker operation;
- **2 ports** are required for neural counter operation.

Attention!

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

22. If necessary, set an alternative Server address—the outside local address for a Server behind the NAT[44]. 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* setup, do the following:
    a. Click the button **Select network interfaces...** 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 will be visible in the list. If you do not 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(see page 901)). 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.

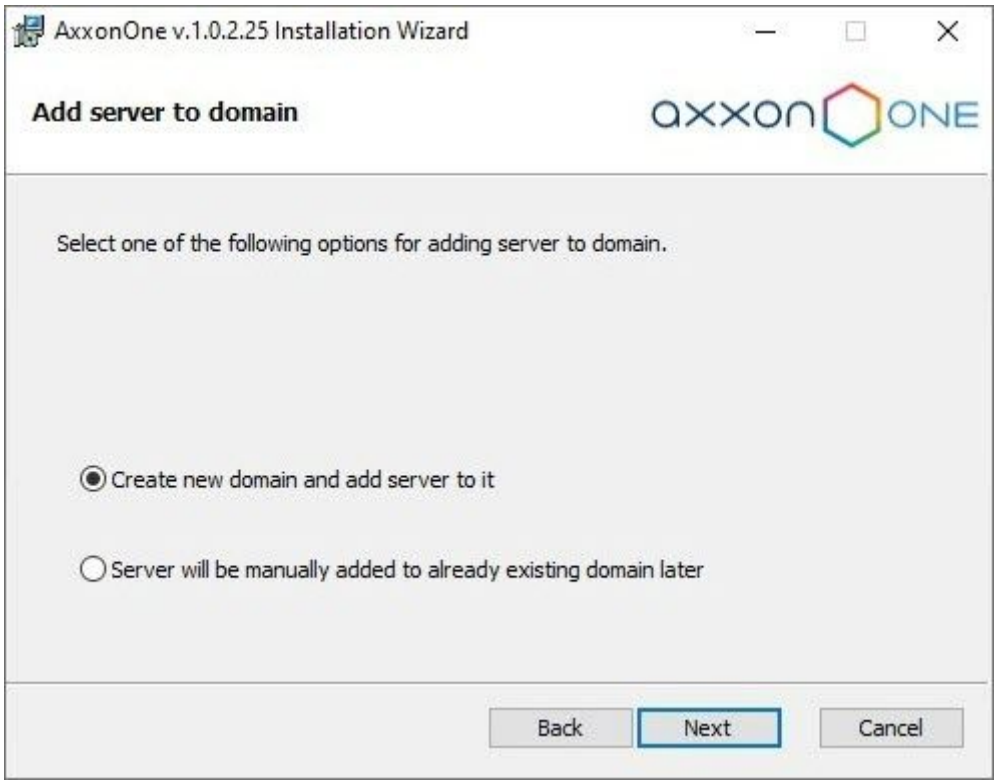
Note

When reinstalling *Axxon One*, you have the option of using the previous domain (select **Use existing configuration**).

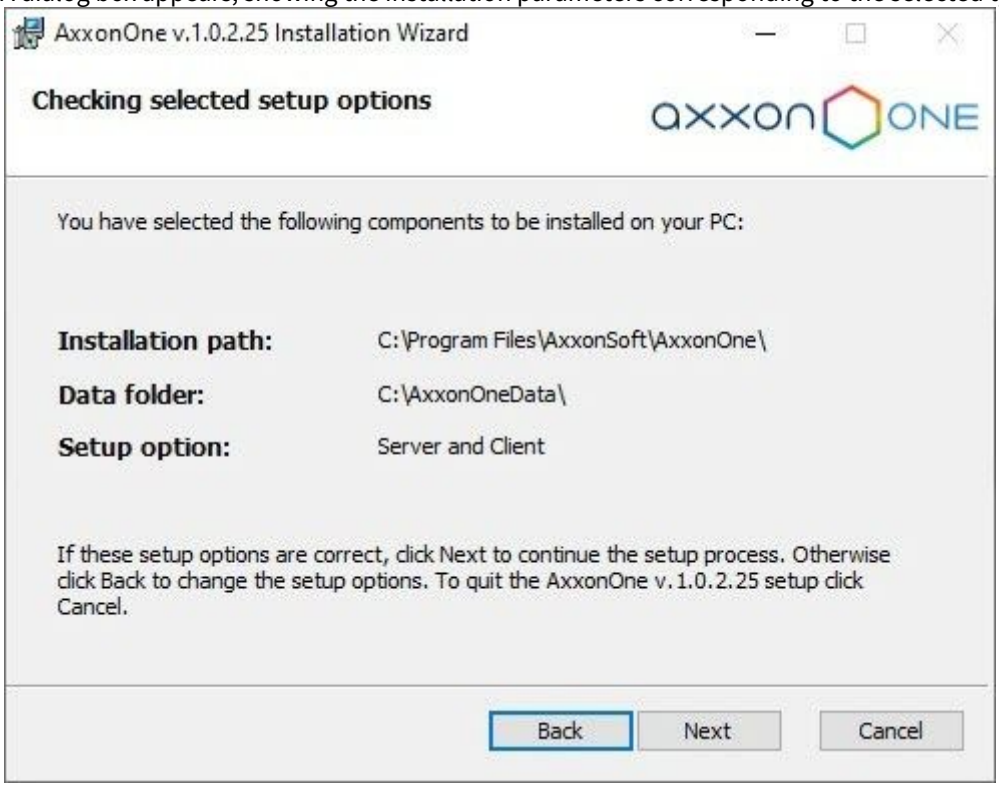
Note

Using the same Axxon-domain name does not guarantee that the Servers will be in the same Axxon-domain. To place all Servers into one Axxon-domain, you should use *Axxon One* interface to add each Server to the necessary Axxon-domain. Axxon-domain configuration is described in detail in Configuring Axxon-domains(see page 107).

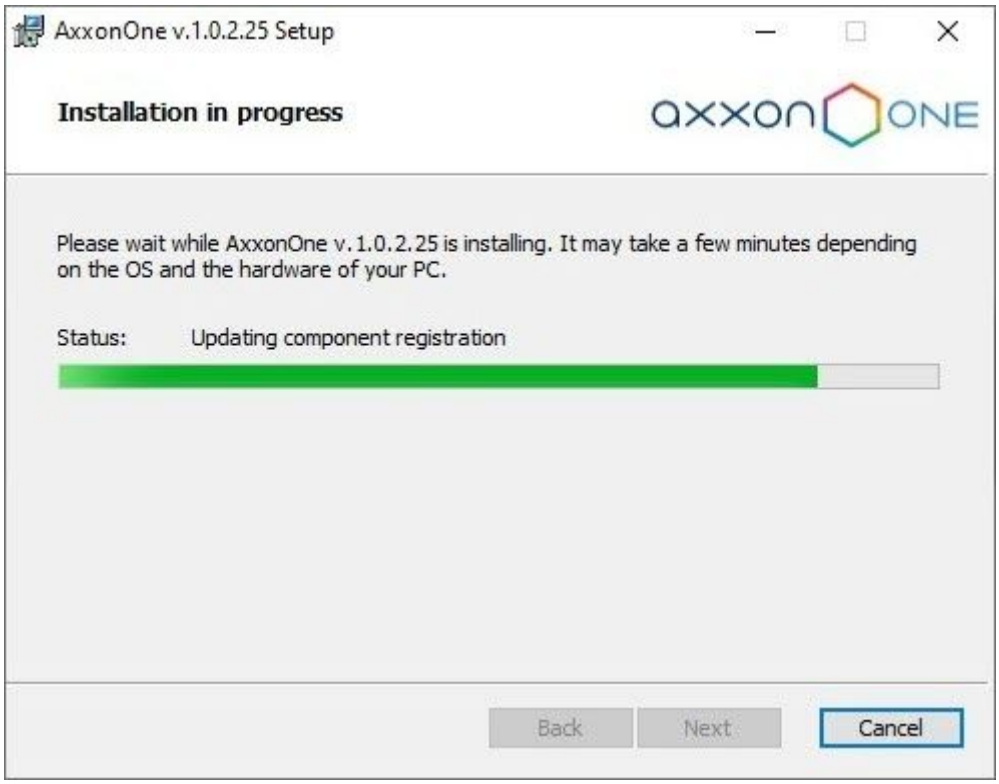
44 https://en.wikipedia.org/wiki/NAT



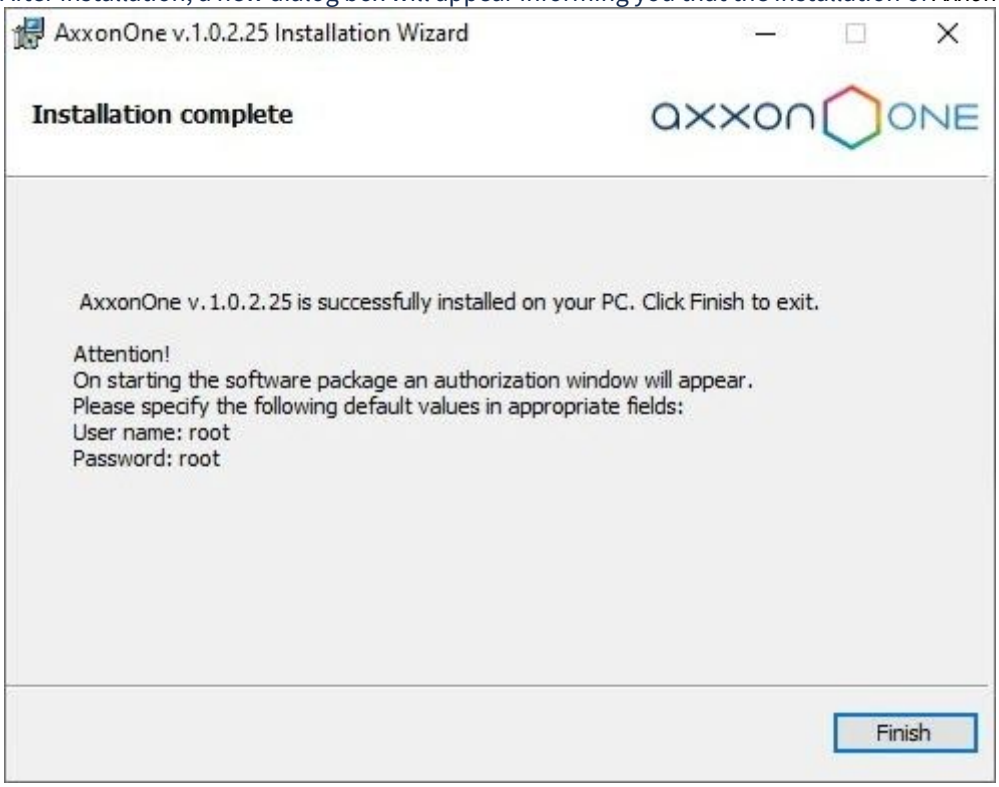
A dialog box appears, showing the installation parameters corresponding to the selected type of installation.



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 will appear 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.

12.2.2 Installing DetectorPack add-ons

By default, the *Axxon One* VMS package only includes the basic *DetectorPack,* which contains the following set of detection tools:

1. Detection tools:

a. Motion detection(see page 249).
b. Object Tracker(see page 260) (without Neural filter).

> **Note**
>
> You need to install the Neuro Pack for the Neural filter operation

c. Tampering detection(see page 251).
d. Audio loss detection.
e. Noise detection(see page 254).
f. Signal detection(see page 254).
g. Queue detection(see page 386).
h. Visitors counter(see page 388).

2. Sub-tools:
   a. Line crossing(see page 268).
   b. Loitering(see page 272).
   c. Stop in area(see page 273).
   d. Motion in area.
   e. Object Appearance in the Area.
   f. Disappearance in area.
   g. Multiple objects(see page 272).
   h. Move from area to area(see page 273).
   i. Abandoned Object(see page 270) (for Object Tracker only).

Additional *DetectorPack* packages (add-ons):

1. The Neuro Pack add-on contains the following tools:
   a. Neural filter(see page 260).
   b. Neural tracker(see page 274).
   c. Neural counter(see page 344).Pose detection tool(see page 373) and its sub-tools:
      i. Sitting person detection(see page 375).
      ii. Man down detection(see page 376).
      iii. Hands up detection(see page 378).
      iv. Handrail holding detection(see page 378).
      v. People counter(see page 379).
      vi. Close-standing people detection(see page 381).
      vii. People masking(see page 382).
   d. Object detection(see page 352).
   e. Smoke detection(see page 349).
   f. Fire detection(see page 349).
   g. Water level detection(see page 390).
   h. Equipment detection (PPE)(see page 358).
   i. Floating objects detection.
   j. Privacy masking(see page 368).
   k. Person-based privacy masking(see page 366).

> **Note**
>
> Neuro Pack is required for the face and people masking feature to be applied to the exported video.

2. The Face Recognition Pack add-on contains Face detection(see page 280) and its Masks detection(see page 291) sub-tool.
3. The Face Recognition Pack (VL) add-on contains Face detection (VL)(see page 285) and its Masks detection (VL) sub-tool.

> **Note**
>
> For the Face detection (VL) to work, it is necessary to install two packages from the *Axxon DetectorPack*:
> - Face Recognition Pack (VL);
> - Face Recognition SDK (VL).

Attention!

- Only one of the optional Face Recognition packs could be installed: Face detection or Face detection (VL). You cannot install both packs in the same system.
- Face Recognition pack Face detection (no vendor name) is guaranteed to work on Linux Debian 11 and Ubuntu 20. Face Recognition packs Face detection (no vendor name) isn't guaranteed to work on Linux Debian 9/10, Ubuntu 18 and Ubuntu 19.

4. The License Plate Recognition (VT) add-on contains License Plate Recognition (VT)(see page 308).
5. The License Plate Recognition (RR) add-on contains the following detection tools:
   a. License Plate Recognition (RR)(see page 330).
   b. License Plate Recognition—Parking (RR)(see page 330).
   c. License Plate Recognition—Search in archive (RR)(see page 330).
   d. Vehicle Recognition (RR).
6. The License Plate Recognition (IV) add-on contains License Plate Recognition (IV)(see page 324).
7. The License Plate Recognition (BRS) add-on contains License Plate Recognition (BRS)(see page 334).
8. The PPE Recognition (VL) add-on contains PPE detection (VL)(see page 355).

Note

For the PPE detection (VL) operation you need to install two packs from the *DetectorPack*:
- PPE Recognition Pack (VL);
- Face Recognition SDK (VL).

To install these add-on packages, do the following:

1. Download the required packages from the official website[45].
2. Stop the Server (see Shutting down a Server[46]).
3. Run the executable file and wait for the installation to complete.
4. Start the Server (see Starting a Server[47]).

Attention!

It is required that the versions of the main *DetectorPack* and the *DetectorPack* add-ons are the same. If the versions differ, it is necessary to update the version of the main *DetectorPack* so it matches the version of the *DetectorPack* add-on.

Creating detection tools(see page 243)

12.2.3 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 previous version of the program.

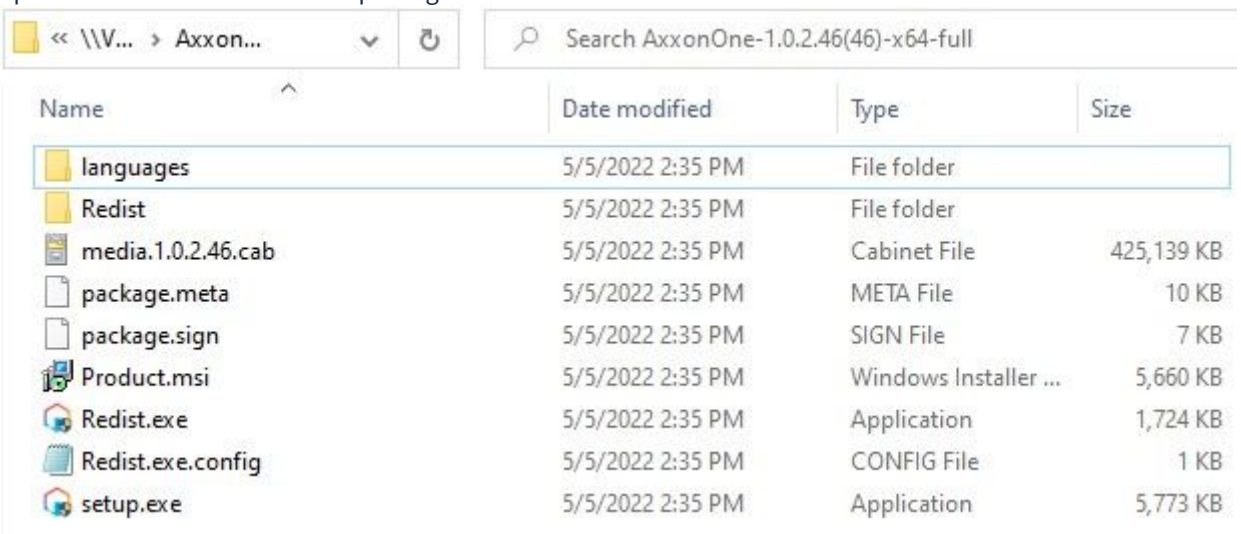
Note

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

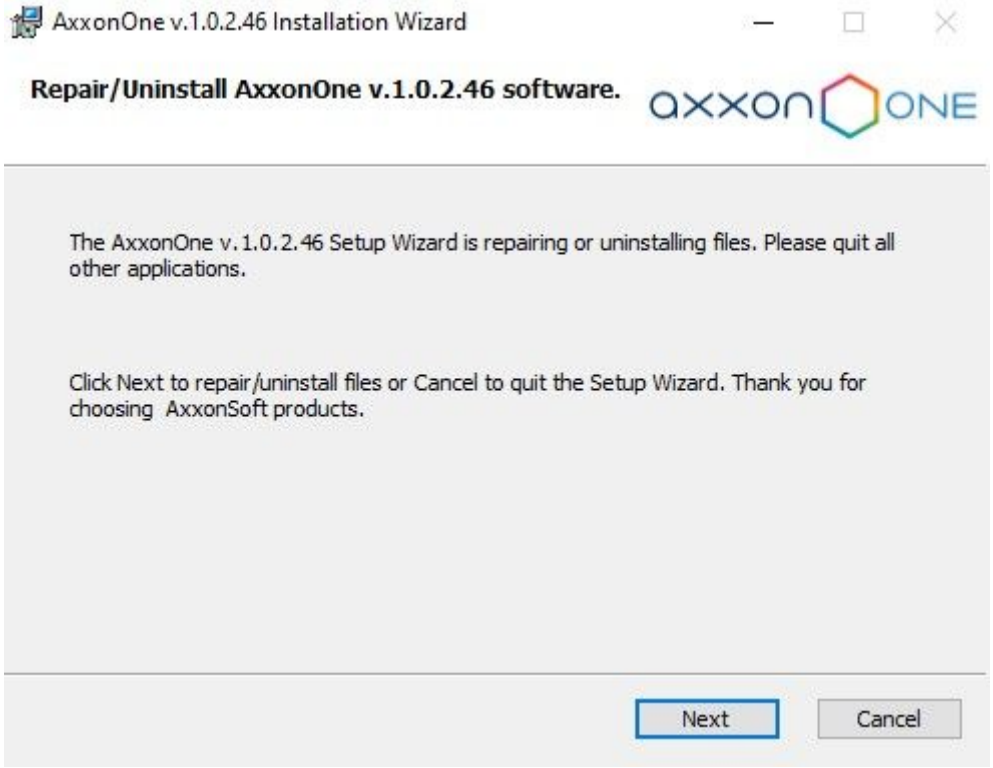
To run a repair installation of the *Axxon One* software, you must perform the following steps:

45 https://www.axxonsoft.com/support/downloads/detector-pack
46 https://docs.axxonsoft.com/confluence/display/next45en/Shutting+down+a+Server
47 https://docs.axxonsoft.com/confluence/display/next45en/Starting+a+Server

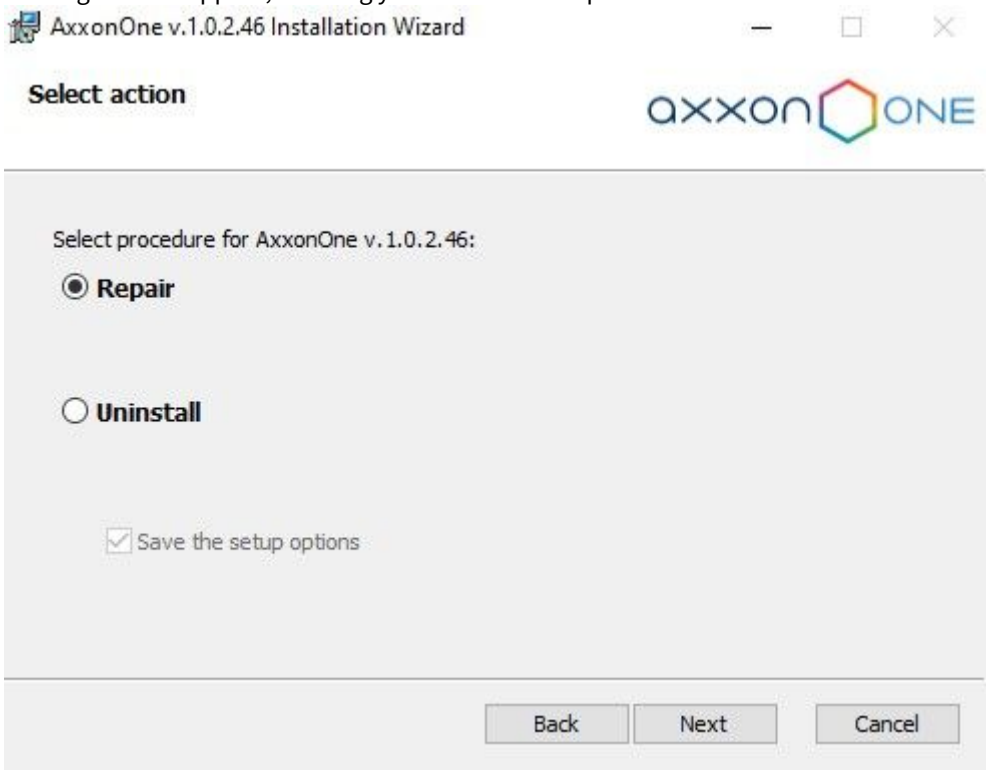
1. Open the *Axxon One* distribution package.



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

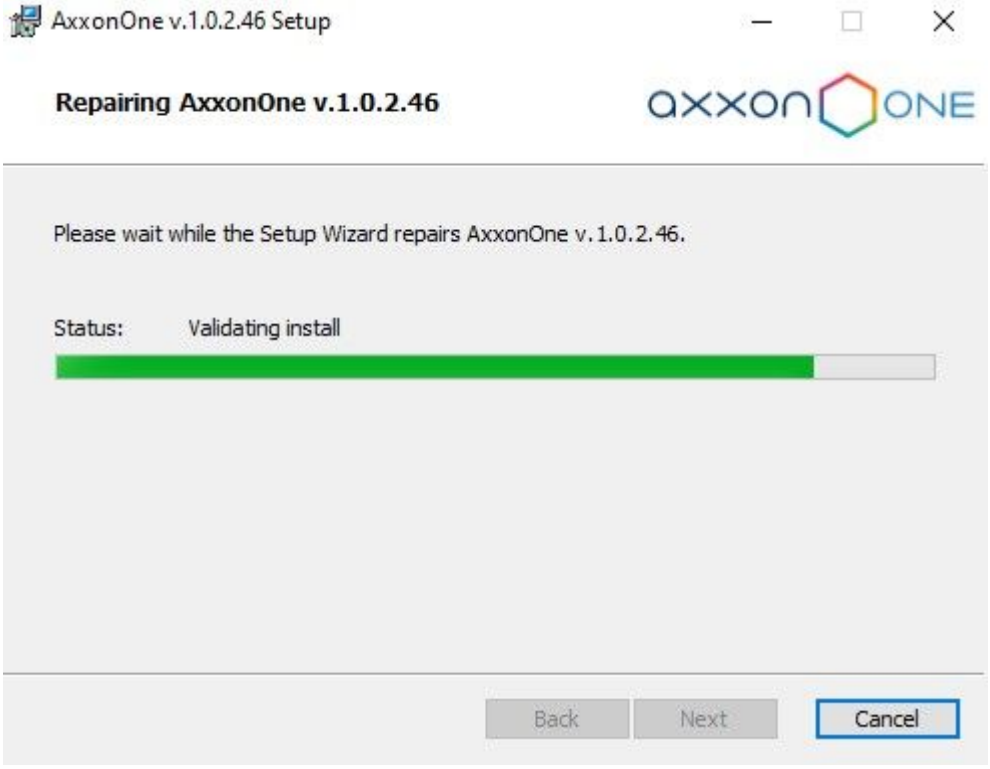


4. A dialog box will appear, allowing you to choose an operation.



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.

12.2.4 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.

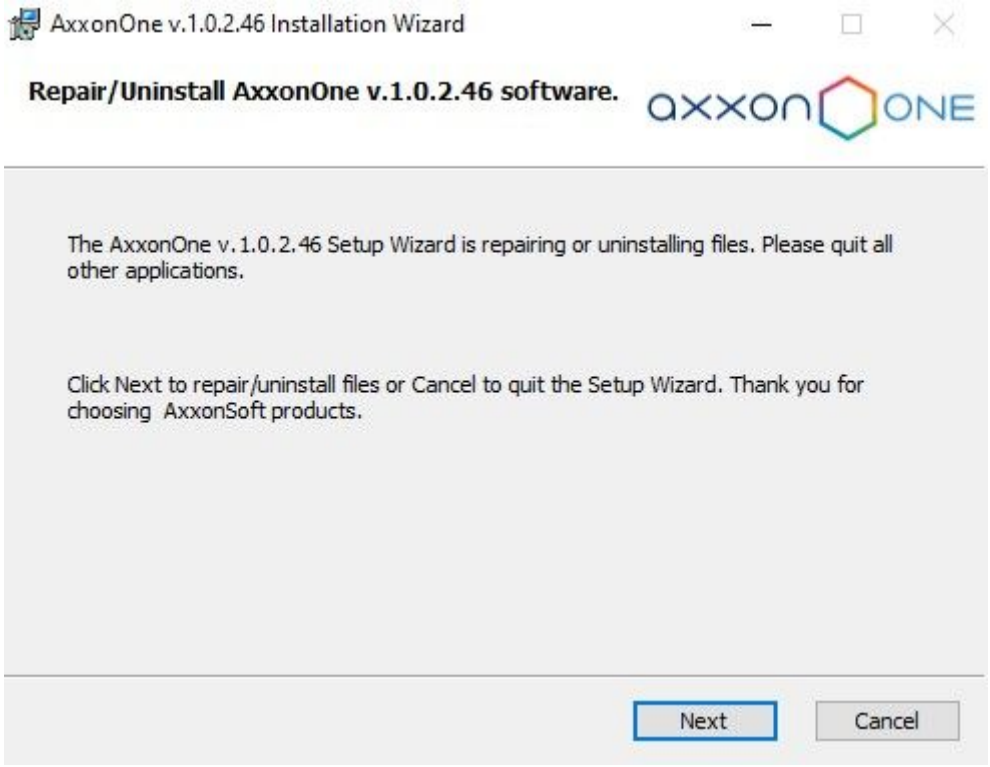
> **Note**
>
> All related applications should be closed before beginning removal of the *Axxon One* software.

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

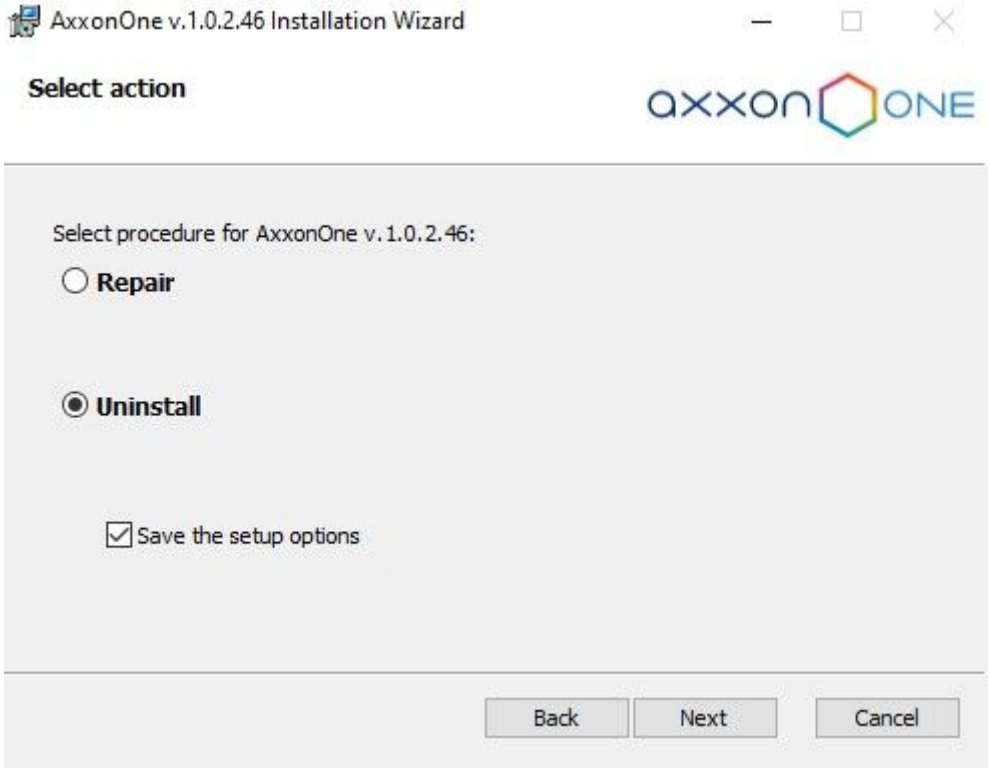
1. From the **Start** menu.
2. Using **Add or Remove Programs** in the Windows control panel.
3. By starting the executable file named setup.exe, which is included with the installed version of the product.

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.

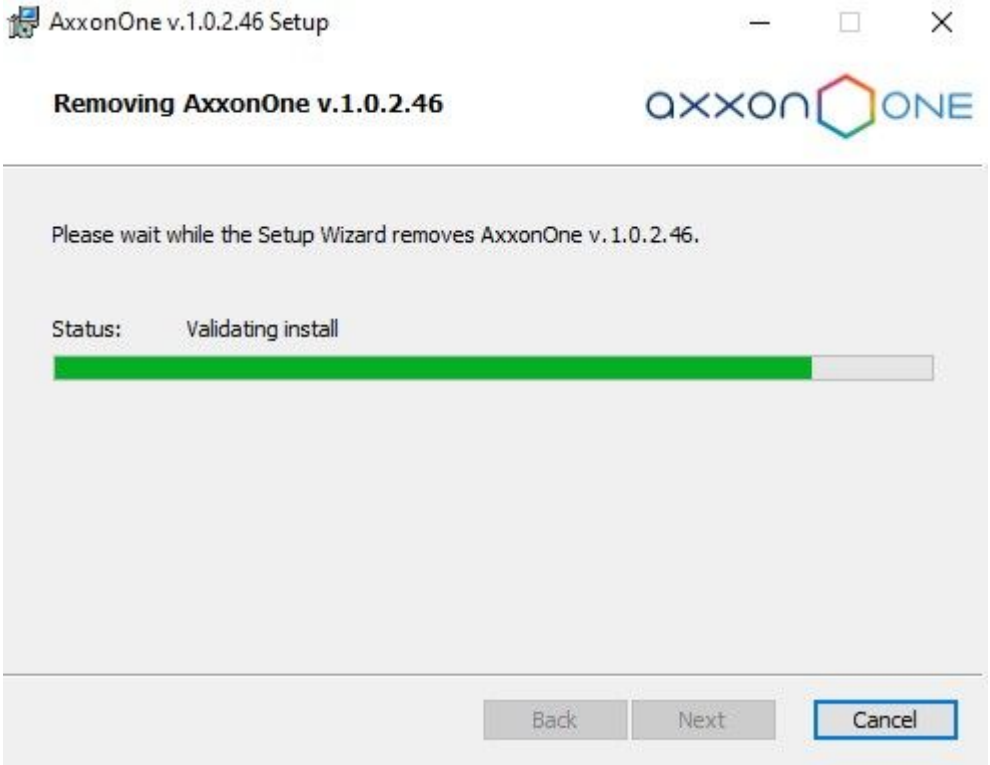


A dialog box will appear, allowing you to choose an operation.



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.

12.2.5 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.

Command-line option	Description
/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

Installation options	Description
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[48]). 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");

48 https://en.wikipedia.org/wiki/NAT

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]').

12.2.6 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(see page 100), Starting a Server(see page 94)).

12.2.7 Update

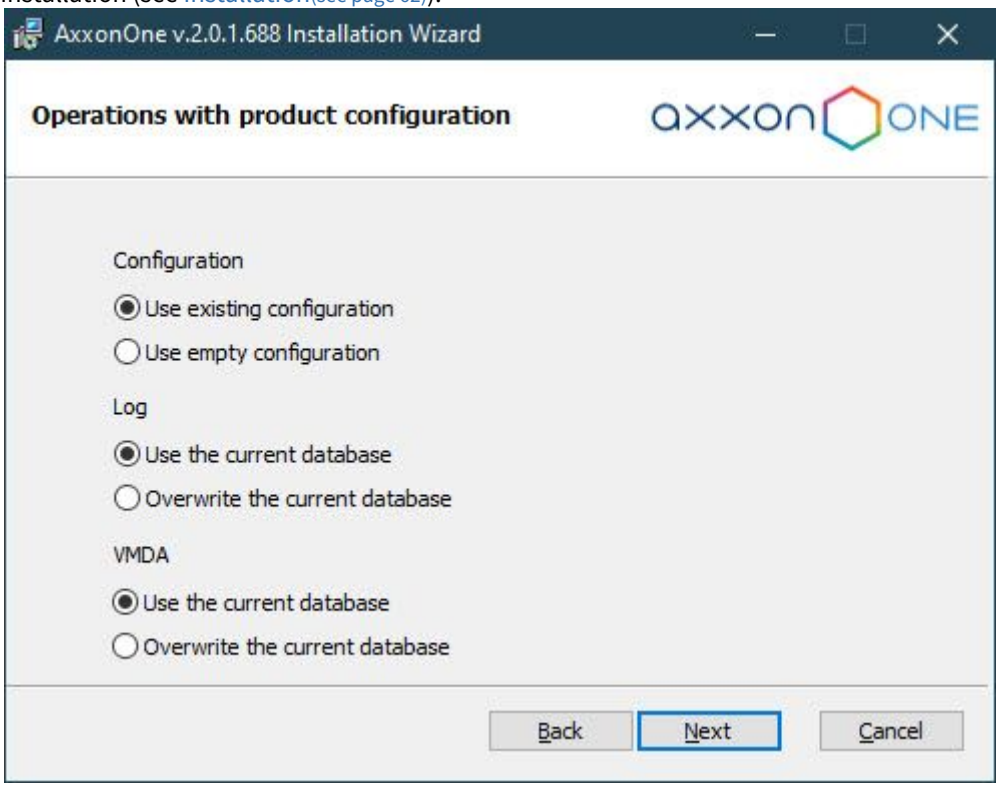
When working with the Failover system, it is recommended to update the Servers through a supervisor (see Updating Servers within a cluster(see page 614)).

Before you start updating, do the following:

- back up your configuration (see Backup and Restore Utility(see page 877));
- stop the Server (see Shutting down a Server(see page 100)) or, in case of Failover system, the NGP_Supervisor service. If you run multiple Servers in the Axxon-domain, make sure to stop them all.

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(see page 62)).



Attention!

In *Axxon One 2.0* and newer, there are no restrictions on database location. To reduce the load on the system disk, it is recommended to store the metadata database and the log database on a separate hard disk.

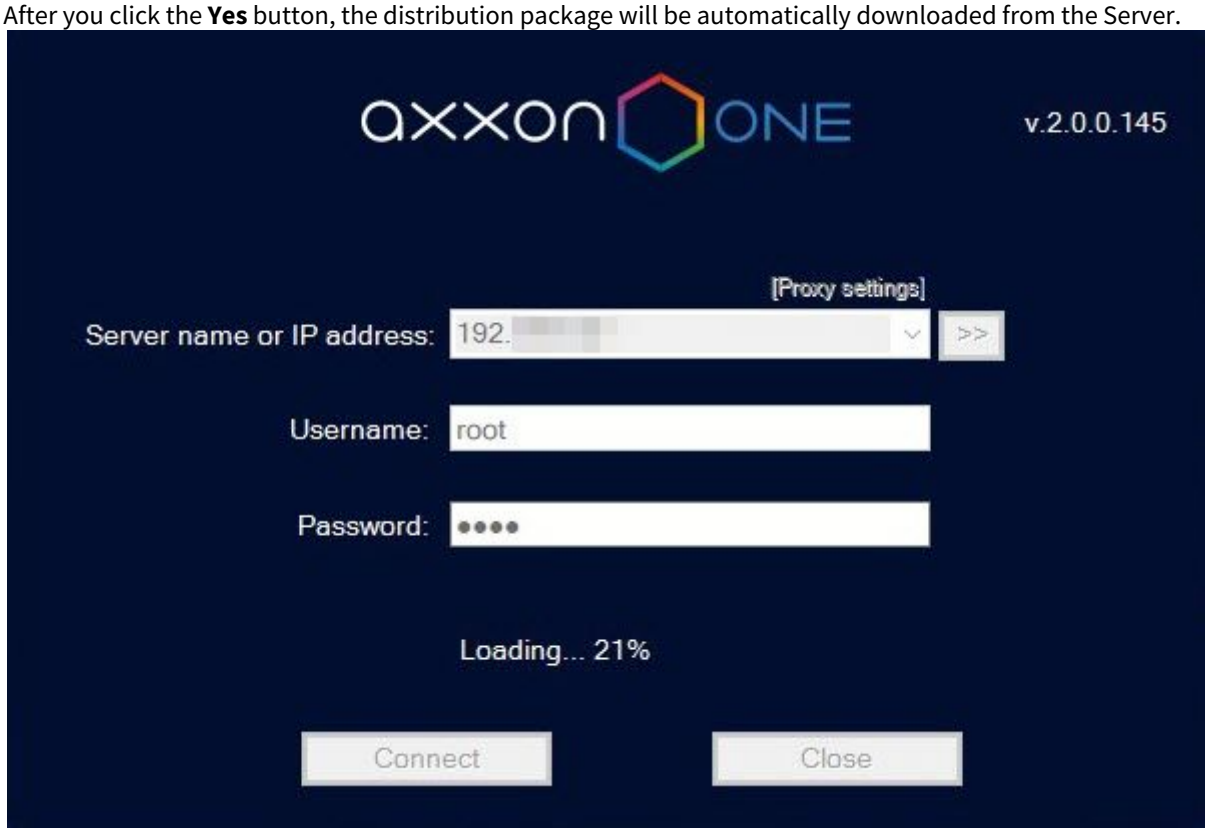
12.2.8 Automatic update of a remote Client

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

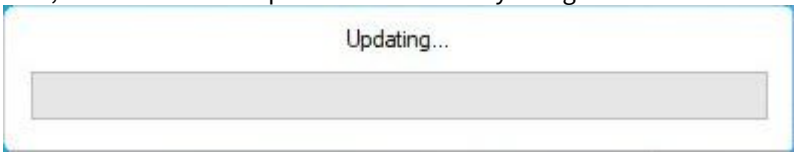
Attention!

- You should 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.

13 Licensing of the software product

13.1 Axxon One license types

Creating an activation request[49]
Activating Axxon One Free[50]

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[51]		Unlimited	1	1	30	30	Unlimited
Maximum number of cameras in a distributed system[52]		Unlimited	4	64	Unlimited	Unlimited	Unlimited
Free Software Updates[53]		No	No	Yes	Yes	Yes	Yes
Support for SD cards (edge storage, playback only)(see page 174)		Yes	No	Yes	Yes	Yes	Yes
Macros (event response wizard)(see page 400)		Yes	No	Yes	Yes	Yes	Yes
AxxonNet Reports[54]		Yes	No	Yes	Yes	Yes	Yes
Scene analytics detection tools(see page 260) (excluding Line crossing, Abandoned objects)		Yes	No[2]	No	Yes	Yes	Yes
Line crossing(see page 268)		No	No	No	Yes	Yes	Yes
Abandoned objects(see page 270)		No	No	No	Yes	Yes	Yes
Time Compressor(see page 699)		No	No	No	Yes[8]	Yes[8]	Yes[8]
Cross-System Client(see page 101)		No	No	No	Yes	Yes	Yes
AI Features and Retail License Pack							

49 https://docs.axxonsoft.com/confluence/display/one20en/Creating+an+activation+request
50 https://docs.axxonsoft.com/confluence/display/one20en/Activating+Axxon+One+Free
51 https://docs.axxonsoft.com/confluence/display/one1en/Configuring+Axxon+domains
52 https://docs.axxonsoft.com/confluence/display/one1en/Configuring+Axxon+domains
53 https://docs.axxonsoft.com/confluence/display/one20en/Upgrading+Axxon+One
54 https://docs.axxonsoft.com/confluence/display/anet/Local+AxxonData+Reports+subsystem

Advanced archive search: • MomentQuest smart forensic search(see page 730) • Face search(see page 744)[6] • LPR search(see page 741)	Yes	No	No[3]	Optional	Yes	Yes
Tag&Track multicamera object tracking(see page 685)	Yes	No	No	Optional	Yes	Yes
Retail Analytics: • Visitors counter(see page 383) • Queue detection(see page 383) • Heat map(see page 849)	Yes	No	No	Optional	Yes	Yes
Face Mask Detection(see page 291)	Yes	No	No	Optional	Yes	Yes
Neural Tracker(see page 274)	Yes	No	No	Optional	Yes	Yes
Smoke and fire detection(see page 350)	Yes	No	No	Optional	Yes	Yes
QR/Barcode reader	Yes	No	No	Optional	Yes	Yes
Neural Counter(see page 344)	Yes	No	No	Optional	Optional	Optional
Human Behavior Analytics						
Pose detection(see page 371)[6] includes: • Man down • Raised arms • Crouched man • Social distancing	Yes	No	No	Optional	Optional	Optional
Personal Protective Equipment Detection						
Personal protective equipment detection(see page 358) includes: • Helmets • Hi-viz vests • Protective Clothing	Yes	No	No	Optional	Optional	Optional
Add-On Modules						
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)(see page 192)	Yes	No	Optional	Optional	Optional	Optional
Custom AI Analytics	No	No	No	Optional	Optional	Optional

Water level detection(see page 390)	Yes	No	No	Optional	Optional	Optional
Offline analytics. Smart search in imported video(see page 531)	No	No	No	No	No	Yes
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]
Datacenter Domain Unification/Private Cloud	Yes	No	No	No	No	Yes
Real-time face recognition(see page 301)	No	No	No	Optional	Optional	Optional
FaceCube external face recognition module(see page 307)	No	No	No	Optional	Optional	Optional
Real-time vehicle license plate recognition(see page 337)[4]	No	No	No	Optional	Optional	Optional
Vehicle recognition[4]	No	No	Yes	Yes	Yes	Yes
Person-based privacy masking(see page 366)	Yes	Yes	Yes	Yes	Yes	Yes
Searching for LPR/ANPR numbers and faces on video from multiple cameras(see page 759)	Yes	No	No	Optional	Yes	Yes
Data replication(see page 226)	No	No	No	No	Yes	Yes
FailOver(see page 587)	No	No	No	No	Yes	Yes
Video walls management(see page 792)	Yes	No	No	No	Yes	Yes
LDAP authentication supported(see page 462)	Yes	No	No	No	Yes	Yes
System features available for all licenses						
Hardware Control panels Security keyboards Joysticks I/O modules	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
AxxonNet cloud service[55]	Yes	No	Yes	Yes	Yes	Yes

55 https://docs.axxonsoft.com/confluence/display/anet/AxxonNet+Setup+and+Operation

Server ONVIF Profiles G, S, T(see page 122) H.265 support(see page 45) Edge analytics (metadata from IP devices) (see page 393) Configuration backup and restore(see page 877) Mass configuration of cameras(see page 127) Multicasting(see page 568) Hotkeys(see page 578)	Yes	Yes	Yes	Yes	Yes	Yes
Recorded Video / Investigation Local and network archives(see page 209) Events search(see page 727) Time slice search (search by time intervals) (see page 728) Simultaneous search in an archive of several video cameras(see page 759) Video bookmarking (searchable text comments)(see page 729)	Yes	Yes	Yes	Yes	Yes	Yes
Live Monitoring Basic audio and video analytics(see page 234) Embedded detection tools (see page 393)(except for Axis on-board tracker(see page 394)[5]) Interactive 3D map(see page 795) GreenStream adaptive bandwidth management(see page 690) Tag& Track Lite(see page 686) OnScreen PTZ mode(see page 683) Support for fisheye cameras and ImmerVision lenses(see page 761) Export of frames and video recordings to multiple formats(see page 808) Information boards(see page 771)	Yes	Yes	Yes	Yes	Yes	Yes
Remote clients Web-Client interface(see page 823) iOS app (including Apple TV)[56] Android app[57]	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.

56 https://docs.axxonsoft.com/confluence/display/mobile/AxxonNet+iOS+Mobile+Client+User+Guide
57 https://docs.axxonsoft.com/confluence/display/mobile/AxxonNet+mobile+client+on+Android+OS.+User+Guide

Note

[1]—the system will operate in demo mode from 8:00 AM to 6:00 PM.

[2]—all Scene analytics detection tools are available in *Axxon One Free* license based on the metadata from the base VMD.

[3]—MomentQuest with metadata search from the base VMD is available in *Axxon One Start* license.

[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)(see page 320));
- License plate recognition (IV) (see Configuring License plate recognition (IV)(see page 326)).

[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.

13.1.1 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.

13.2 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.

13.3 Product activation utility

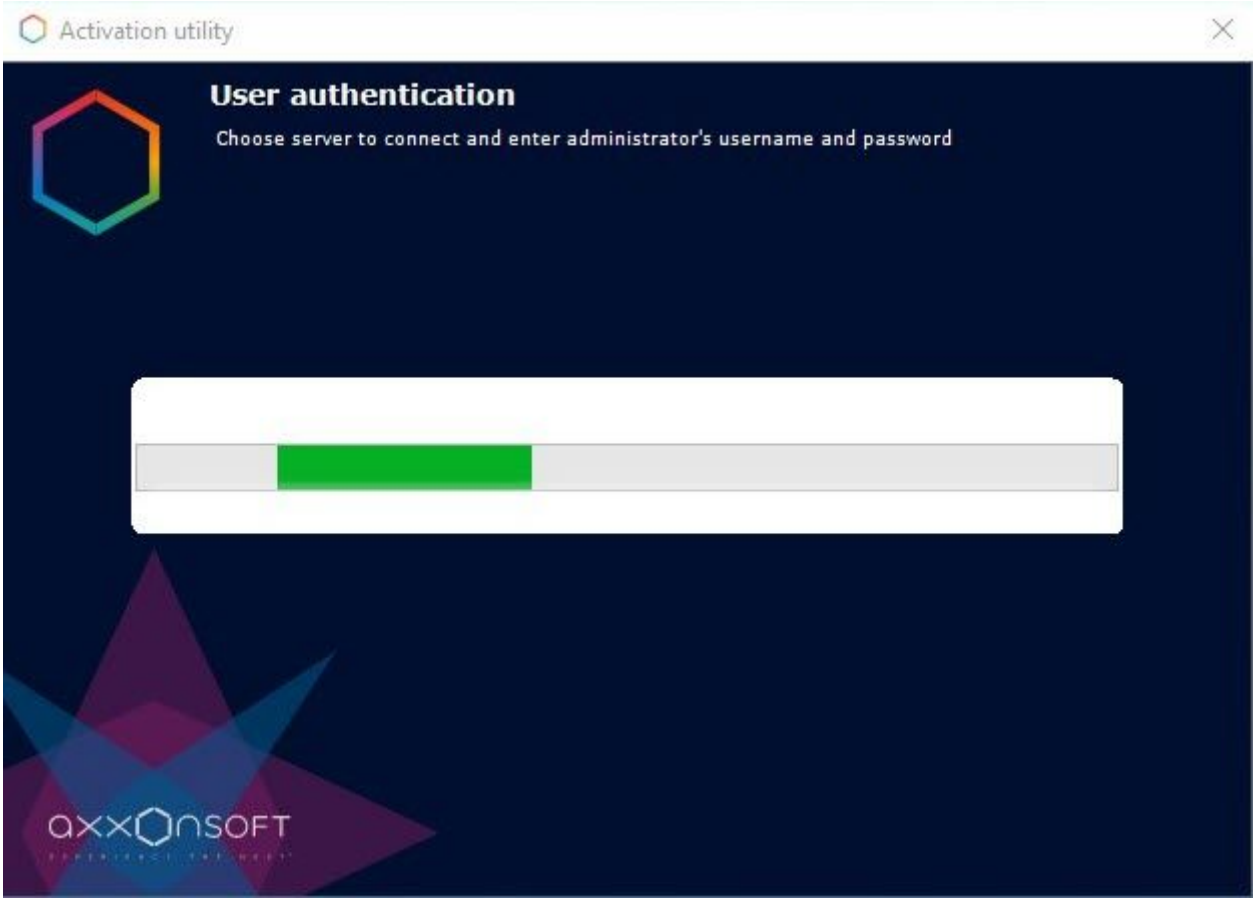
License activation for the *Axxon One* software package is carried out through the product activation utility.

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

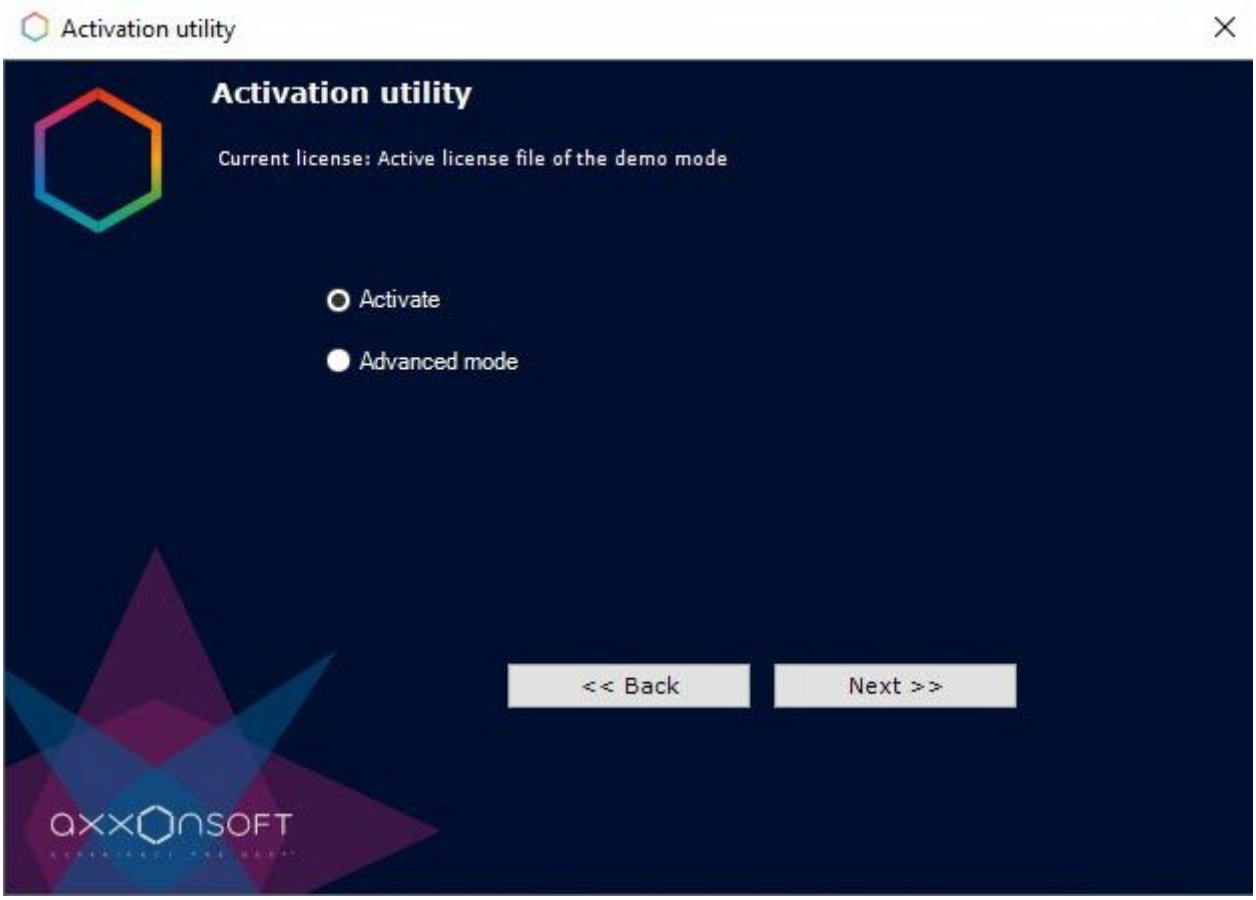
> **Note**
>
> The product activation utility program file LicenseTool.exe is located in the folder <Directory where *Axxon One* is installed>\AxxonSoft\Axxon Smart\bin\

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.

13.4 License Activation

To activate *Axxon One*, please refer to the document titled Activation Guide[58], 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.

58 https://docs.axxonsoft.com/confluence/display/one20en/Activation+Guide

14 Launching and closing the Axxon One software package

14.1 Startup

14.1.1 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(see page 860)).

   > **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 10. Creating system variable(see page 951)) to increase the Server start time. The value of the variable should be specified in milliseconds.

14.1.2 Starting an 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 have to specify the following parameters: login, password and server.
> 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, 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**
   >
   > The *Axxon One* Client can also be started from the *Axxon One Tray Tool* utility (see Axxon One Tray Tool(see page 860)).
   > *Axxon One* executable file Axxon One.exe is located in the <*Axxon One* installation directory>\Axxon One\bin\ folder.

   > **Note**
   >
   > 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 appear.

> **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(see page 613).

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

> Connecting the Client to the Server behind NAT(see page 946)

> **Note**
>
> If the software is accessed by a remote user, the name or the IP address of the computer with which the connection is established should be entered in the **Server name or IP address** field.

> **Note**
>
> The order of the Servers in the list is the following:
>
> a. Preferred Servers (see Selecting Preferred Servers(see page 571)).
> 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.

> **Note**
>
> The first login to the system is done with the root user, which has administrator permissions. Enter **root** in the **Username** and **Password** fields. The administrator then needs to configure the system for multi-user access (for details, see Configuring user permissions(see page 450)).

Attention!

You need to match software versions between the Server and the Client. The *DriversPack* version must be the same as well.
It is strongly recommended to avoid any connections if the product versions do not match.

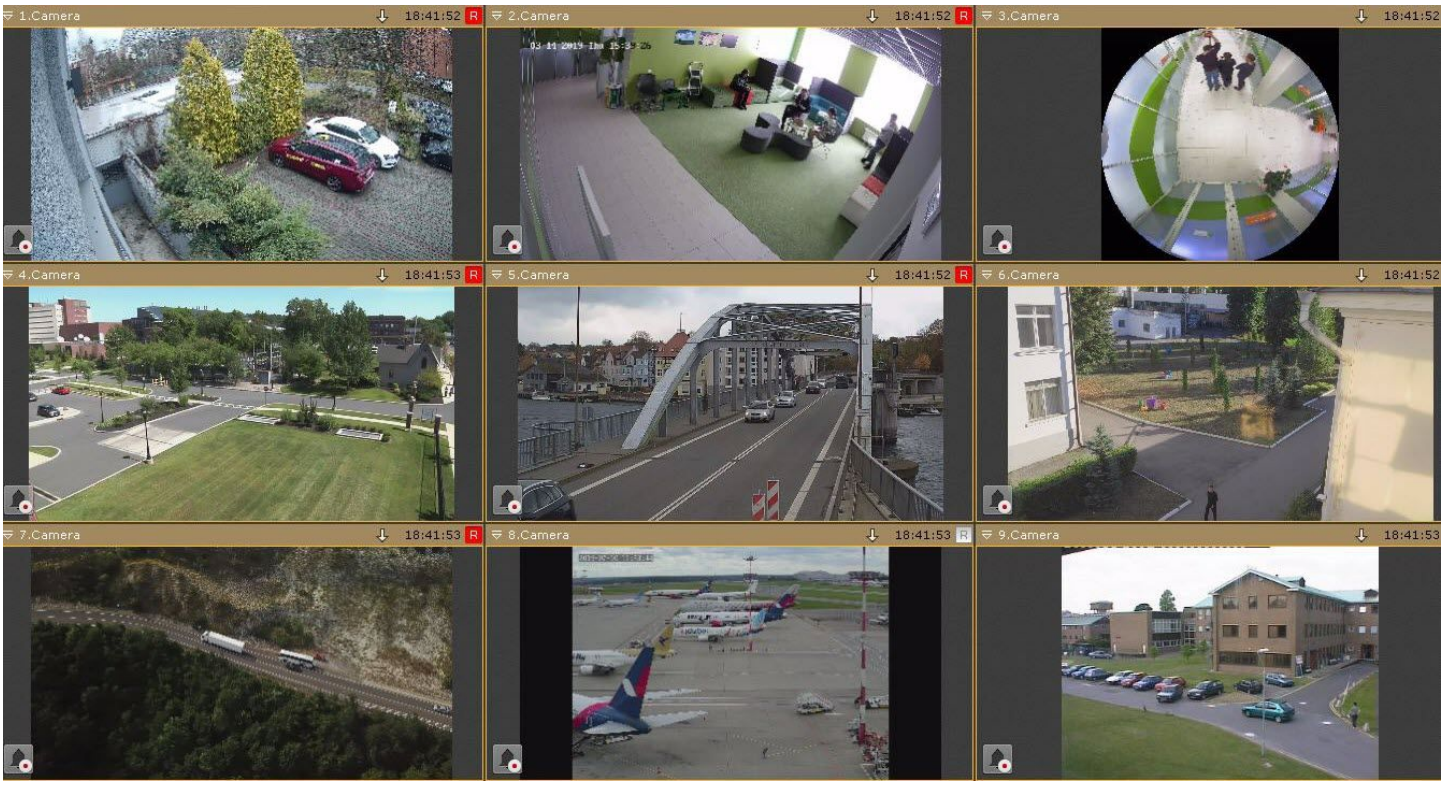
Connecting LDAP users(see page 102)

4. If the user requires the access confirmation by the system administrator (see Creating and configuring roles(see page 452)), enter the corresponding credentials and click the **Connect** button.

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

Attention!

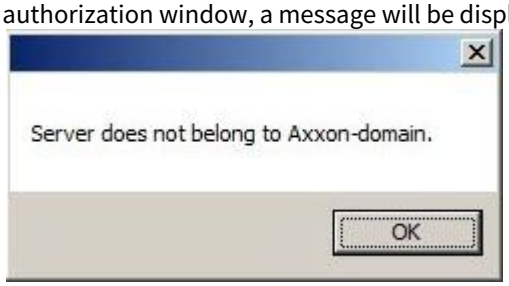
When you first start the Client, the archive settings tab opens (see Configuring archives(see page 206)).
After the archive is created, you will be automatically switched to creating IP devices (see Adding and removing IP devices(see page 112)). IP Device Discovery Wizard will launch automatically.



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(see page 98)).

If the Server to which *Axxon One* is connecting does not belong to any Axxon-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 Axxon-domain based on the Server or add the Server to an existing Axxon-domain.
If you choose the first option, click **OK** in the message and follow the instructions given in Creating a new domain(see page 108). For the second option, click the ✕ button and follow the instructions given in Adding a Server to an existing Axxon-domain(see page 109).

14.1.3 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.

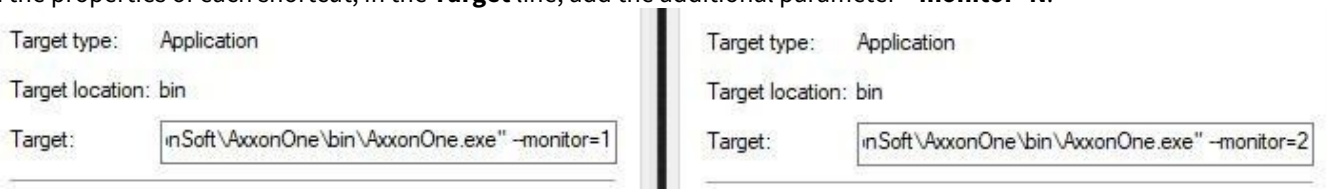
Attention!

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(see page 46)).

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)(see page 557)) 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.

14.1.4 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(see page 86)).

The different types of demo modes are presented in table.

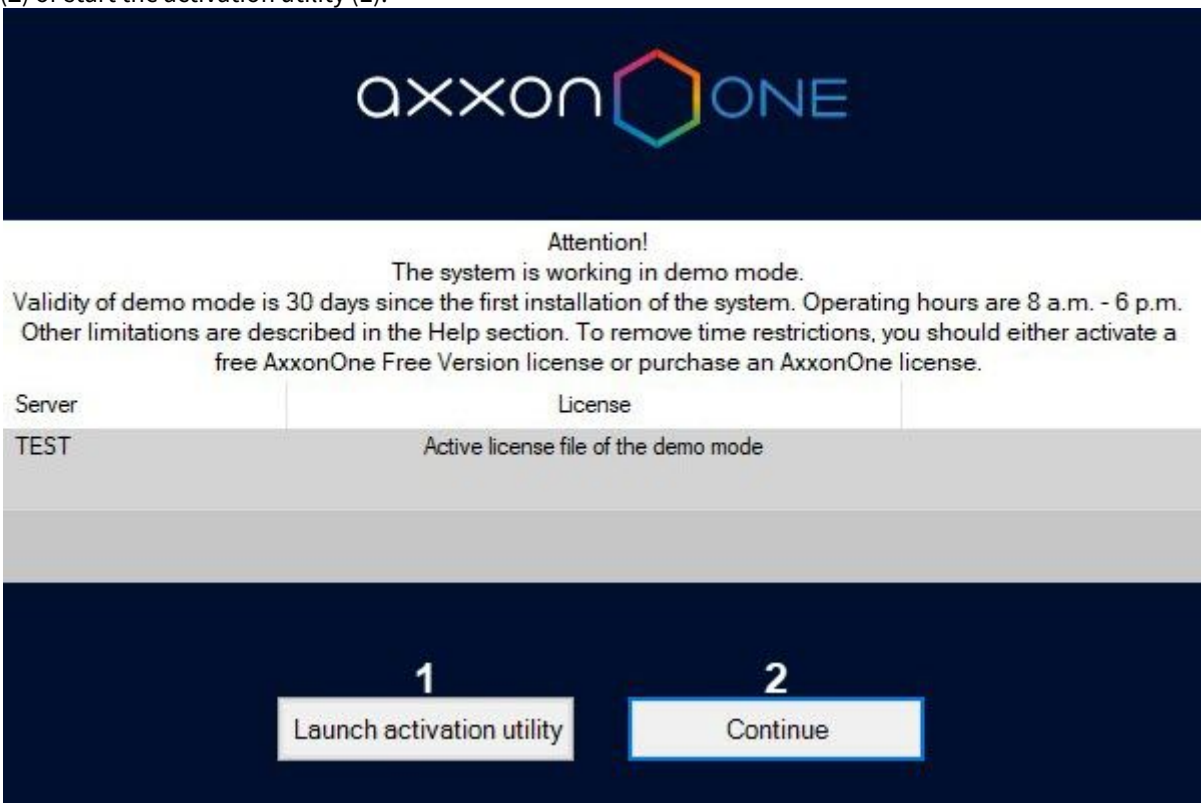
Type of demo mode	Conditions	Axxon One operation
Active	*Axxon One* can be started between the hours of 8:00 AM and 6:00 PM	Using *Axxon One* in demo mode
Inactive	*Axxon One* started outside the hours of 8:00 AM and 6:00 PM	The *Axxon One* server is not available, only the system configuration can be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



14.1.5 Automatic Start of the Client

You can use Windows Task Scheduler[59] 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 Configuring Cross-System Client and autologon(see page 568)).

14.2 Shutdown

14.2.1 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.

59 https://technet.microsoft.com/en-us/library/cc721931(v=ws.11).aspx

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.

14.2.2 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(see page 860)).

   > **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 10. Creating system variable(see page 951)) to increase the Server shutdown time. The value of the variable should be specified in milliseconds.

14.3 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.

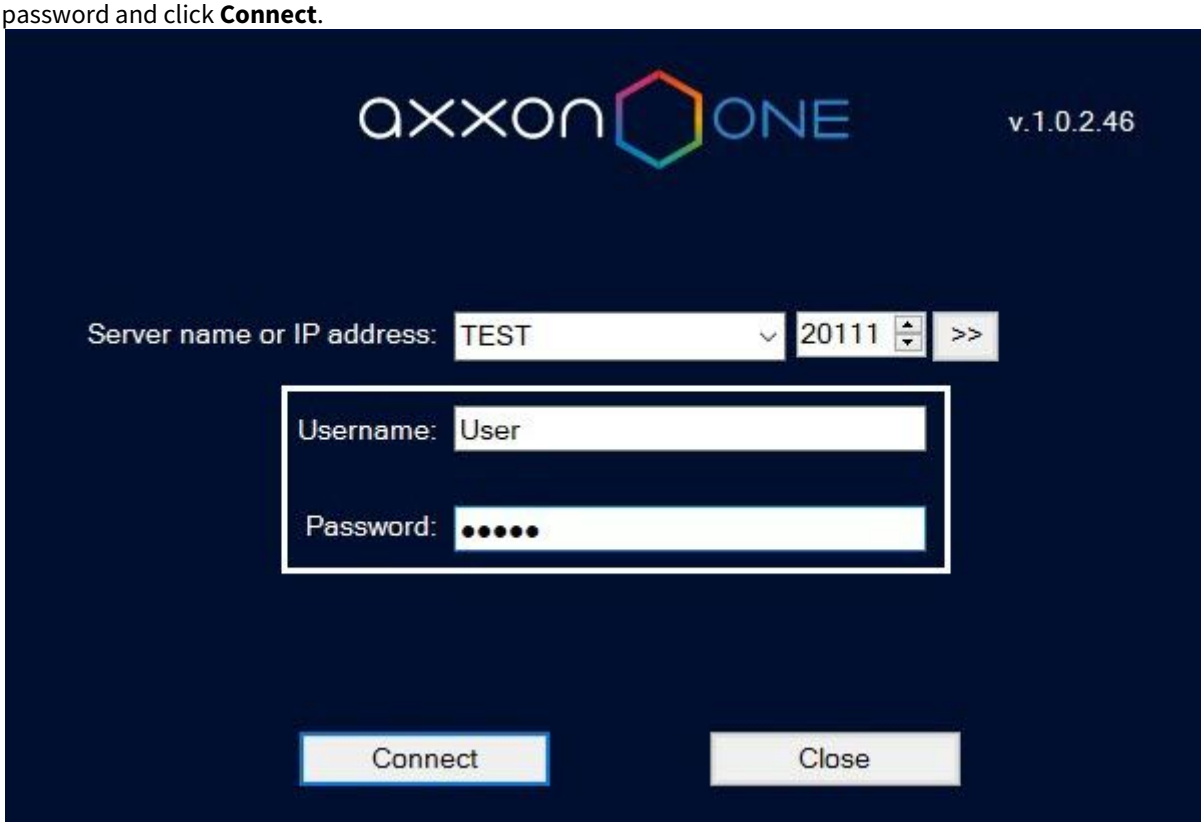
> **Attention!**
>
> While the Server restarts, the connection to cameras is temporarily lost and recording stops.

14.4 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(see page 99)).
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.

14.5 Cross-System Client

Cross-System Client empowers users to connect to multiple servers on various domains and in different systems from a single client workstation. All settings and cameras associated with these servers are consolidated in a single convenient view. That way you can access multiple independent surveillance systems simultaneously, even if the customer cannot or does not want to combine these systems.

This may happen for various reasons, such as:

1. your facilities are geographically dispersed, or
2. you want to mass configure multiple cameras from different systems.

A typical scenario may involve police plugging Cross-System Client in security systems at different retail chains/stores.

Cross-System Client automatically connects to specified Axxon domains when you start it (see Configuring Cross-System Client and autologon(see page 568)). The client first connects to the primary Axxon domain; connection to the other Axxon domains is established in the background after the client starts.

Note

You can also configure the Client connections to Axxon domains in the sign-up in the authorization dialog box. To do this, enter comma-separated values for Servers as follows: <Server 1 Name or IP address>:<Connection port>, <Server 2 Name or IP address>:<Connection port>. Server 1 is the primary connection.

14.6 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 Creating LDAP connections(see page 468)). The login and password in the LDAP directory are not used when connecting to the Server.

14.7 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(see page 99)).

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**.

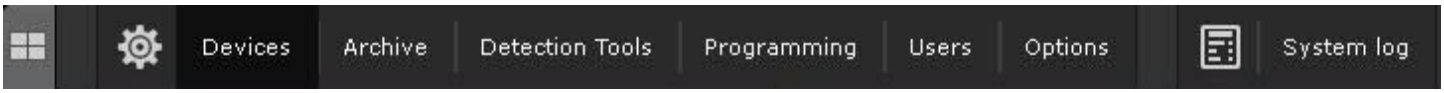
Connection to another Server is now complete.

15 Configuration of the Axxon One Software Package

15.1 General information on system configuration

15.1.1 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.

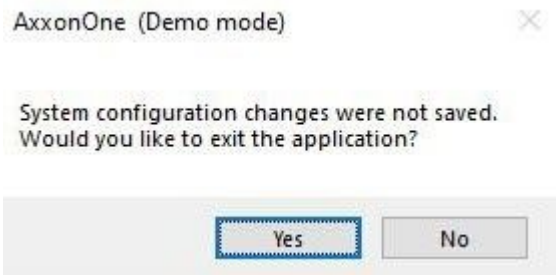
15.1.2 Applying and resetting settings

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.

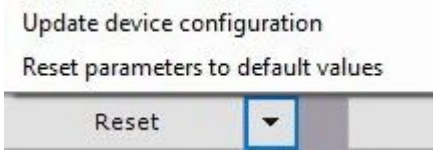


When setting up hardware, you can reset parameters to default values, or read configuration from the device at any time.

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**.



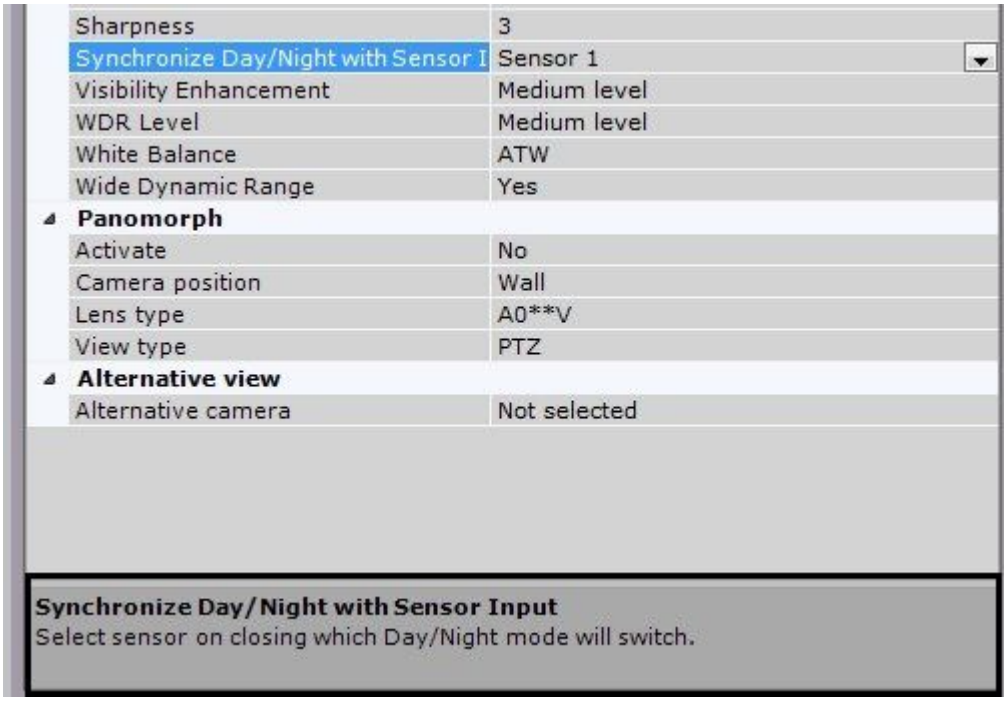
If a device's configuration differs from settings specified within the system, you can download the configuration from the device. To do it, follow the steps below:

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

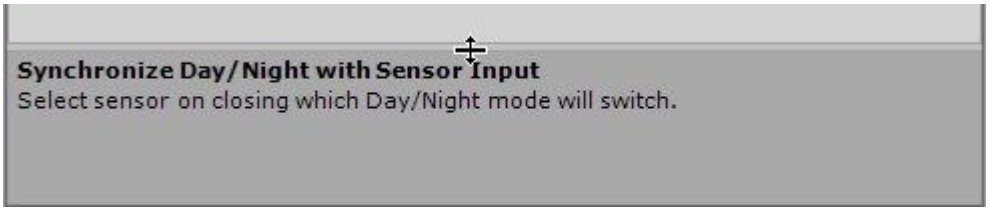
15.1.3 Display of parameters in interface

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.



15.1.4 System objects

Axxon One VMS has the following types of system objects:

1. Axxon domain objects (see Configuring Axxon-domains(see page 107)).
2. Hardware objects: Server, IP Server, Camera, Microphone, PTZ, Input, Output, Embedded Storage (see Configuring system objects for devices(see page 118)).

3. **Event Source** objects are used to integrate *Axxon One* with external systems (see Receiving Events from External Systems(see page 192)).
4. **E-mail** objects used in macros and automatic rules for e-mail notifications (see The E-mail notifier object(see page 435)).
5. **Export Agent** objects used in macros and automatic rules for exporting video recordings and snapshots (see Configuring export(see page 572)).
6. Archive objects (see Configuring archives(see page 206)).
7. Detection tool objects (see Configuring detection tools(see page 234)).
8. Role and user objects (see Configuring user permissions(see page 450)).
9. Macro objects (see Configuring macros and counters(see page 400)).

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

15.1.5 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**.

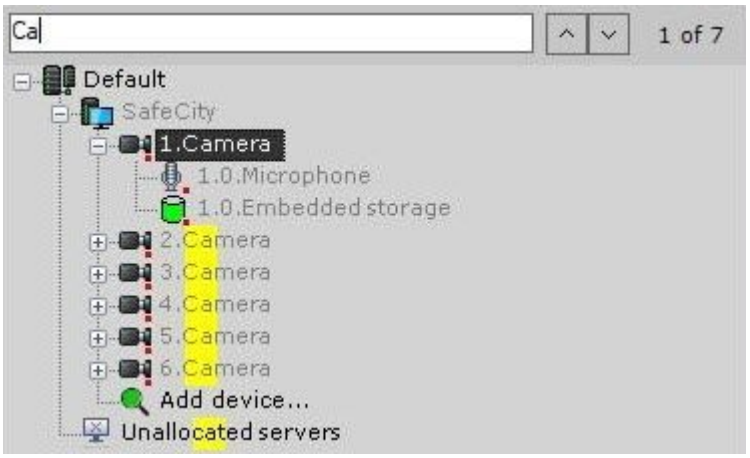
To search for objects, complete the following steps:

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 ID.

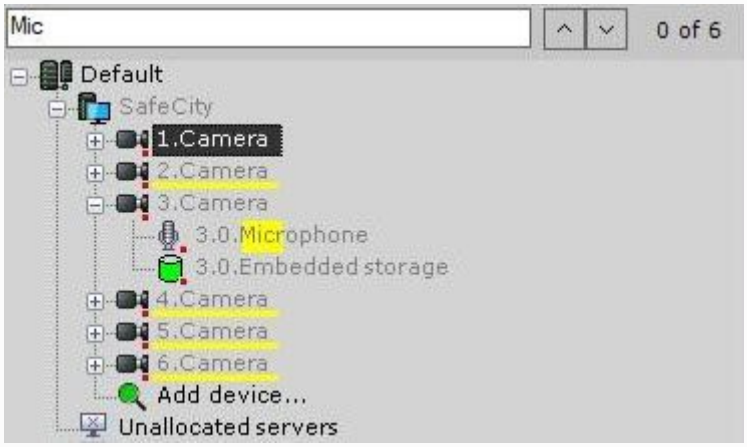
The search starts automatically once you enter something in the box. When the search is complete, you will see the number of objects found in the tree.



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.

15.2 Hardware configuration

15.2.1 Configuring Axxon domains

A distributed system based on the *Axxon One* software package is created within an Axxon Domain, i.e., a selected group of *Axxon One* Servers.

When configuring Axxon Domains, the following operations are used in the necessary combinations:

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

Attention!

You cannot combine regular and Failover Servers within the same Axxon domain (see Configuring Failover VMS(see page 587)).

To configure Axxon Domains, you must have the appropriate permissions (see the section Configuring user permissions(see page 450)).

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

15.2.1.1 Axxon-domain object

The **Axxon-domain** system object is at the base of the system.

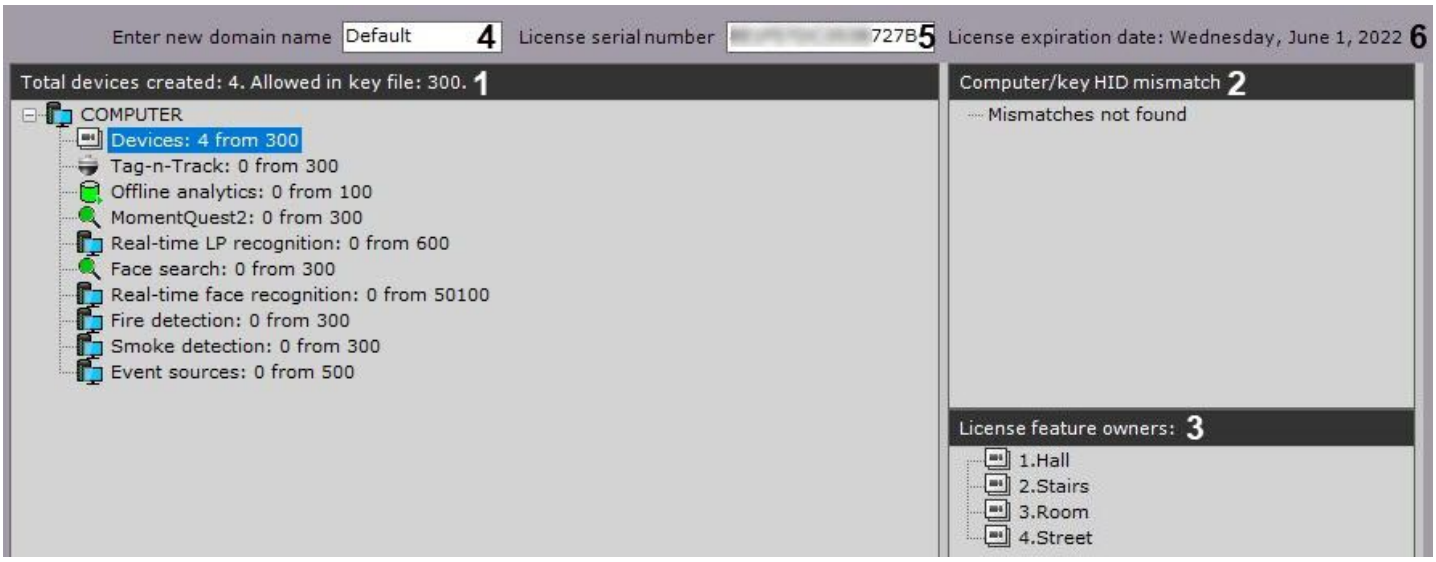
The **Axxon-domain** object is the parent of the **Server** objects, which correspond to the servers that are in the Axxon-domain.

When you select the **Axxon domain** object in the **Total devices created** group (**1**), the software displays information about the Axxon 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 Axxon-domain. To do so, enter the new name in the corresponding field (**4**) and click the **Apply** button.

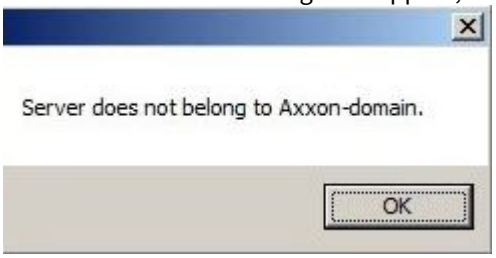
15.2.1.2 Axxon Domain operations

15.2.1.2.1 Creating a new domain

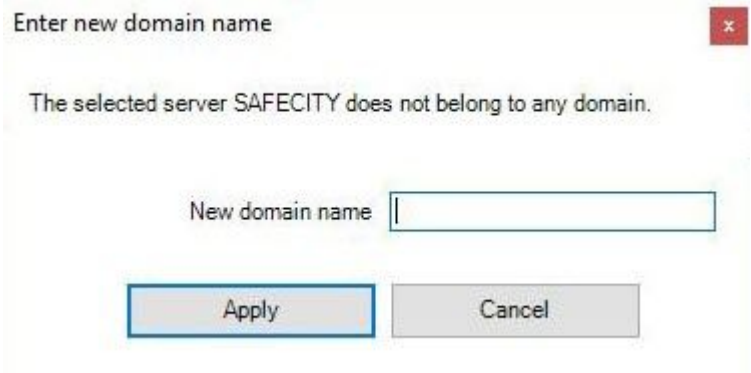
A new Axxon Domain can be created in one of two ways:

1. During installation of the *Axxon One* software package with the Server and Client configuration type (see step 8 of the instructions in the section Installation(see page 62)).
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 should click **OK** (see also the section Startup(see page 94)).



The **Enter new domain name** window will appear. In the **New domain name** field, enter the Axxon 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 Axxon Domain. Assigning the same Axxon Domain name to several Servers does not guarantee that those Servers will be in the same Axxon Domain. Different Axxon Domains can have identical names.

This will create a new Axxon Domain based on the Server. The *Axxon One* software package will then be launched with the entered authorization parameters (see the section Startup(see page 94)).

15.2.1.2.2 Adding a Server to an existing Axxon-domain

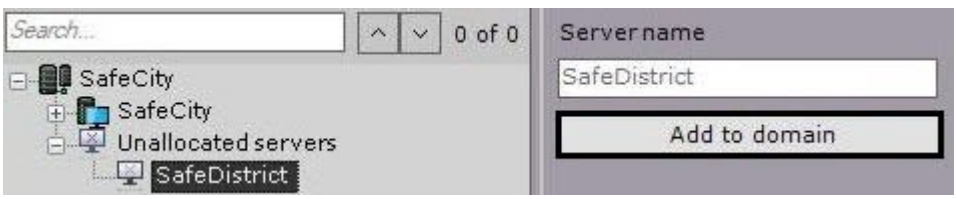
A Server can be added to the existing Axxon-domain from any Server within that Axxon-domain.

Attention!

- Before configuring a distributed system, be sure to consolidate your Servers into the Axxon-domain.
- When consolidating the Servers into the Axxon-domain, each Server should have a unique IP address.
- Only unallocated Servers can be added to the Axxon-domain. Unallocated Servers are the Servers that don't belong to any Axxon-domain.

There are two ways to add a Server to the Axxon-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.



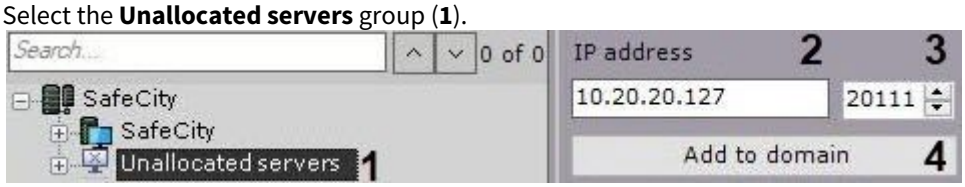
The Server will then be added to the Axxon-domain from the **Unallocated servers** group.
Since the search for the unallocated Servers is conducted using the broadcast packets, the results may not include Servers located in a different subnetwork (for example, beyond a router that blocks broadcast packets).

In this case, you can add a Server to the Axxon-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(see page 944)
Network settings utility(see page 899)

To add a Server to the Axxon-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 the Axxon-domain.
After a Server is added to the Axxon-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 the Axxon-domain, it will be displayed in the objects tree with the icon.

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

15.2.1.2.3 Removing a Server from an domain

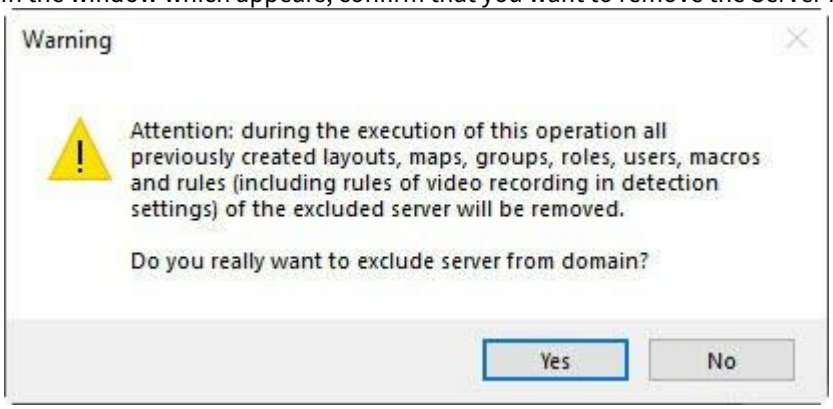
Any Server on an domain can be used to remove a Server from an domain.

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 an 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 the section Startup(see page 94)).

> **Note**
>
> You can also exclude a Server from an domain using the activation utility (see Excluding the Current Server from an domain[60]).

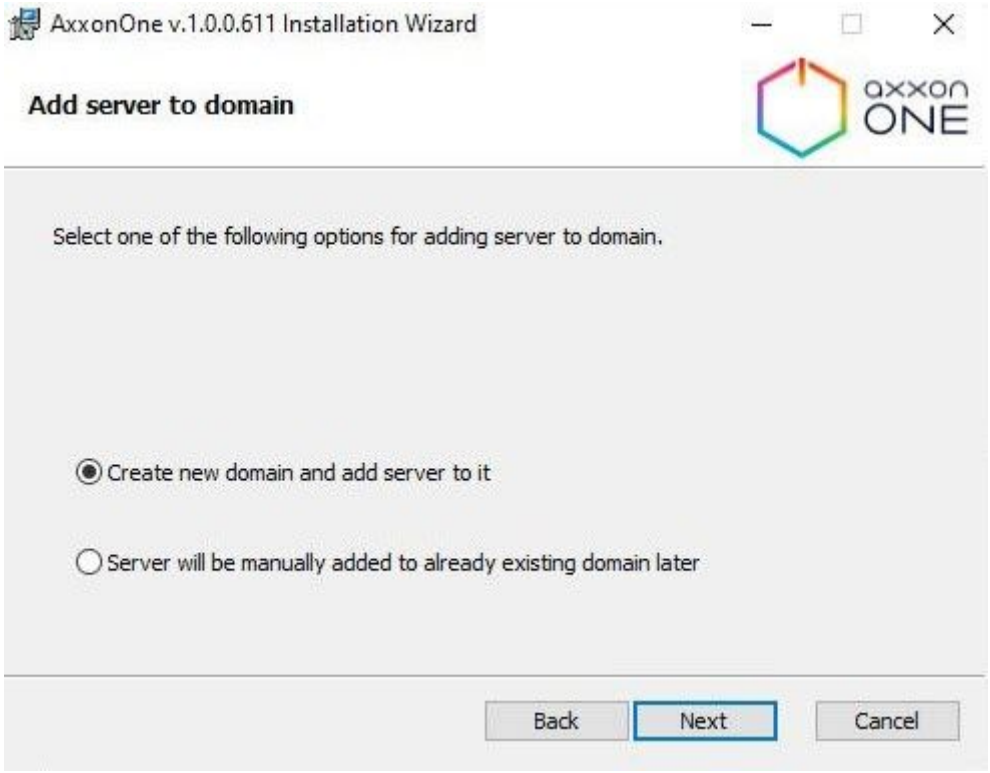
15.2.1.3 Cases of Axxon Domain configuration

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

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

1. Selecting a Server on the basis of which the new Axxon Domain will be created. Installing the *Axxon One* software package with the Server and Client configuration type, indicating the name of the new Axxon Domain (see also step 8 of the instructions in the section Installation(see page 62)).

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

2. Installing the *Axxon One* software package with the **Server and Client** configuration type on the other servers of the future Axxon Domain, without adding them to the Axxon Domain (see also step 8 of the instructions in the section Installation(see

60 https://docs.axxonsoft.com/confluence/display/one20en/Excluding+the+Current+Server+from+an+domain

page 62)).

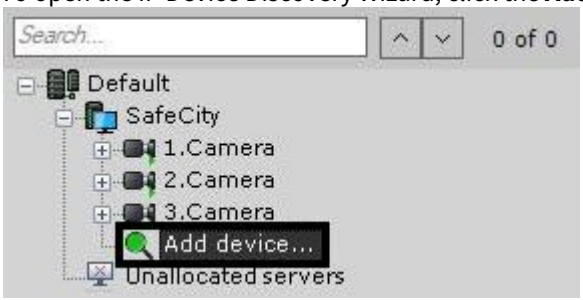
3. Connecting to the primary server.
4. Adding the remaining Servers to the Axxon Domain from the primary Server according to the instructions in the section Adding a Server to an existing Axxon-domain(see page 109).

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

1. Excluding all the Servers which are to be added to the new Axxon Domain from their current Axxon Domains, according to the instructions in the section Removing a Server from an domain(see page 110).
2. Naming the new Axxon Domain according to the instructions in the section Creating a new domain(see page 108), when attempting to connect to one of the Servers excluded in step 1.
3. Adding the remaining Servers to the Axxon Domain from the primary Server according to the instructions in the section Adding a Server to an existing Axxon-domain(see page 109).

15.2.2 Adding and removing IP devices

You can add video cameras and IP Servers to the system by using the IP Device Discovery Wizard.
To open the IP Device Discovery Wizard, click the **Add device ...** link at the end of the Server device list.



When the Wizard is opened for the first time after the Client is started, automatic search for new devices will begin. During subsequent sessions, to launch the Wizard you must click the corresponding button. A progress bar indicates search progress.

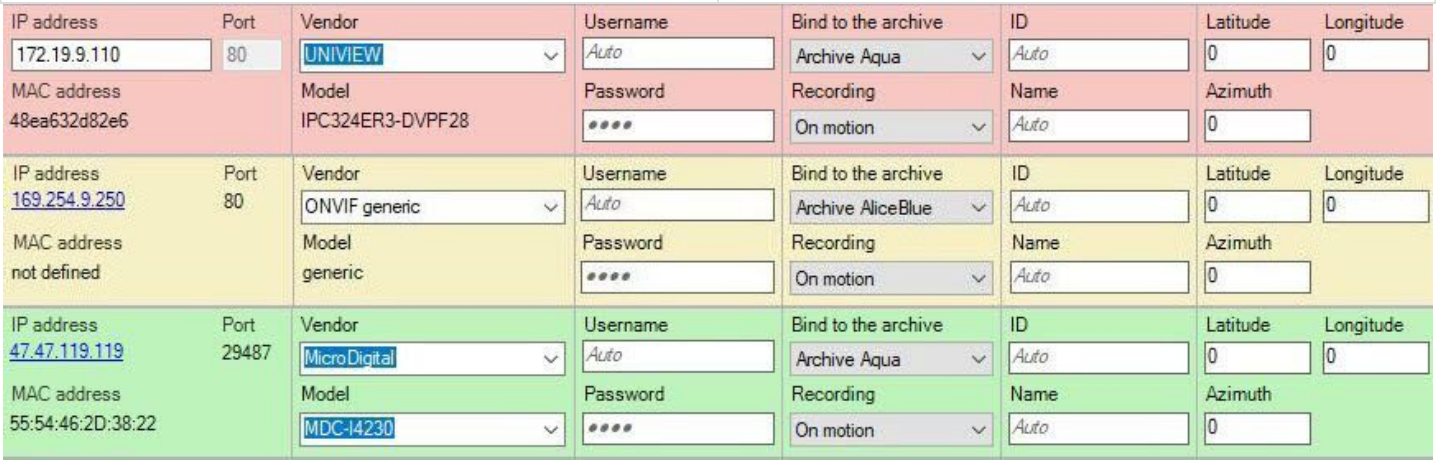
To stop devices search at any time, click the **Stop** button.

Note

Since multicast packets are used for device search, the search results may not contain the Servers and devices from other subnets.

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

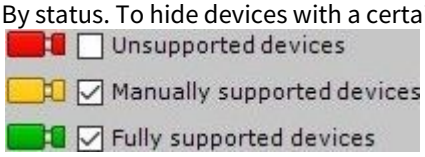


Note

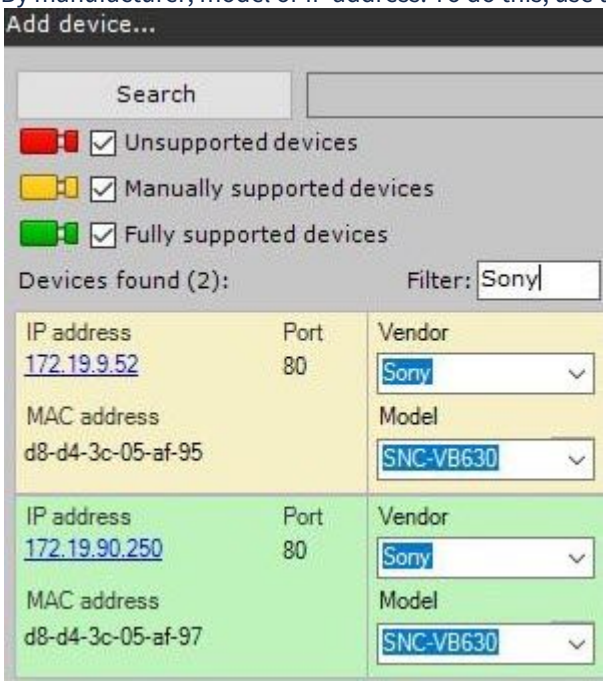
If you click the IP address, you will jump to the device web interface.

Search results can be filtered in two ways:

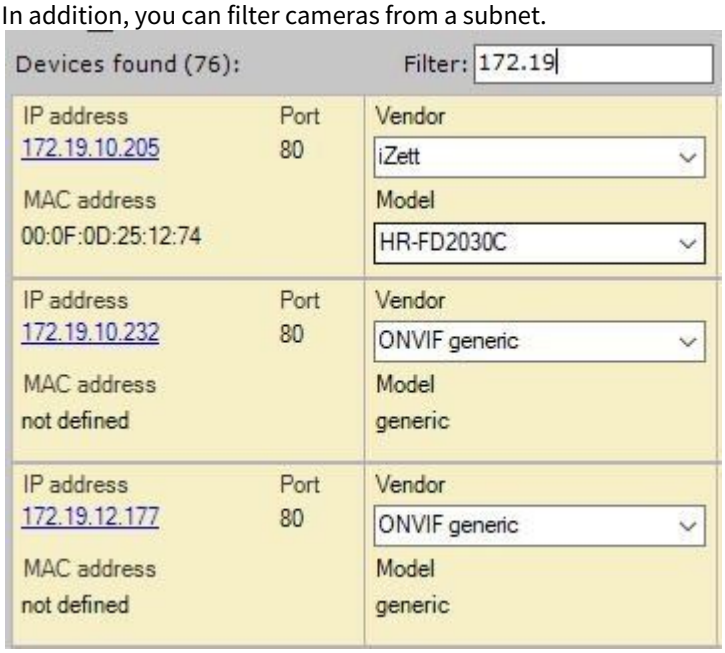
1. By status. To hide devices with a certain status, deselect the relevant checkbox.



2. By manufacturer, 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.

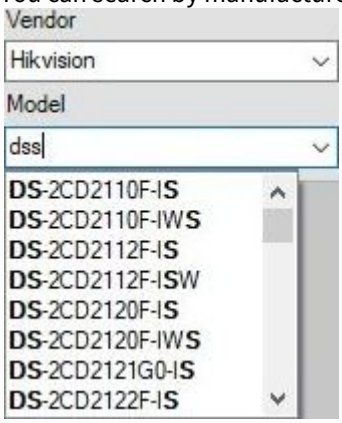


When adding a device, you can immediately set several configuration options, such as:

1. Manufacturer and model.

> **Note**

You can search by manufacturer and model of the device.



2. Login and password.
3. ID and object name.

> **Note**
>
> An object identifier must contain: numbers, English characters and the "_" sign.
> In the Object Tree, added devices will be sorted by ID.

4. In the Object Tree, added devices will be sorted by ID.
5. Select an archive and set the recording parameters (see Configuring recording to an archive(see page 224)):
   a. **No** – camera is linked to the archive, no recording.
   b. **Always** – continuous recording.
   c. **On motion** (default setting) – a VMD tool and an automatic rule for writing to the specified archive are automatically created for the camera you are adding. By default, recording stops when an event detection is finished.
   d. **On motion/Embedded detection** – an embedded VMD tool and an automatic rule for writing to the specified archive are automatically created for the camera you are adding. By default, recording stops when an event detection is finished.

   > **Note**
   >
   > This option is available only for devices that have on-board VMD.

   > **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(see page 224)).

   e. Camera coordinates (latitude, longitude, azimuth) which are used when the camera is added to the geo map (see Adding video cameras and changing size of their icons on the map(see page 512)).

In addition, three modes are available for adding a device to a configuration. These are described in the following table.

	Device addition mode	Description
1	Add device 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.

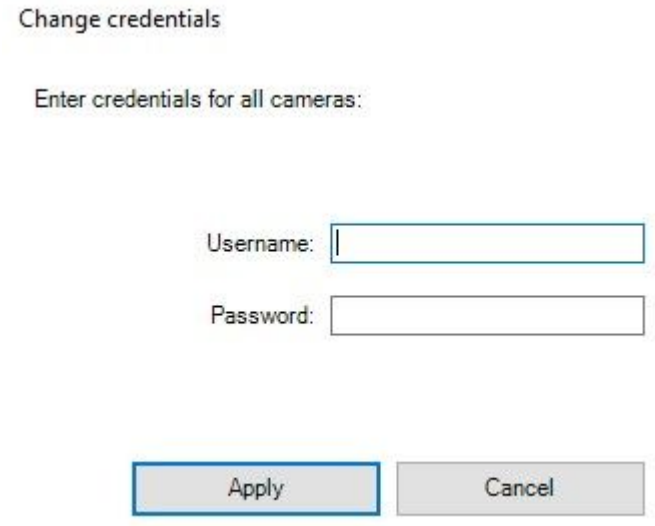
	Device addition mode	**Description**
2	Add device with current settings	The IP device is added to the configuration with the current settings, as specified in the web interface.
3	Add device with template settings	The IP device is added to the configuration with the settings that have been previously 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. The following settings will be copied from the template device to the new, similar device: firmware, video stream settings, buffering settings, **Other** settings (see The Camera object(see page 122)), 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.

To add an IP device to a configuration:

1. Set device settings, if necessary.
2. Select a mode for adding the device to the configuration.
3. The device is then added to the configuration.

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.

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



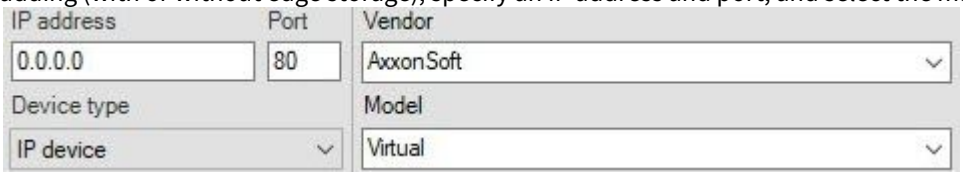
Note

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

Note

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

If an IP device is not shown in the search results (because it is located on another subnet or contact has been temporarily lost), you can add it manually. To do so, in the neutral-colored area above the search results, select the type of IP device that you are adding (with or without edge storage), specify an IP address and port, and select the manufacturer and model.



Then add the device to the configuration by following the steps described previously.

To remove IP devices, select them in the device list (by left-clicking one or more devices, holding down the CTRL key to select multiple devices) and click the **Delete** button.

If you click the IP address, you will jump to the device Web interface.

15.2.2.1 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.
> You should include commas even if no additional parameters are set.
> 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).

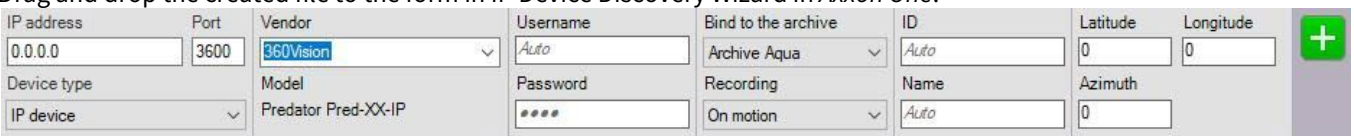
For example:

```
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[61].
> For correct display of the object name in *Axxon One*, the CSV file must be UTF-8 BOM or UTF-32 BOM encoded.

61 https://docs.axxonsoft.com/confluence/display/DDP/En

2. Drag and drop the created file to the form in IP Device Discovery Wizard in *Axxon One*.



> **Note**
>
> If *Axxon One* is running in the safe mode, the CSV file must be dragged-and-dropped to the IP Device Discovery Wizard from the application window, which is running with the administrator rights.

The specified devices will be added to the configuration.

15.2.3 Configuring system objects for devices

15.2.3.1 The Server Object

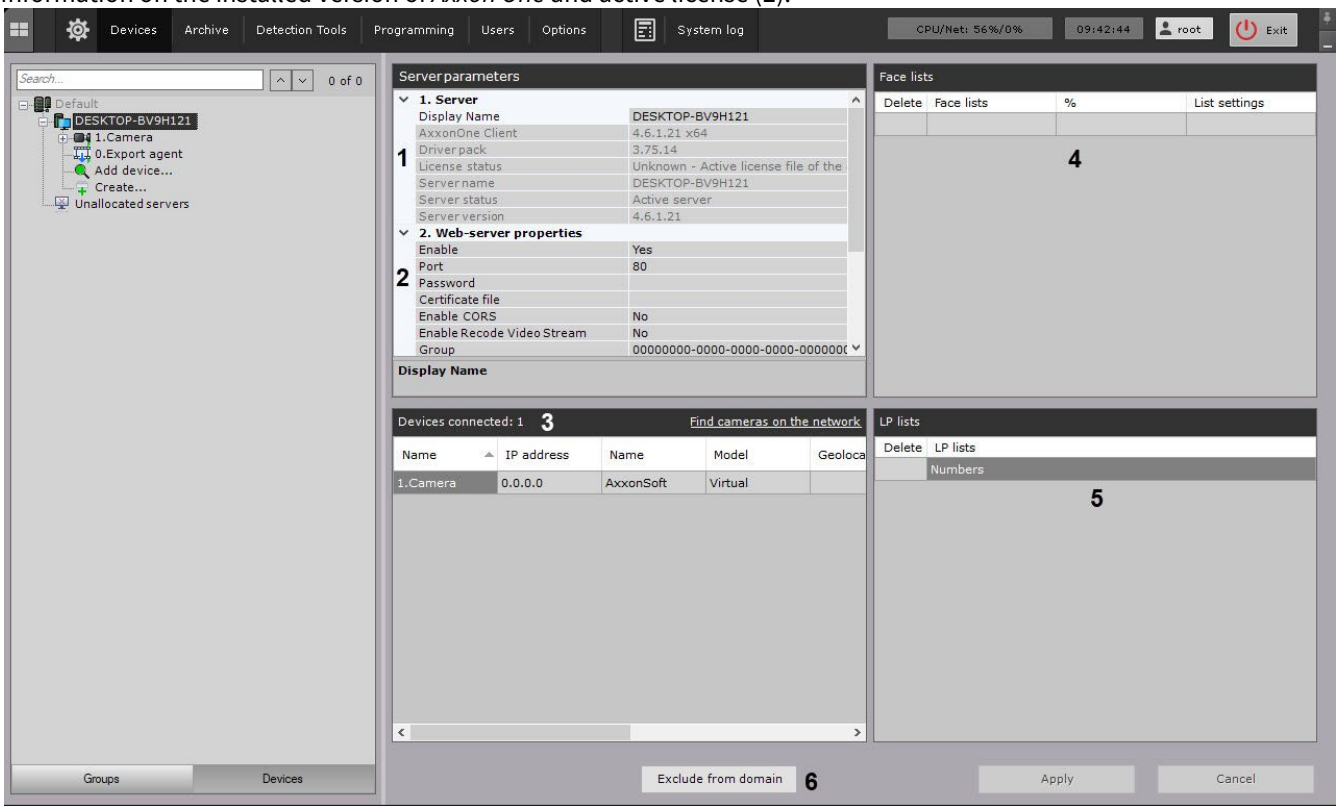
The **Server** object corresponds to a computer:

- 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(see page 119)).
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 Adding and removing IP devices(see page 112)).

> **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 real-time face recognition(see page 301)).
5. Created ANPR lists (**5**, see Configuring real-time vehicle license plate recognition(see page 337))
6. The button to remove Server from an Axxon-domain (**6**, see Removing a Server from an Axxon-domain(see page 110)).

15.2.3.1.1 Configuring the Web-Server

The Web-Server allows accessing *Axxon One* remotely over the Internet (see Working with Axxon One through the Web-Client(see page 823)).

> **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 **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(see page 838)) or change the video codec of the camera to the video codec supported by the browser (see The Camera object(see page 122)).
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.

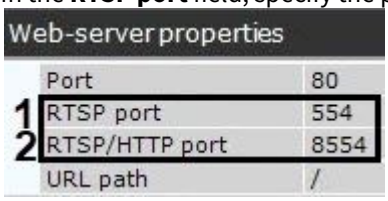
Working with Axxon One through the Web-Client(see page 823)

15.2.3.1.2 Configuring an RTSP Server

Axxon One supports RTSP streaming from cameras (see Get camera live stream[62] and Get archive stream[63]).

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.
- **N** – camera ID in the *Axxon One* VMS.
- **SourceEndpoint.video:0**:0 – permanent section of a link.

62 https://docs.axxonsoft.com/confluence/display/one20en/Get+camera+live+stream
63 https://docs.axxonsoft.com/confluence/display/one20en/Get+archive+stream

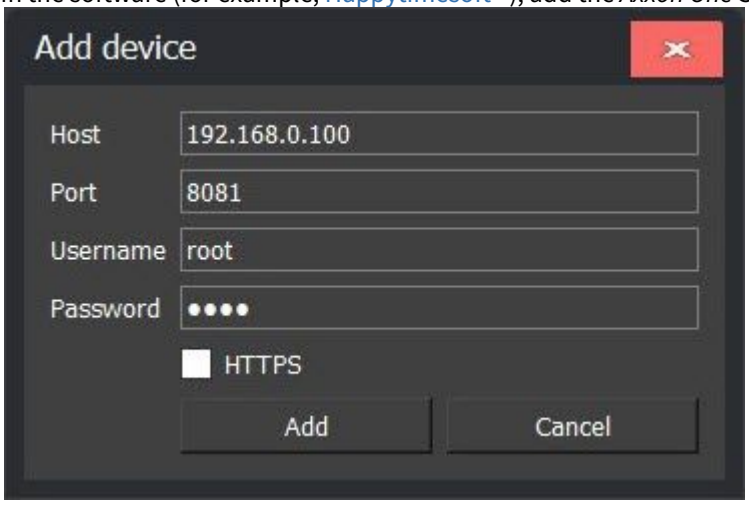
- **speed** – a parameter required for receiving video streams from an Archive.

15.2.3.1.3 Configuring the ONVIF Server

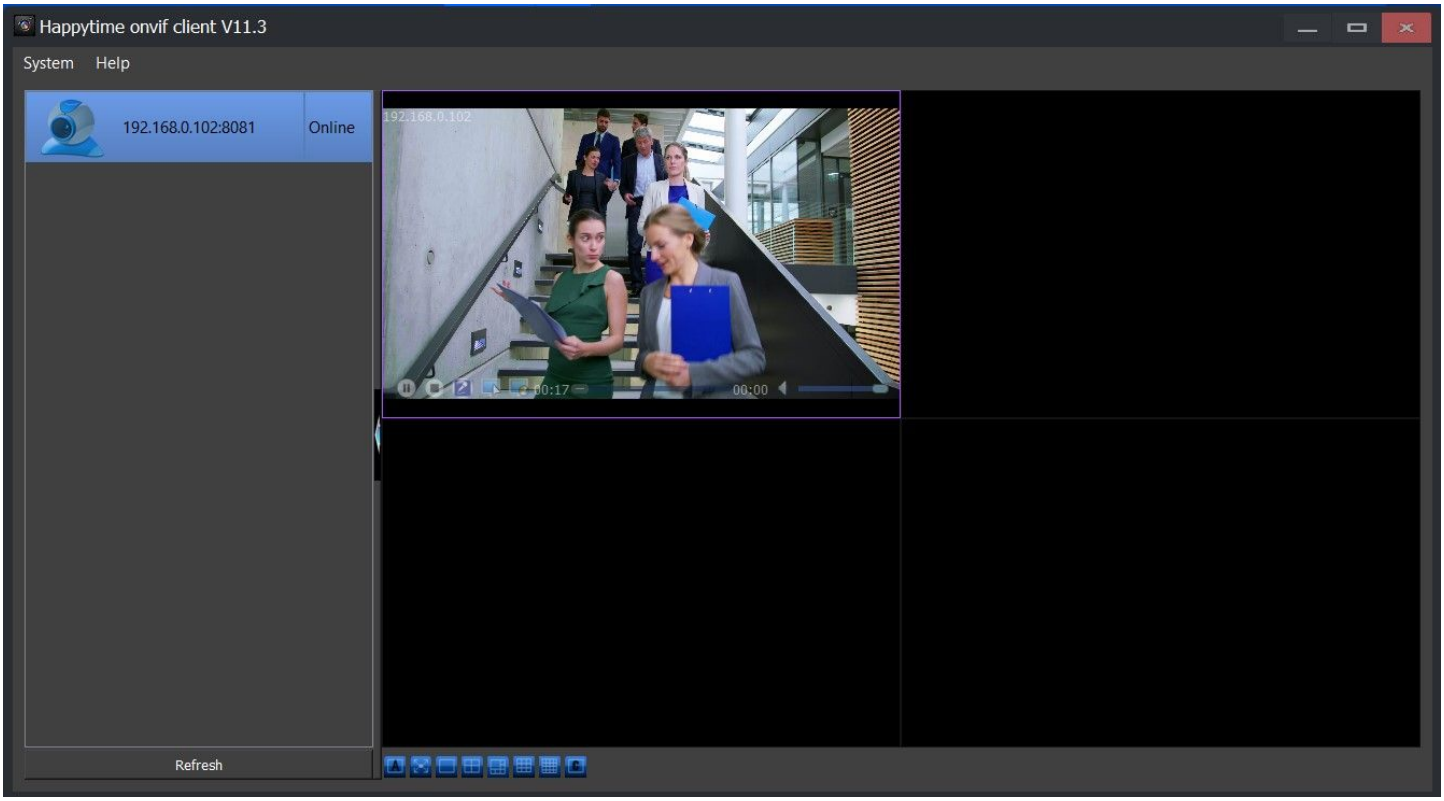
Axxon One has a built-in ONVIF Server using which *Axxon One* can be added as a video recorder to other software (for example, Onvif Device Manager (ODM) or Happytimesoft).

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(see page 100)).
3. Create the NGP_ONVIFSERVER_ENDPOINT system variable (see Appendix 10. Creating system variable(see page 951)). In the **Variable value** field,field, specify the IP address of the local *Axxon One* Server.
4. Start the Server (see Starting a Server(see page 94)).
5. In the software (for example, Happytimesoft[64]), add the *Axxon One* Server as a device using the 8081 port.

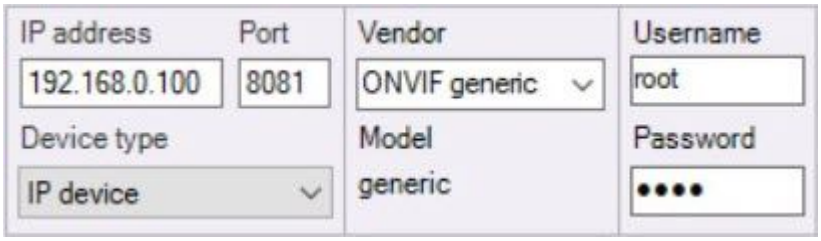


The ONVIF Server configuration is complete. The software will broadcast the video image from *Axxon One* in real time.

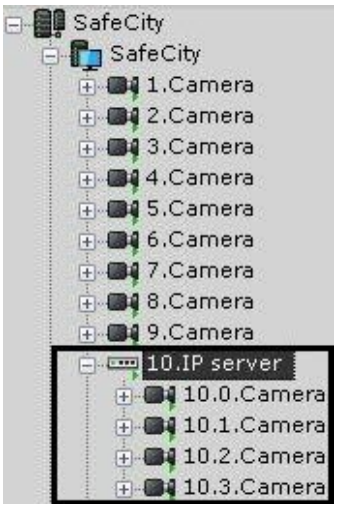


64 https://www.happytimesoft.com/products/onvif-client/index.html

You can also add the ONVIF Server to another *Axxon One* Server as an ONVIF generic IP device (see Adding and removing IP devices(see page 112)).



The ONVIF Server will be added to the configuration as an **IP server** (see The IP Server Object(see page 161)) with corresponding video cameras.



15.2.3.2 The Camera object

On the page:

- Configuring the camera settings(see page 122)
- Configuring video stream settings(see page 125)
- Camera preview window(see page 126)

Creation and configuration of the **Camera** object is done in 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, etc.).

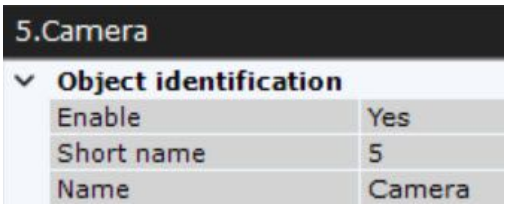
Note

You can configure the camera recording to the archive in the corresponding tab (see Configuring archives(see page 206)).

15.2.3.2.1 Configuring the camera settings

When you have added a camera via the IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)), you can edit the camera's parameters. The camera parameters are grouped as follows.

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



Note

- You can use camera's short name in hotkeys (see Notes regarding hot key actions(see page 579)).
- By default, the short name is a camera's ID. The full name of the video camera in the objects tree is displayed in the <Short name>. <Name> format.
- After changing the short name and restarting the Client, the cameras in the objects tree will be sorted by their short names.

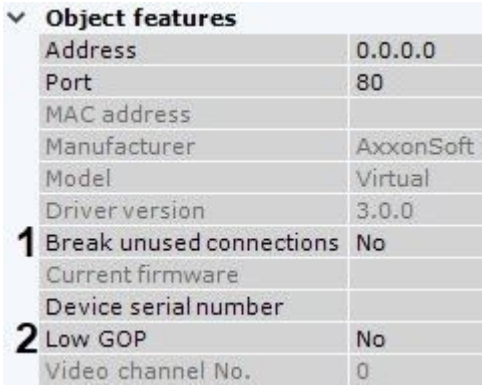
Also, you can disable the camera by selecting **No** in the **Enable** field**.**

Attention!

Every camera enabled in the system (including analog cameras, see The IP Server Object(see page 161)) is a video channel in terms of licensing (see Axxon One licensing(see page 91)). Disabled cameras are not subject to licensing. If you run out of camera licenses, disable offline/unused cameras.

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 the camera and the *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(see page 177)).

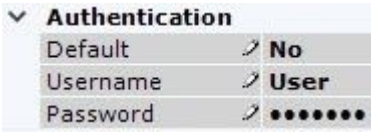


You can also customize a number of options shared by all video cameras in this group:

1. If you want to interrupt video streaming from the camera to the Server whenever it is not needed, select **Yes** for **Break unused connections** (**1**).
   Conditional interruption of video transmission from a camera to the Server, if:
   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.
2. After starting the Client, the default setting is to display video only after the first I-frame (key frame) is received. If the stream comes with a relatively long GOP length (Group of Pictures) or GOV length (Group of Video Object Planes), i.e. the number of P- and B-frames between I-frames in the stream, the video may be not available for a minute. In this case, select **Yes** for the **Low GOP** keyframe rate setting (**2**). This will reduce the waiting time for video by pushing the preceding

I-frame that can be stored in the memory buffer on the Server. In some cases, the I-frame will not be buffered, but in most cases this means that it will soon be received from the device.

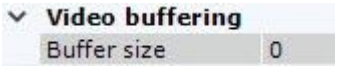
In the **Authentication** group, you can set the username and password to connect to the camera.



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 symbol " **:** " to the last character of the password.

To enable video buffering on Clients, set the buffer length in milliseconds in the **Video buffering** group. This value should be between 50 and 1000 milliseconds. If the value **0** is selected, video buffering is disabled.

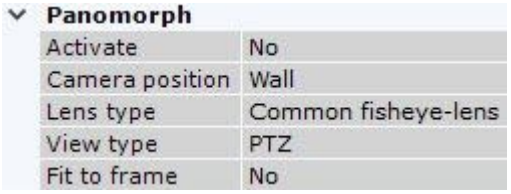


In the **Video stream settings** group, you can see video image parameters (contrast, brightness, color saturation, etc.). When configuring these, you can look up their descriptions in *Axxon One* interface. For more detailed information, please refer to the camera manual.

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 with the parameters that were set in the web interface (see Adding and removing IP devices(see page 112)). To configure these parameters in *Axxon One*, set the **Send settings to device** checkbox.

In the **Panomorph** group, you can configure fisheye cameras (see Configuring fish-eye cameras(see page 127)).



In the **Other** group, you can configure the parameters for the devices connected via the RTSP protocol (see Configuring connection of devices via RTSP(see page 131)).

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

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

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 and changing size of their icons on the map(see page 512)).

Geolocation	
Geo location azimuth	0
Geo location latitude	0
Geo location longitude	0

In a special case, when configuring an alarm layout (see Configuring Alarmed cameras layout(see page 502)), in these fields, you can specify the closest cameras this one for the simultaneous display.

15.2.3.2.2 Configuring video stream settings

You can configure video streams below the Surveillance window. If a camera supports multistreaming, you can configure two video streams separately: **Main stream** and **Second stream**. If necessary, you can configure additional video streams using the **Add video stream** field. When creating an IP device with a main video stream, a stream with a higher resolution is selected. To configure video streams, you should make sure that the **Send settings to device** checkbox is set.

> **Note**
>
> In most cases, the following parameters are set for video streams: bitrate, compression rate, frame rate, and resolution. Detailed information on configurable parameters can be found in the official reference documentation for the camera.

Main stream	0. vstream-virtual
Compression Rate	1
Folder	C:
Frames per second (fps)	25
Resolution	100 x 100
Use for GreenStream	Yes
Video codec	Auto
Second stream	1. vstream-virtual
enabled	Yes
Compression Rate	1
Folder	
Frames per second (fps)	25
Resolution	100 x 100
Use for GreenStream	Yes
Video codec	Auto
Add video stream	

Note

When changing a video stream to a stream that:

- were added as a main or additional stream, the parameters of one stream are replaced by the parameters of the other;
- weren't added as the main or additional stream, the parameters of this video stream are changed to the default parameters.

By default, to use the video stream when displaying in the Auto (GreenStream)/High quality/Low quality modes, the **Yes** value is set in the **Use for GreenStream** field. If you set the **No** value, the stream is excluded from display in Auto (GreenStream)/High quality/Low quality modes (see Selecting video stream quality in a Surveillance window (GreenStream)(see page 690)).

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(see page 777)).

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(see page 444), Starting an external program on Servers(see page 439), Starting an external program on Clients(see page 439)).

Attention!

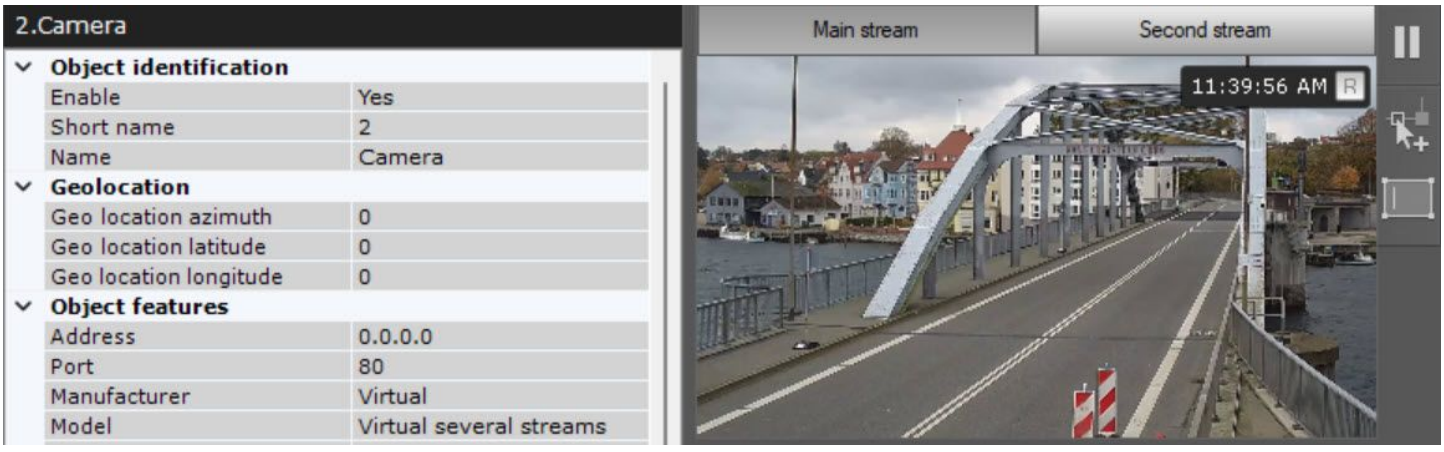
You can select any video stream for recording into archive and displaying in the Surveillance window (see Selecting video stream quality in a Surveillance window (GreenStream)(see page 690), Configuring recording to an archive(see page 224)).

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).

15.2.3.2.3 Camera preview window

Image from the camera will be displayed in the preview window.



Note

The indicator in the upper right corner displays the current time and recording status (see Time Display(see page 631)).

To switch between streams in the preview window, click the **Main stream** and **Second stream** tabs.

Note

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.

15.2.3.2.4 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.

15.2.3.2.5 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.

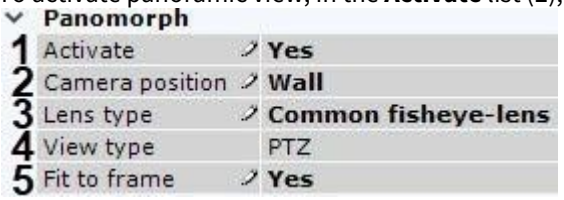
Note

The number in brackets refers to the number of configured cameras.

15.2.3.2.6 Configuring fish-eye cameras

If you are using a fish-eye 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.

> **Important!**
>
> 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 fish-eye 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 fish-eye-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 fish-eye 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**)**.**

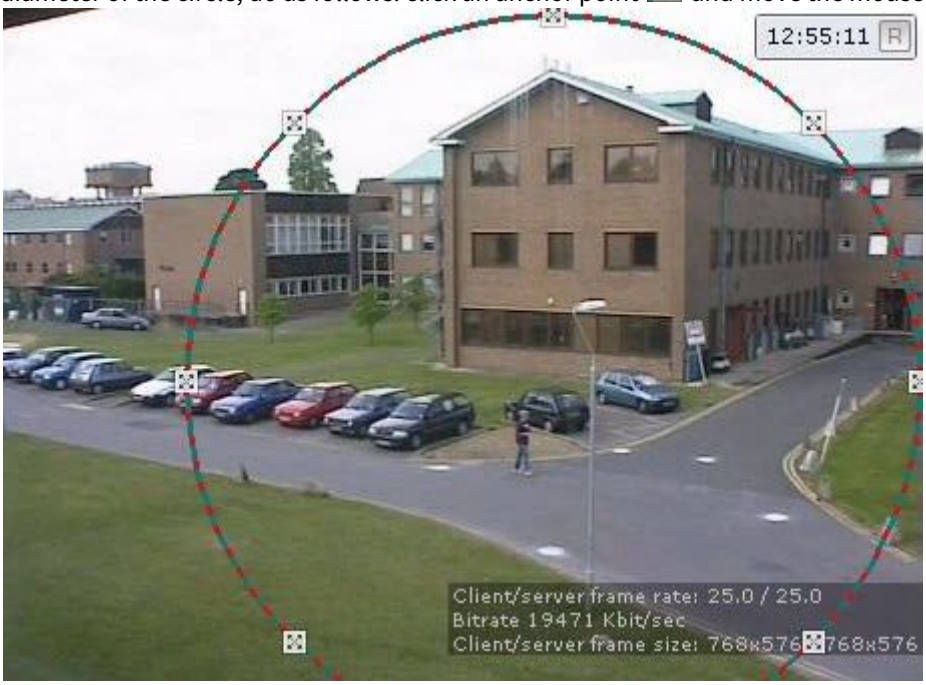
> **Important!**
>
> If you have multiple streams from a camera, you need to calibrate each stream. To do this, before applying the settings, switch to the required stream tab in the viewing tile (see The Camera object(see page 122)).

> **Important!**
>
> 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 fish-eye camera is complete.

15.2.3.2.7 Connecting and configuring cameras over standard protocols

15.2.3.2.7.1 Notes on configuring video cameras connected via ONVIF

On page:

- Connection through ONVIF Generic driver(see page 129)
- Resolution(see page 130)
- IP devices on other subnets (behind a NAT)(see page 130)
- IP devices which partially support the ONVIF protocol(see page 130)

By default, all ONVIF devices in the system are added as multistreaming (the **ONVIF 2.0** driver, see Adding and removing IP devices(see page 112)).

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

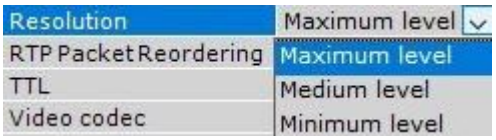
With the ONVIF Generic driver, you have the following options:

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)(see page 134)).
   b. When the device comes online, reset its parameters (see Applying and resetting settings(see page 104)).
   c. Load the configuration from the device (see Applying and resetting settings(see page 104)).
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)(see page 134)).
   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(see page 122)).
   d. Reset device settings (see Applying and resetting settings(see page 104)).
   e. Load the configuration from the device (see Applying and resetting settings(see page 104)).

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.



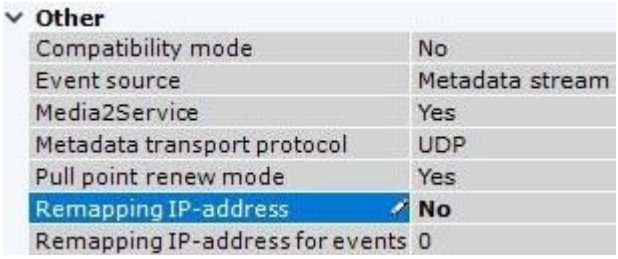
A description of the resolution levels is given in the table.

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[65]-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.

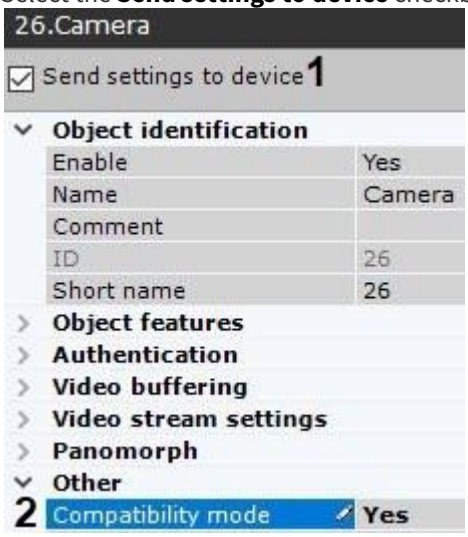
> **Note**
>
> Such video cameras include Hikvision models and early versions of firmware from Sony, Samsung, and others.

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.

65 https://en.wikipedia.org/wiki/NAT

To enable it you need:

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



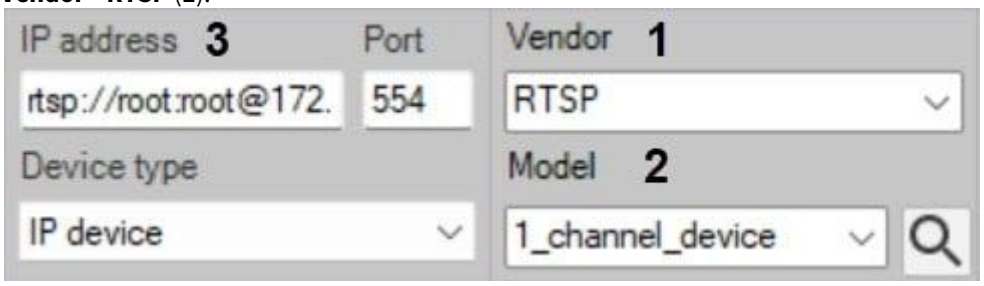
2. Select **Yes** for **Compatibility mode** (**2**).

15.2.3.2.7.2 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 Adding and removing IP devices(see page 112)), add a camera with the following parameters:

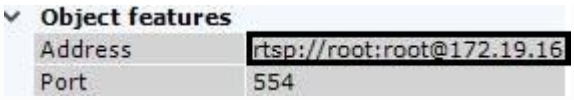
1. **Vendor**—**RTSP** (**1**).



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/...

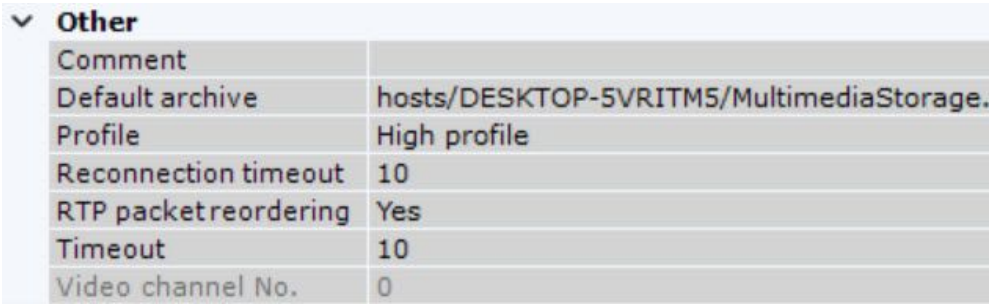
The **Camera** object will be created. If the address of the RTSP transmission is correctly specified, the preview window will display the image from this camera.

> **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 Logging levels(see page 872)). 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.

Main stream	0. video_streaming_rtsp
Authorization token	
Frames per second (fps)	25
Message for keepAliveCommand property	OPTIONS
Proxy URL for RTSP tunneled over HTTP	
Range header for RTSP PLAY	npt=now-
Resolution	Auto
RTSP range value	
Scale header for RTSP PLAY	
SSRC identifier checking	Yes
Transport protocol	Tunneling RTSP over HTTP
Use for GreenStream	Yes
Video codec	Auto

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.

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 Adding and removing IP devices(see page 112)).
2. In **IP address**, enter the device address (**1**).

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

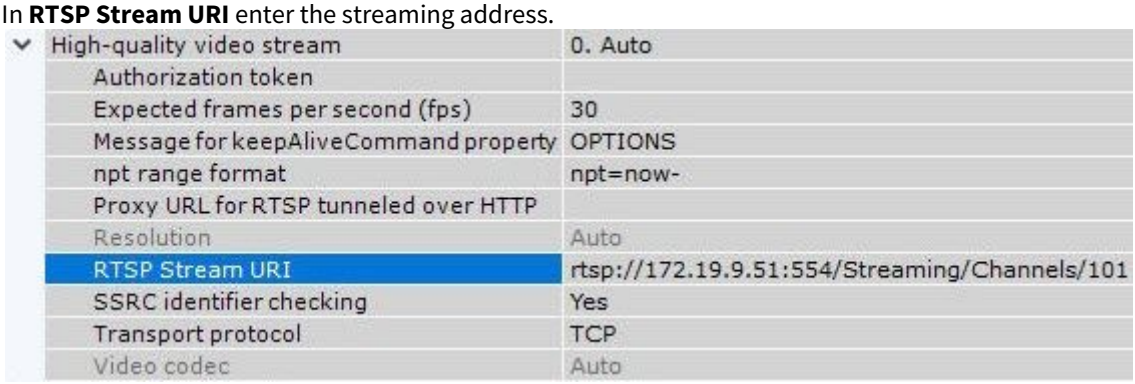
3. Select **RTSP** in the **Vendor** field (**2**).
4. In **Model**, select the model name, that shows the corresponding number of device channels (**3**). For example, for a four-channel device, select **4_channel_device**.
5. Enter the username (**4**) and password (**5**).
6. Click .

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.

15.2.3.2.7.3 Generic Drivers (General device, generic)

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

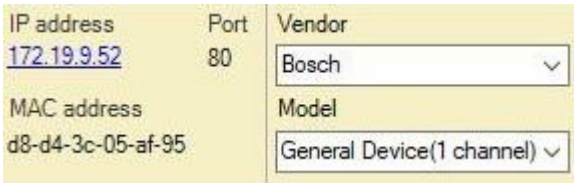
There are 2 types of generic drivers:

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[66] 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 Adding and removing IP devices(see page 112)).

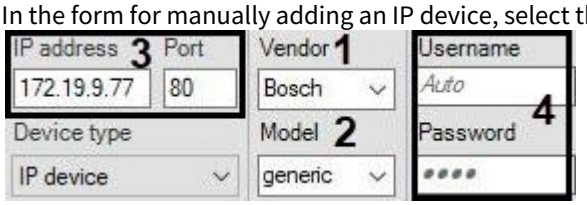


> **Note**
>
> Axis devices are affected by a special restriction: if the user name and password for device access do not equal the default values, the number of channels for the device is not discoverable. Therefore, all non-integrated devices whose user name and password for device access do not equal 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**).



66 https://docs.axxonsoft.com/confluence/display/DDP/Documentation+Drivers+Pack

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.

15.2.3.2.7.4 Connecting cameras via the GB/T28181 protocol

On the page:

- General information on GB/T28181 standard and supported functions(see page 135)
- Configuring an IP-device to operate via GB/T28181 standard(see page 136)
- Configuring IP-device connection via GB/T28181(see page 136)

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[67].

67 https://docs.axxonsoft.com/confluence/display/DDP/En

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(see page 137)

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 Adding and removing IP devices(see page 112)).
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(see page 138)
- Bosch(see page 140)
- Huawei(see page 141)
- Hikvision(see page 142)
  - GB/T28181-2011(see page 144)
  - GB/T28181-2016(see page 146)
- Dahua(see page 148)

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.

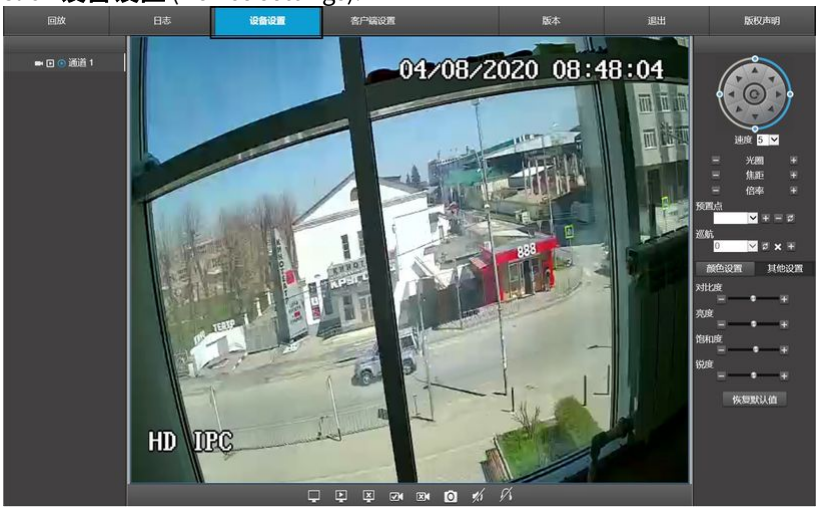
Jovision

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.

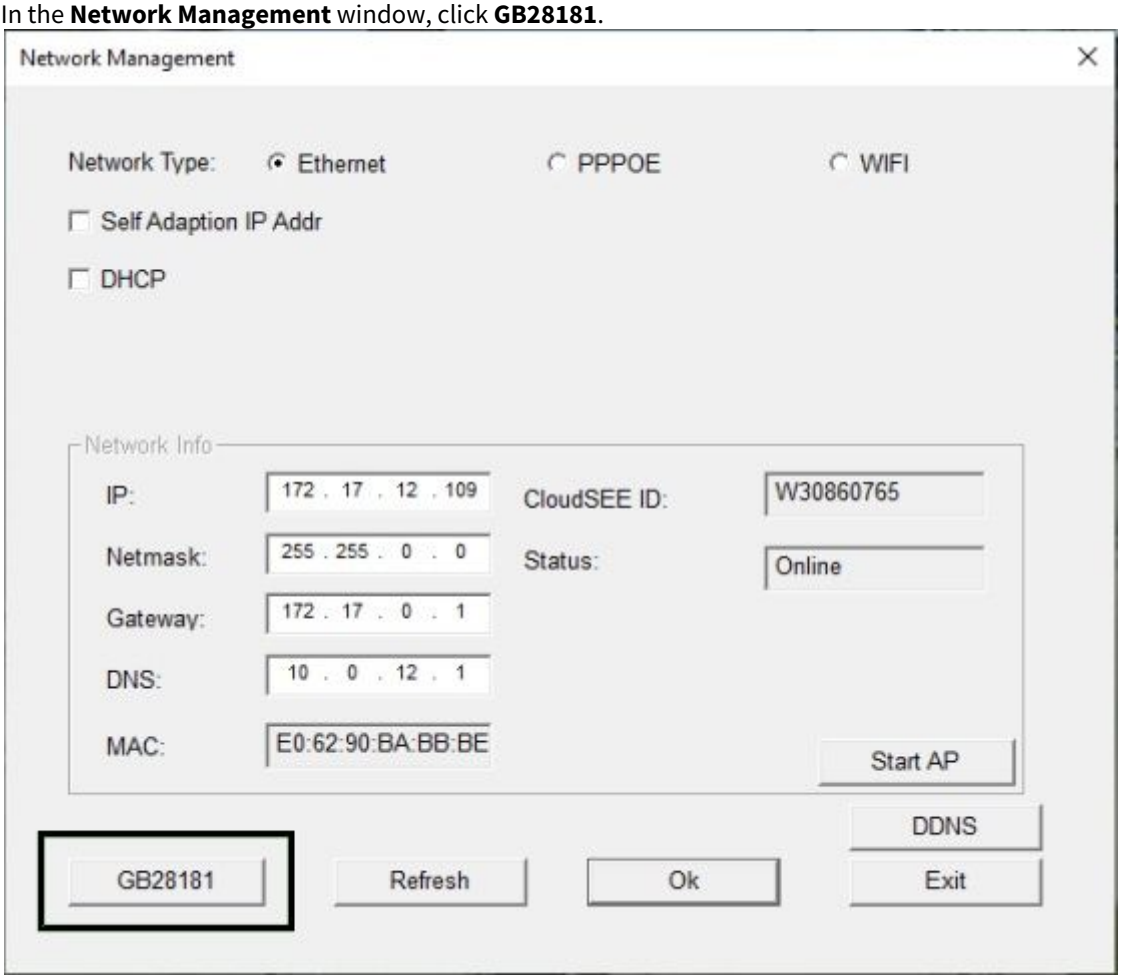
   c. Click **确定** (Confirm) in the dialog box opened.

   d. Click **设备设置** (Device settings).

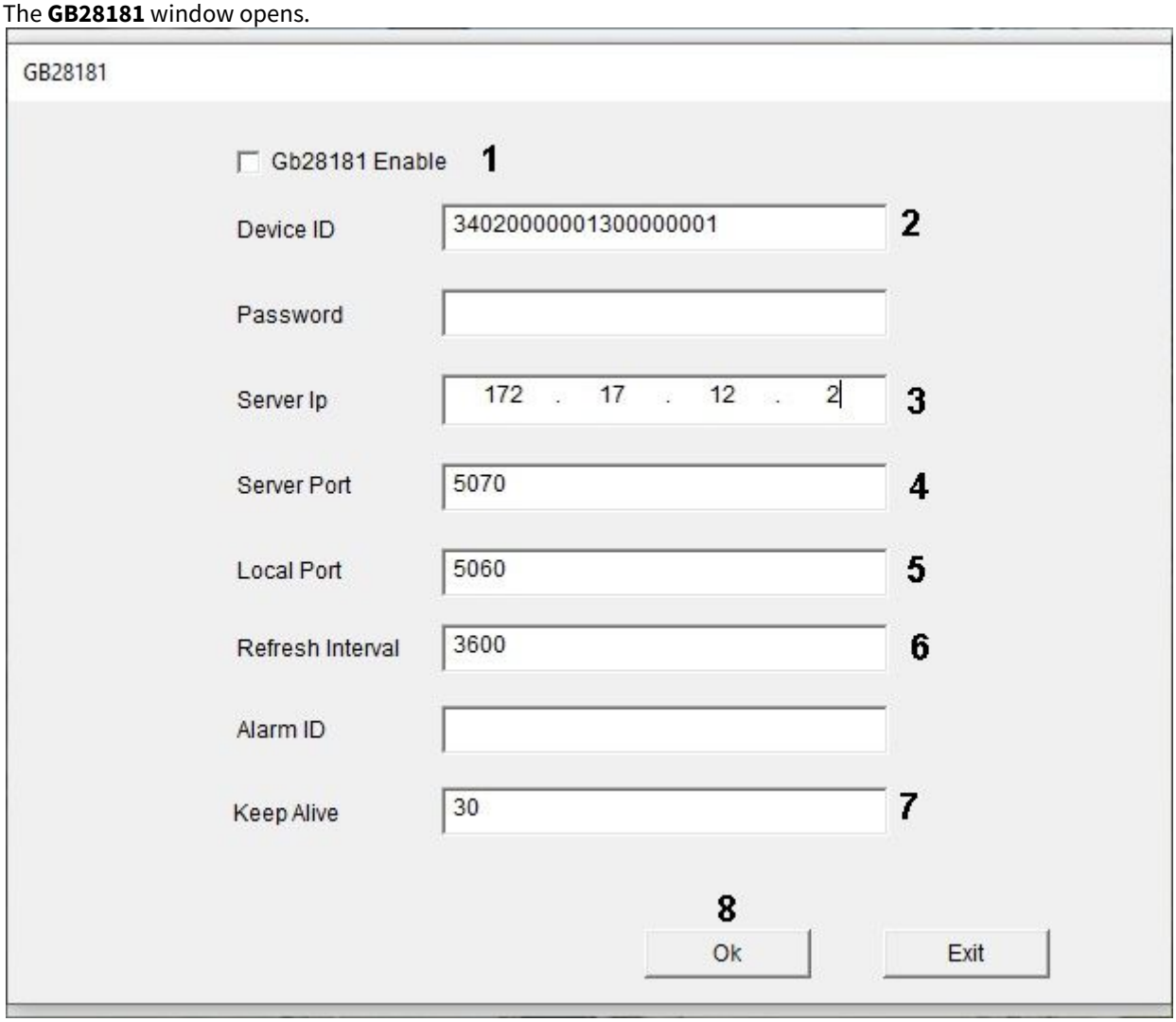


e. Select **Network** in the dialog box.

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(see page 135) (**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**).

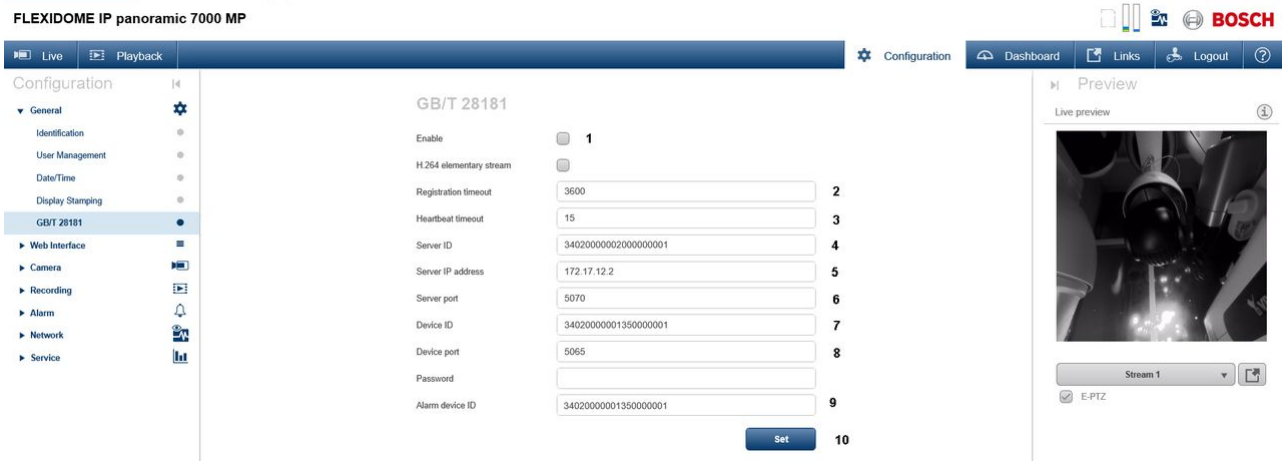
2. In *Axxon One*:
   a. Example value for the **IP address** field: 34020000001300000001@34020000001300000002-10.0.40.246/179.17.12.2 The Server ID 34020000001300000002 is not set on the Jovision device, so any Server ID can be chosen as per the conditions set in Connecting cameras via the GB/T28181 protocol(see page 135).
   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**.



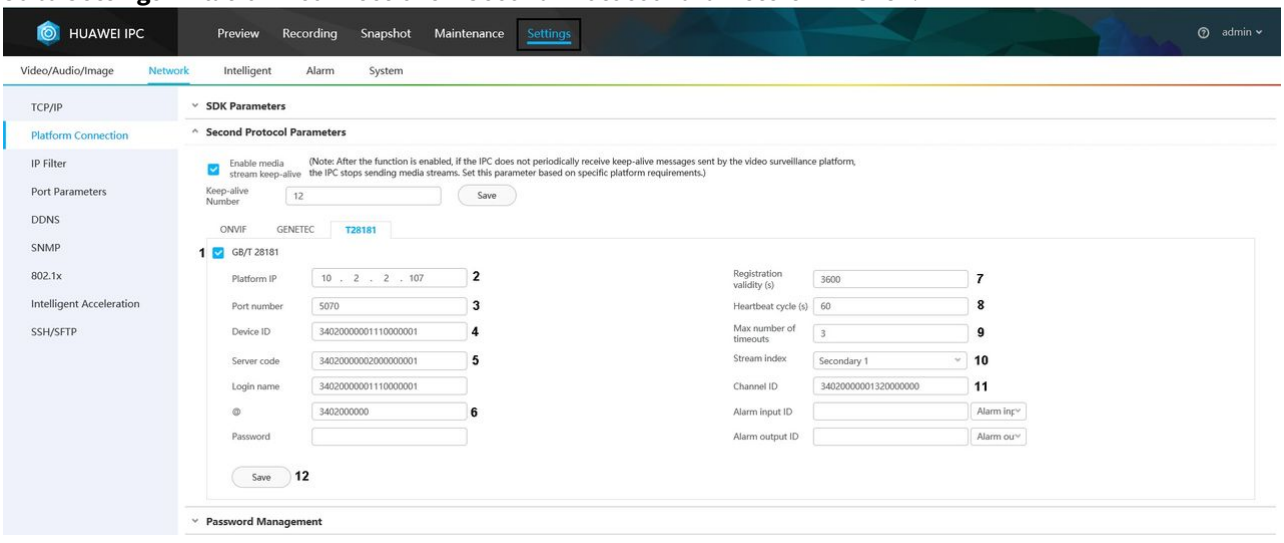
c. Set the **Enable** checkbox checked (**1**).
d. In the **Registration timeout** field, enter the devise discovery period in seconds (**2**). The value shall not be less than 600.
e. In the **Heartbeat timeout** field, enter the period in seconds for sending messages confirming the device activity (**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(see page 135) (**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(see page 135) (**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 **配置 - 视音频 - 视频** (Settings **–** Video and Audio **–** Video).
2. Configure the main stream:

a. From the **码流类型** (Stream type) drop-down list, select **主码流 (定时)** (Main stream) (**1**).

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

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

3. Configure the second stream:

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

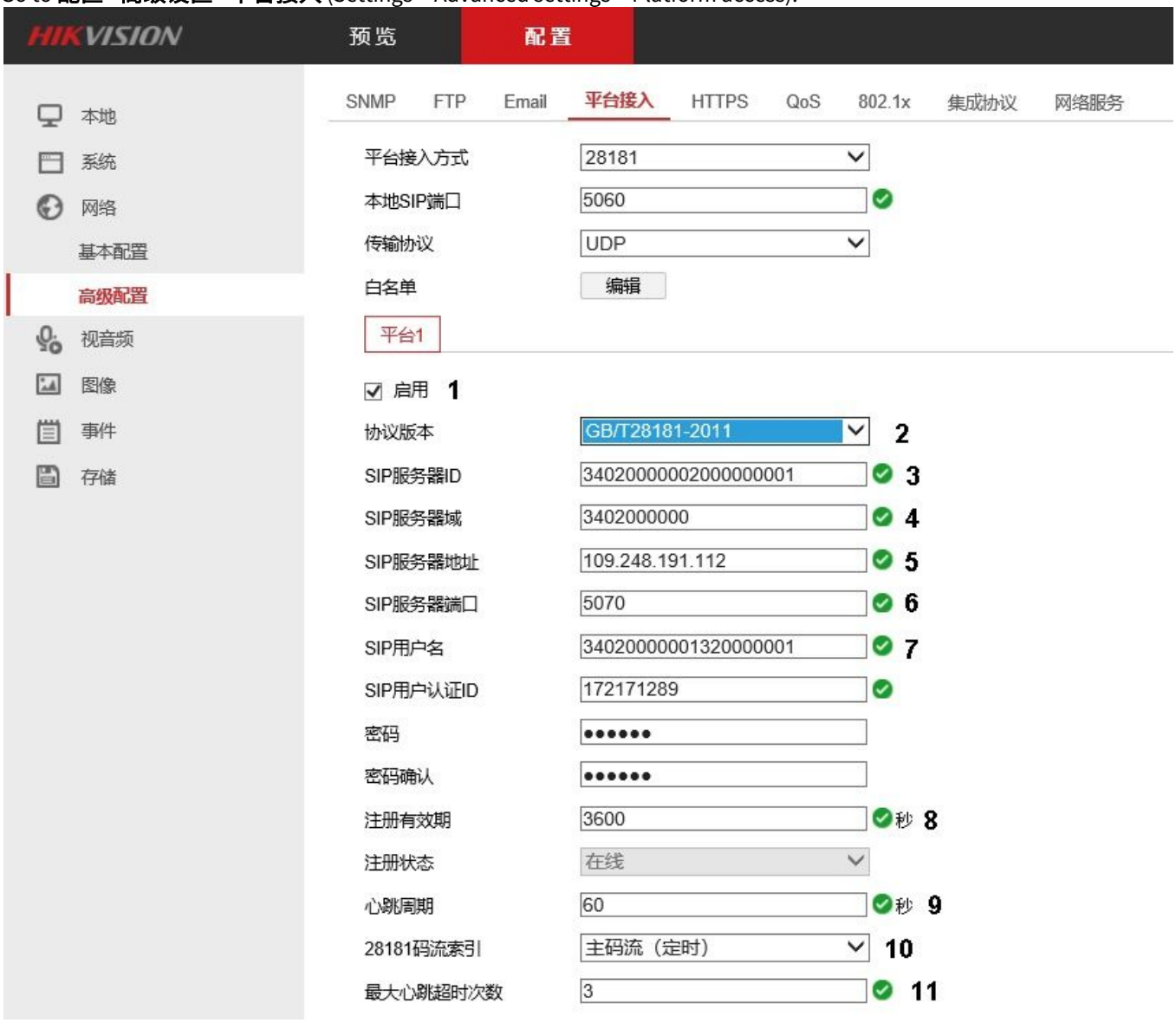
b. From the **分辨率** (Resolution) drop-down list, select the second stream resolution (**2**).

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

4. Click **保存** (Save).

GB/T28181-2011

1. Go to **配置 - 高级设置 - 平台接入** (Settings – Advanced settings – Platform access).



2. Set the **启用** (Enable) checkbox (**1**).
3. From the **协议版本** (Protocol version) drop-down list, select **GB/T28181-2011** (**2**).
4. In the **SIP服务器ID** (SIP Server ID) field, enter the *Axxon One* Server ID (**3**). The example shows Server ID 34020000002000000001.
5. In the **SIP服务器域** (SIP Server domain) field, enter first 10 digits of the address according to GB/T-2260-2007 (**4**).
6. In the **SIP服务器地址** (SIP Server address) field, enter the *Axxon One* server IP-address (**5**). The example shows IP 109.248.191.112.
7. In the **SIP服务器端口** (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用户名** (SIP user name) field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol(see page 135) (**7**). Example on the picture shows Device ID 34020000001320000001.
9. In the **注册有效期** (Registration period) field, enter the devise discovery period in seconds (**8**). The value shall not be less than 600.
10. In the **心跳周期** (Heartbeat period) field, enter the period in seconds for sending messages confirming the device activity (**9**).
11. From the **28181码流索引** (Video stream) drop-down list, select one of the streams configured earlier (**主码流 (定时)** for Main stream or **子码流** for Second stream) (**10**).
12. In the **最大心跳超时次数** (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 **视频通道编码ID** (Video channel ID) tab at the bottom of the setings page (**1**).

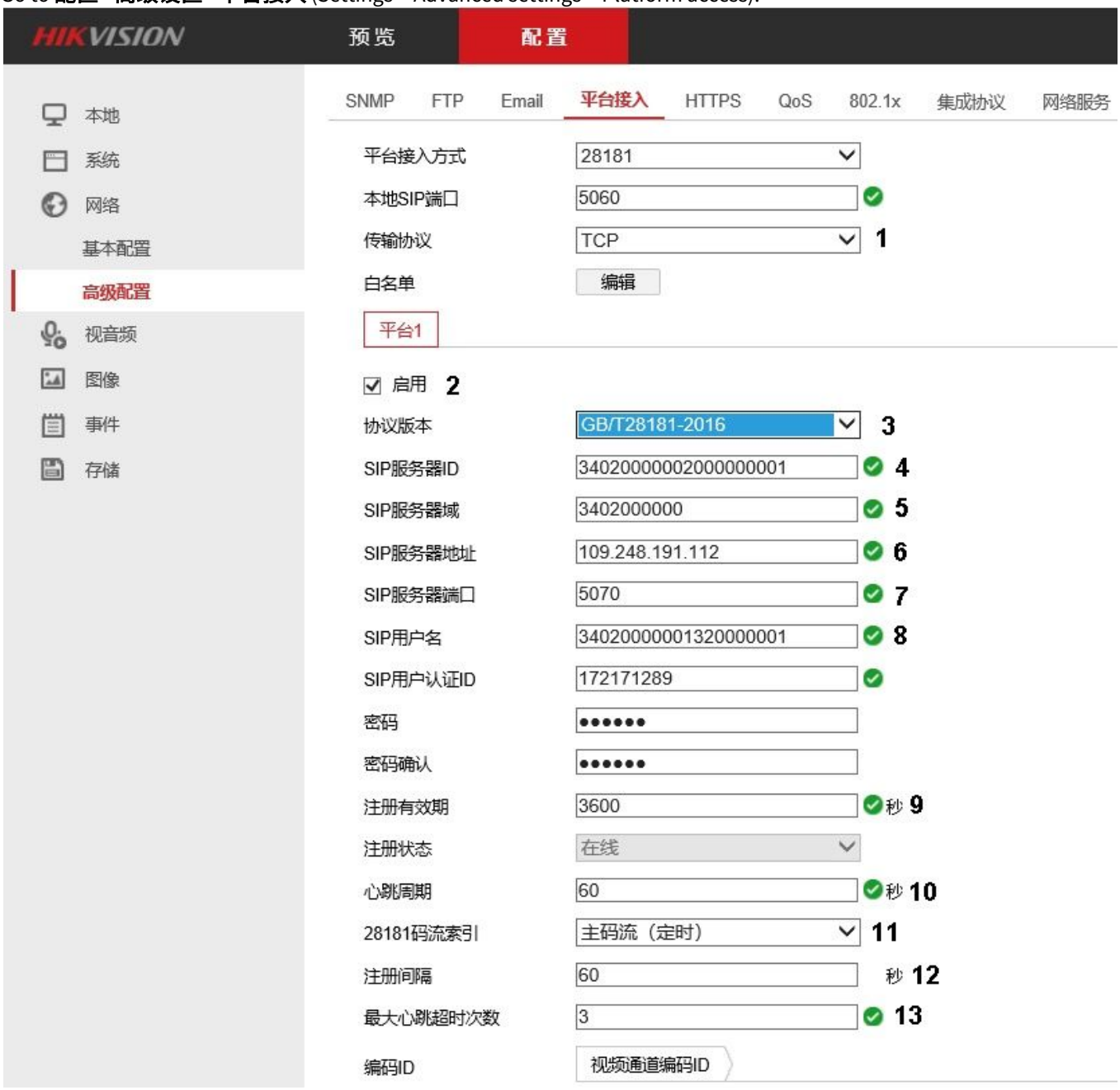
14. Enter the identifiers of all channels of the IP device in the same format as the device identifiers (**2**). The example shows ID 34020000001320000002.
15. Click the **保存** (Save) button (**3**).

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 **配置 - 高级设置 - 平台接入** (Settings – Advanced settings – Platform access).



2. From the **传输协议** (Transport protocol) drop-down list, select the transport level protocol to be in use: UDP or TCP (**1**).
3. Set the **启用** (Enable) checkbox (**2**).
4. From the **协议版本** (Protocol version) drop-down list, select **GB/T28181-2016** (**3**).
5. In the **SIP服务器ID** (SIP Server ID) field, enter the *Axxon One* Server ID (**4**). The example shows Server ID 34020000002000000001.
6. In the **SIP服务器域** (SIP Server domain) field, enter first 10 digits of the address according to GB/T-2260-2007 (**5**).
7. In the **SIP服务器地址** (SIP Server address) field, enter the *Axxon One* server IP-address (**6**). The example shows IP 109.248.191.112.
8. In the **SIP服务器端口** (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用户名** (SIP user name) field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol(see page 135) (**8**). Example on the picture shows Device ID 34020000001320000001.
10. In the **注册有效期** (Registration period) field, enter the devise discovery period in seconds (**9**). The value shall not be less than 600.
11. In the **心跳周期** (Heartbeat period) field, enter the period in seconds for sending messages confirming the device activity (**10**).

12. From the **28181码流索引** (Video stream) drop-down list, select one of the streams configured earlier (**主码流 (定时)** for Main stream or **子码流** for Second stream) (**11**).
13. In the **注册间隔** (Registration interval) field, enter the device discovery interval in seconds (**12**).
14. In the **最大心跳超时次数** (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 **视频通道编码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 **保存** (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 **网络设置** - **平台接入 - 国标28181** (Network settings – Platform access – GBT28181).

   c. Set the **接入使能** (Enable connection) checkbox (**1**).
   d. In the **SIP服务器编号** (SIP server number) enter the *Axxon One* Server ID (**2**). The example shows Server ID 34020000002000000001.
   e. In the **SIP服务器IP** (SIP server IP address) enter the *Axxon One* server IP address (**3**). The example shows IP 192.168.88.33
   f. In the **设备编号** (Device number) field, enter the device identification number as described in Connecting cameras via the GB/T28181 protocol(see page 135) (**4**). Example on the picture shows Device ID 34020000001300000001.
   g. In the **本地SIP服务器端口** (Local SIP port) field, enter the IP device SIP port number (**5**).

h. In the **心跳周期** (Heartbeat period) field, enter the period in seconds for sending messages confirming the device activity (**6**).
i. In the **SIP服务器端口** (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 **注册有效期** (Registration period) field, enter the devise discovery period in seconds (**8**). The value shall not be less than 600.
k. In the **最大心跳超时次数** (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 **刷新** (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.

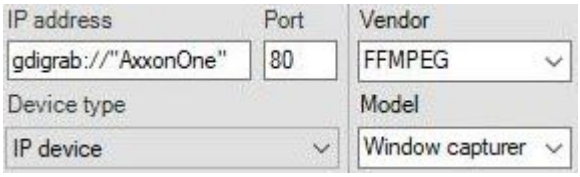
Receiving video from the application window on the Server with the FFmpeg driver

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

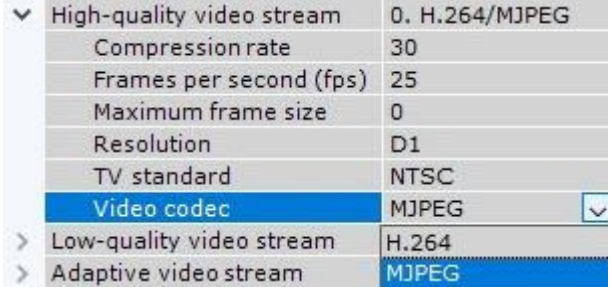
```
gdigrab://"Window title"
```

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.



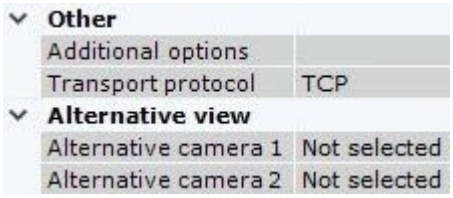
By default, videos are transmitted in MJPEG format. YUV422[68], H.264 and MPEG4 formats are also available.



68 https://ru.wikipedia.org/wiki/YUV

> **Note**
>
> The YUV422[69] 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:

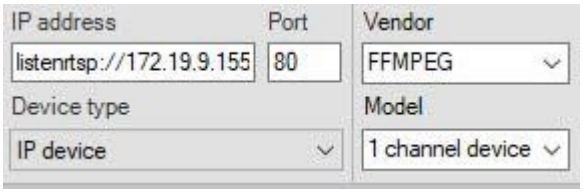
1. On the Server:
   a. Open the port for receiving data from the remote Client.

   > **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>
   ```

69 https://en.wikipedia.org/wiki/YUV



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[70].
   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.

70 https://www.ffmpeg.org/download.html

- 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.

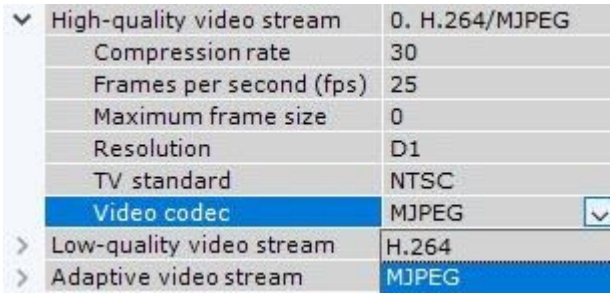
Receiving video from the Server monitor with the FFmpeg driver

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(see page 150)), or install Axxon One's Server services on your Client (see Installation(see page 62)).

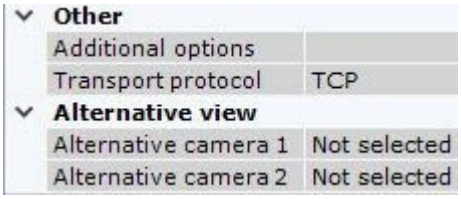
By default, videos are transmitted from all Server monitors in MJPEG format. YUV422[71] and H.264 format is also available.



71 https://en.wikipedia.org/wiki/YUV

> **Note**
>
> The YUV422[72] 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:

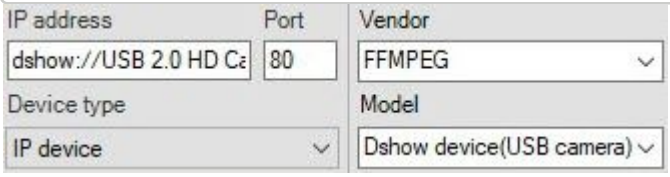
```
-draw_mouse 1 -show_region 1 -framerate 25 -video_size 640x480 -offset_x 10 -offset_y
10
```

Receiving audio and video from connected USB devices

If a device is added automatically (see Adding and removing IP devices(see page 112)), 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:

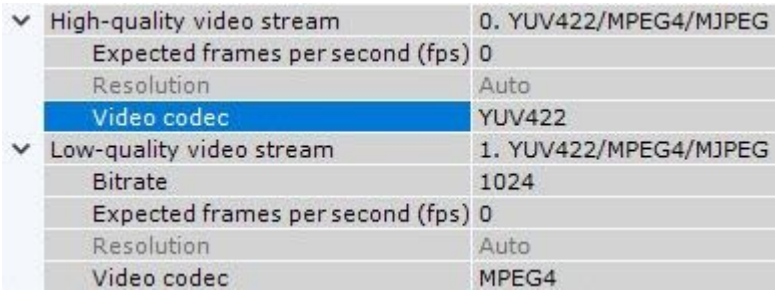
72 https://en.wikipedia.org/wiki/YUV

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

Note

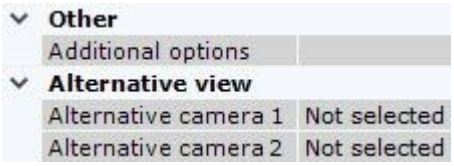
If a video or audio device is not present, it may be not specified in the address.

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.



High-quality video stream	0. YUV422/MPEG4/MJPEG
Expected frames per second (fps)	0
Resolution	Auto
Video codec	YUV422
Low-quality video stream	1. YUV422/MPEG4/MJPEG
Bitrate	1024
Expected frames per second (fps)	0
Resolution	Auto
Video codec	MPEG4

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



Other	
Additional options	
Alternative view	
Alternative camera 1	Not selected
Alternative camera 2	Not selected

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

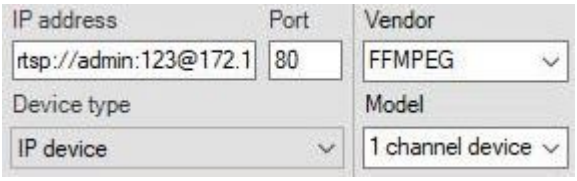
Attention!

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]
```



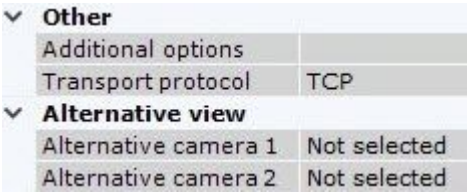
Note

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[73].

15.2.3.2.8 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.

15.2.3.2.9 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 Specifications of the Axxon One software package(see page 45)).

Note

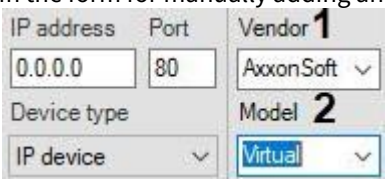
Do not use video with B-frames[74].

To create and configure a virtual video camera, complete the following steps:

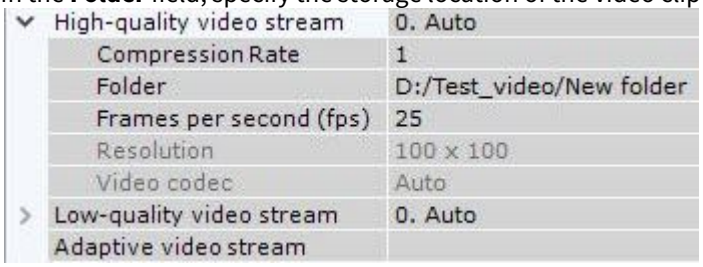
1. Run IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)).

73 https://ffmpeg.org/ffmpeg-protocols.html#rtsp
74 https://en.wikipedia.org/wiki/Video_compression_picture_types#Macroblocks

2. In the form for manually adding an IP device, select **AxxonSoft** in the **Vendor** drop-down list (**1**).



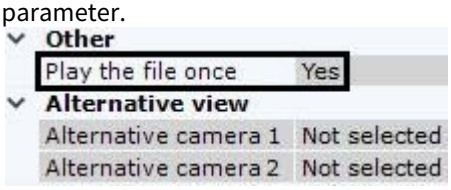
3. Select **Virtual** from the models list to emulate a single-stream video camera. Select **Virtual several streams** to emulate a video camera supporting multiple streams (**2**).
4. Click the button.
5. In the **Folder** field, specify the storage location of the video clip that will be used to imitate a video signal.



> **Note**
>
> The name of the video file and its file path must consist only of Latin characters.

> **Note**
>
> 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 corresponding parameter.



7. Click the **Apply** button.

15.2.3.2.10 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 Face detection(see page 280);
- Configuring Face detection (VL)(see page 285);
- Configuring Face Detection and Temperature Control(see page 298);
- Configuring Masks Detection(see page 291) (detection of a medical or similar mask on the face);
- Person-based privacy masking configuration(see page 367);
- Specific settings for People masking detection tool(see page 382) (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(see page 452)).

> **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.

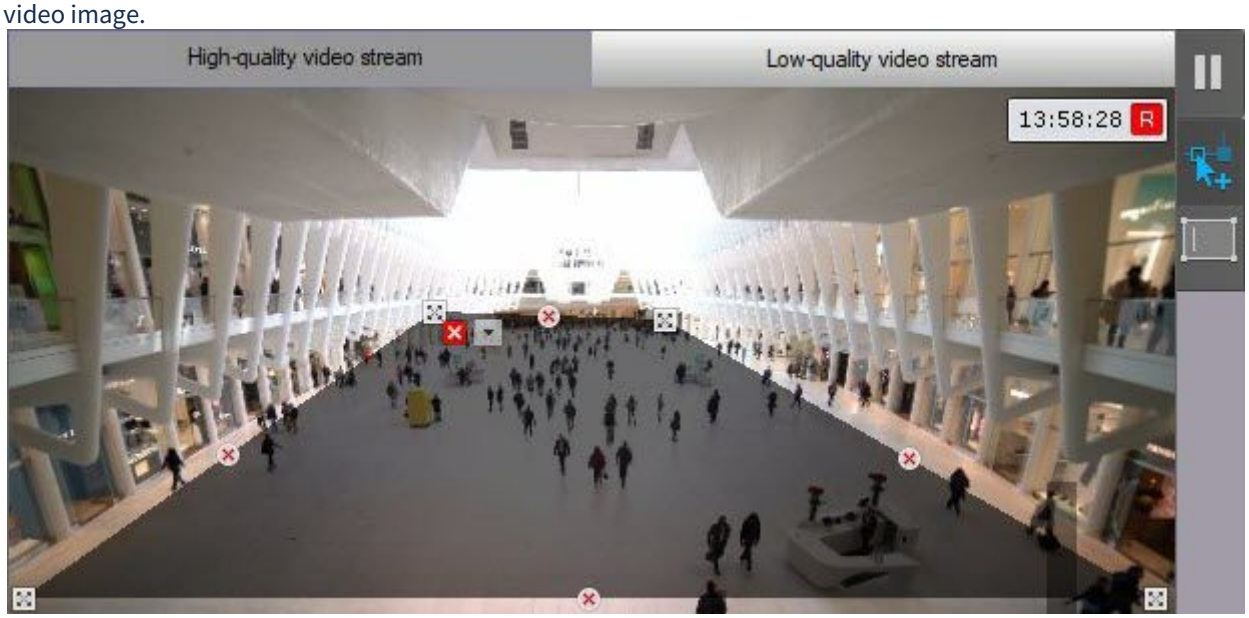
To configure privacy mask, do the following:

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(see page 159)).

> **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.

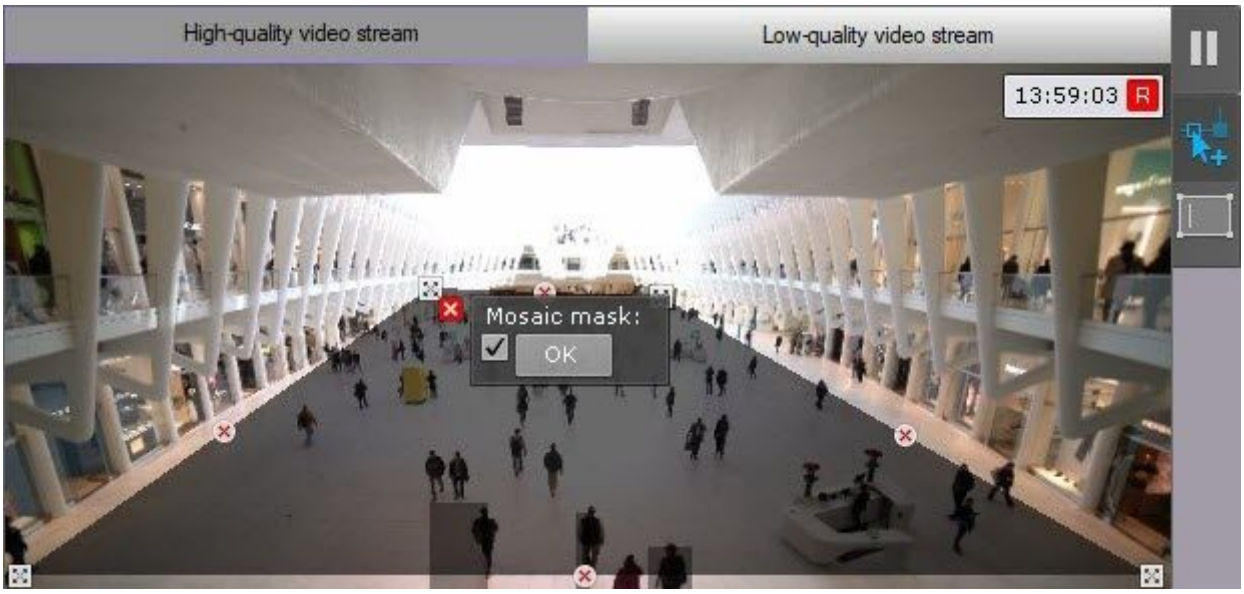


> **Note**
>
> When the area is being constructed, the anchor points are connected by a two-color dotted line which outlines the area's borders.

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

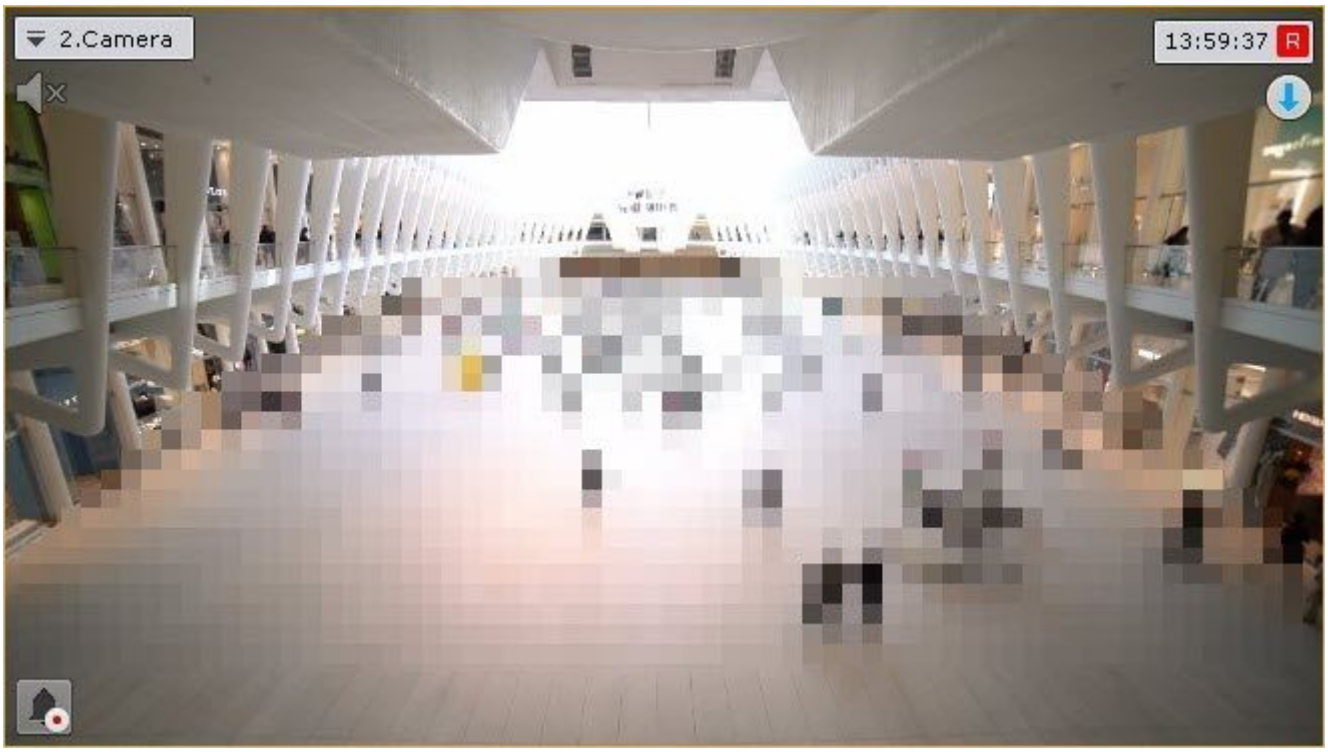
Click the button	Delete the area

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.



15.2.3.2.11 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(see page 157)).

   Note

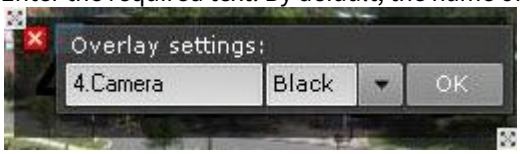
   For your convenience, you can click the button and configure the mask on a still frame/snapshot. To undo, click this button again.

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.

15.2.3.3 The IP Server Object

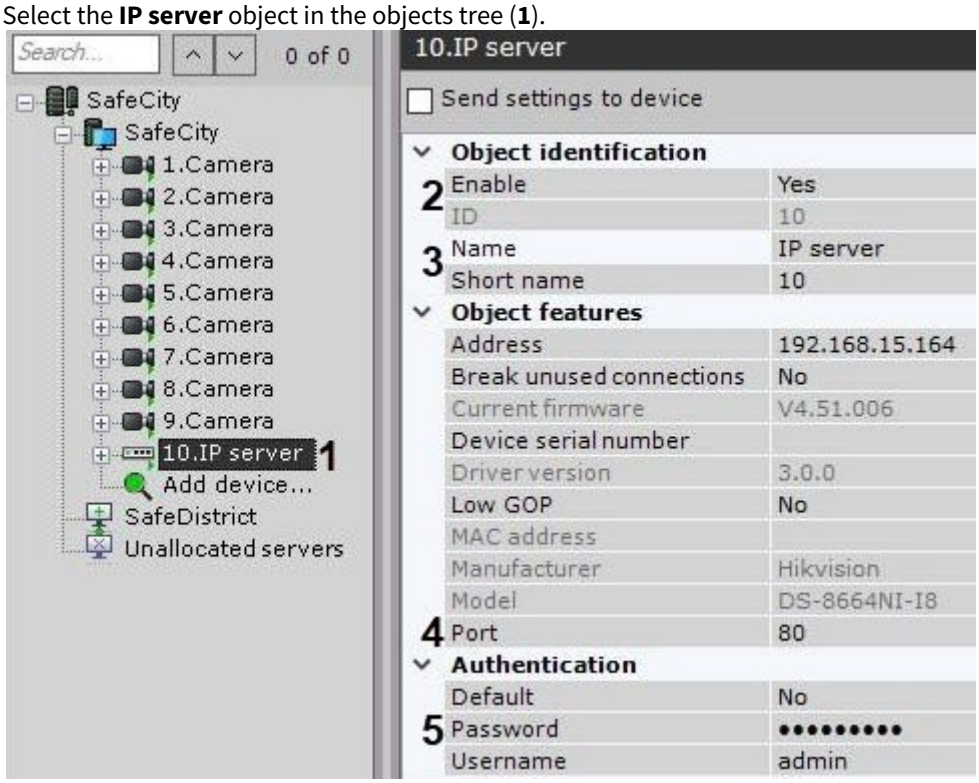
In the *Axxon One* VMS, an **IP Server** object relates to:

- 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**.

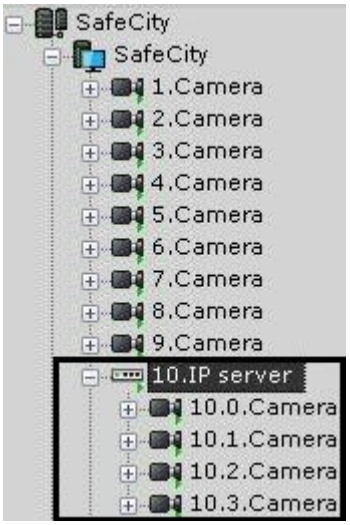
> **Note**
>
> The port number is initially set through the IP server's Web interface.

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**).

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.

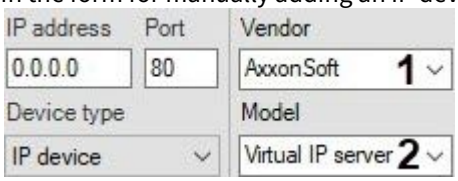
15.2.3.3.1 Configuring Virtual IP Servers

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 Adding and removing IP devices(see page 112)).

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(see page 156)).

15.2.3.4 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.

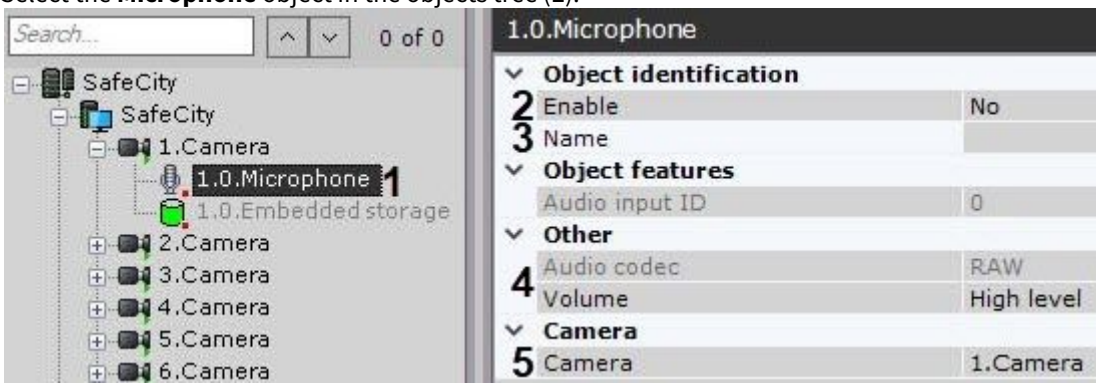
> **Atteintion**
>
> When a microphone is reassigned from one camera to another, all previously recorded audio is also transferred; when recorded video on the new camera is played, the transferred audio is played back.

> **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(see page 793)).

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**).

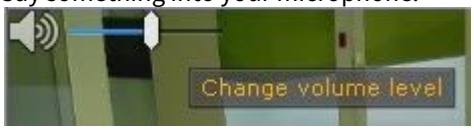


2. Enable the microphone by selecting **Yes** in the **Enable** field (**2**).
3. Enter the name of the microphone in the **Name** field (**3**).
4. Configure additional microphone parameters (audio codec, bit rate, etc.) in the **Other** group (**4**) using their descriptions in the interface of the *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.

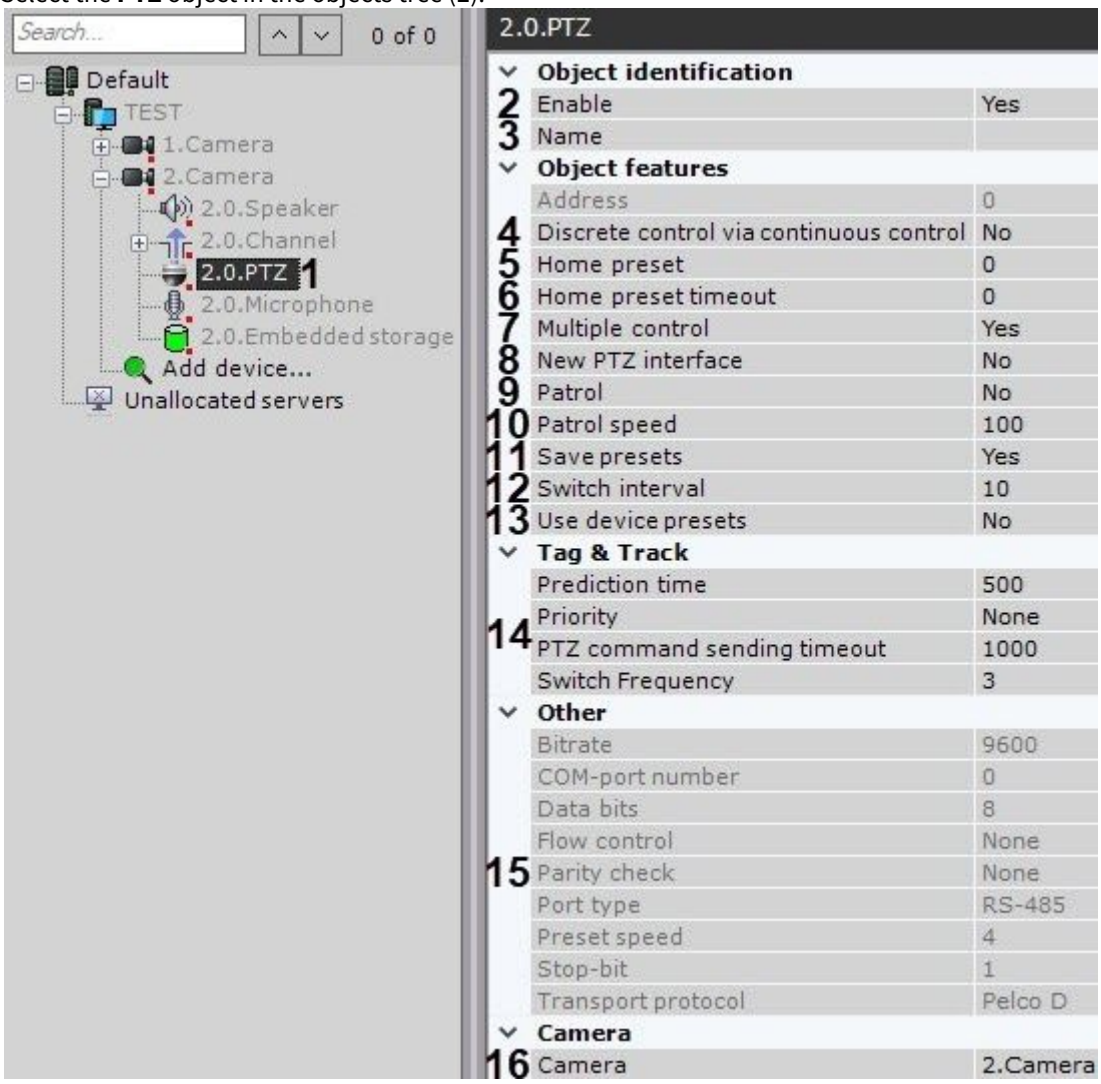
Checking microphone operation is now complete.

15.2.3.5 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(see page 681)). 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(see page 540)), 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(see page 675)).
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.

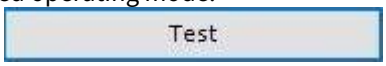
> **Attention!**
>
> If the use of the existing presets is disabled, they can be lost if the following conditions are met:
> 1. The recording of the presets to the device is enabled in *Axxon One* (see step 9).
> 2. The preset with the same ID is created in *Axxon One* (see Creating and editing presets(see page 678)).

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(see page 682)). 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(see page 678)), set **Yes** for the **Use device presets** parameter (**13**).
11. If necessary, configure the Tag & Track function (**14**, see Configuring Tag&Track Pro(see page 189)).
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(see page 675)

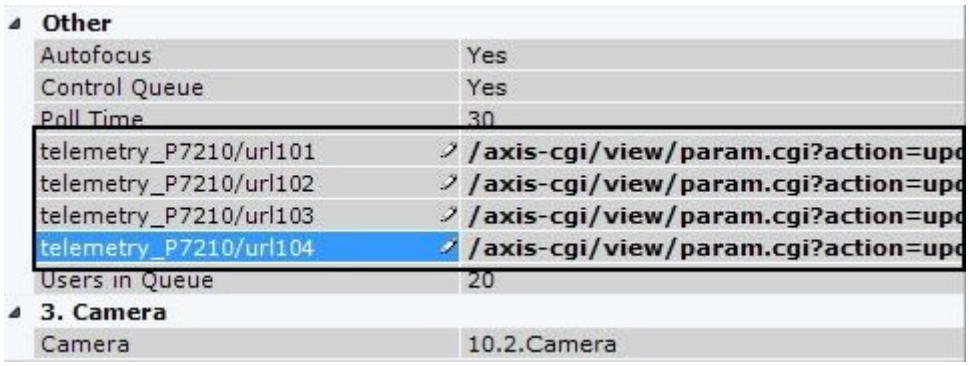
15.2.3.5.1 Configure HTTP-CGI commands to control Wash&Wiper

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(see page 678)).
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(see page 122)).



3. Click the **Apply** button.

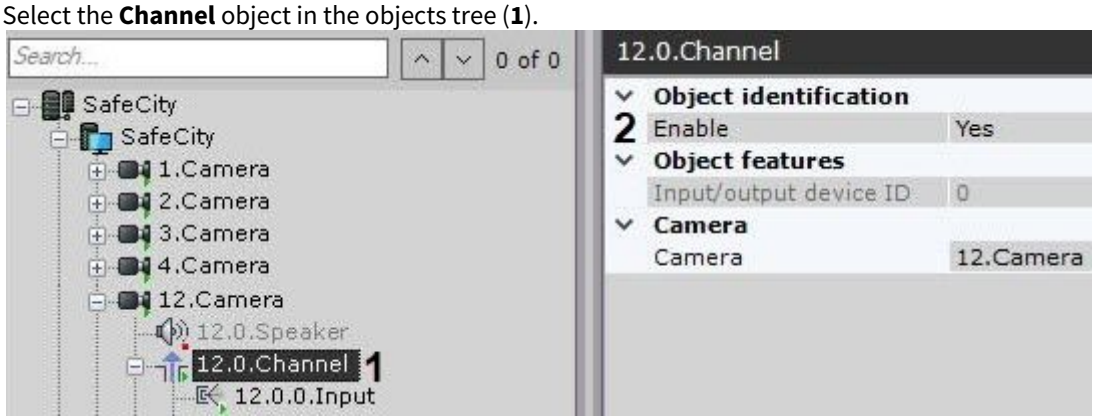
When the camera goes to the presets 101-104, this triggers a pre-configured command.

15.2.3.6 The Channel object

For I/O modules or video surveillance control panels (see CCTV Keyboards(see page 178)), the **Channel** object is displayed as a child object of an IP Server in the object tree (see The IP Server Object(see page 161)).

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**.

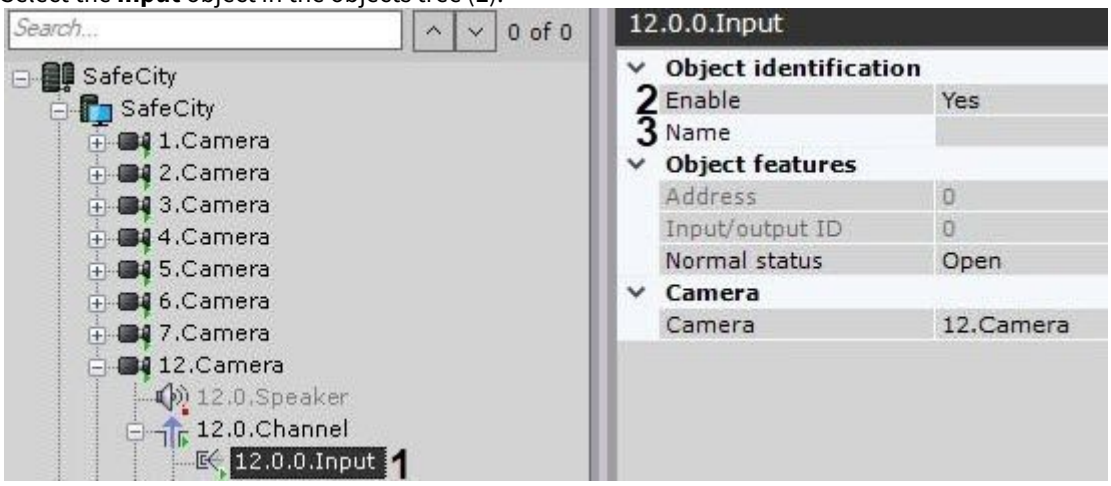
15.2.3.7 The Input Object

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(see page 166)).

To configure a **Input** object, perform the following:

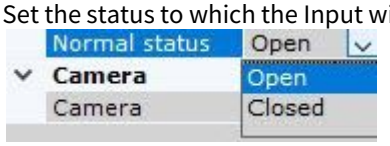
1. Select the **Input** object in the objects tree (**1**).



2. Enable the device (**2**).

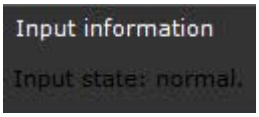
> **Note**
>
> If a input is a child of a **Channel** object, then:
> a. Turning on a input automatically enables its parent **Channel** object.
> b. Turning off all **Input** and **Output** child objects automatically disables their parent **Channel** object.

3. Enter the name of the Input (**3**).
4. Set the status to which the Input will be set when no alarm is present.

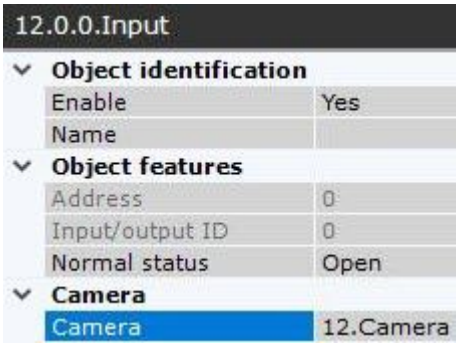


5. Click the **Apply** button.

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.



15.2.3.7.1 Configure virtual inputs

Switch between virtual IP-device states (HttpListener)[75].

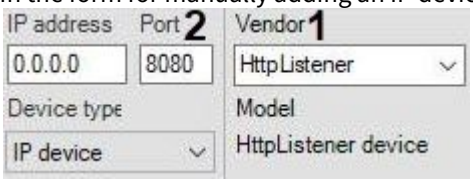
75 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=246487043

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.**

15.2.3.7.1.1 Creating and configuring virtual inputs

To create and configure a virtual input, complete the following steps:

1. Run IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)).
2. In the form for manually adding an IP device, select **HttpListener** in the **Vendor** drop-down list (**1**).

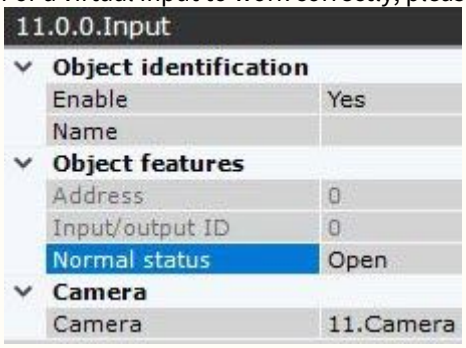


3. In the **Port** field, specify the port number that will be used Input status queries (**2**).
4. Click the button.

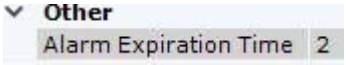
The **IP Server** object is automatically created to host 4 virtual inputs.

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.



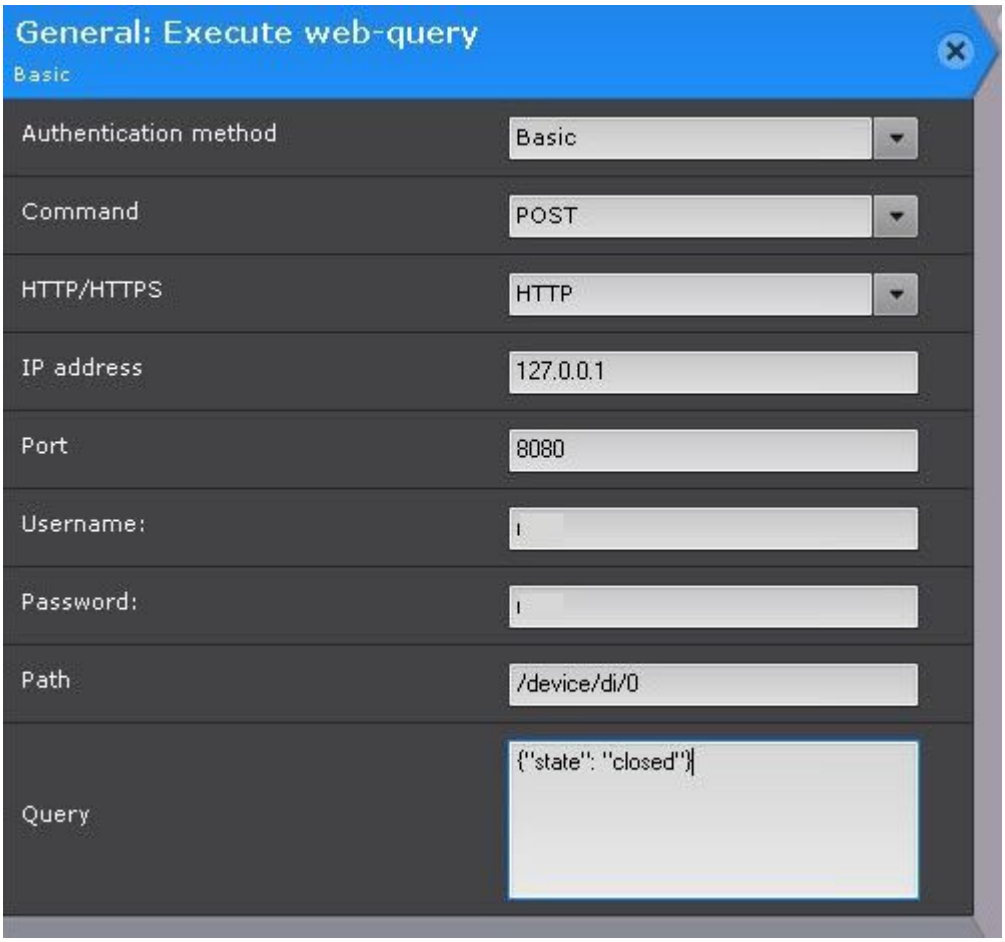
This setting is applied only after you disable and enable the input again.

15.2.3.7.1.2 Switching virtual inputs

To switch virtual inputs, the HTTP request is used (see Switch between virtual IP-device states (HttpListener)[76]).

The requests can be handled by macros (see Executing a web query(see page 444)). Create 2 macros for each virtual input: to switch to **Closed** and to switch to **Opened**.

76 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=246487043



You can run macros and requests from Dialog board (see Configuring a Dialog Board(see page 495)).

15.2.3.7.1.3 Virtual inputs' status on map

You can add virtual inputs to maps just as you do with real ones (see Adding inputs and outputs(see page 512)).

Virtual inputs status is color-coded (see Displaying device status(see page 805)).

15.2.3.8 The Output Object

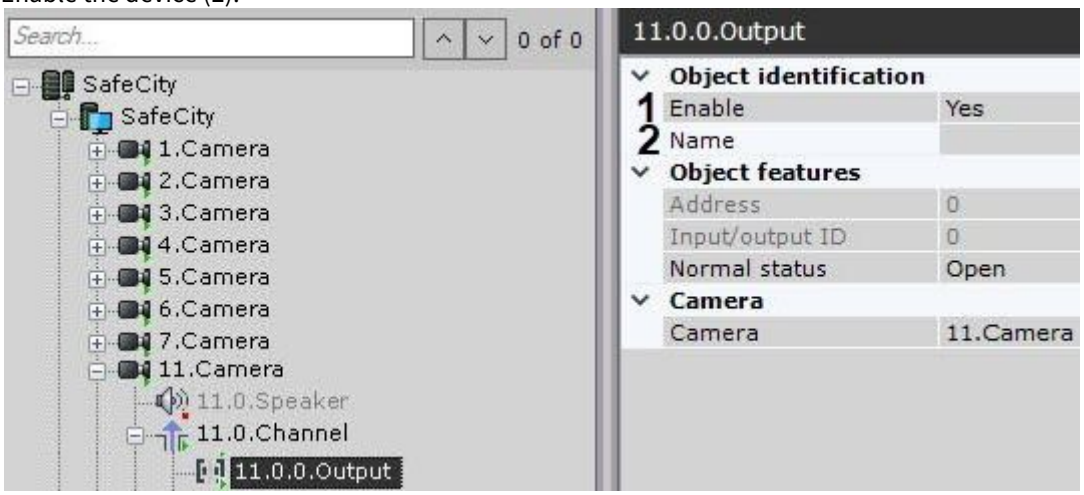
If a camera has a built-in or pluggable digital output, the **Output** object is displayed as a child object of the **Camera** in the object tree. The total number of **Output** objects for a camera corresponds to its number of pluggable digital outputs.

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(see page 166)).

To configure a **Output** object, perform the following:

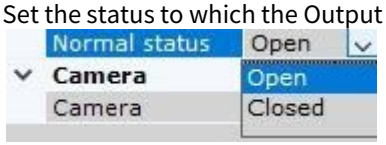
1. Select a **Output** object in the objects tree.

2. Enable the device (**1**).



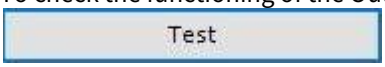
> **Note**
>
> If a output is a child of a **Channel** object, then:
> a. Turning on a output automatically enables its parent **Channel** object.
> b. Turning off all **Input** and **Output** child objects automatically disables their parent **Channel** object.

3. Enter the name of the Output (**2**).
4. Set the status to which the Output will be set when no alarm is present.

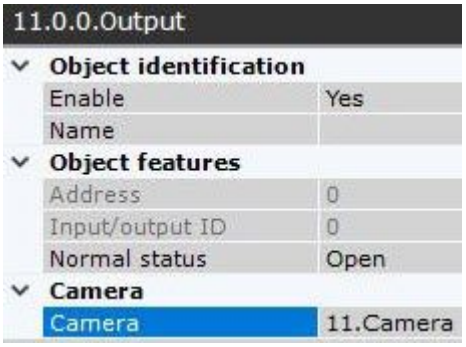


5. Click the **Apply** button.

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.



15.2.3.9 The Speaker Object

The **Speaker** object is used for configuration of the sound alert triggered by a macros.

> **Attention!**
>
> Audio notifications cannot be played back via the system speakers on a remote Client. In this case, you are advised to run an external program on Clients(see page 439).

In *Axxon One* you can create the following types of **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 play audio notification files with the extensions:

1. .wav
2. .mp3
3. .mkv
4. .avi

The following audio notification file encoding formats are supported:

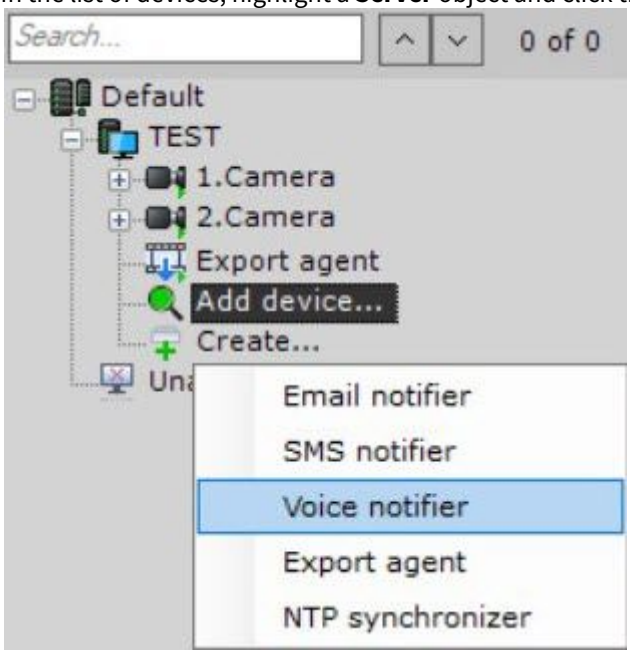
1. G.711
2. G.726
3. PCM

The audio notification file should be stored on the computer corresponding to the **Server** object on the basis of which the **Speaker** object is registered.

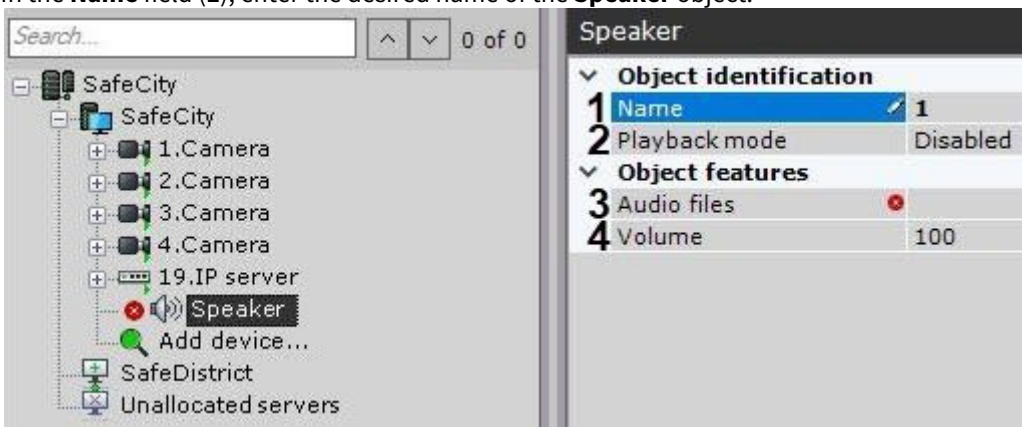
15.2.3.9.1 Creating and Configuring an Object

To create a **Speaker** system object, you must perform the following steps:

1. In the list of devices, highlight a **Server** object and click the **Create voice notifier** button (**1**).

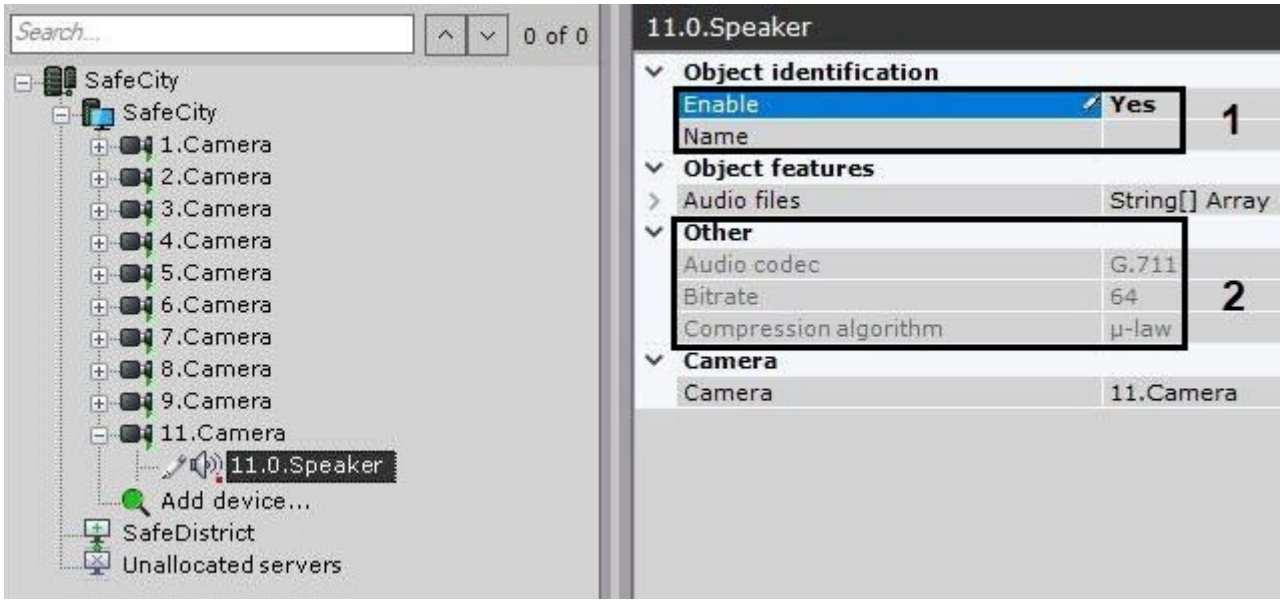


2. In the **Name** field (**1**), enter the desired name of the **Speaker** object.



3. Select the speaker mode: disabled, play back on Server, play back on Clients (**2**).
4. In the **Audio files** field (**3**), enter the full path to the audio notification file. This parameter is mandatory.
5. In the **Volume** field (**4**), enter the desired speaker volume level.

> **Note**
>
> By default, IP device speakers are disabled. To enable, for the **Enable** value (**1**), select **Yes**. When configuring the speaker of an IP device, you can set other parameters as well, such as the compression algorithm for the audio signal sent to the speaker for playback (**2**). Which speaker parameters you can configure is determined by the protocol for integration of the IP device and the *Axxon One* software package.



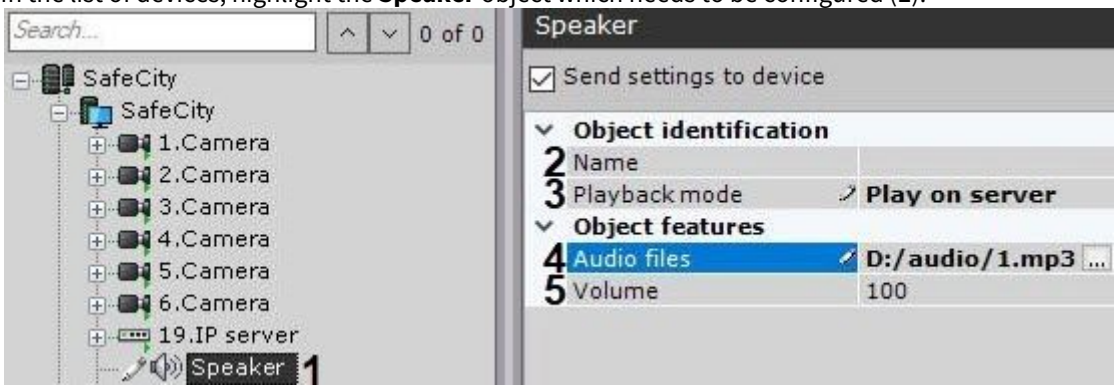
6. Click the **Apply** button.

Creation of the **Speaker** object is complete.

15.2.3.9.2 Configuring a Speaker Object

To configure a **Speaker** object, you must perform the following steps:

1. In the list of devices, highlight the **Speaker** object which needs to be configured (**1**).



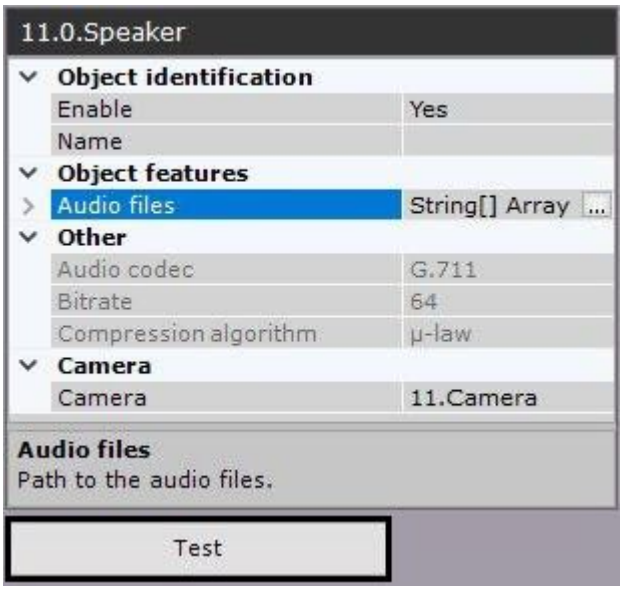
2. In the **Name** field (**2**), enter the desired name of the **Speaker** object.
3. Select the speaker mode: disabled, play back on Server, play back on Clients (**3**).
4. In the **Audio files** field (**4**), enter the full path to the audio notification file.
5. In the **Volume** field (**5**), enter the desired speaker volume level.
6. To parent an IP device to a speaker:
   a. By default, IP device speakers are disabled. To enable, for the **Enable** value (**1**), select **Yes**.

   b. When configuring the speaker of an IP device, you can set other parameters as well, such as the compression algorithm for the audio signal sent to the speaker for playback (**2**). Which speaker parameters you can configure is determined by the protocol for integration of the IP device and the *Axxon One* software package.
   c. Choose a video camera to associate this speaker with (**3**). As a result of this operation, the selected camera will become a parent object for the speaker.
7. Click the **Apply** button.

Configuration of the **Speaker** object is now complete.

15.2.3.9.3 Checking Audio Notification

To check audio notification from a **Speaker** object, click the **Test** button.



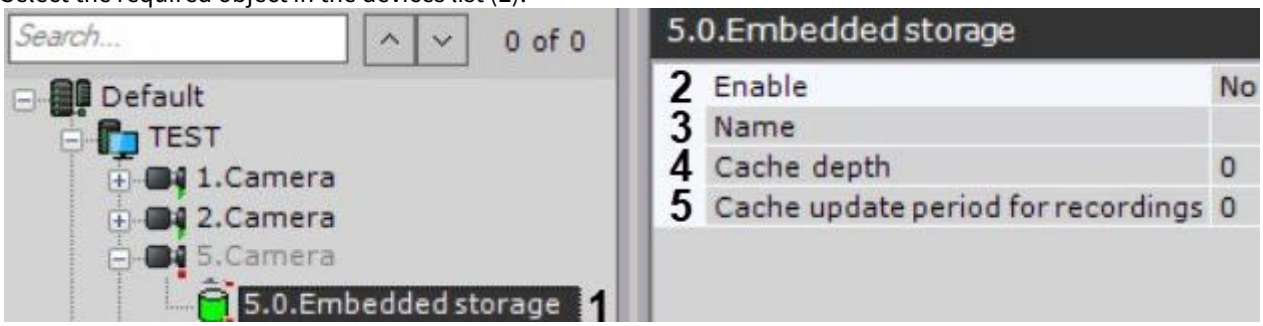
When you do this, the audio notification file whose path you indicated in the corresponding field plays back (see the section Configuring a Speaker Object(see page 172)).

15.2.3.10 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(see page 226)).

15.2.4 Particulars of Configuration of Devices

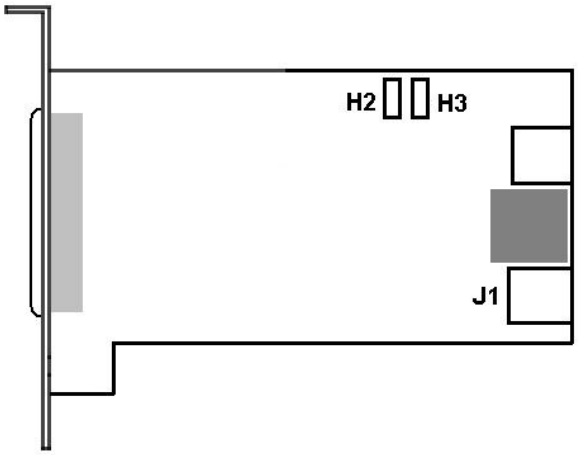
15.2.4.1 AGRG-IO-16/8-WD-DS Sensor-Relay cards

15.2.4.1.1 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(see page 176) 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

Connector	Application	Connector	Application
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.

15.2.4.1.2 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.

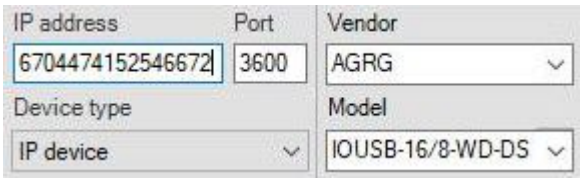
Parameter	Specification
Galvanic isolation on inputs/outputs	3750 V

Parameter	Specification
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

15.2.4.1.3 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 Adding and removing IP devices(see page 112)).

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[77].

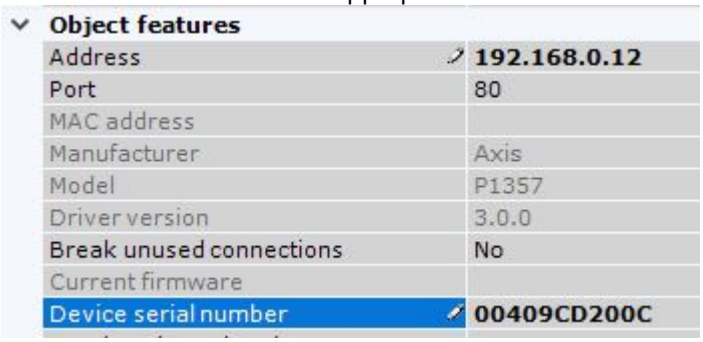
15.2.4.2 Axis IP Devices

15.2.4.2.1 Serial number check

To check serial numbers of Axis IP devices, do the following:

77 http://it-agregator.ru/owncloud/index.php/s/uetnCUVVDcTwxiC

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.

15.2.4.2.2 Bonjour function

For Axis IP devices on which the Bonjour function is supported and enabled, changing the default value of the **Friendly name** parameter is strongly discouraged. If an arbitrary **Friendly name** value is set for an Axis IP device, a search for connected equipment in the *Axxon One* software package will give incorrect results for this IP device.

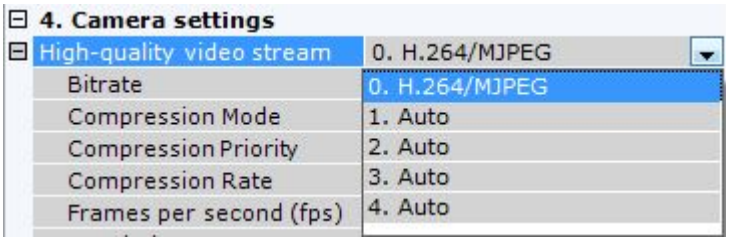
> **Note**
>
> - The **Friendly name** parameter is configured through the Web interface of the IP device: Setup -> System options -> Network -> Bonjour.
> - The default value of the **Friendly name** parameter is as follows: AXIS <model name> - <mac address>, where <model name> is the model of the Axis IP device and <mac address> is its MAC address (for example, AXIS 214 – 00408C7D2610).

15.2.4.2.3 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(see page 122)).



15.2.4.3 CCTV Keyboards

15.2.4.3.1 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(see page 578)).

> **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 Adding and removing IP devices(see page 112)).

> **Attention!**
>
> To connect a control panel in this way, you need the *Axxon One* software to be installed in the **Server and Client** configuration. 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	-	+

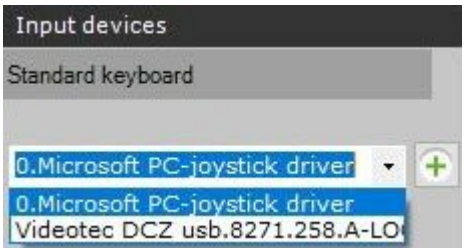
15.2.4.3.2 Axis T8310 specific configuration features

15.2.4.3.2.1 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(see page 100), Starting a Server(see page 94)).

15.2.4.3.2.2 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[78].

T8310	All devices

78 https://www.axis.com/products/axis-t8310-video-surveillance-control-board

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

15.2.4.3.3 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.

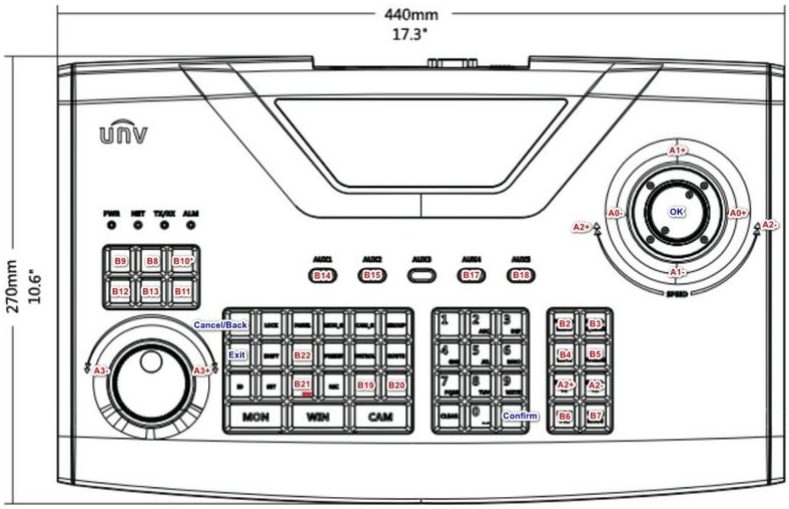
15.2.4.3.4 UNIVIEW KB-1100 specific configuration features

On page:

- General description of the UNIVIEW KB-1100 PTZ control device(see page 180)
- Configuring a remote control before adding it to Axxon One(see page 181)
- Configuring UNIVIEW KB-1100 in Axxon One(see page 181)

15.2.4.3.4.1 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.

15.2.4.3.4.2 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.

15.2.4.3.4.3 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 Adding and removing IP devices(see page 112)).

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.

15.2.4.3.5 Hikvision DS-1200KI specific configuration features

On the page:

- Configuring the Hikvision DS-1200KI control device before adding it to Axxon One(see page 182)
- Features of the Hikvision DS-1200KI control device operation in Axxon One(see page 184)

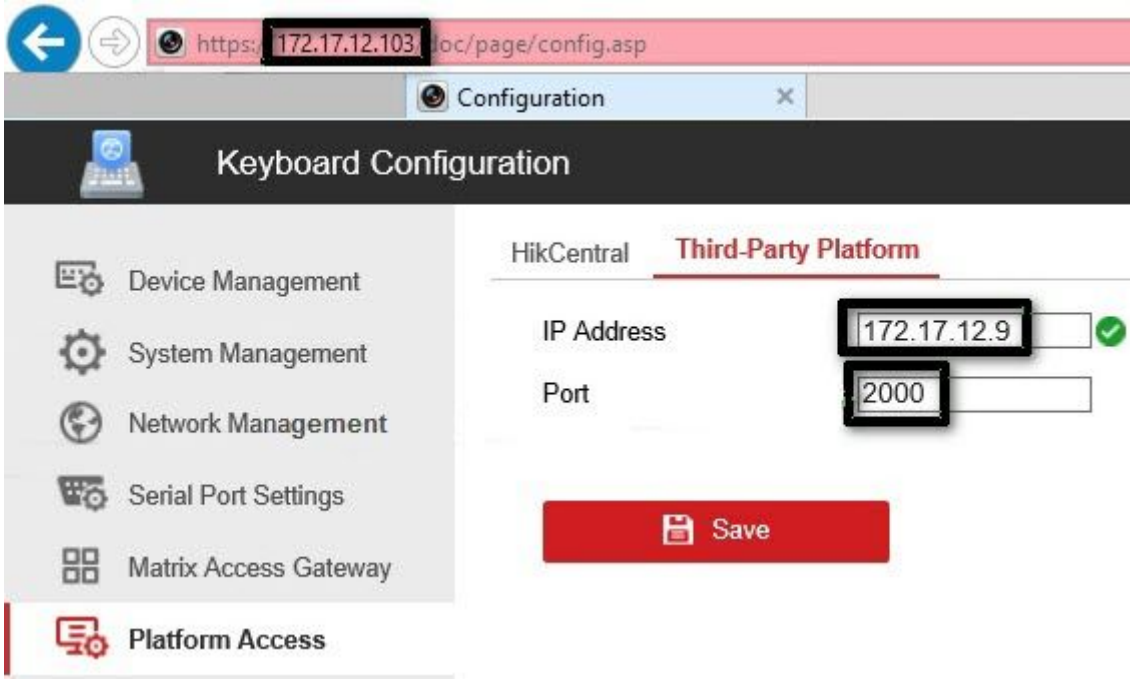
15.2.4.3.5.1 Configuring the Hikvision DS-1200KI control device before adding it to *Axxon One*

Configure the Hikvision DS-1200KI PTZ control device as follows before creating the corresponding object in *Axxon One*:

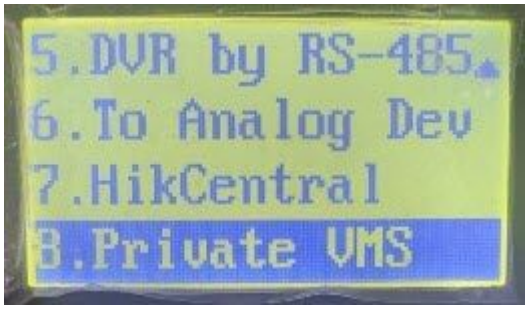
1. Set the control device address: **Select System – Network** in the device internal menu, then disable DHCP and set IP address and gateway.

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.

15.2.4.3.5.2 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.

15.2.4.3.6 Dahua DH-NKB1000 specific configuration features

15.2.4.3.6.1 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.

15.2.4.3.6.2 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.

15.2.4.3.6.3 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.

15.2.4.4 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 (see page 909).

15.2.4.5 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[79].
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(see page 684)) and Point&Click functions (see Control using Point&Click(see page 684)).

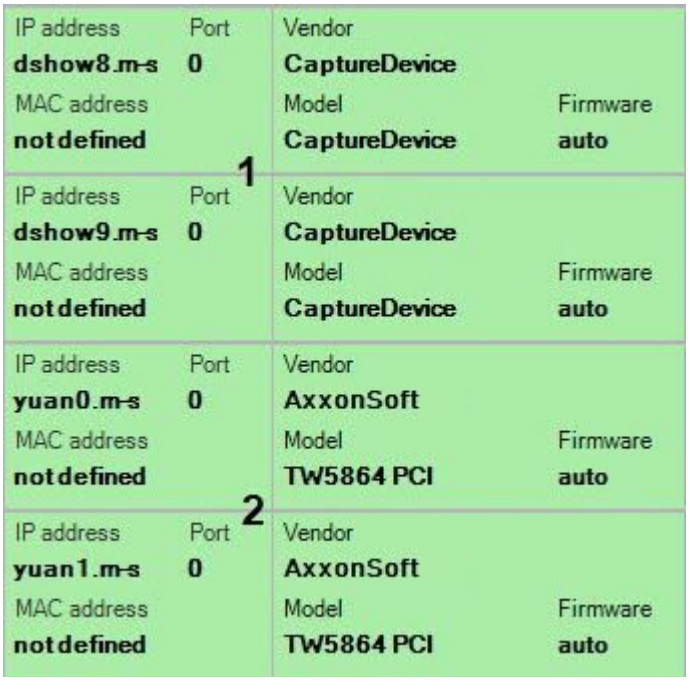
15.2.4.6 Video capture cards

Axxon One supports 3 PCIe and one USB video capture cards:

1. PCIe:
   a. Yuan SC300Q16.
   b. Yuan SC3C0N8.[80]
   c. Yuan WS216.
2. USB: Yuan PD652[81].

15.2.4.6.1 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[82].

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(see page 122)).

79 http://www.vivotek.com/panoramic%20ptz/
80 https://www.yuan.com.tw/products/capture/analog/sc3c0n8_l.htm
81 https://www.yuan.com.tw/products/capture/external/pd652.htm
82 https://technet.microsoft.com/en-us/library/dd759187(v=ws.11).aspx

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).

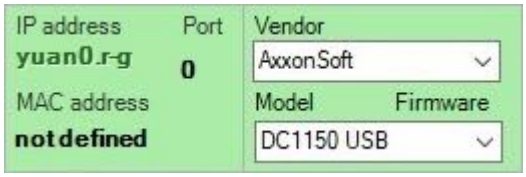
15.2.4.6.2 YUAN PD652 cards

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[83] manufacturer.

1. Disable the system check for the digital signature of the drivers and install the card driver[84].
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.

15.2.4.7 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[85].

Note

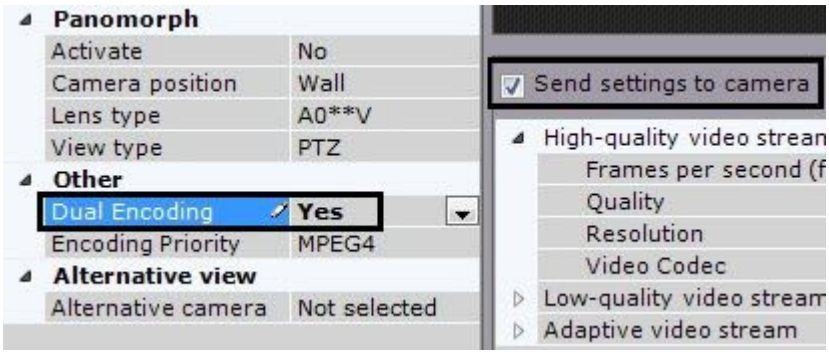
We recommend that you calibrate the joystick before you start working with *Axxon One*.

15.2.4.8 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.

83 http://www.yuan.com.tw/products/capture/external/pd652.htm
84 http://www.yuan.com.tw/download.htm
85 http://support.microsoft.com/kb/831361/en-us

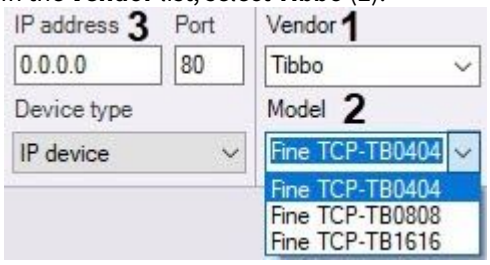


15.2.4.9 Setting up Tibbo relay/loop boards

Tibbo relay/loop boards allow monitoring air temperature and humidity on your premises.

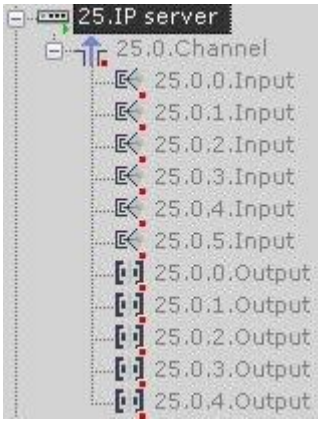
To add a board to the configuration, do the following:

1. Go to IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)).
2. In the **Vendor** list, select **Tibbo** (**1**).



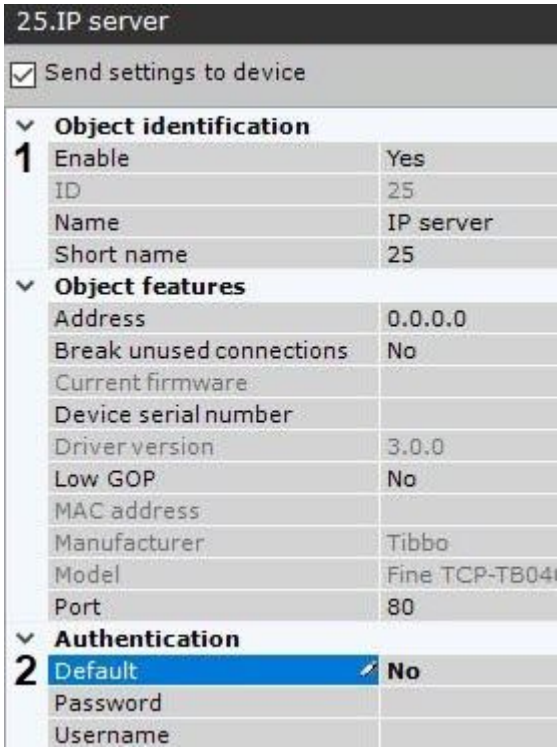
3. Select your board from the **Model** list (**2**).
4. Enter the IP address of the board (**3**).
5. Click the button.

The parent **IP Server** object, and **Channel**, **Input** and child objects under it will be added.

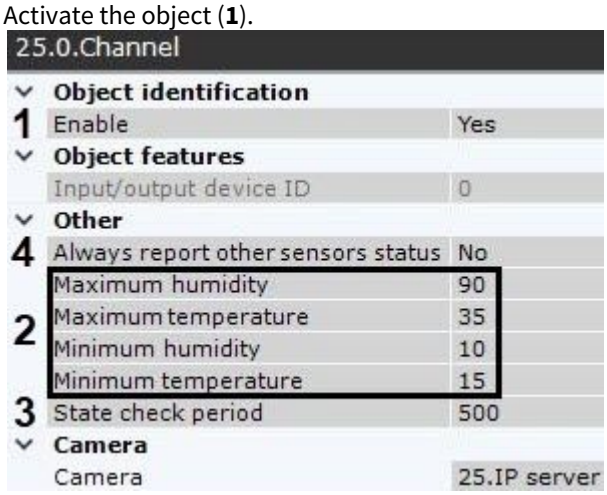


To configure the board, do the following:

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(see page 805)).

15.2.5 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[86]. 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.

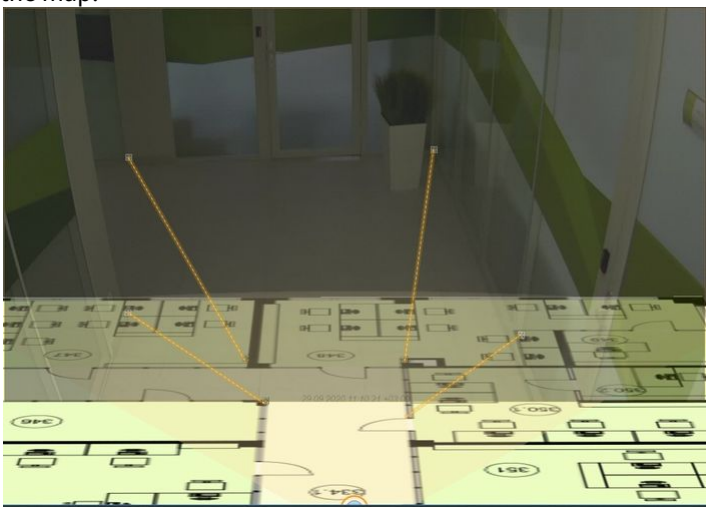
For these functions to work, all video cameras involved must have an activated **Object tracker** or **Neurotracker** object (see General information on Scene Analytics detection tools(see page 254)).

15.2.5.1 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.

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(see page 474)).
3. Add video cameras to the map (see Adding video cameras and changing size of their icons on the map(see page 512)).
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(see page 515)). 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(see page 517)).
   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(see page 499)).

15.2.5.2 Configuring Tag & Track Pro

To configure Tag & Track Pro:

1. Link panoramic cameras to a PTZ camera.
2. Calibrate cameras.

---

86 https://docs.axxonsoft.com/confluence/display/DDP/En

3. Set the PTZ mode.

15.2.5.2.1 Camera requirements for Tag&Track Pro

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(see page 256).

15.2.5.2.2 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.

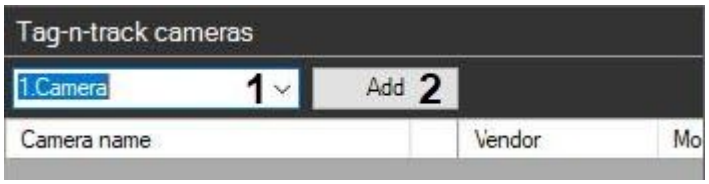
15.2.5.2.3 Linking panoramic cameras to a PTZ camera

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** button (**2**).

> **Note**
>
> To search for a camera, enter its ID, the full or partial name in the **1** box.

> **Note**
>
> You can add only those cameras for which the Object Tracking(see page 254) 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.

15.2.5.2.4 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(see page 190)).
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(see page 684)).
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.

15.2.5.2.5 Setting PTZ mode for Tag & Track Pro

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**).

Tag & Track	
Prediction time	500
1 Priority	Automatic
PTZ command sending timeout	1000
2 Switch Frequency	3

To save changes, click the **Apply** button.

15.2.6 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

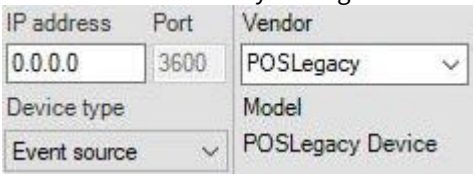
In *Axxon One*, information from external sources is superimposed on video from a selected camera.

15.2.6.1 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 Adding and removing IP devices(see page 112)).

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.

15.2.6.2 Configuring POS devices

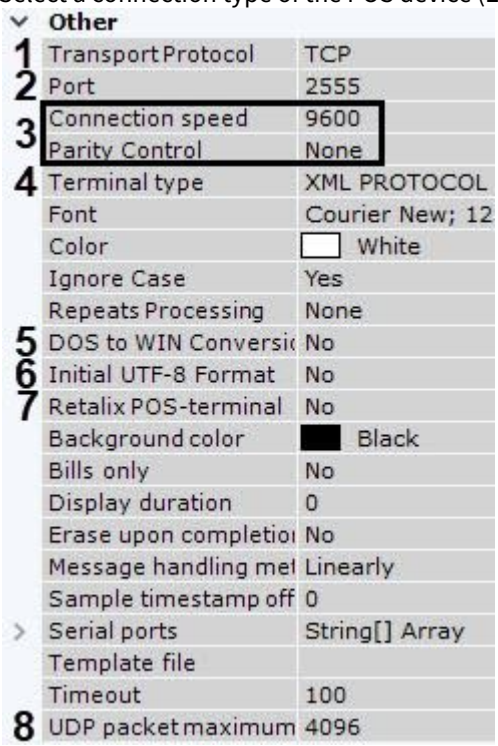
Axxon One can obtain data from POS devices and offers the following capabilities:

1. Show titles in live and recorded video.
2. Search titles in recorded video.

15.2.6.2.1 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.

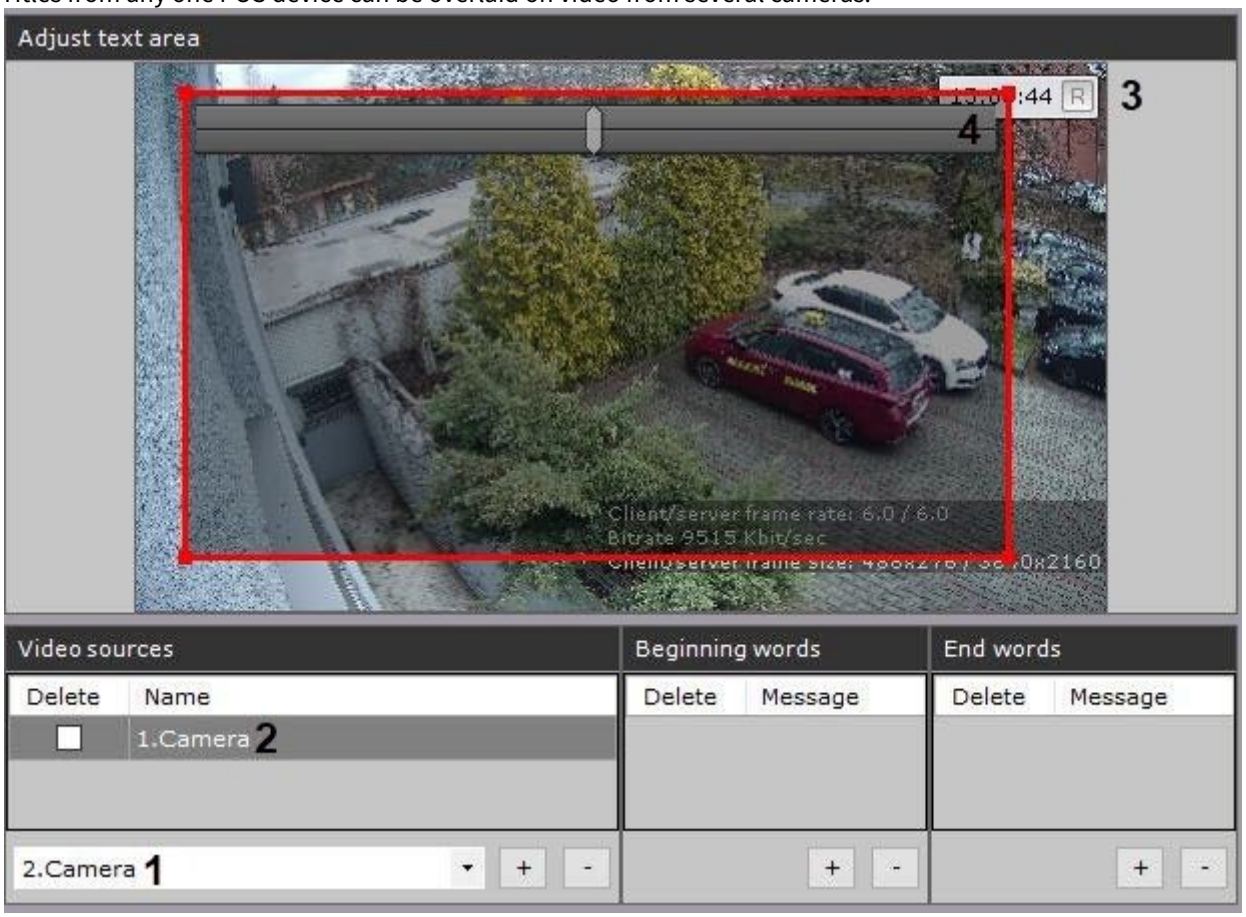
You have successfully connected your POS device.

15.2.6.2.2 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.

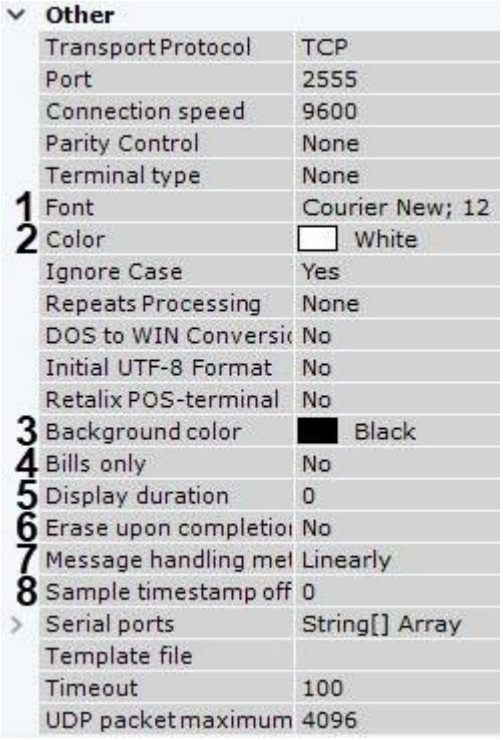


> **Note**
>
> To disable titles overlay for a camera, select the **Delete** checkbox and click the **–** button.

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.[87]
4. Change transparency with the slider (**4**). Slide left for more transparency, slide right for less.

87 https://en.wikipedia.org/wiki/Drag-and-drop

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 (**4**).
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.

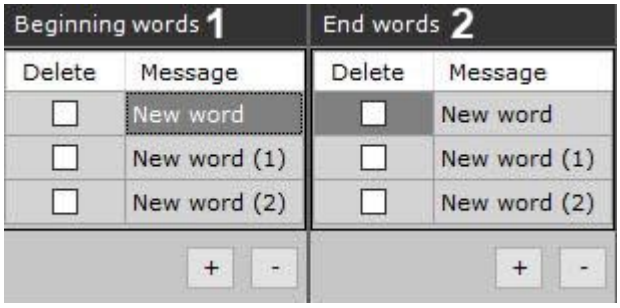
15.2.6.2.3 Configuring receipt beginning/end

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 Titles search(see page 740)).

> **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:

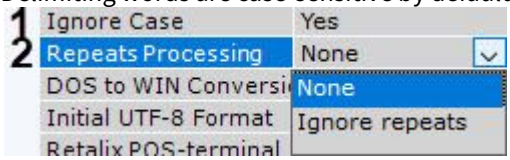
1. Populate the **Beginning words** (**1**) group. To add words, click the **+** button. To remove words, select their **Delete** check boxes and click the − button.



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.

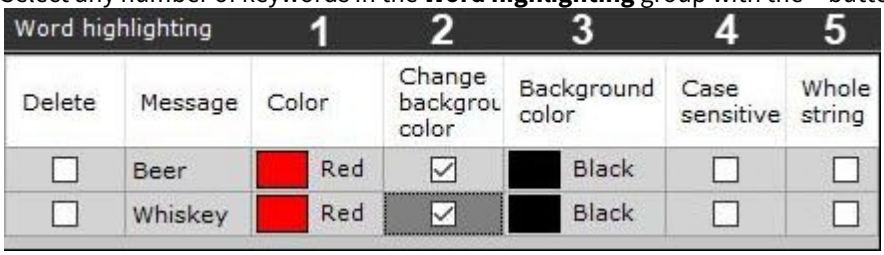
You have configured how receipts are delimited.

15.2.6.2.4 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.

15.2.6.2.5 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:

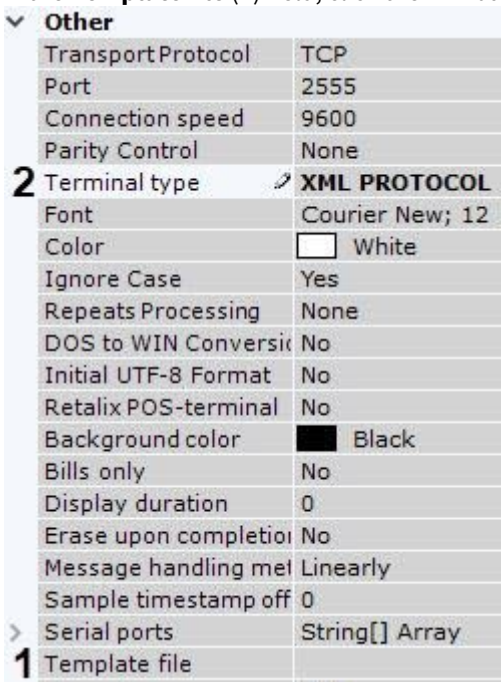
1. XML parcer for .txt files;
2. POS parcer for .prl files.

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.

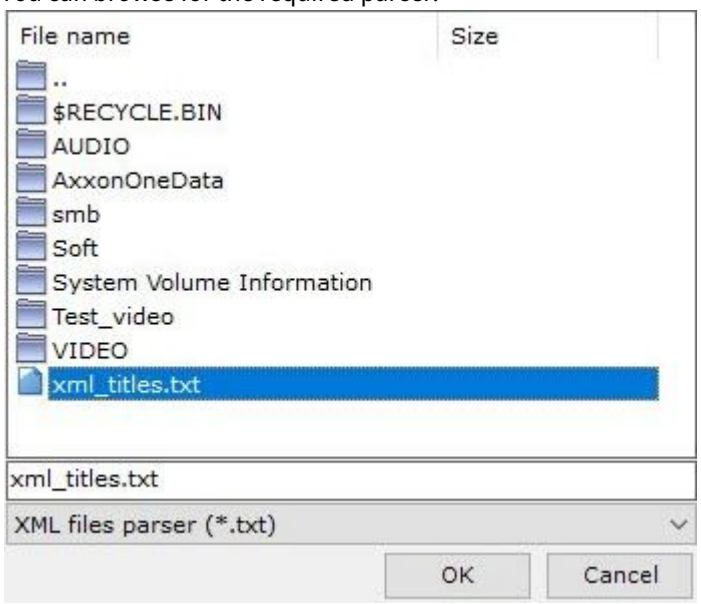
The POS parser specifies the rules for adding data to the receipts database if the data is from a POS terminal is other than XML. The parser depends on the POS terminal data structure.

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.

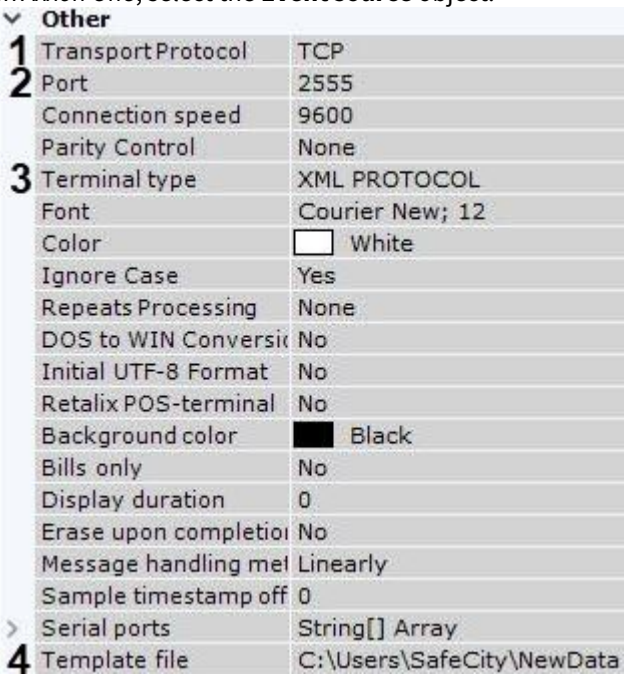
3. If you use an XML parser, select **XML PROTOCOL** in the **Terminal type** field (**2**).
4. Click the **Apply** button.

You have imported the parcer.

15.2.6.3 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[88]).
7. Configure the data output similar to that of the POS device (see Configuring titles view(see page 194)).
8. Configure keywords, if necessary (see Configuring keywords(see page 196)).
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(see page 670)).

15.2.6.4 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(see page 199)).
2. As events from virtual inputs. This creates a virtual IP Server in the VMS (see Configuring Commax Complex Server via virtual IP server(see page 199)).

> **Note**
>
> CommaxComplexServer is smart apartment complex management software. It receives input from gates, doors, elevator call buttons etc.

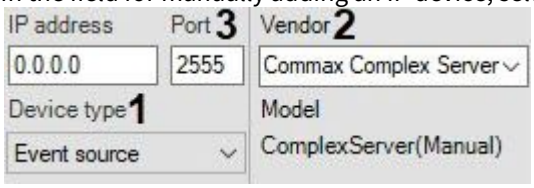
Configure CommaxComplexServer before connecting to *Axxon One*.

88 https://docs.axxonsoft.com/confluence/display/posPSIM100en/Configuring+parser+in+the+POS+PSIM+software

15.2.6.4.1 Configuring Commax Complex Server via Event Source

Connect Commax Complex Server via **Event Source** as follows:

1. Run IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)).
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.

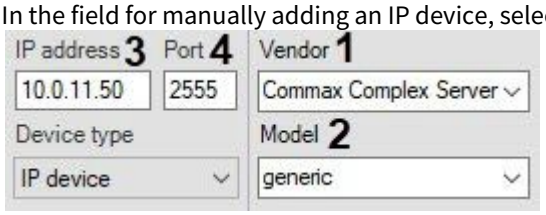
The Commax Complex Server connection is now configured.

> **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(see page 193)).

15.2.6.4.2 Configuring Commax Complex Server via virtual IP server

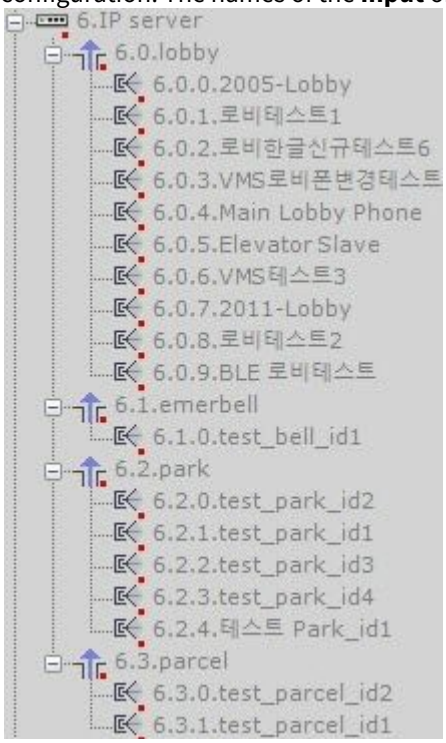
Connect to Commax Complex Server via virtual IP server as follows:

1. Run IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)).
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.

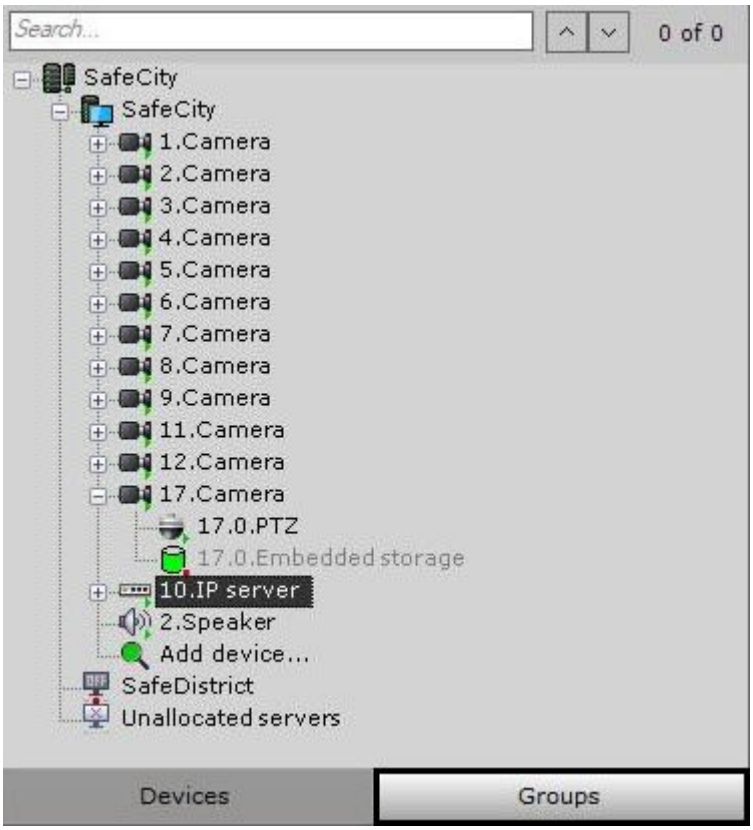


The Commax Complex Server connection is now configured.

15.2.7 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.



15.2.7.1 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.

15.2.7.2 Creating a Group object

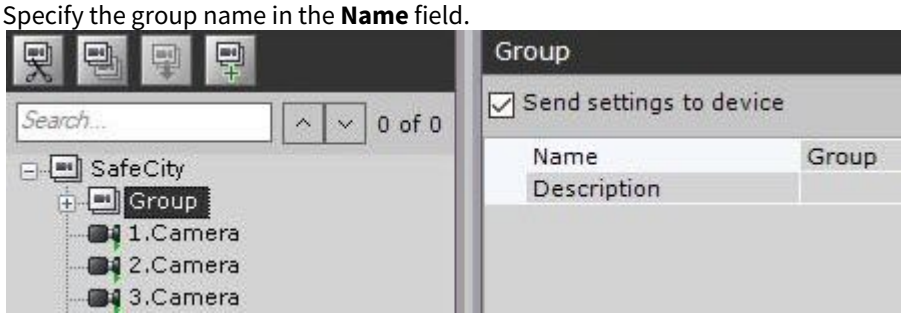
To create a **Group** object, complete the following steps:

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.

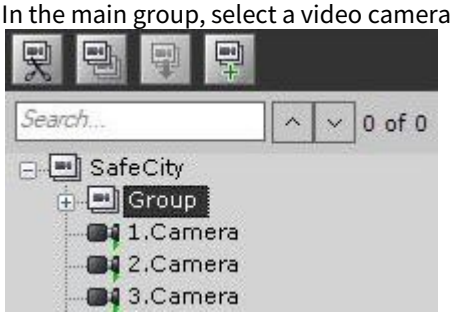
The **Group** object has now been created.

15.2.7.3 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(see page 203)). 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).

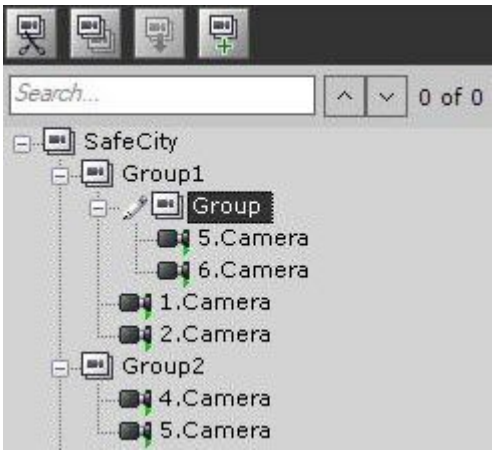
> **Note**
>
> One video camera can be assigned to multiple groups.

6. Click the **Apply** button.

Adding video cameras to groups is now complete.

15.2.7.4 Creating a system of groups and subgroups

Groups can be included within other groups, forming a system of groups and subgroups.

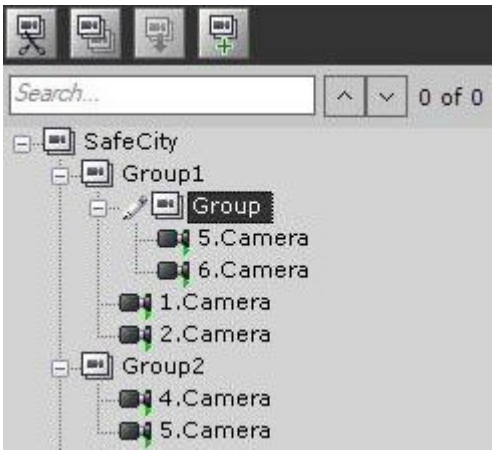


A system of groups and subgroups can be created via group management operations and video camera management operations (see the section titled Managing Group and Video camera objects(see page 203)).

Group objects can be moved or copied to other **Group** objects or to the main group.

15.2.7.5 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.

Action	Execution
	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.

15.2.8 Autocopy data from local to centralized servers

Axxon One VMS supports automatic copying of the archive (video, audio, alarms) and camera events from local servers that are not in the same Axxon domain with the centralized server.

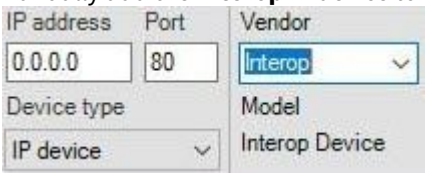
Note

This is useful, for example, in the following case:

- The video from a bus on the route network is written 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:

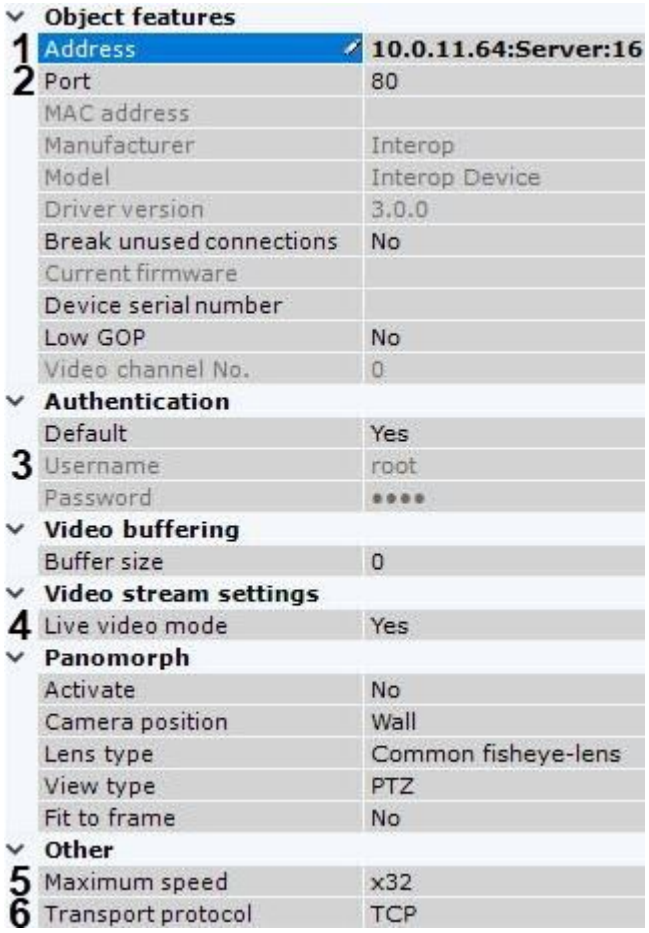
1. Manually add the **Interop** IP device to the configuration (see Adding and removing IP devices(see page 112));



2. Enable The Embedded storage object(see page 174).
3. 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 name is Server1, no connection will occur if you enter server1 or SERVER1.



4. Specify a port of the local Server from which data is transmitted (**2**). If you use TCP protocol (see 8), please specify the RTSP port number (554 by default, see Configuring an RTSP Server(see page 120)). If you use rtspoverhttp or rtspoverhttps protocol, specify the Web server's port (80 by default, Configuring the Web-Server(see page 119)).
5. Specify the user name and password (**3**). The user must have permissions to access the local server.
6. If you want to display live video from the local server when it is available, select **Yes** in the appropriate field (**4**).
7. Specify the maximum playback speed (**5**).
8. Select the data transfer protocol (**6**).
9. Click the **Apply** button.
10. Repeat the above steps for all the required cameras from all local servers.
11. Configure automatic replication from the embedded storages of the added devices to the centralized server archive (see Configuring data replication(see page 226)).

Attention!

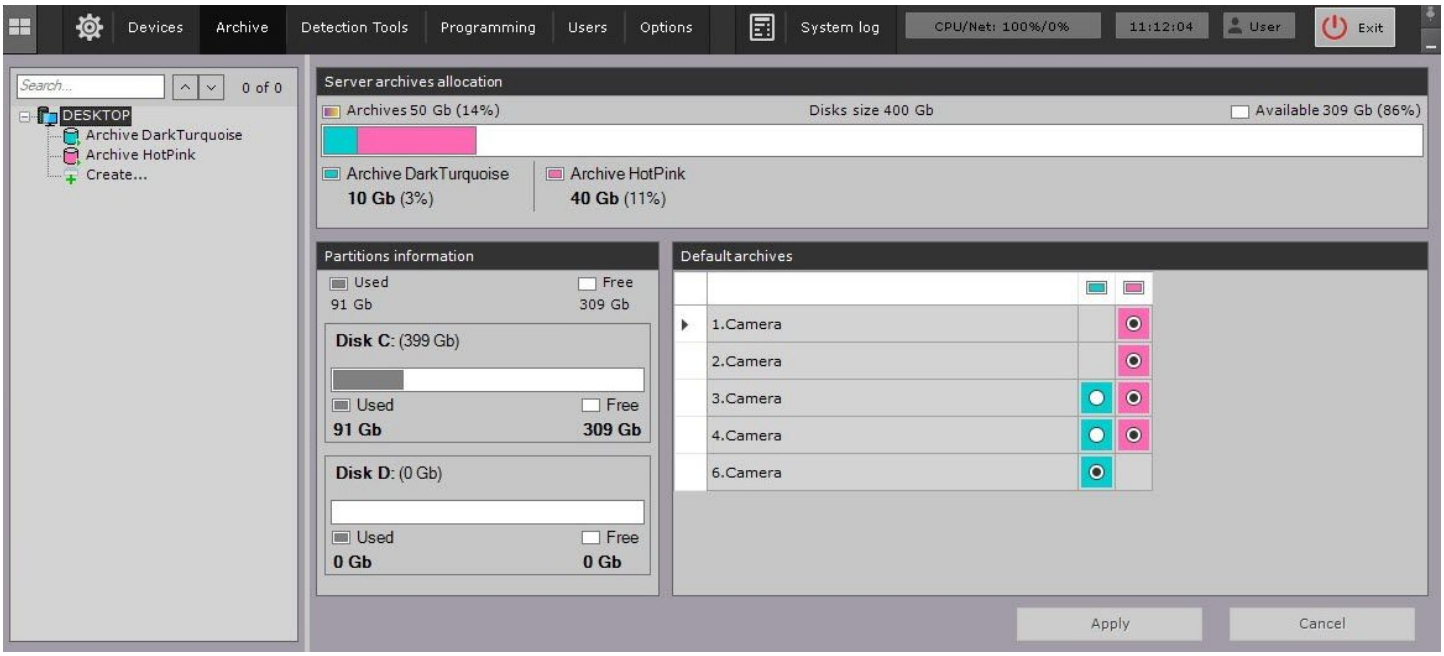
With a high network load, there may be gaps in the centralized server archive.

You have successfully set up automatic data copying from the local servers to the centralized server.

15.3 Configuring archives

15.3.1 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:

- both on local disks and on remote disks;
- in cloud storages (see General information about the cloud archive(see page 208)).

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.
You can configure archives as follows:

1. Create archives (see Creating archives(see page 209)).
2. Configure recording of the video stream from video cameras to the archives (see Configuring recording to an archive(see page 224)).
3. Configure data replication, if necessary (see Configuring data replication(see page 226)).

You can also connect external archives—a set of video recordings with time links.

Video surveillance in archive mode(see page 695)

15.3.2 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(see page 209)). 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.

15.3.3 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[89].

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/[90].
2. Microsoft Azure: https://azure.microsoft.com/en-gb/services/storage/blobs/.
3. Wasabi: https://wasabi.com/.

89 https://aws.amazon.com/s3/faqs/?nc1=h_ls#Durability_.26_Data_Protection
90 https://aws.amazon.com/s3/?nc=sn&loc=0

4. Huawei Cloud: https://huaweicloud.com/.
5. Seagate Lyve Cloud: https://www.seagate.com/.
6. MinIO: https://min.io/.

Creating a cloud archive(see page 214)

15.3.3.1 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.

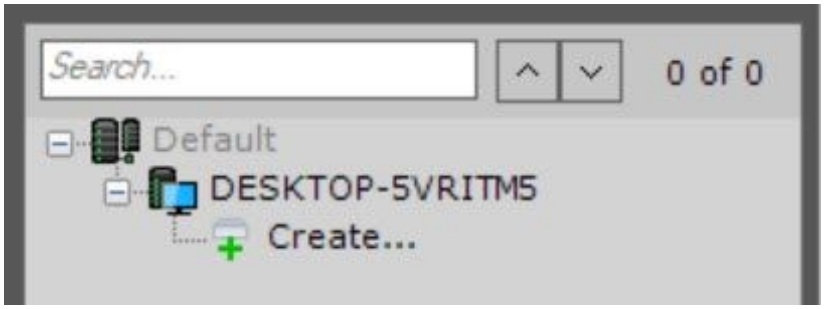
This algorithm allows increasing the writing speed of the archive, as well as preventing the loss of records for a certain period, in case there are problems with the archive volumes, i.e., if the archive volume is lost, the records for the previous period will be available with frame decimation. This behavior is ensured because the key frames of records are distributed evenly over all available volumes of the archive.

15.3.4 Creating archives

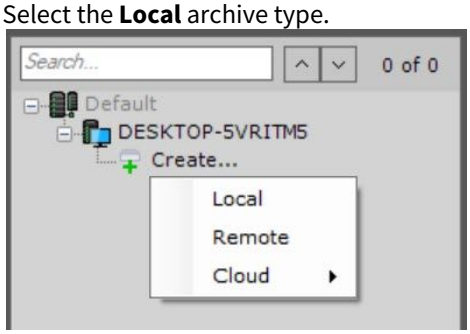
15.3.4.1 Creating a local archive

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** link.



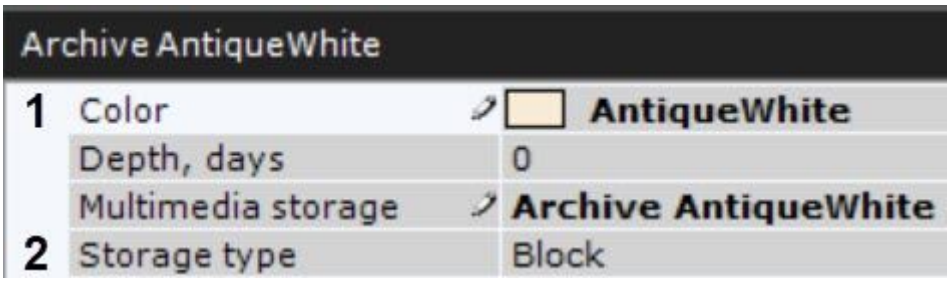
2. Select the **Local** archive type.



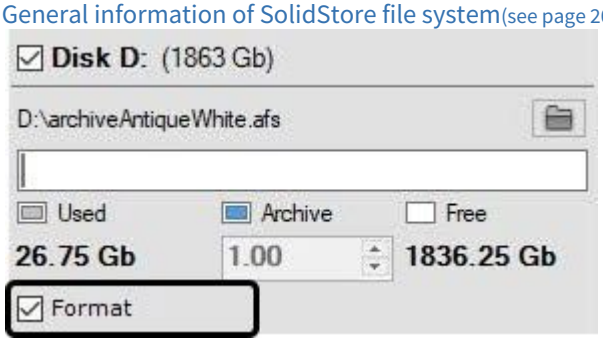
3. Specify the name and color of the archive (**1**).
4. Select the storage type (**2**):
   - block, if you need low latency and high performance in various situations. For example, for tasks with a large read and write load;
   - object, if a technical support specialist recommended you to use this type of storage.

Attention!

It is not recommended to use object type of storage without prior consultation with AxxonSoft technical specialist.



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(see page 208)).



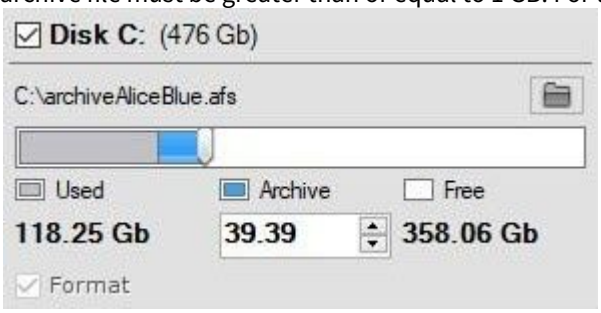
Attention!

- 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[91]. 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 unformatted 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.

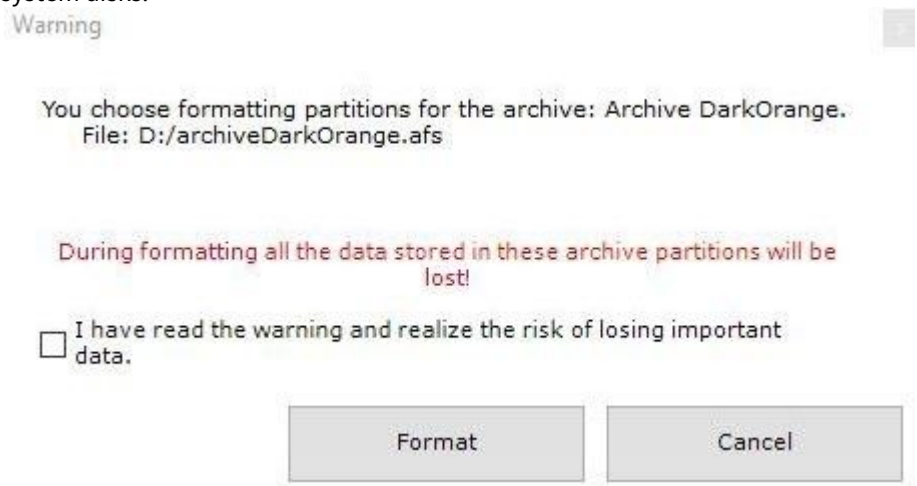


91 https://support.microsoft.com/en-us/windows/create-and-format-a-hard-disk-partition-bbb8e185-1bda-ecd1-3465-c9728f7d7d2e

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.

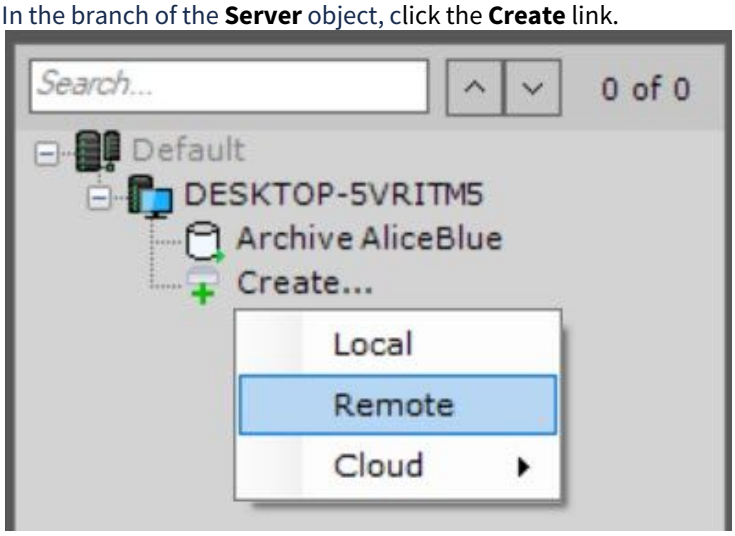
Creation of the local archive is now complete.

15.3.4.2 Creating a remote archive

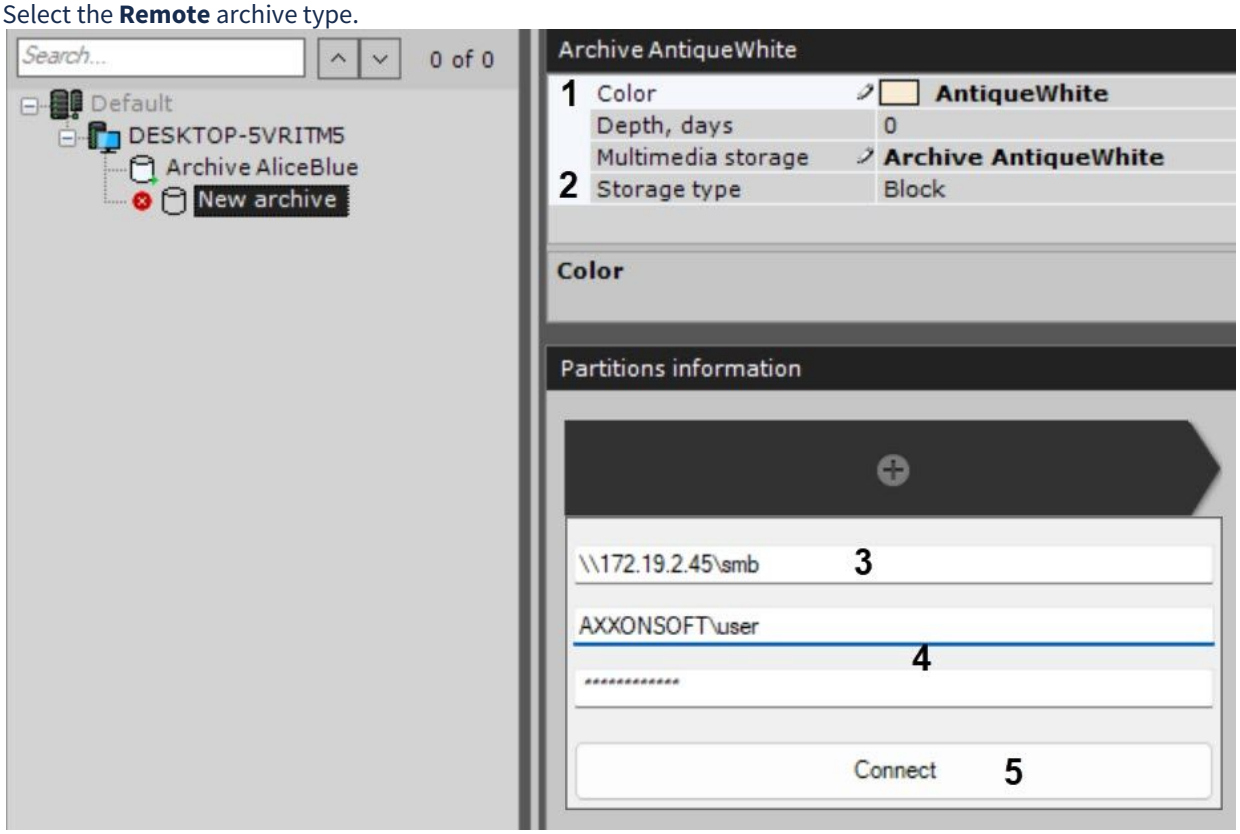
A remote archive can only be a file on one or several remote storages.

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 a technical support specialist recommended you to use this type of storage.

   > **Attention!**
   >
   > It is not recommended to use object type of storage without prior consultation with AxxonSoft technical specialist.

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(see page 599)), 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.

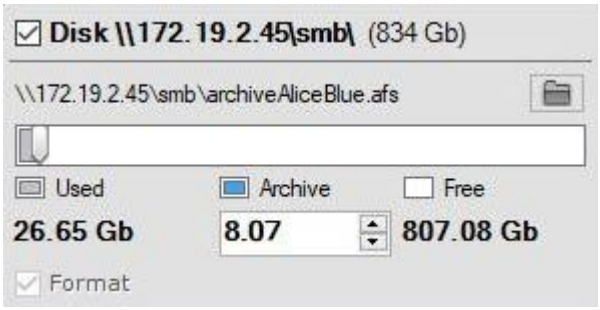
   > **Attention!**

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[92] command.
   2. Use PsExec[93] 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.

   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 remore archive is complete. After the archive is created, the status of the remote storages, where the archive is located, will be displayed.

15.3.4.3 Creating an archive based on existing archive volumes

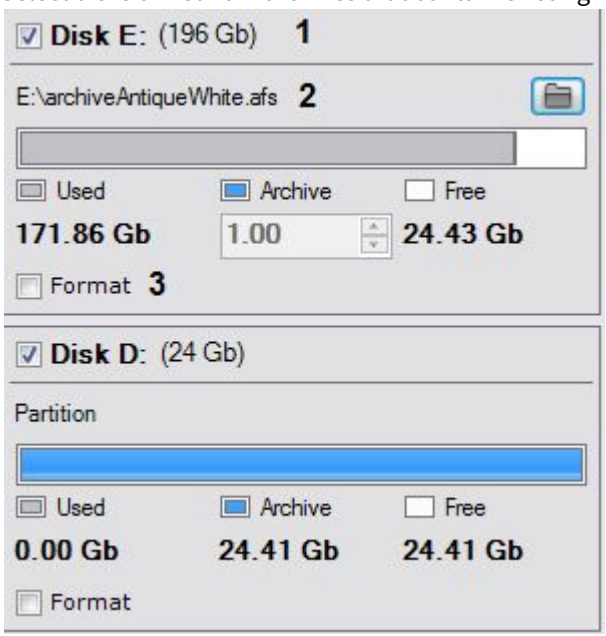
If an archive is created from an existing volume, it will be possible to extract saved video from the file only if the following conditions are met:

92 https://technet.microsoft.com/en-us/library/bb490717.aspx
93 https://docs.microsoft.com/en-gb/

- 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(see page 209)).
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.

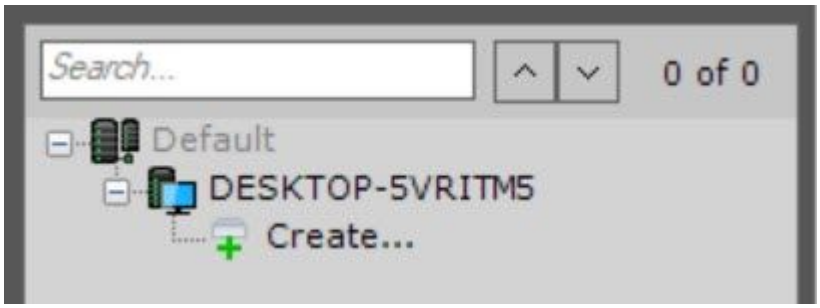
5. If necessary, create new archive volumes on free partitions.
6. Click the **Apply** button.

The archive is created and, if all requirements are met, the archive recordings are available.

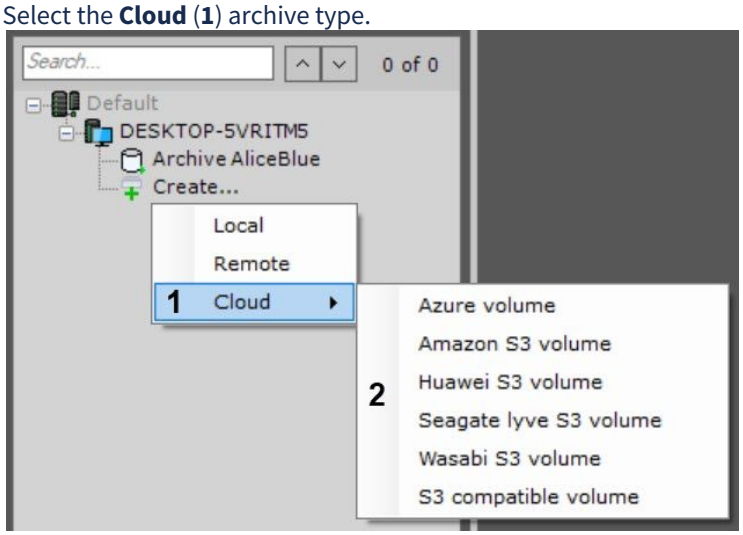
15.3.4.4 Creating a cloud archive

You can create a cloud archive through the interface of archive creation. To do this, do the following:

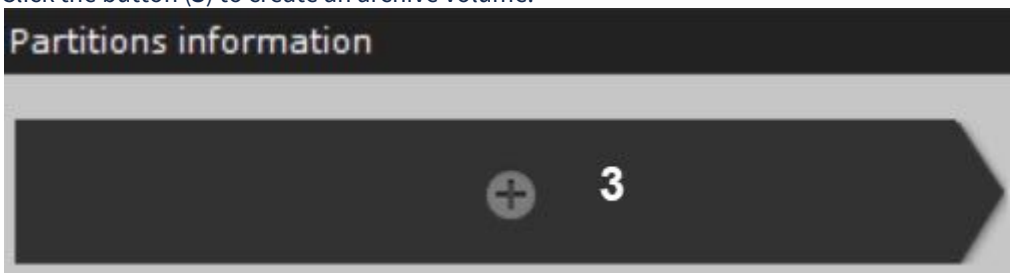
1. In the branch of the **Server** object corresponding to the computer on which you need to organize an archive, click the **Create** link.



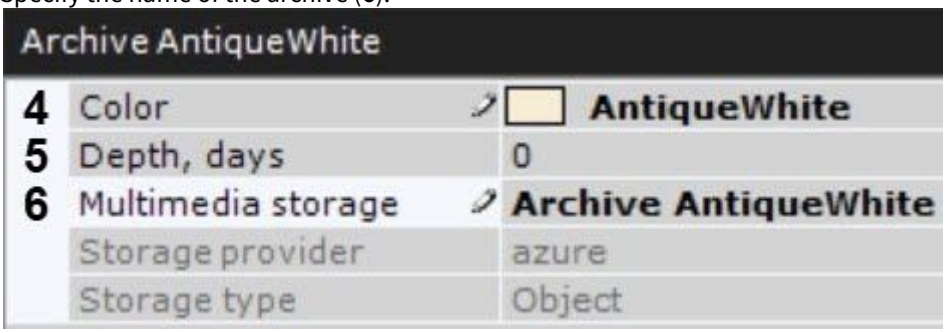
2. Select the **Cloud** (**1**) archive type.



3. Select an archive from the suggested solutions (**2**).
4. Click the button (**3**) to create an archive volume.

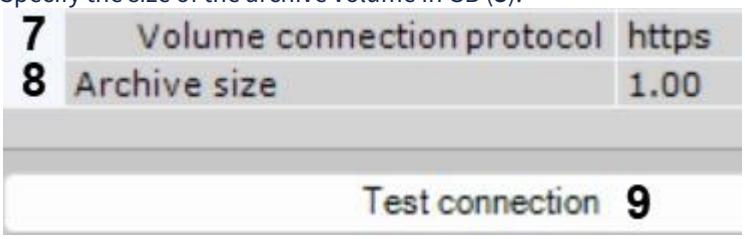


5. Specify general parameters for archive volumes:
   a. Specify the color of the archive (**4**).
   b. Specify the depth of the archive in days (**5**). If the value is set to **0**, the entire archive will be available for viewing.
   c. Specify the name of the archive (**6**).



   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.

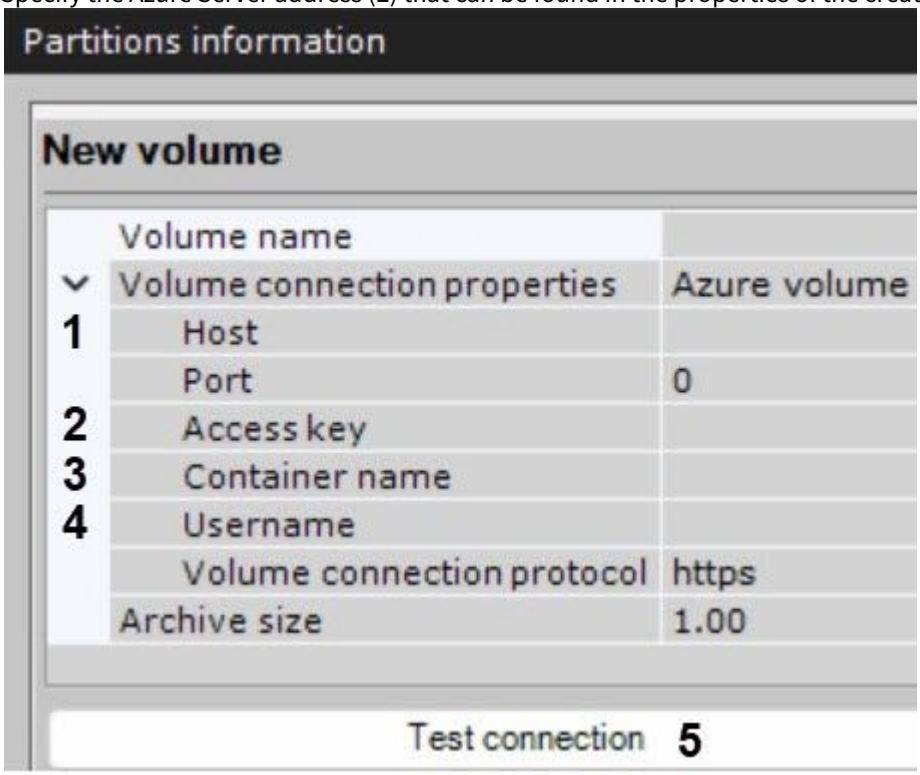
Manage archives using gRPC API (ConfigurationService)[94]

15.3.4.4.1 Configuring an archive volume based on the Microsoft Azure solution

General information about the cloud archive(see page 208)

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(see page 214)).
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[95] section.
4. Specify the Azure container (**3**) that can be found in the properties of the created container.

94 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=246487079
95 https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal

5. Specify the username (**4**) that can be found in the Access keys[96] 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

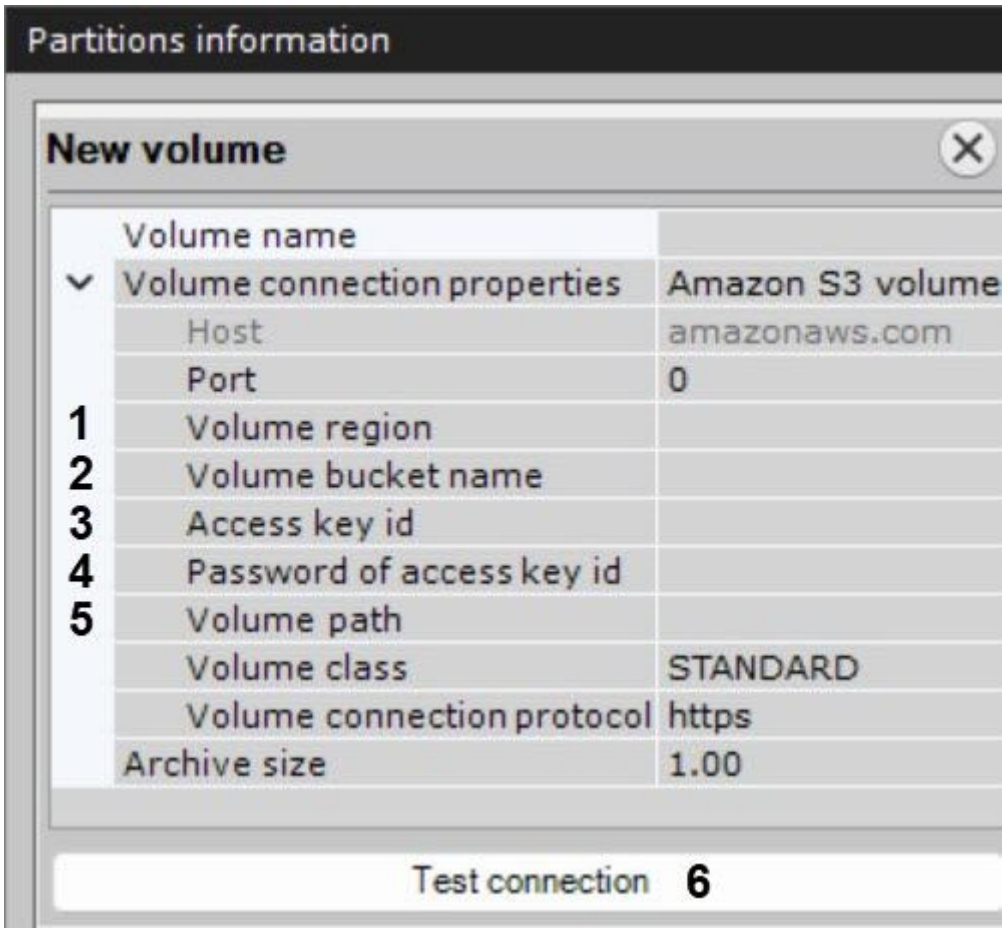
15.3.4.4.2 Configuring an archive volume based on the Amazon solution

General information about the cloud archive(see page 208)

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(see page 214)).
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[97]

96 https://learn.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal
97 https://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:

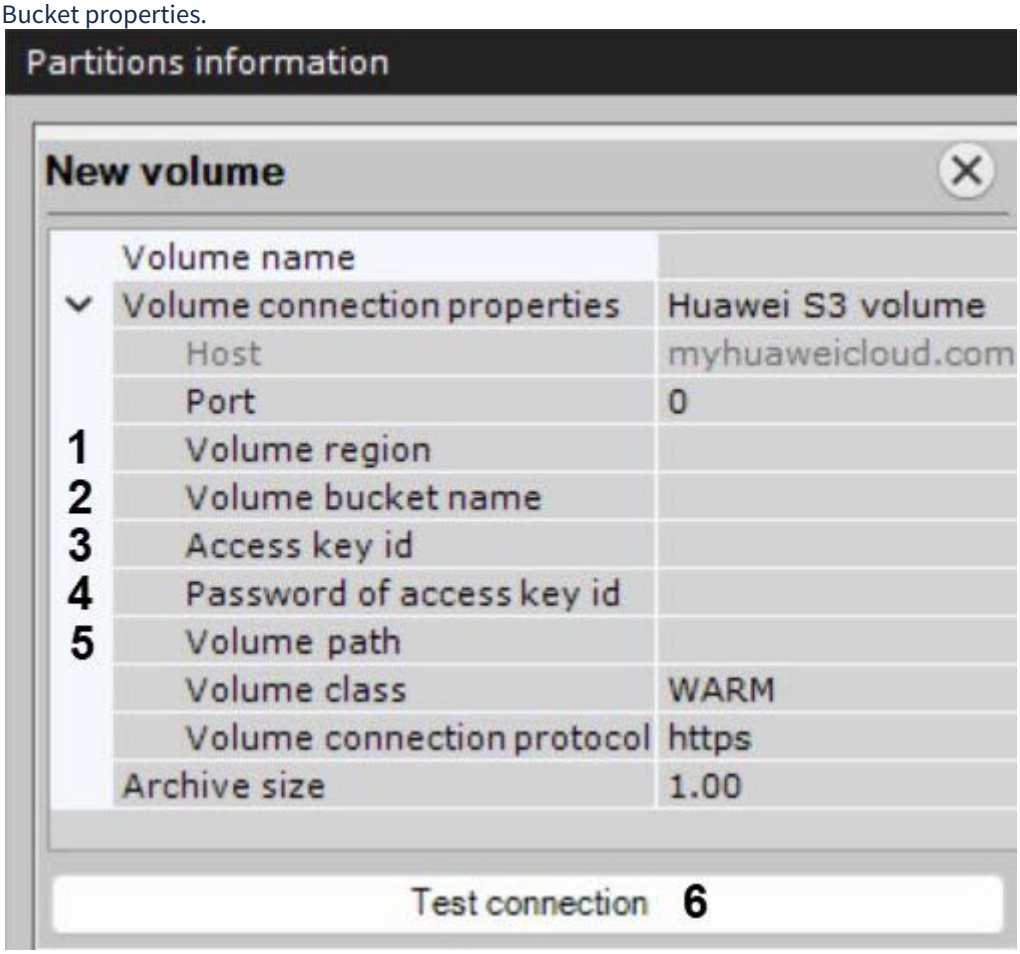
Parameter	Value
Volume region	us-west-1
Volume bucket name	axxonsoft-test
Access key id	youraccesskeyid
Password of access key id	yoursecretaccesskey
Volume path	path

15.3.4.4.3 Configuring an archive volume based on the Huawei Cloud solution

General information about the cloud archive(see page 208)

You must fill in the following fields for an archive volume based on the Huawei Cloud solution:

1. Specify the general parameters for an archive volume (see Creating a cloud archive(see page 214)).
2. Specify the region of the volume storage (**1**) that is set during its creation and specified in the Endpoint parameter in the Bucket properties.



3. Specify the name of the archive partition (Bucket Name) previously set by the user on the Object Storage Service tab (**2**).
4. Specify the access key id that you must create by clicking the “Obtain access keys (AK and SK)” link (**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 (**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 Huawei Cloud solution is complete.

Example of configuring a volume of a cloud archive in Huawei Cloud:

Parameter	Value
Volume region	ap-southeast-1
Volume bucket name	axxon-test-1

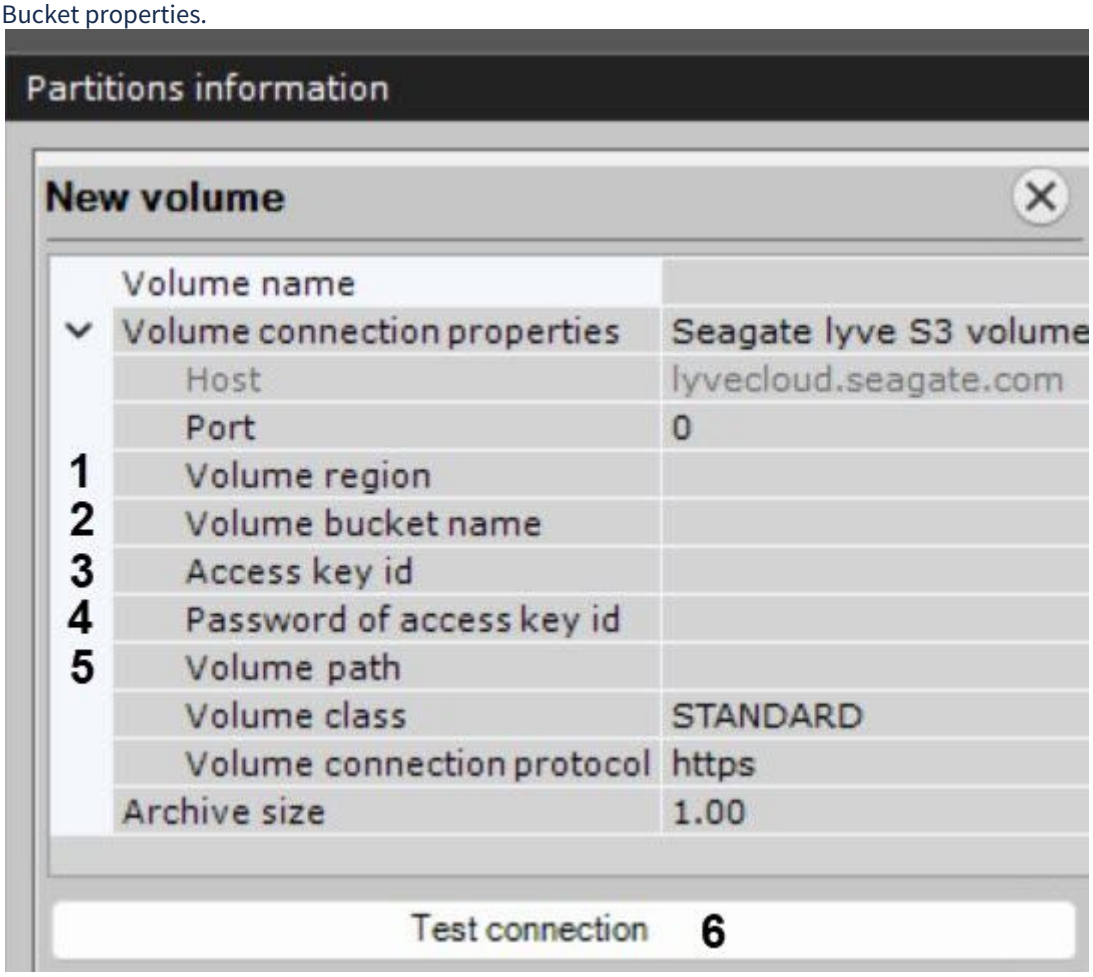
Parameter	Value
Access key id	youraccesskeyid
Password of access key id	yoursecretaccesskey
Volume path	path

15.3.4.4.4 Configuring an archive volume based on the Seagate Lyve Cloud solution

General information about the cloud archive(see page 208)

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(see page 214)).
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:

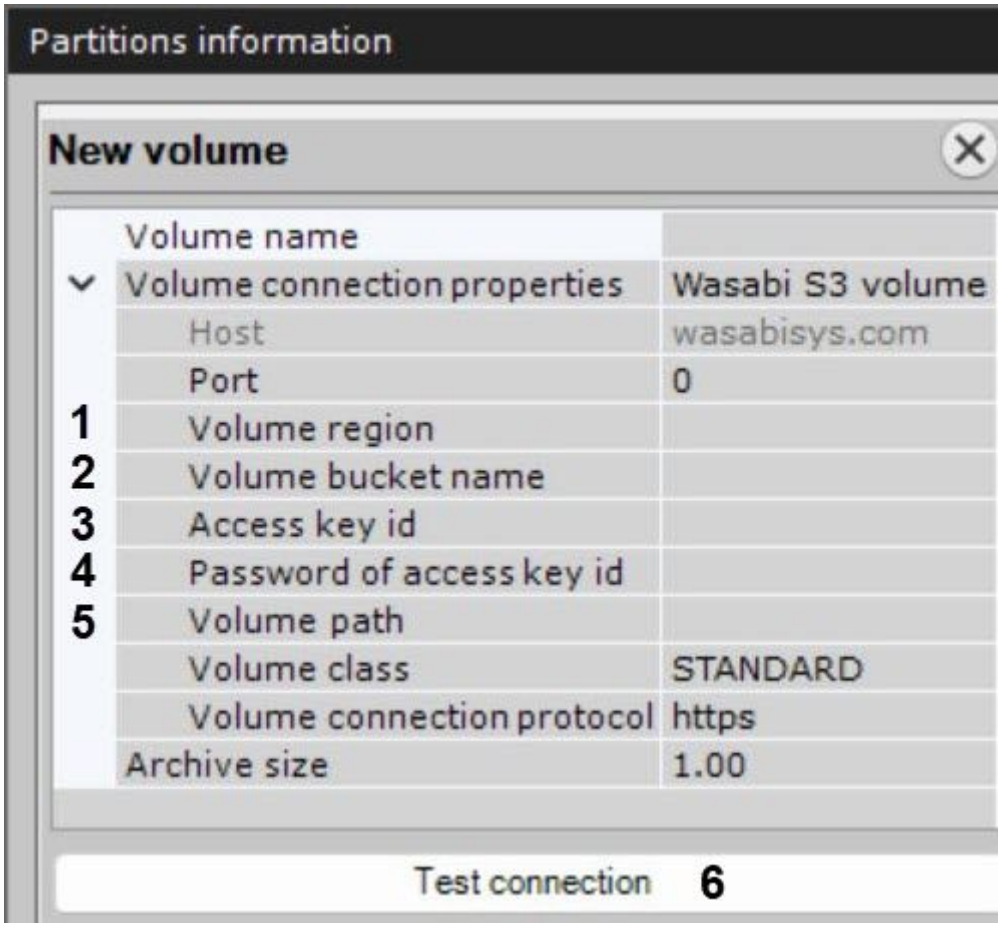
Parameter	Value
Volume region	us-west-1
Volume bucket name	axxonsoft-test
Access key id	youraccesskeyid
Password of access key id	yoursecretaccesskey
Volume path	path

15.3.4.4.5 Configuring an archive volume based on the Wasabi solution

General information about the cloud archive(see page 208)

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(see page 214)).
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[98] on the Wasabi website.



98 https://wasabi.com/locations/

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

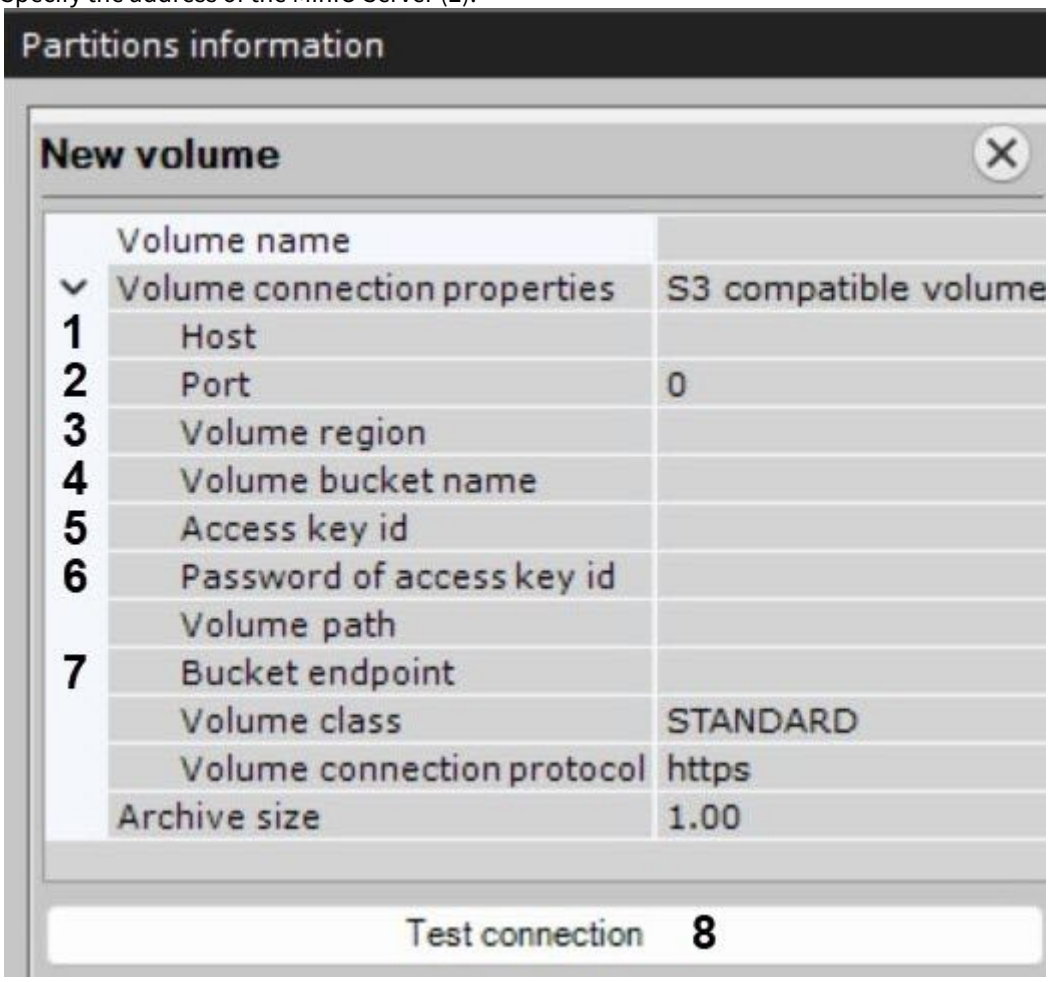
15.3.4.4.6 Configuring an archive volume based on the MinIO solution

General information about the cloud archive(see page 208)

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(see page 214)).

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/

15.3.5 Configuring recording to an archive

Video and audio streams are recorded synchronously.

You can configure recording to the archive both for one video camera, and for several, using the same parameters.

To configure recording to the archive of one video camera, do the following:

1. Select the created archive.
2. Set the checkbox next to the camera for which you want to configure the archive recording (**1**).

3. Configure the parameters for archive recording:
   a. From the **Constant recording** list (**2**), select the archive recording mode.
      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(see page 541)), 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 configuring the archive depth for each camera, it is recommended to calculate the storage capacity of an archive (see Disk storage subsystem requirements(see page 48)) to avoid the situations when the archive is stored for fewer days than specified.
When specifying the archive depth for a particular camera, note that the priority of the total archive depth is higher (see Configuring access restrictions to archive(see page 227)). 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 should 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(see page 418)).

d. If it is necessary to use decimation when recording to the archive, select the required value from the **Recording frame key only** list (**5**): **By keyframes** (for all video streams except MJPEG), or **1/0,5/0,25 FPM** (frames per minute). Decimation reduces the size of the archive, but the video will be less "smooth".

e. Select a stream for archive recording (**6**).

Note

This setting is relevant for cameras that support multistreaming.

4. Click the **Apply** button.

To configure recording to the archive of several cameras, do the following:

1. Set the checkboxes next to the cameras for which you want to configure archive recording. To select all cameras, set the **Select all** checkbox.

2. Configure the settings for the archive recording for a group of cameras (marked with yellow). The specified settings will be 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.

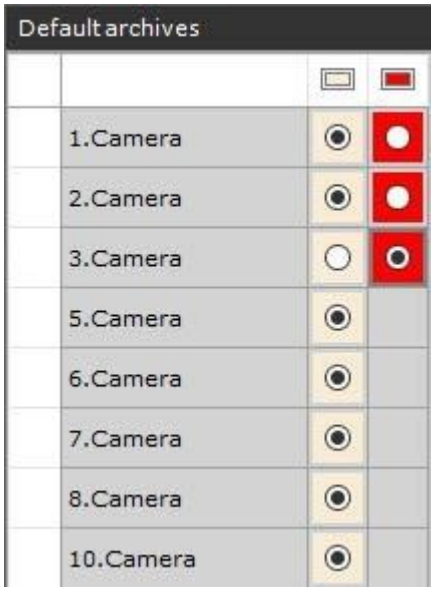
15.3.6 Setting the default archive

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(see page 224)).

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.

15.3.7 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:

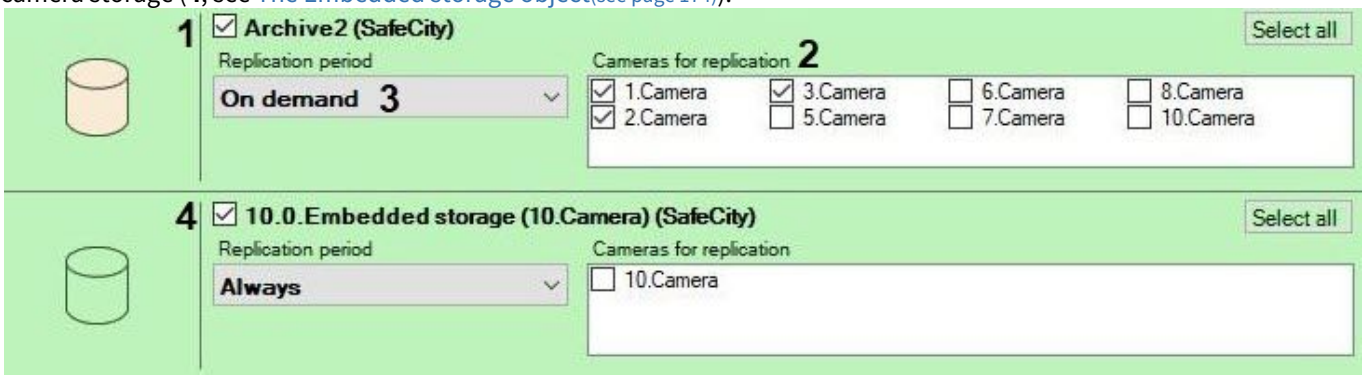
1. Replicate the data from **Archive 1** to **Archive 2**, while **Archive 2** cannot be written to.
2. Configure the camera to write to **Archive 2**.

The events indicating the start and successful completion of data replication will be generated in the system (see Event control(see page 818)). These events can be used in macros (see Configuring macros and counters(see page 400)).

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(see page 174)).



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(see page 541)). 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(see page 712), Start replication(see page 429)).

> **Attention!**
>
> If you change the replication period in an existing replication archive, the archive records for the previous period will be deleted.

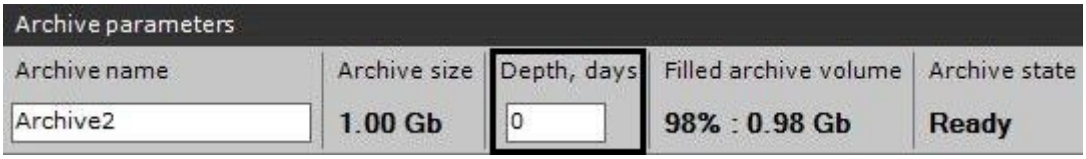
5. Click the **Apply** button.

Configuring data replication is complete. If the replication period was set to **Always**, data replication starts immediately after the settings are applied.

15.3.8 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.

15.3.9 Editing archives

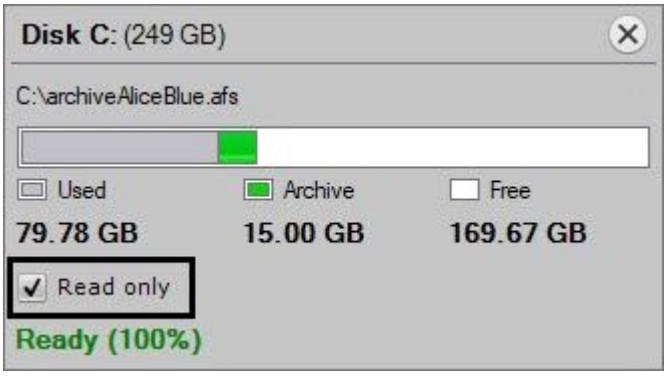
You can edit the archives that have been created in the system. You can do the following:

1. Rename an archive (see Creating archives(see page 209)).
2. Add new volumes. You can add new volumes in the same way as when creating an archive (see Creating archives(see page 209)).
3. Configure a write limit on the archive volume(see page 228).
4. Delete and format archive volumes(see page 231).
5. Change settings for archive recording (see Configuring recording to an archive(see page 224)).
6. Change replication settings (see Configuring data replication(see page 226)).

15.3.10 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.

15.3.11 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:

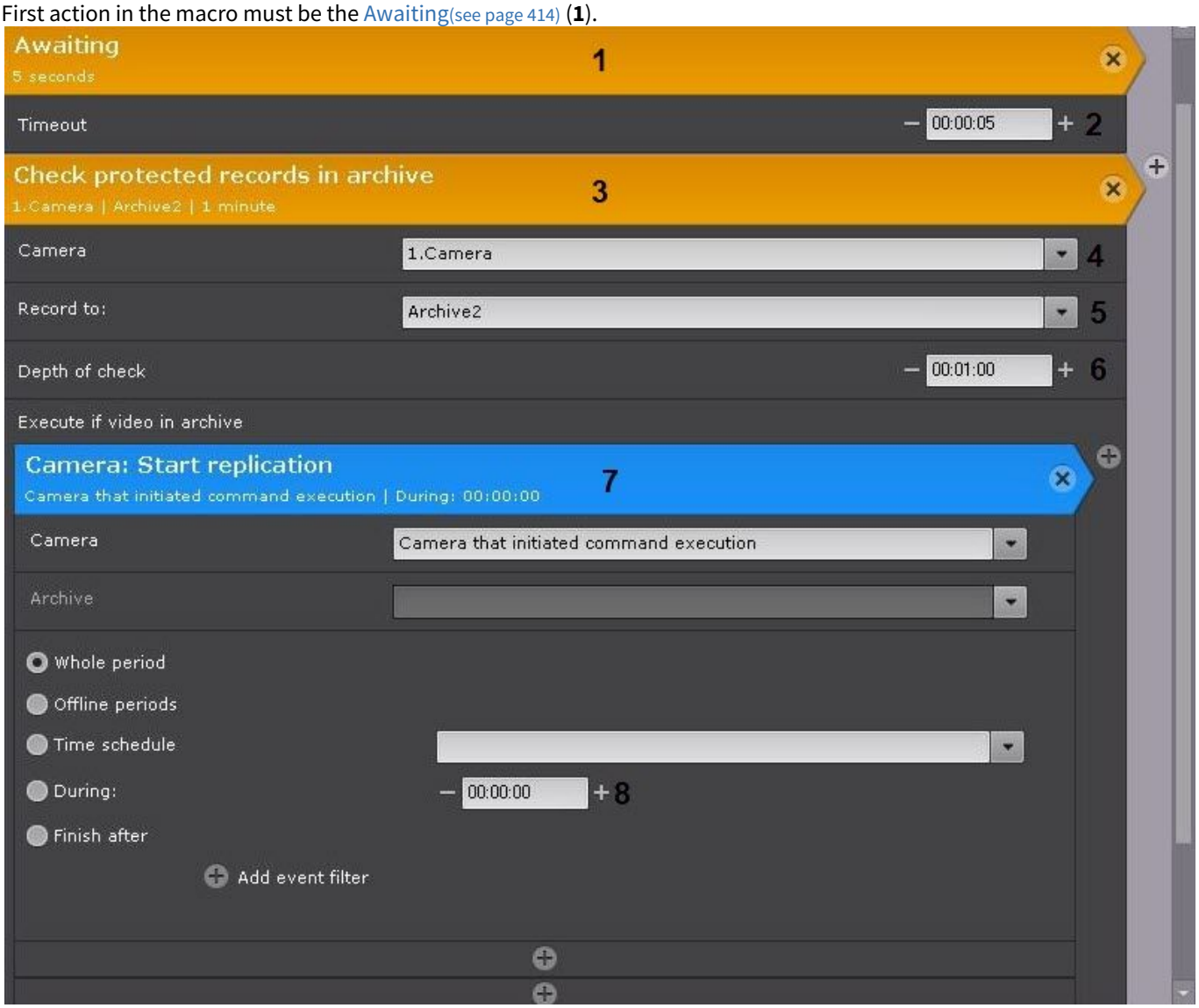
1. Configure on-demand replication (see Configuring data replication(see page 226)).
2. Configure a macro (see Setting up a macro for automatic copying of protected records(see page 229)).
3. Configure protection for necessary videos (see Setting up record protection(see page 230)).

You can further edit the list of protected recordings through the web client.

15.3.11.1 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(see page 400)) as follows:

1. First action in the macro must be the Awaiting(see page 414) (**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(see page 225)).
   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(see page 429)).
   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.

15.3.11.2 Setting up record protection

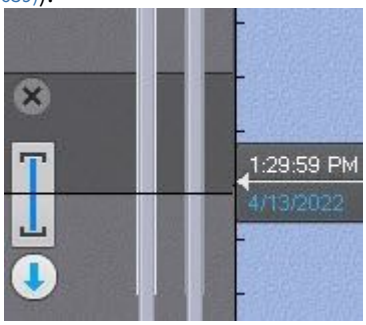
To protect a record, create a bookmark – a special case of the operator comment (see Operator comments(see page 667)).

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(see page 695)).

   > **Note**
   >
   > If you need to protect the same time interval in multiple camera archives, switch the necessary cameras to the archive mode.

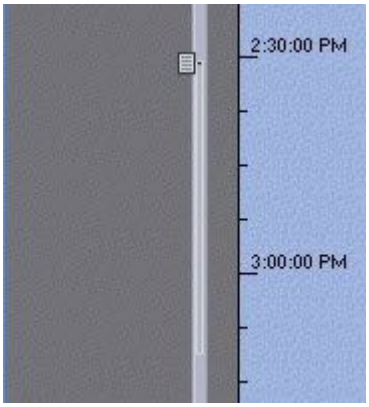
2. Set the protected time interval on the timeline in the archive with the and buttons (see The Timeline(see page 639)).

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.

15.3.12 Increasing capacity of an archive volume

You can increase the capacity of an archive volume.

15.3.12.1 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(see page 100)).
2. Use the Windows disk management utility to increase[99] volume capacity.
3. Start the Server (see Starting a Server(see page 94)).

15.3.12.2 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(see page 897)).

15.3.12.3 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(see page 214)), and via gRPC API (see Resize cloud archive using gRPC API methods[100]).

15.3.13 Removing archive volumes

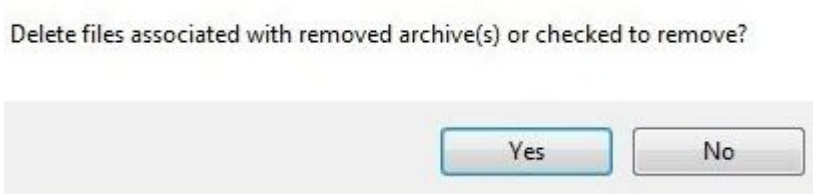
You can remove archive volumes.

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.

99 https://docs.microsoft.com/en-us/windows-server/storage/disk-management/extend-a-basic-volume
100 https://docs.axxonsoft.com/confluence/display/one20en/Resize+cloud+archive+using+gRPC+API+methods

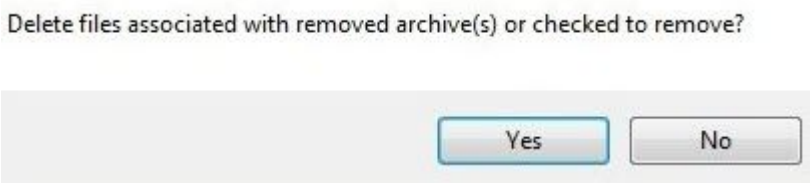
If you do not delete archive files, you can re-use them to create another archive (see Creating an archive based on existing archive volumes(see page 213)). You can also use a partition to re-create an archive.

Removing an archive volume is complete.

15.3.14 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!

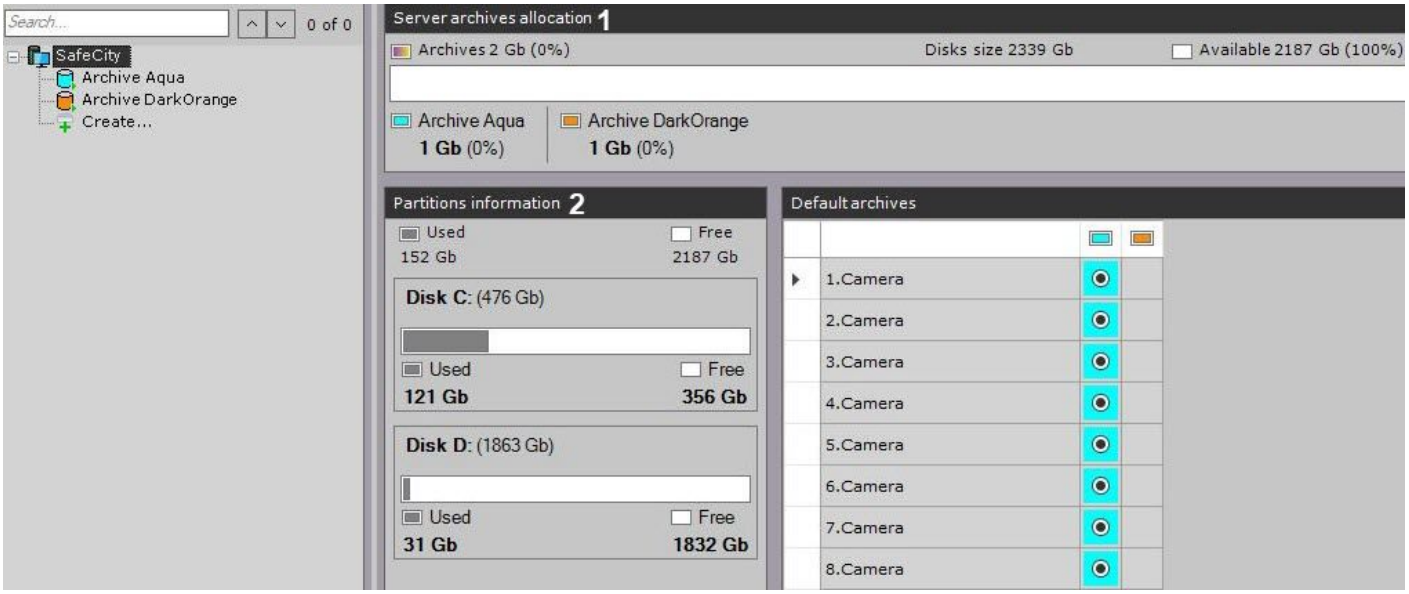
If you remove the archive files, then all the video footage that they contained will be lost.
If you do not remove the archive files, you can re-use them to create another archive (see Creating an archive based on existing archive volumes(see page 213)). You can as well use a partition to re-create an archive.

Removing an archive from the system is now complete.

15.3.15 View information about the size of archives and Server disk space

Selecting a **Server** object displays statistical information about the available Server disks and created archives.

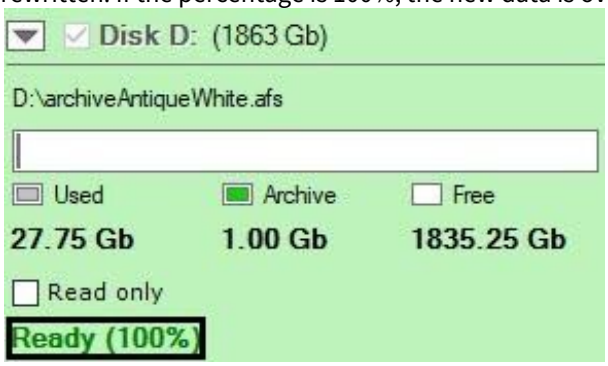
Figure (**1**) shows the overall balance of free disk space between the Server archives.



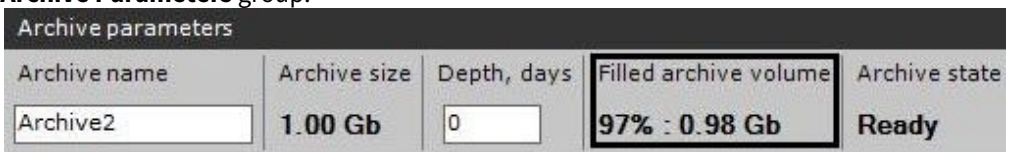
In addition, a list of disks is displayed, containing information about the total disk capacity, space used, and total free space (**2**).

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.

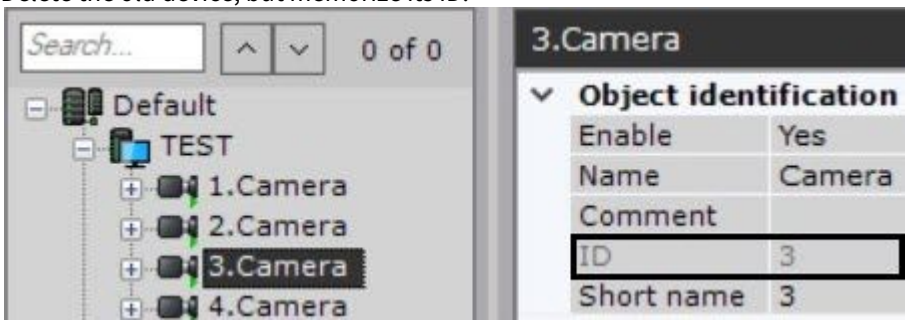
Reindexing progress bar is displayed.

15.3.16 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 Adding and removing IP devices(see page 112)).

> **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.

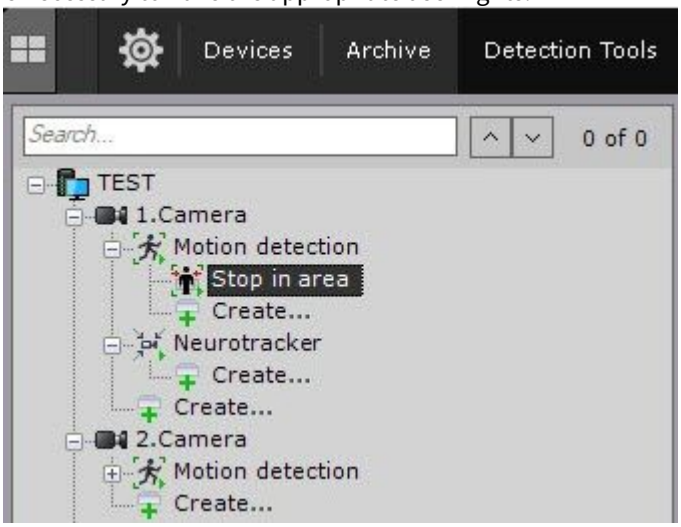
15.4 Configuring detection tools

15.4.1 General Information on Configuring Detection

In the *Axxon One* software package, several types of detection tools process incoming data:

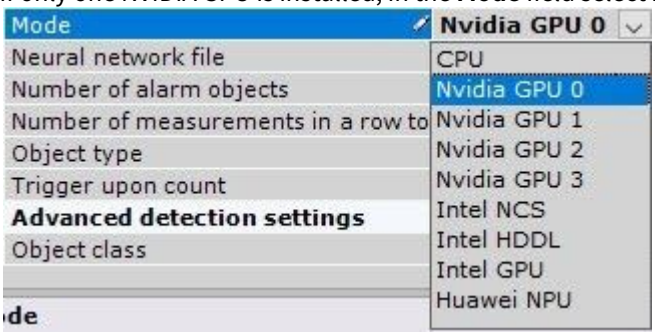
1. Face detection.
2. License Plate Recognition.
3. Trackers.
4. Pose detection.
5. Personal protective equipment detection tools.
6. Person-based privacy masking.
7. Privacy masking detection tool.
8. Fire detection and smoke detection.
9. Water level detection.
10. Motion in area detection.
11. Retail analytics:
    a. Queue detection.
    b. Visitors counter.
    c. Neurocounter.
12. Service detection:
    a. Audio detection.
    b. Tampering detection.
13. Embedded detection (IVA).

Detection tools are configured using the **Detection Tools** tab interface (within the **Settings** tab). To configure detection tools, it is necessary to have the appropriate user rights.



When configuring the detection, in the **Mode** field, select NVIDIA GPU one by one.

If only one NVIDIA GPU is installed, in the **Mode** field select **Nvidia GPU 0**.



If more than one NVIDIA GPU is installed, in the **Mode** field select the video card which should be used for detection.

It is possible to change the order of NVIDIA GPUs display using the CUDA_DEVICE_ORDER system variable (see Appendix 10. Creating system variable(see page 951)) by specifying the required value:

1. The FASTEST_FIRST value numbers the GPUs from the most powerful card to the less powerful ones, i.e. **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, i.e. **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 a command line as an administrator.
2. In the command line type the nvidia-smi query.
3. Press **Enter**.

The command line window will display information about the installed NVIDIA GPUs.

```
Administrator: Command Prompt

Microsoft Windows [Version 10.0.19044.1706]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>nvidia-smi
Thu Jun 09 12:02:45 2022
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 457.09       Driver Version: 457.09       CUDA Version: 11.1     |
|-------------------------------+----------------------+----------------------+
| GPU  Name            TCC/WDDM | Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  GeForce GT 710     WDDM  | 00000000:01:00.0 N/A |                  N/A |
| 50%   50C    P8    N/A /  N/A |    692MiB /  1024MiB |     N/A      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+

C:\WINDOWS\system32>
```

Attention!

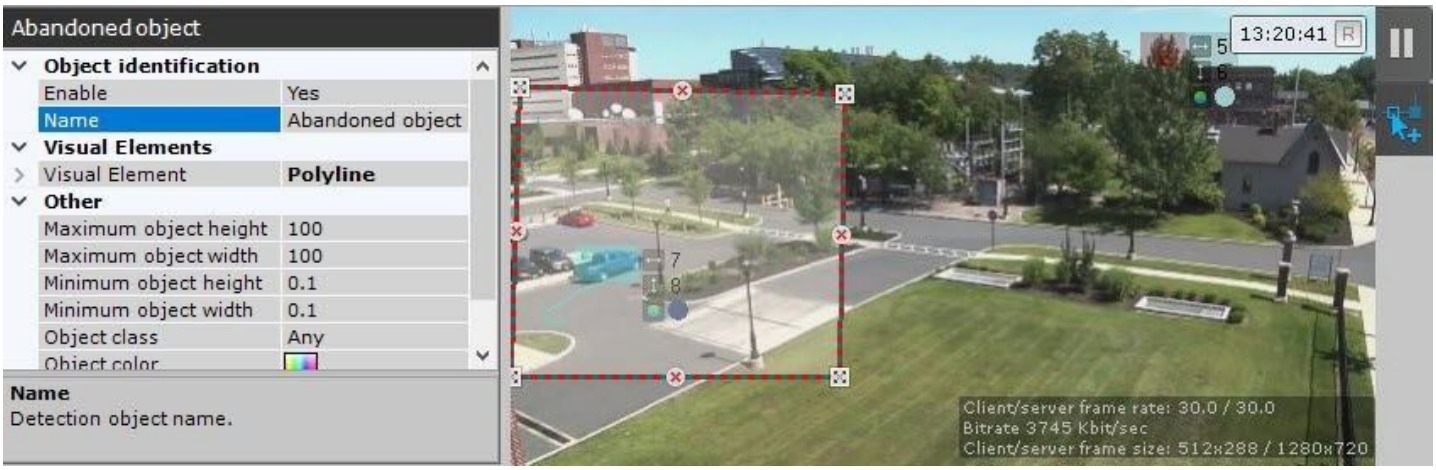
If you select a non-installed NVIDIA GPU in the **Mode** field, detection will not be performed.

For a video camera and its corresponding branch to appear in the detection tools list, the camera should be enabled in *Axxon One*.

Note

By default, camera inputs that can be activated through an automatic rule are displayed on the list of detection tools.

In the viewing tile, on the right side of the detection configuration window, you can set visual parameters.



> **Note**
>
> The indicator in the upper right corner displays the current time and recording status (see Time Display(see page 631)).

The default system setting to a detection event is not to trigger any response actions. To set system response, create an automatic rule or a macro (see Configuring macros and counters(see page 400), Automatic Rules(see page 399)).

15.4.2 General information on metadata

Metadata is information that describes object-related content in the camera FOV.

In *Axxon One* metadata can be obtained in two ways:

1. By analyzing video stream on Server by detection tools.
2. By receiving metadata from camera built-in analytics (see Embedded Detection Tools(see page 393)).

> **Attention!**
>
> To extract metadata from video, you have to de-compress and analyze the video stream, which increases the Server's workload, thus limiting the number of available camera channels.

The following tools are used for server-side analysis and metadata generation:

1. Object Tracker(see page 260).
2. Neural Tracker(see page 274).

   > **Note**
   >
   > Object tracker and Neural Tracker generate metadata containing the following information about moving objects in FOV: object type, position, size and color, motion speed and direction, etc.

3. VMD(see page 277).

   > **Note**
   >
   > VMD generates less accurate data. It does not detect object type and color.

4. Face detection tools(see page 278).

   > **Note**
   >
   > Face detection metadata contains face bounding boxes and their positions, as well as face vectors.

5. Automatic Number Plate Recognition (LPR/ANPR) tools(see page 308).

   > **Note**
   >
   > ANPR metadata contains license plate bounding boxes and their positions, as well as vehicle registration numbers.

6. Pose detection(see page 373).

   > **Note**
   >
   > Metadata from pose detection tools contains information on positions and pose (skeleton) of all people in FOV.

7. Personal protective equipment detection tools(see page 355).

   > **Note**
   >
   > Equipment detection metadata contains information about the position of all the people in FOV.

The metadata is used for the following system options:

Option	Required source of metadata
Scene Analytics(see page 260)	Object Tracker(see page 260), Neural Tracker(see page 274), Embedded Detection Tools(see page 393), or VMD(see page 277)
Forensic search MomentQuest(see page 730)	Object Tracker(see page 260), Neural Tracker(see page 274), Embedded Detection Tools(see page 393), VMD(see page 277), Face detection tools(see page 278), Automatic Number Plate Recognition (LPR/ANPR) tools(see page 308), Pose detection tools(see page 371), Personal protective equipment detection tools(see page 355)
Face search(see page 744)	Face detection tools(see page 278)
LPR search(see page 741)	Automatic Number Plate Recognition (LPR/ANPR) tools(see page 308)
TimeCompressor(see page 699)	Object Tracker(see page 260), Neural Tracker(see page 274), Embedded Detection Tools(see page 393), or VMD(see page 277)
Tag&Track Pro(see page 685)	Object Tracker(see page 260), Neural Tracker(see page 274), Embedded Detection Tools(see page 393), or VMD(see page 277)
Object tracking(see page 663)	Any
Autozoom(see page 691)	Any

Attention!

If a camera uses several sources of metadata, the required source is selected automatically, except for MomentQuest(see page 525).
To perform face/license number searches, only metadata from corresponding detection tools is used.

By default, metadata is stored as files in the object trajectory database in the local Server directory that was selected when installing *Axxon One* (see Installation(see page 62)) in the vmda_db\VMDA_DB.0\vmda_schema subfolder.

Note

If necessary, you can place metadata on any available network storage (see Configuring storage of the system log and metadata(see page 539)).

15.4.3 General information on Neural Analytics

The *Axxon One* VMS offers AI analytics based on neural networks. These AI tools include:

1. **Face detection tools** (see Face detection tools(see page 278)).
   Neural network detects faces.
2. **Automatic Number Plate Recognition (LPR/ANPR) tools** (see Automatic Number Plate Recognition (LPR/ANPR) tools(see page 308)).
   Neural network recognizes vehicle license plates.
3. **Neural Network Filter for Object Tracker** (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)).
   The neural network filter processes the results of the tracker and filters out false alarms on complex video images (foliage, glare, etc.).
4. **Neural Tracker** (see Setting up Neural Tracker-based Scene Analytics detection tools(see page 274)).
   Neural Tracker detects only objects of a specified class. The Neural Tracker is more accurate than the regular one, and detects even static objects, but it requires more computing resources.
5. **Neural Counter** (see Neural Counter(see page 344)).
   The Neural Counter relies on a neural network to work out the number of objects in the zone.

6. **Smoke and Fire Detection Tools based on Neural Network** (see Fire and Smoke Detection Tools(see page 349)).
   Neural network detects fire and smoke in FOV.
7. **Object detection** (see Object presence detection tool(see page 352)).
   Neural network is trained on a particular object that will be detected in the frame.
8. **Posture Detection based on Neural Network** (see Configure Pose detection tools(see page 373)).
   Neural network identifies each person's "skeleton" and detects poses that may represent a security threat.
9. **Equipment detection tool based on Neural Network** (see Personal protective equipment detection tools(see page 355)).
   Neural network detects the necessary equipment and PPE in the frame. Segmenting and classifying neural networks are used to operate the Equipment detection tool (PPE).
10. **Person-based privacy masking** (see Person-based privacy masking(see page 366)).
    Segmenting neural network is used to structure up an image of a human body.
11. **Privacy masking detection tool** (Privacy masking detection tool(see page 368)).
    Neural network detects and masks moving and stationary objects.
12. **Water Level Detection** (see Water Level Detection(see page 390)).
    The detection tool may use the neural network to detect water transparency and level.

Hardware requirements for neural analytics operation(see page 52)

15.4.3.1 Data collection requirements for neural network training

To train neural networks, it is necessary to collect and submit to AxxonSoft video recordings and images from your actual cameras taken in the same resolution and under the same conditions as in your future application.

For example, if your neural network is intended to analyze outdoor video feeds, your footage must contain all range of weather conditions (sun, rain, snow, fog, etc.) in different times of day (daytime, twilight, night).

General requirements for collected data:

- When collecting video recordings and images, specific requirements for object images, scene, angle, illumination and video stream are met for those detection tools that you plan to use (see Configuring detection tools(see page 234));
- If it is required to train the neural network in different conditions of time of day, lighting, angle, object types or weather, then the video material should be collected in equal shares for each condition, that is, it should be balanced.

Note

Example. It is necessary to detect a person in the surveillance area at night and during the day.
Data collected correctly:
- 4 video recordings of the surveillance area, each 5 minutes long;
- the object of interest appears in the frame in each video fragment;
- 2 fragments were recorded in night conditions, 2—in daytime conditions.

Data collected incorrectly:
- 3 video recordings of the surveillance area, each 5 minutes long;
- the object of interest appears in the frame in each video fragment;
- 2 fragments were recorded in night conditions, 1—in daytime conditions.

Extra requirements for video footage for each neural analytics tool are listed in the following table:

Tool	Requirements
Neural Filter	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)
Neural Tracker	3 to 5 minutes of video containing objects of interest in the given scene conditions. The more the number and variability of the situations in the scene, the better

Tool	Requirements
Posture detection tools	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 postures of an individual in scene (tilting, different limbs patterns, etc.)
Personal protective equipment detection tools	A list of all reference equipment with examples should be collected from the object and agreed with the analytics manufacturer (see Example of providing a list of valid equipment at the facility(see page 363)). Several video recordings 3-5 minutes each with personnel in the given scene conditions. Personnel should move and change posture in the collected video recordings, as well as remove and put on equipment at intervals of 30 seconds. Since the Personal protective equipment detection tools are designed for artificial constant lighting, video recordings in other lighting conditions are not required
Fire and Smoke detection tools	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)
Object presence detection tool	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)
Food recognition *	Images of at least 80% of the actual menu items should be provided. Each menu item requires 20 to 40 images shot in different conditions.

If the above requirements for the collection of data transmitted for training the neural network model are met, and if the neural network is operated in the conditions that are as similar as possible to the conditions in which the material for its training was collected, then the overall accuracy** of neural network analytics is guaranteed from 90% to 97% and the percentage of false positives is 5-7%. For general networks***, an overall accuracy of 80-95% and a false positive rate of 5-20% are guaranteed.

Note

* Will be available in future versions of *Axxon One*.
** Accuracy is indicated for a neural network model, which was trained under operating conditions.
*** A general network is a network that was not trained under operating conditions.

The requirements may be changed or added to at any time.

15.4.3.2 Optimizing the operation of neural analytics on GPU

It may take several minutes to launch neuroanalytics algorithms on NVIDIA GPU after Server restart. Meanwhile, the neuromodels 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(see page 74)), which allows you to create GPU 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 the neural analytics on GPU, do the following:

1. Stop the Server (see Shutting down a Server(see page 100)).

   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(see page 951)) 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.

> **Attention!**
>
> This function works in beta mode for all detection tools which use neuroanalytics (see General information on Neural Analytics(see page 238)), except Face detection(see page 280). To optimize Face detection(see page 280) operation using the GPU_CACHE_DIR system variable, you need to perform additional actions (see Optimizing the operation of Face detection on GPU(see page 284)).

3. To call the utility, open in the command line: C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe and press **Enter**.
4. Specify the ID of the required GPU (see General Information on Configuring Detection(see page 234)) and press **Enter**.

Optimizing the operation of the neural analytics on GPU is complete. The utility will create the caches of four 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 Neural Tracker (see Image Search(see page 756)).

```
C:\Program Files\Common Files\AxxonSoft\DetectorPack>NeuroPackGpuCacheGenerator.exe
Nvidia driver version: 517.40
Cuda driver version: 11.7
------------------------------
------------------------------
Available Devices:
   [ORDINAL]. [NAME] [UUID] [CUDA-CC] [CURRENT-FREE-GPU-MEM (MB)]
   0. [Quadro P2200] [GPU-5b904aa8-0bfb-b193-e05a-15408245a6ee] [6.1] [4751.51]
------------------------------
------------------------------
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: 0
------------------------------
Generating cache for "C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK\smokeScanned_v1_onnx.ann".
Generating cache for "C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK\fireScanned_v1_onnx.ann".
Generating cache for "C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK\GeneralNMHuman_v1.0GPU_onnx.ann".
Generating cache for "C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK\reid_15_0_256__osnetfpn_segmentation
_noise_20_common_29_onnx.ann".
------------------------------

Done!

C:\Program Files\Common Files\AxxonSoft\DetectorPack>
```

> **Attention!**
>
> The cache must be recreated in the following cases:
> - if you update the Neuro Pack add-ons (see Installing DetectorPack add-ons(see page 74)),
> - if you change the NVIDIA GPU model,
> - if you update the NVIDIA GPU drivers.

Creating GPU network caches using parameters:

1. **-p** is a parameter to create a cache for a particular network.
   Command example:

```
C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe -p
"<System disk>\<Network location directory>\Network_name.ann"
```

   To create a cache for multiple networks, list the paths to the selected networks, separated by a space.
   Command example:

```
C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe -p
"<System disk>\<Network location directory>\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 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>\<Network location directory>\Network_name.ann" -v
```

3. **--int8=1** is a parameter to create a quantized version of the cache for those networks for which quantization is available. By default, the **--int8=0** parameter is disabled.
Command example:

```
C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroPackGpuCacheGenerator.exe --
int8=1
```

> **Attention!**
>
> The networks for which the quantization mode is available are included in the Neuro Pack add-ons together with the *.info file.

The networks for which the quantization mode is available (see Setting up Neural Tracker-based Scene Analytics detection tools(see page 274)):

- GeneralNMCar_v1.0GPU_onnx.ann—vehicles.
- GeneralNMHuman_v1.0GPU_onnx.ann—human.
- GeneralNMHumanTopView_v0.8GPU_onnx.ann—human, top view.

Starting with *DetectorPack* 3.11, the following networks were added:

- GeneralNMHumanAndVehicle_Nano_v1.0_GPU_onnx.ann—human and vehicle (Nano).
- GeneralNMHumanAndVehicle_Medium_v1.0_GPU_onnx.ann—human and vehicle (Medium).
- GeneralNMHumanAndVehicle_Large_v1.0_GPU_onnx.ann—human and vehicle (Large).

15.4.4 Processors used for detection tools operation

Refer to the following table to check the compatibility of detection tools and processors.

Detection tool	Windows x64			Linux AMD64		
	CPU	GPU	VPU	CPU	GPU	VPU
VMD(see page 249)	✓	✓	⊖	✓	✓	⊖
Tampering detection tool(see page 252)	✓	⊖	⊖	✓	⊖	⊖
Service audio detection tool(see page 254)	✓	⊖	⊖	✓	⊖	⊖

Object Tracker(see page 260)	✓	⊖	⊖	✓	⊖	⊖
Neural Tracker(see page 274)	✓	✓	✓	✓	✓	✓
Neural network filter(see page 260)	✓	✓	✓	✓	✓	✓
Neurocounter(see page 345)	✓	✓	✓	✓	✓	✓
Face detection tools(see page 278)	✓	✓	⊖	✓	✓	⊖
VT Automatic Number Plate Recognition (see page 314)	✓	⊖	✓	✓	⊖	✓
RR Automatic Number Plate Recognition (see page 329)	✓	✓	⊖	✓	✓	⊖
IV Automatic Number Plate Recognition(see page 326)	✓	✓	⊖	✓	✓	⊖
BRS Automatic Number Plate Recognition(see page 334)	✓	⊖	⊖	✓	⊖	⊖
Smoke and Fire detection tools(see page 350)	✓	✓	✓	✓	✓	✓
Object presence detection tool(see page 353)	✓	✓	✓	✓	✓	✓
Pose detection tools(see page 373)	✓	✓	✓	✓	✓	✓
Retail analytics detection tools(see page 386)	✓	⊖	⊖	✓	⊖	⊖
Water level detection tool(see page 390) without using a neural network	✓	⊖	⊖	✓	⊖	⊖
Water level detection tool(see page 390) using a neural network	✓	✓	✓	✓	✓	✓
Personal protective equipment detection tools(see page 355)	✓	✓	✓	✓	⊖	⊖
Person-based privacy masking(see page 367)	✓	✓	✓	✓	✓	✓
Privacy masking detection tool(see page 368)	✓	✓	✓	✓	✓	✓

15.4.5 Creating detection tools

In *Axxon One*, you can create detection tools and their sub-tools (child detection tools). The sub-tools process data received from the parent detection tools.

Attention!

You cannot create detection sub-tools if the parent detection tools don't have the settings applied.

The following table lists all *Axxon One* detection tools and their sub-tools:

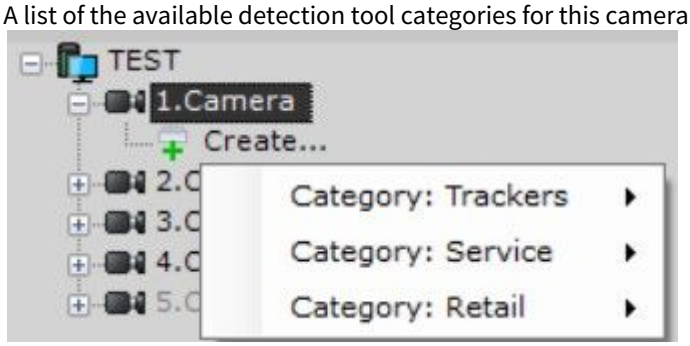
Category	Detection tool	Sub-tool
Face	Face detection(see page 280)	Line crossing(see page 268) Loitering(see page 272) Stop in area(see page 273) Motion in area Object Appearance in the Area Disappearance in area Multiple objects(see page 272) Move from area to area(see page 273) Masks detection(see page 291) (for Face detection only) Masks detection (for Face detection (VL) only)
	Face detection (VL)(see page 285)	
Vehicle	License Plate Recognition (VT)(see page 308)	Line crossing Loitering Stop in area Motion in area Object Appearance in the Area Disappearance in area Multiple objects Move from area to area
	License Plate Recognition (IV)(see page 324)	
	License Plate Recognition (RR)(see page 330)	
	License Plate Recognition—Search in archive (RR)(see page 330)	
	License Plate Recognition—Parking (RR)(see page 330)	
	Vehicle Recognition (RR)	
	License Plate Recognition (BRS)(see page 334)	
Service	Tampering detection(see page 251)	–
	Audio loss detection	
	Noise detection(see page 254)	
	Signal detection(see page 254)	
Trackers	Motion detection(see page 249)	Line crossing Loitering Stop in area Motion in area Object Appearance in the Area Disappearance in area Multiple objects Move from area to area Abandoned Object (for Object Tracker only)
	Neural Tracker(see page 274)	
	Object Tracker(see page 260)	
	Privacy masking(see page 368)	-

Category	Detection tool	Sub-tool
Poses	Pose detection(see page 373)	Only for the Pose detection: Sitting person detection(see page 375) Man down detection(see page 376) Hands up detection(see page 378) Handrail holding detection(see page 378) People counter(see page 379) Close-standing people detection(see page 381) People masking(see page 382) Common sub-tools: Line crossing Loitering Stop in area Motion in area Object Appearance in the Area Disappearance in area Multiple objects Move from area to area
	Equipment detection (PPE)(see page 358)	
	PPE detection (VL)(see page 355)	
	Person-based privacy masking(see page 366)	–
Natural environment	Fire detection(see page 349)	–
	Floating Objects Detector	
	Object detection(see page 352)	
	Smoke detection(see page 349)	
	Water level detection(see page 390)	
Retail	Queue detection(see page 386)	–
	Visitors counter(see page 388)	
	Neurocounter(see page 344)	
Other	Embedded Motion Detection	–
	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	

Category	Detection tool	Sub-tool
	Embedded License Plate Recognition	
	Embedded temperature detection	Face Detection and Temperature Control
	Embedded body temperature detection	–
	Tracker Analytics	Line crossing Loitering Stop in area Motion in area Object Appearance in the Area Disappearance in area Multiple objects Move from area to area
	Embedded analytics	
	Embedded AxxonSoft tracker	

To create detection tools, do the following:

1. Click the **Create** link in the corresponding video camera tree.
   A list of the available detection tool categories for this camera will be displayed.



2. Select the required detection tool.
3. Click the **Apply** button.

The detection tool is now created.

> **Note**
>
> Mass creation of the detection tools of the same type for the selected cameras is described in Mass creation of detection tools(see page 247).

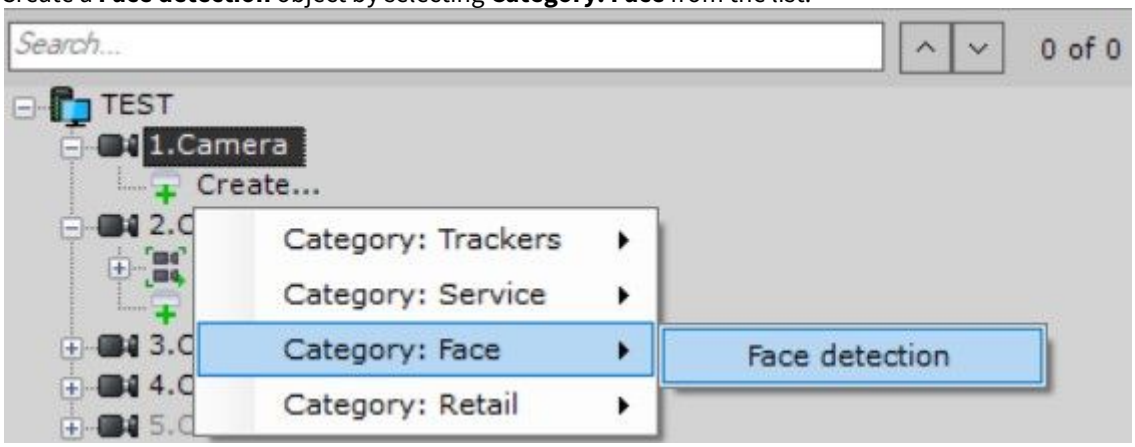
Several identical detection tools can work on the same camera stream:

Detection tools	The number of identical detection tools on the same video camera
Motion detection(see page 250), Neural Tracker(see page 274), Object Tracker(see page 274), Neurocounter(see page 345)	10
Water level detection(see page 390), Queue detection(see page 386), Visitors counter(see page 388), Masks detection(see page 291)	Unlimited

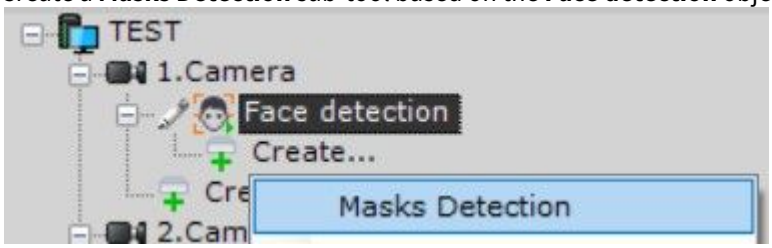
> **Attention!**
>
> For other detection tools and their detection sub-tools in *Axxon One* it is not possible to create the same detection tools and their detection sub-tools on the same video camera.

Example of creating a **Masks detection** sub-tool:

1. Create a **Face detection** object by selecting **Category: Face** from the list.



2. Create a **Masks Detection** sub-tool based on the **Face detection** object.



Other detection sub-tools are created in a similar way.

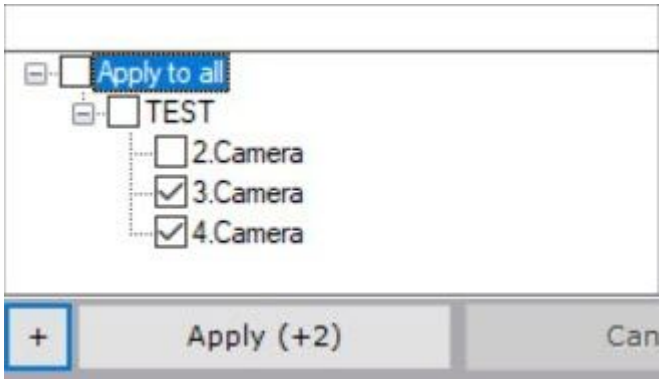
15.4.6 Mass configuration of detections tools

15.4.6.1 Mass creation of detection tools

You can create the same type of detection tool for several selected cameras with a few clicks.

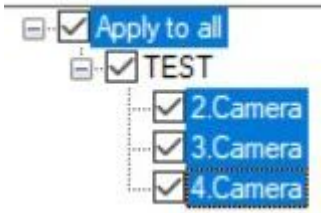
Please follow the steps below:

1. Create (see Creating detection tools(see page 243)) and configure the necessary detection tool or select an existing one in the object tree for one of the video cameras.
2. Click the + button and select other target cameras. If you add the second-level tool, then only those cameras that have the same tool at the first level will be listed.



To quickly select multiple cameras, hold down the Shift key, select the first and last cameras the newly created detection

tool should be applied to. Selecting any camera from highlighted ones will result in selecting them all.

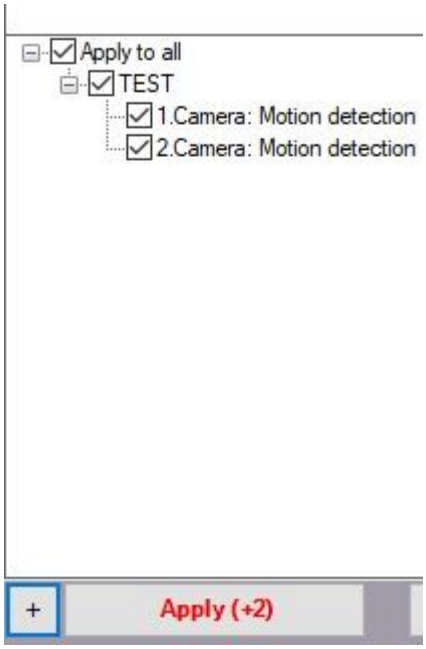


3. Click **Apply**. You can see the number of target cameras in brackets.

15.4.6.2 Mass configure detection tools

You can mass configure detection tools as follows:

1. Configure one detection tool.
2. Click the button + and select detections tools the same settings should be applied to.



> **Attention!**
>
> Detection zones cannot be changed by bulk configuration.

The list of detection tools of the same type in the current Axxon-domain opens. To select multiple detection tools, hold down the Shift key, select the first and last one the settings should be applied to. Selecting any tool from highlighted ones will result in selecting them all.

3. Click the **Apply** button.

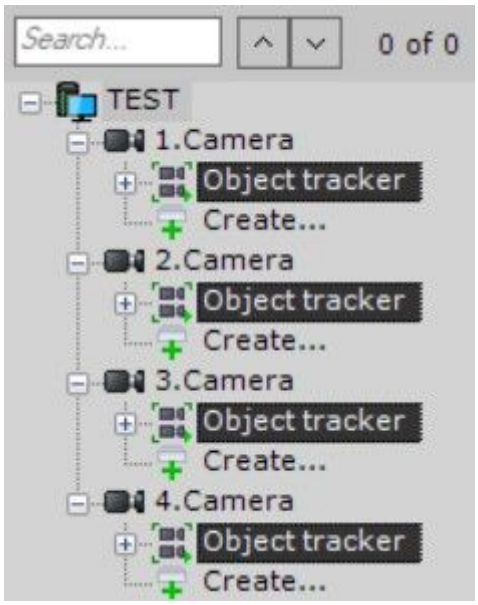
> **Note**
>
> The number in brackets refers to the number of configured detection tools.

15.4.6.3 Mass removal of tools

You can delete a bunch of detection tool for several selected cameras with a few clicks.

Please follow the steps below:

1. Press and hold the Ctrl key to select the tools in the object tree that you want to delete. Only detection tools of the same level be selected. For example, if you selected **Facial recognition tools**, you cannot then select **Cross Line detection** and vice versa.



2. Click **Delete** and then **Apply**.

15.4.7 VMD (video motion detection)

15.4.7.1 Video requirements for VMD

Motion detection runs properly if video match the following requirements:

1. Camera requirements:
   a. Resolution: Min. 320x240 pixels.
   b. Frames per second: Min. 1 fps.
   c. 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 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.
   c. The width and 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).

15.4.7.2 VMD features and specifications

The motion detection tool is triggered by motion in a video camera's field of view (FOV).

VMD metadata can be used in Scene Analytics detection tools (see Setting up VMD-based Scene Analytics detection tools(see page 277)).

15.4.7.3 Configuring VMD

Creating detection tools(see page 243)
General Information on Configuring Detection(see page 234)
Displaying information from a detection tool (mask)(see page 672)

To configure a VMD:

1. To record **Motion mask** to archive, set **Yes** for the corresponding parameter (**1**).

Motion detection	
Object features	
1 Record mask to archive	No
2 Record objects tracking	No
3 Video stream from camera	Low-quality video stream
Other	
4 Alarm end delay	10
5 Camera position	Wall
6 Decode only key frames	No
7 Decoder mode	CPU
8 Frames processed per second	20
9 Motion mask	Yes
10 Object tracking	No
11 Sensitivity: Contrast	12
12 Sensitivity: Size	9

2. The Video Motion Detection tool can receive tracking metadata generated by the Motion mask. The metadata are recorded into the database by default. To disable, select **No** in the **Record objects tracking** (**2**).
3. If a camera supports multistreaming, select the stream for which detection is needed (**3**). Selecting a low-quality video stream allows reducing the load on the Server.
4. In the **Alarm end delay** field, set a value in seconds for the time interval within which the detection tool remains triggered after motion stops (**4**). If motion is re-detected within this interval, no new event will be created.
5. To reduce false alarms rate from a fish-eye camera, you have to position it properly (**5**). For other devices, this parameter is not valid.
6. If necessary, enable the video stream grooming (**6**). In this case, only the I-frames will be decoded.

   Important

   This setting applies to all codecs. If a codec has keyframes and p-frames, the keyframe is decoded no more often than every 500 milliseconds. For the MJPEG codec, each frame is considered to be I-frame.
   This feature reduces the Server load but, as can be expected, negatively impacts the quality of detection.
   This setting should be activated on "blind" Servers (Servers that do not display video) on which it is necessary to perform detection.

7. Select a processing resource for decoding video streams (**7**). When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVidia NVDEC chips). If there's no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding.
8. Set the frame rate value for the detection tool to process (**8**). This value should be in the range [0,016; 100].
9. The VMD analyzes differences between the current frame and the static background (**11**, **12**). Depending on a particular scene, we recommend the following sensitivity values for contrast and size:
   a. Maximum sensitivity (street scenes where target objects are smaller):
      i. **Sensitivity: contrast** = 16.
      ii. **Sensitivity: size** = 10.

b. Medium sensitivity (default values for generic scenes):
   i. **Sensitivity: contrast** = 12.
   ii. **Sensitivity: size** = 9.
c. Low sensitivity (indoor cameras with an average distance to object of ca. 4m):
   i. **Sensitivity: contrast** = 8.
   ii. **Sensitivity: size** = 8.

   For your convenience with setting sensitivity value, in the preview window you can see the Motion mask. To disable it, select **No** in the **Motion mask** (**9**) field.

   If there is motion, but it does not exceed the threshold value (because of the detection sensitivity), the mask cells are colored green. If motion triggers VMD, the cells turn red.

10. To get tracked objects and their parameters (percentage of the FoV width/height, color) displayed in the Preview window, select **Yes** in the **Object tracking** field (**10**).
11. By default, VMD (video motion detection) covers the entire FoV. In the FoV, you can set exclude areas – closed areas, inside of which you want no detection.
    Exclude area are created similar to scene analysis configuration (see Setting General Zones for Scene analytics detection tools(see page 262)).
12. Click **Apply**.

VMD configuration is now complete.

Checking the Triggering of a Detection Tool(see page 398)

15.4.8 Tampering Detection

15.4.8.1 Functions of tampering detection

The camera tampering detection analyzes the video image to determine the nature of its change.

Name of detection tool analysis	Analysis result
Compression artifacts analysis	The detection triggers when compression artifacts appear on the image
Quality degradation analysis	The detection triggers when the video image received from a video camera loses quality. For example, the detection tool may trigger upon excessive light, loss of focus, lens blocking, or sudden drop in scene illumination.

Name of detection tool analysis	Analysis result
Image noise analysis	The detection triggers when video noise appears on the image For example, the detection tool may trigger upon low bit rate or ripples in the image (snow)
Scene change analysis	The detection triggers when the background of the video image changes, indicating a change in the position of the video camera in space
Blurred image analysis	The detection triggers when the blurred contours appear on the image. For example, the detection tool may trigger when the image is blurry due to a dirty lens.

15.4.8.2 Video requirements for tampering detection

To ensure the correct operation of the tampering detection, the following requirements should be met:

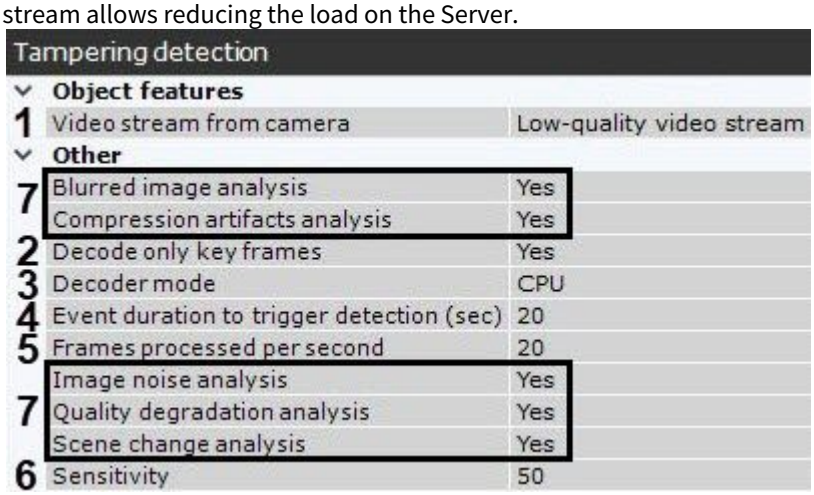
1. Camera requirements:
    a. Resolution: Min. 320x240 pixels.
    b. Frames per second: Min. 1 fps.
    c. Color: video analytics work with both black-and-white and color images.
    d. Camera shaking must not cause image shifting of more than 1% of the frame size.
2. Lighting requirements:
    a. 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 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.
    c. The width and 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).

15.4.8.3 Configuring tampering detection

Video requirements for tampering detection(see page 252)

To set up the Tampering detection, do the following:

1. If a camera supports multi-streaming, select the stream for which detection is needed (**1**). Selecting a low-quality video stream allows reducing the load on the Server.



2. The default setting for all detection tools is **Decode only key frames** (**2**). In this case, only key frames are decoded. To disable the decoding of key frames, select **No** in the corresponding field.

> **Attention!**
>
> This feature reduces the Server load but, as can be expected, negatively impacts the quality of detection.
> This setting should be activated on "blind" Servers (Servers that do not display video) on which it is necessary to perform detection.
> For the MJPEG codec, each frame is considered a key frame.

3. Select a processing resource for decoding video streams (**3**). When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there's no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding.
4. Set the frame rate value for each detection tool to process (**5**). This value should be in the range [0.016, 100].

> **Attention!**
>
> **Frames processed per second** and **Decode only key frames** parameters **are** correlated.
> If no local Clients are connected to a Server, the following rules are set for remote Clients:
> - If the interval between consecutive I-frames exceeds the value specified in the **Frames processed per second** field, the detection tool will process I-frames.
> - If the I-frame frequency is lower than the value specified in the **Frames processed per second** field, the detection tool will use the set value.
>
> If at least one local Client connects to the Server, the detection tool is forced to use the set value. After the local Client disconnects, the indicated rules become valid again.

5. Select one or more analyzes to be applied to the video image. If you select Blurred image analysis, Compression artifacts analysis, Image noise analysis, Quality degradation analysis, or Scene change analysis, configure the following parameters:
   a. **Event duration to trigger detection (sec)** is the maximum time of the event duration after which the detection tool will trigger (**4**). But, the detection tool can trigger even earlier if the algorithm undoubtedly determines the noise. If the detection tool does not trigger after the event duration time expires, it means that the corresponding image defect was not detected with the specified detector sensitivity (**6**).
   b. **Sensitivity** of detection tool operation in standard units from 0 to 100 (**6**).
6. To save settings, click the **Apply** button.

Tampering detection is now configured.

15.4.9 Service Audio Detection Tools

15.4.9.1 Functions of Service Audio Detection Tools

The following detection tools enable analysis of the audio signal from a microphone.

Name of a Detection Tool object	Detection description
Audio loss	A detection tool which is triggered by the line break from the microphone to the Server (complete absence of sound).
Signal detection	A detection tool which is triggered by the reception of an audio signal from an audio device.
Noise detection	A detection tool which is triggered by the appearance of noise.

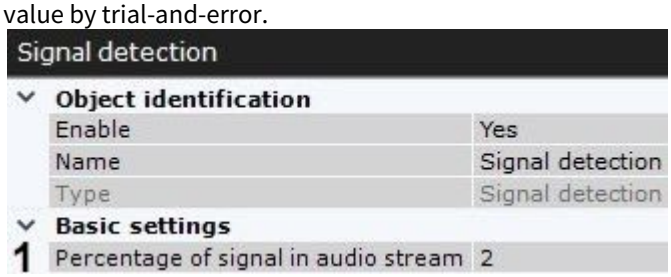
Attention!

Audio loss detection may operate incorrectly with video cameras emitting a background signal with a non-zero volume, even if the integrated microphone is physically disabled.

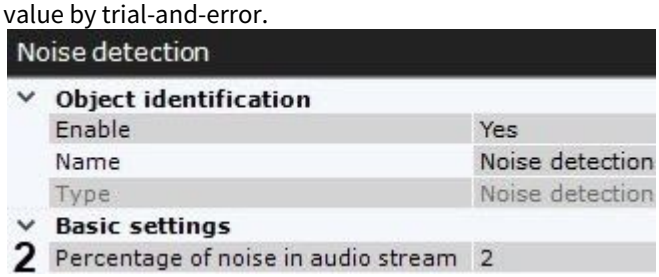
15.4.9.2 Set Parameters of Audio Detection

To set audio detection tools, do the following:

1. For the signal detection tool, set the threshold in percentage (**1**). The tool triggers on exceeding the threshold. Set the value by trial-and-error.



2. For the noise detection tool, set the threshold in percentage (**2**). The tool triggers on exceeding the threshold. Set the value by trial-and-error.



3. To save settings, click the **Apply** button.

Sound detection tools setup is complete.

15.4.10 Scene Analytics detection tools

15.4.10.1 General information on Scene Analytics detection tools

Axxon One uses two different trackers for moving objects detection and metadata calculation:

1. **Object Tracker** is a primary tool.
2. **Neural Tracker** is essentially the same but operates through neural networks. The neural one is more accurate and detects even static objects, but it requires more computing resources.

The Scene Analytics detection tools work with both trackers.

> **Attention!**
>
> The abandoned objects detection tool works only with the primary tracker.

When created, both **Object Tracker** and **Neural Tracker** objects are enabled by default. Tracked objects' parameters (relative width and height, color) are displayed in the camera window.

> **Note**
>
> Up to 25 objects can be tracked at the same time.

15.4.10.2 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 does 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 does is not triggered if an object disappears (or becomes idle) inside the area without crossing its perimeter (refer to **Stop in Area**).

Name of a Detection Tool object	Detection description
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(see page 74)).

15.4.10.3 Video requirements for scene analytics detection tools

15.4.10.3.1 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).

15.4.10.3.2 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(see page 259).

15.4.10.3.3 Video requirements for VMD-based scene analytics detection tools

For video analytics to work correctly, the following requirements must be met:

1. Camera requirements:
   a. Resolution min. 640x360.
   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).

15.4.10.3.4 Video stream and scene requirements for neural tracker operation

The neural tracker operation imposes the following requirements:

1. To the video stream from the camera:
   a. The resolution is at least 640x360 pixels. It is also not recommended to use a resolution higher than 1920×1080, since higher resolution does not increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 (see Examples of configuring neural tracker for solving typical tasks(see page 278)).
   b. The frame rate per second in the video stream from the camera is at least 8 for solving typical tasks.
   c. Both colorless (gray) and color images.
2. To lighting:
   a. 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 video analytics is not guaranteed.
   b. There are no abrupt changes in lighting.
3. To the scene and camera angle:
   a. Moving objects are visually separable from each other.
   b. The background is mostly static and does not change abruptly.
   c. Moving objects are minimally obscured by static objects in the scene (columns, trees, etc.).
   d. The analyzed scene does not have reflective surfaces and sharp shadows from moving objects. If present, they should be masked.
   e. Camera shake does not result in image offsets greater than 1% of the frame size.

Attention!

Correct operation of the neural tracker is not guaranteed when using a fish-eye lens.

Hardware requirements for neural analytics operation(see page 52)
Objects image requirements for neural tracker(see page 258)

15.4.10.3.5 Objects image requirements for neural tracker

To ensure the correct operation of detection tools based on the neural tracker, the following image requirements should be met:

1. The object to be detected is clearly distinguishable by the human eye.
2. The width or height of the objects does not exceed 75% of the frame size.
3. The image is not noisy and not distorted by compression algorithm artifacts.
4. The duration of the object's visibility is at least 6 frames.
5. The object moves in the certain direction between two adjacent frames at a distance which does not exceed the object's size. This condition is necessary for the correct calculation of the trajectory of the object (track).
6. 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%

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
1280x720	Light vehicle (2 axles)	35	~240x205	~20%
640x360	Light vehicle (2 axles)	17	~132x112	~20%

Video stream and scene requirements for neural tracker operation(see page 258)

15.4.10.3.6 Camera requirements for abandoned objects detection

Make sure the following requirements for abandoned object detection are met:

1. Camera requirements:

1. Resolution must be not less than 640x480 pixels.
2. Color: analytics works both with color and monochromatic images.
3. It is not allowed to the image shift be more than 1% from the frame size due to camera shake.

- Lighting requirements:

1. Moderate lighting. The quality of analytics performance can be lower in case of low lighting (night) or over lighting (overexposure).
2. There must be no dramatic changes in lighting.

- Scene and camera angle requirements:

1. Background is mostly static and is not changed.
2. Incorrect analytics performance can be caused by reflective surfaces.
3. Abandoned objects are hidden by moving objects not longer than 10% of the time.

- Object images requirements:

1. An abandoned object must be visible on the image.
2. The digital noise and compression-related artifacts are minimal.
3. 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.
4. 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.

15.4.10.3.7 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.

15.4.10.4 Configuring Scene Analytics Detection Tools

15.4.10.4.1 Setting up Tracker-based Scene Analytics detection tools

15.4.10.4.1.1 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.

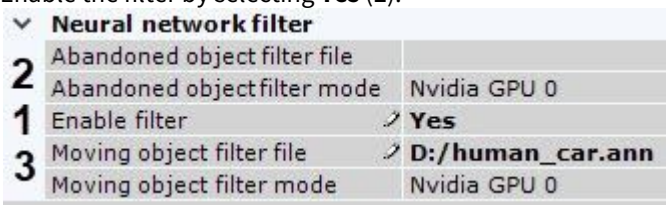
   > **Note**
   >
   > For example, the source image resolution is 2048*1536, and the specified value is set to **1000**.
   > In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the limit (1024 > 1000).

   > **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(see page 52)). 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**).



    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(see page 52), General Information on Configuring Detection(see page 234)).

    > **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(see page 240)).
- Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

Camera requirements for neural filter operation(see page 259)

c. Select a neural network (**3**). To access a neural network, contact AxxonSoft[101] 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.

Setting General Zones for Scene analytics detection tools

By default, the entire FoV is a Scene analytics detection tools zone. If you need to exclude parts of the scene prone to false alarms from detection (leaves, water, etc.), you should set exclude areas – zone with Scene analytics detection tools and metadata generation disabled.

To do so, follow the steps:

1. Select the **Object Tracker** object and click the button.
2. In the FoV, set the nodes of the closed area, in order, inside of which you want no detection.

Note

When the area is being constructed, the nodes are connected by a two-color dotted line which outlines the area's borders.

Note

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

Action	Result
Click in the viewing tile.	Creates a new area node
Right-click on a created node.	Deletes the area node

101 https://support.axxonsoft.com/

Position the cursor on a node and hold down the left mouse button while you move the mouse.	Moves the area node
Click the button.	Deletes the area

Once the area is closed, you will see the buttons on the borderlines. If you click them, a new node is added. This allows you to be more flexible with zoning.

3. Set the required masking areas.
4. Click the **Apply** button.

You have successfully created the detection zone.

> **Note**
>
> These settings will apply for all Scene analytics detection tools on the selected camera.

Set the minimum and maximum object size for detection

You can set the minimum and maximum object size for detection by specifying numerical values or reference areas on screen. Objects of all sizes beyond the set values will not trigger detection.

To specify the size, do as follows:

1. Select the **Object tracker** object.
2. In the **Max. object height** and **Max. object width** fields (**1**)**,** enter the maximum height and width of a detectable object as a percent of the FOV height. The values should be in the range [0,05; 100].

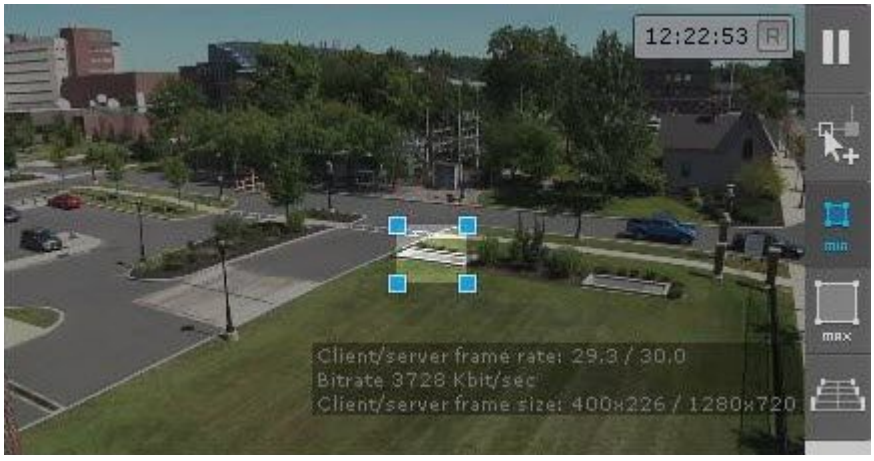
1	Max. object height	100
	Max. object width	100
2	Min. object height	2
	Min. object width	2

> **Attention!**
>
> If you activate the **Object calibration** parameter in tracker settings, please note that in this case min/max size of objects is specified in decimeters, not in FOV percentage (see Configure Perspective(see page 264)).

3. In the **Min. object height** and **Min. object width** fields (**2**), enter the minimum height and width of a detectable object as a percent of the FOV height. The values should be in the range [0,05; 100].
4. Click the **Apply** button.

To set the reference area on screen, do as follows:

1. Select the **Object tracker** object.
2. Click the **min** button and set the minimum size of a detectable object. You can do so by dragging and dropping the nodes of the reference area.



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

3. Click the **max** button and set the maximum size of a detectable object.

> **Note**
>
> By default, the maximum size is the whole size of FOV, so the nodes are located in the corners.

4. Click the **Apply** button.

You have successfully set the minimum and maximum object size for detection.

> **Note**
>
> These settings will apply for all Scene Analytics detection tools on the selected camera.

Configure Perspective

The Perspective enhances detection tools performance and helps evaluate real sizes of objects based on simplified calibration system.

To configure the perspective, do the following:

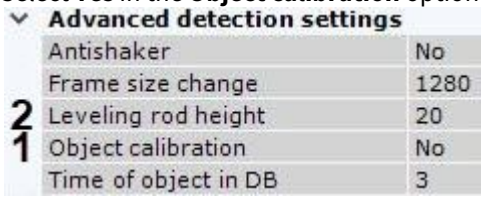
1. Select the **Object tracker** object and click the button.
2. Set the size of the same object in different areas of the field of view. To create a calibration length, left-click within the video image in the viewing tile and add two anchor points. Set at least three calibration lengths. You can resize the length

by stretching its anchor points . You can move it on screen by dragging and dropping[102].

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

> **Note**
>
> To delete it, click the button.

3. Select **Yes** in the **Object calibration** option (**1**).



4. Enter the height in decimeters of the object you want to find in the **Leveling rod height** field (**2**).

> **Attention!**
>
> Objects smaller than the specified value will not be detected.

5. Click the **Apply** button.

Perspective is now configured.

> **Note**
>
> These settings will apply for all Scene Analytics detection tools on the selected camera.

Recommendations on configuring Object Tracker

To avoid false positives of Scene Analytics detection tools, please follow the recommendations here:

1. Configure the **Tracker object** object iteratively and check operation quality in each iteration.
2. The parameters that affect operation quality most are: **Minimum size**, **Maximum size** (see Set the minimum and maximum object size for detection(see page 263)), and **Sensitivity** (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)).

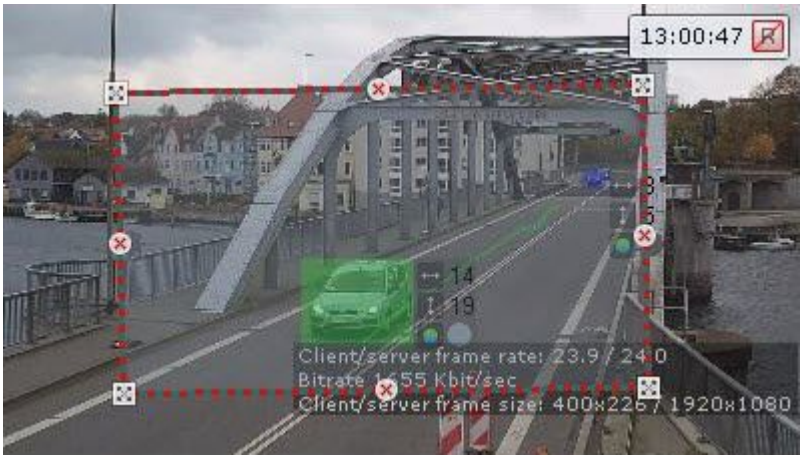
102 https://en.wikipedia.org/wiki/Drag_and_drop

3. It is recommended to use **Auto sensitivity** mode to ensure quality of the Tracker operation in changing lighting conditions.
4. If lighting is stable, it could be reasonable to adjust the **Sensitivity** value manually. Set **Sensitivity** value about 35 to detect objects with low contrast or about 15 to detect contrast object.
5. Minimum size is to be selected so that it is a little less than typical object size on the image.
6. Maximum size is to be selected so that it is a little greater than typical object size on the image, considering that the object can be joined with its shadow.
7. Lowering the **Time of Object in DB** allows excluding triggering of false static objects, while setting it to a higher value could allow not breaking off alarms for overlapping or temporarily disappearing objects in some cases.

Configuring the Detection Zone

For each type of Scene analytics detection tool you can set a detection zone.

After creating a detection tool, its rectangular detection zone is displayed in a bright color. If you have set privacy masks, they are grayed out (see Setting General Zones for Scene analytics detection tools(see page 262)).



Configuration of the detection zone is carried out in the same way as for general zones for Scene analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)).

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.

	Other	
1	Maximum object height	100
2	Maximum object speed	500
3	Maximum object width	100
4	Minimum object height	0.1
5	Minimum object width	0.1
6	Minimum object speed	0
7	Object class	Any
8	Object color	
9	X-axis offset	15
10	Y-axis offset	10

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(see page 737)).

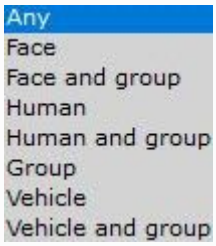
Note

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**).

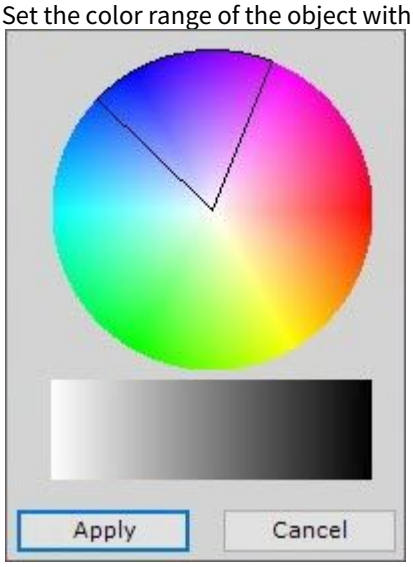
Note

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[103] 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.

15.4.10.4.1.2 Settings specific to Cross Line Detection

After you create and select a line crossing detection tool, you can see a virtual "tripwire" line in the FoV.

To set up line crossing detection, do the following:

1. Set up a virtual line in FoV.

103 https://en.wikipedia.org/wiki/Drag_and_drop

a. Set the end points of the line .

> **Note**
>
> When the line is being constructed, the end points are connected by a two-color dotted line. The direction of the object's motion across the line is indicated by dotted arrows.

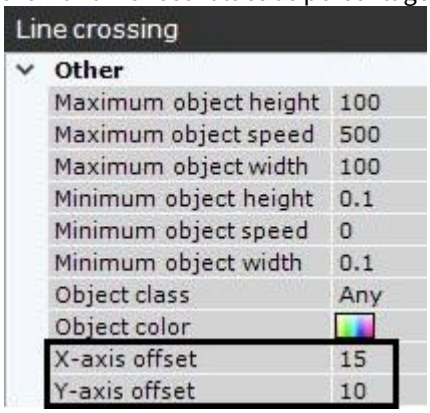
Action	Result
Position the cursor on an end point and, holding down the left mouse button, move the mouse	Moves the line end point
Position the cursor on the line, holding down the left mouse button, move the mouse	Moving the line

b. By default, Line crossing detection monitors object motion across the line in both directions. To suspend detection of motion in one direction, click the button to that direction.

> **Attention!**
>
> At least one direction must be selected for detection.

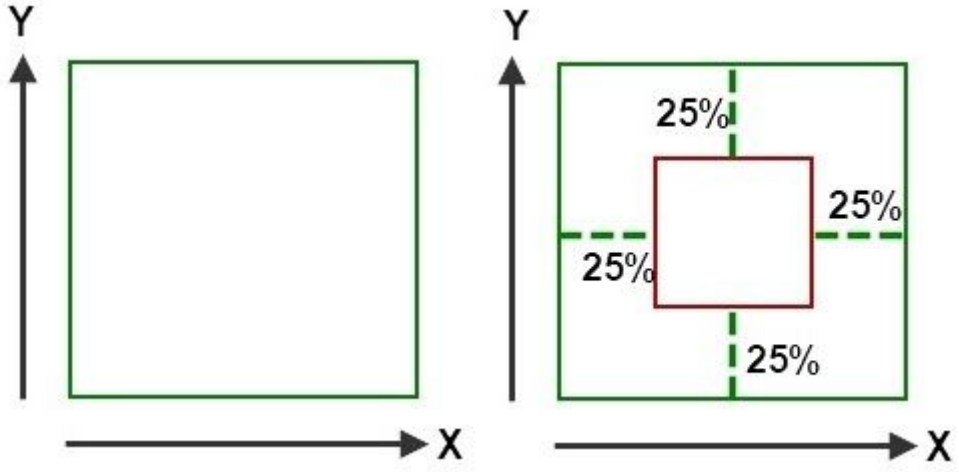
> **Note**
>
> An unmonitored direction of object motion is indicated by a dimmed arrow.

2. If an object in FoV performs repetitive movements near the virtual line, it may cause excessive triggering of the detection tool. In this case, set an area within the object's track which must cross the line completely to trigger the tool. To do it, set the X and Y offset values as percentage of track width and height.



Here's an example: the green triangle is the track of the object. If you specify X and Y offset values as 25%, the tool will be

triggered only if the entire red triangle goes beyond the virtual line.



3. Click the **Apply** button.

15.4.10.4.1.3 Settings specific to Abandoned object detection

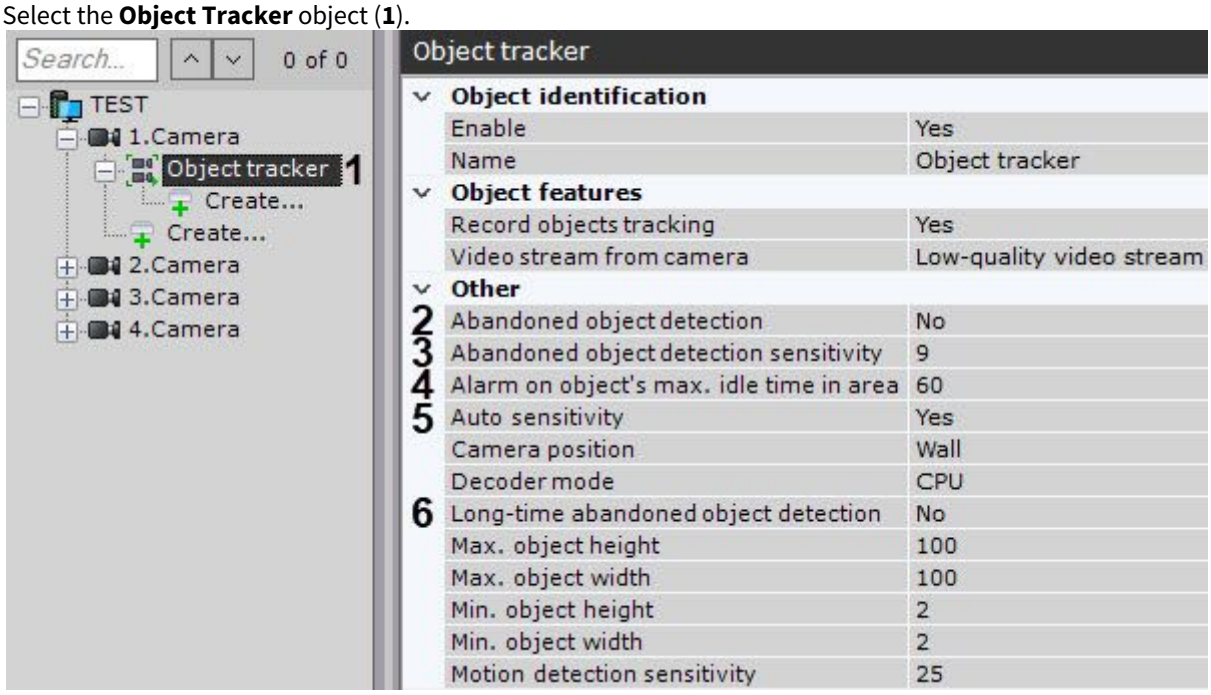
Camera requirements for abandoned objects detection(see page 259)

Attention!

The **Abandoned object** detection can operate only with the basic **Object tracker**.

To configure Abandoned object detection, do as follows:

1. Select the **Object Tracker** object (**1**).



2. To enable the **Abandoned object detection** (**2**), select **Yes** for the corresponding parameter.

Note

Objects abandoned for 10 seconds or longer will be detected.

3. In the **Abandoned object detection sensitivity** field (**3**), set the sensitivity for **Abandoned object detection** (**2**) and **Long-time abandoned object detection** (**6**). This value should be in the range [1, 100].

> **Note**
>
> This parameter depends on the lighting conditions and should be chosen empirically. It is recommended to select the parameter value starting from 20.

4. In the **Alarm on object's max. idle time in area** field (**4**) specify the time in seconds. If the object remains idle for the time longer than the specified, it will be detected. This value should 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.

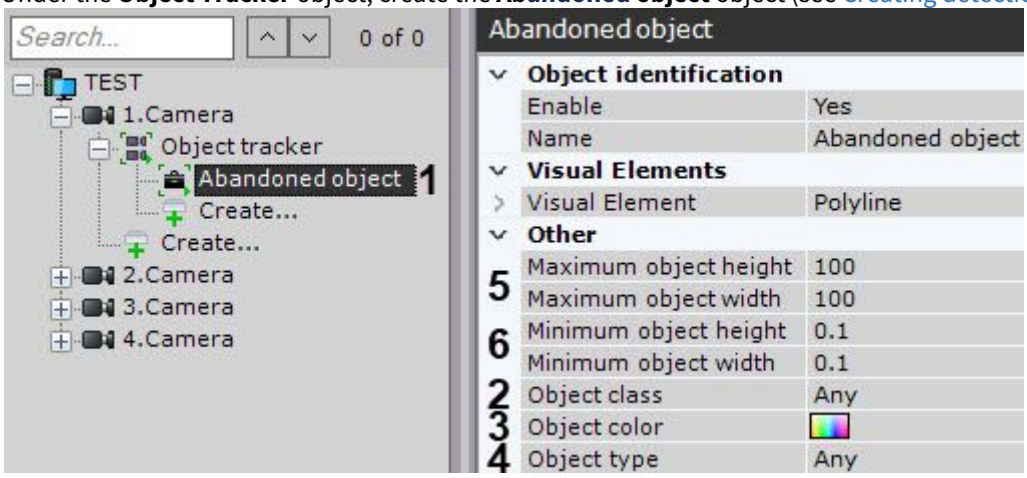
5. To enable the **Auto sensitivity** (**5**), select **Yes** for the corresponding parameter.

> **Attention!**
>
> 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.

6. To enable the **Long-time abandoned object detection**, select **Yes** for the corresponding parameter (**6**).

> **Note**
>
> If you enable the **Long-time abandoned object detection** parameter (**6**) and the **Neural network filter** (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)), it can reduce the number of false positives during detection.

7. Under the **Object Tracker** object, create the **Abandoned object** object (see Creating detection tools(see page 243)).



8. To enable the **Abandoned object** detection sub-tool, do the following:
   a. Select object class (**2**).
   b. Select object color (**3**).
   c. Select object type (**4**).
   d. Specify the maximum height and width of the object (**5**). The value should be in the range [0.05, 100].
   e. Specify the minimum height and width of the object (**6**). The value should 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 should be equal.

9. Click the **Apply** button.

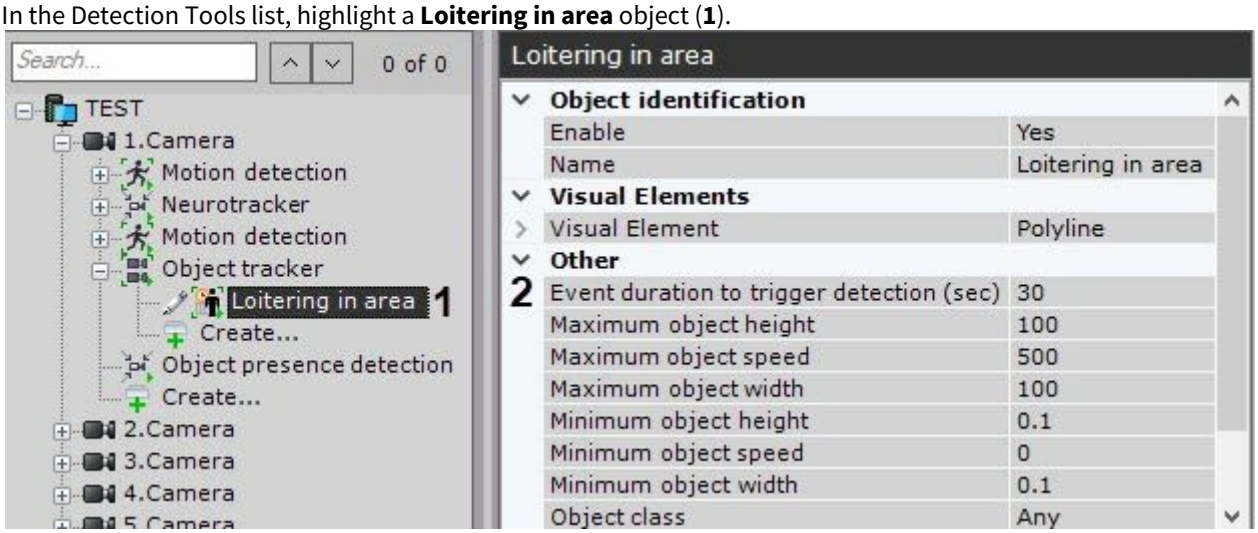
Abandoned object detection is now configured.

15.4.10.4.1.4 Settings specific to Loitering Detection

When configuring the Loitering detection tool, you must set the maximum time an object can be in the analyzed area: when the maximum time is exceeded, the detection tool is triggered.

To set a maximum time, you must perform the following steps:

1. In the Detection Tools list, highlight a **Loitering in area** object (**1**).



2. In the **Event duration to trigger detection (sec)** field (**2**), enter the maximum object loitering time in seconds. This value should be in the range [0, 3600].
3. Click the **Apply** button.

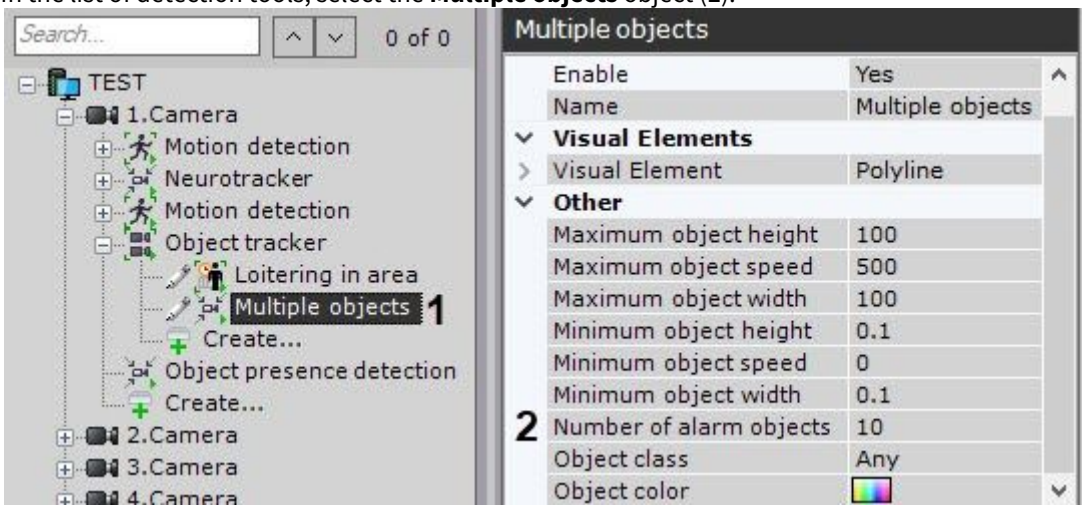
The maximum loitering time is now set.

15.4.10.4.1.5 Settings specific to Multiple objects

When configuring the Multiple objects detection tool, you should set the maximum number of objects within the analyzed zone. Exceeding this number leads to triggering the tool.

To configure the detection tool, do the following:

1. In the list of detection tools, select the **Multiple objects** object (**1**).



2. Enter the corresponding value into the **Number of alarm objects** (**2**) field.
3. Click the **Apply** button.

When the specified number of objects in the zone is exceeded, the detection tool generates the **Start Time of Detection Tool Trigger** event. When the number of objects in the zone decreases below the specified value, the **End Time of Detection Tool Trigger** event is generated.

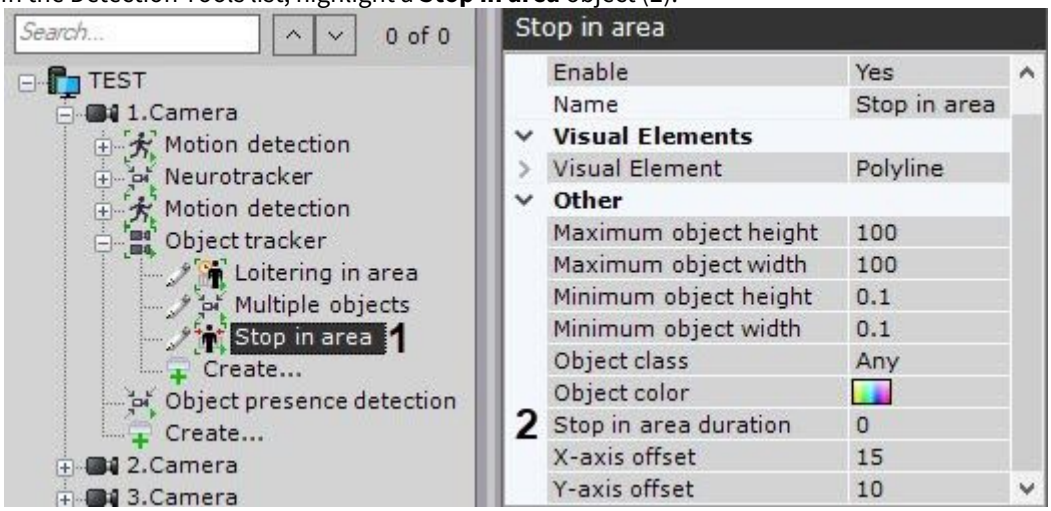
15.4.10.4.1.6 Settings specific to Stop in area detection

The detection tool will trigger if an object stops and remains idle for a specified time period.

> **Note**
>
> The object doesn't have to be completely idle, minor jitter is permitted.

To set a specified time period, you must perform the following steps:

1. In the Detection Tools list, highlight a **Stop in area** object (**1**).



2. Set the idle period duration for triggering the tool (**2**). This value should fall into the range of [0, 3600].

> **Attention!**
>
> Set this parameter to a value lower than the **Time of object in DB** in Object tracker settings (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)).

> **Attention!**
>
> If a detection tools runs on VMD metadata, the **Stop in area duration** should be set to 0. Otherwise, the detection tools will not work.

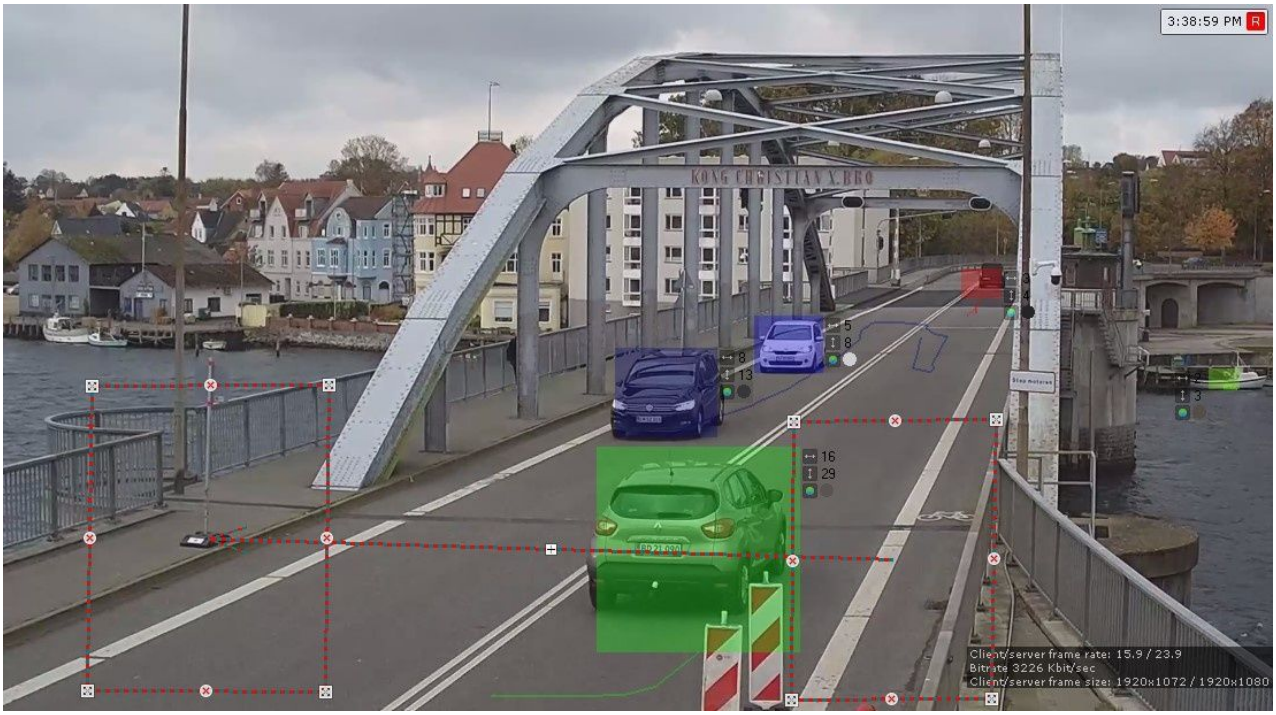
3. Click the **Apply** button.

15.4.10.4.1.7 Settings specific to Move from area to area detection tool

To configure the Move from area to area detection tool, do the following:

1. Set the general parameters (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)).
2. Set two areas in the preview window. The tool is triggered 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. To reshape the area, drag its anchor points . To move the entire area, left click and drag its border. To add the anchor points, click .
3. In the preview window, set 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.



4. Click the **Apply** button.

The Move from area to area detection tool is configured.

15.4.10.4.2 Setting up Neural Tracker-based Scene Analytics detection tools

Video requirements for scene analytics detection tools(see page 256)
Video stream and scene requirements for neural tracker operation(see page 258)
Objects image requirements for neural tracker(see page 258)
Hardware requirements for neural analytics operation(see page 52)

To configure the neural tracker-based Scene Analytics detection tools, do the following:

1. Select the **Neurotracker** object.

Neurotracker	
Object identification	
Enable	Yes
Name	Neurotracker
Object features	
1 Record objects tracking	Yes
2 Video stream from camera	Low-quality video stream

2. By default, metadata are recorded into the database. To disable metadata recording, select **No** from the **Record object tracking** (**1**) list.
3. If the camera supports multistreaming, select the stream for which detection is needed (**2**).

4. To reduce the number of false positives from a fish-eye camera, you have to position it properly (**3**). For other devices, this parameter is not valid.

	Other	
3	Camera position	Wall
4	Decoder mode	CPU
5	Detection threshold	30
6	Frames processed per second	6
7	Minimum number of detection triggers	6
8	Neural network file	
9	Neurofilter	Yes
10	Neurofilter file	
11	Neurofilter mode	CPU
12	Neurotracker mode	CPU
13	Object type	Human
14	Similitude search	Yes
15	Time of processing similitude track (sec)	6

5. Select a processing resource for decoding video streams (**4**). 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.
6. Set the **Detection threshold** for objects in percent (**5**). If the recognition probability falls below the specified value, the data will be ignored. The higher the value, the higher the accuracy, but some triggers may not be considered.
7. Set the frame rate value for the neural network to process per second (**6**). The higher the value, the more accurate tracking, but the load on the CPU is also higher.

> **Attention!**
>
> 6 FPS or more is recommended. For fast moving objects (running individuals, vehicles), you should set the frame rate at 12 FPS or above (see Examples of configuring neural tracker for solving typical tasks(see page 278)).

8. Specify the **Minimum number of detection triggers** for the neural tracker to display the object's track (**7**). The higher the value, the more is the time interval between the object's detection and the display of its track on the screen. Low values may lead to false positives.
9. If you use a unique neural network, select the corresponding file (**8**).

> **Attention!**
>
> - To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training(see page 239)).
> - A trained neural network for a particular scene allows you to detect only objects of a certain type (e.g. person, cyclist, motorcyclist, etc.).
> - If the neural network file is not specified, the default file will be used, which is selected automatically depending on the selected object type (**13**) and the selected processor for the neural network operation (**4**). 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 should be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

10. You can use the neural filter to sort out certain tracks. For example, the neural tracker detects all freight trucks, and the neural filter sorts out only video recordings that contain trucks with cargo door open. To set up a neural filter, do the following:
    a. to use the neural filter, select **Yes** in the corresponding field (**9**).
    b. in the **Neurofilter file** field, select a neural network file (**10**).
    c. in the **Neurofilter mode** field, select a processor to be used for neural network work (**11**, see General Information on Configuring Detection(see page 234)).
11. Select the processor for the neural network—CPU, one of NVIDIA GPUs or one of Intel GPUs (**12**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

Attention!

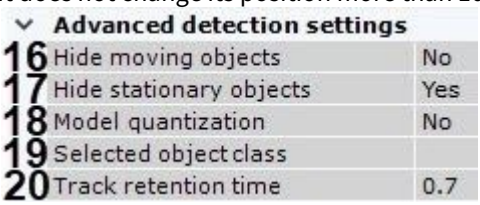
- We recommend using the GPU. It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU(see page 240)).
- If Neural Tracker is running on GPU, object tracks may be lagging behind the objects. If this happens, set the camera buffer size to 1000 milliseconds (see The Camera object(see page 122)).
- Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

12. In the **Object type** field (**13**), select the recognition object:
    a. Human.
    b. Human (top view).
    c. Vehicle.
    d. Human and Vehicle (Nano)—low accuracy, low processor load.
    e. Human and Vehicle (Medium)—medium accuracy, medium processor load.
    f. Human and Vehicle (Large)—high accuracy, high processor load.
13. To enable the search for similar persons, in the **Similitude search** field (**14**), select **Yes**. It increases the processor load.

Attention!

The Similitude search(see page 756) works only on tracks of people.

14. In the **Time of processing similitude track (sec)** field (**15**), set the time in the range [0; 3600] required for the algorithm to process the track to search for similar persons.
15. If you don't need to detect moving objects, select **Yes** in the **Hide moving objects** field (**16**). An object is treated as static if it does not change its position more than 10% of its width or height during its track lifetime.



16. If you don't need to detect static objects, select **Yes** in the **Hide stationary objects** field (**17**). This parameter lowers the number false positives when detecting moving objects. An object is considered stationary if it has not moved more than 10% of its width or height during the whole time of its track existence.

Attention!

If a stationary object starts moving, the detection tool will trigger, and the object will no longer be considered stationary.

17. If necessary, enable the **Model quantization** option (**18**). It allows you to reduce the consumption of the GPU processing power.

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%.
Model quantization is only applicable to NVIDIA GPUs.
The first launch of a detection tool with quantization enabled may take longer than a standard launch.
If GPU caching(see page 240) is used, next time a detection tool with quantization will run without delay.

18. If necessary, specify the class of the detected object (**19**). 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 view), **10**—Vehicle.
    a. If you leave the field blank, the tracks of all available classes from the neural network will be displayed (**8**, **13**).

b. If you specify a class/classes from the neural network, the tracks of the specified class/classes will be displayed (**8**, **13**).
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 (**8**, **13**).
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 (**8**, **13**).

> **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 (**8**, **13**).

19. In the **Track retention time** field, set a time interval in seconds after which the object track is considered lost (**20**). This helps if objects in scene temporarily overlap each other. For example, a larger vehicle may completely block the smaller one from view.
20. By default, the entire FOV is a detection area. If you need to narrow down the area to be analyzed, you can set one or several detection areas in the preview window.

> **Note**
>
> The procedure of setting areas is identical to the primary tracker's (see Setting General Zones for Scene analytics detection tools(see page 262)). The only difference is that the neural tracker areas are processed while the primary tracker areas are ignored.

21. Click the **Apply** button.
22. The next step is to create and configure the necessary detection tools on the basis of neural tracker. The configuration procedure is the same as for the primary tracker (see Setting up Tracker-based Scene Analytics detection tools(see page 274)).

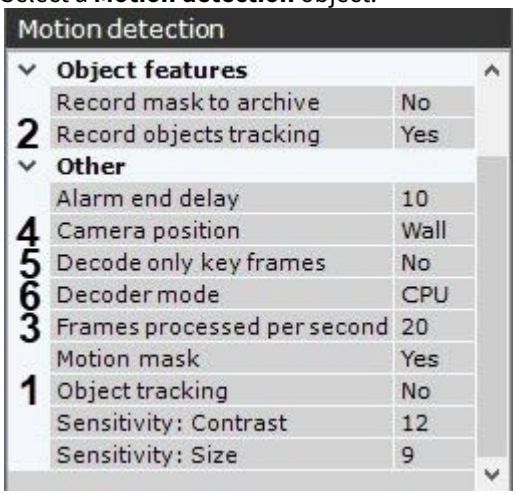
> **Attention!**
>
> - To trigger a **Motion in Area** detection tool under a neural network tracker, an object should be displaced by at least 25% of its width or height in FOV.
> - The abandoned objects detection tool works only with the primary tracker.

15.4.10.4.3 Setting up VMD-based Scene Analytics detection tools

Video requirements for VMD(see page 249)

To configure Scene Analytics detection tools based on video motion detection, do the following:

1. Request an updated license file from AxxonSoft manager.
2. Select a **Motion detection** object.



3. Select **Yes** in the **Object tracking** field (**1**).
4. By default, metadata are not recorded into the database. To enable metadata recording, select **Yes** from the **Record objects tracking** list (**2**).
5. For a proper operation of VMD-based Scene Analytics detection tool, it must analyze a frame at least every 500 milliseconds (see Configuring VMD(see page 250) section for **Frames processed per second** (**3**) and **Decode key frames** (**5**) parameters description).
6. 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.
7. To reduce false alarms rate from a fish-eye camera, you have to position it properly (**4**). For other devices, this parameter is not valid.
8. Click the **Apply** button.
9. Next, you have to create and configure the necessary VMD-based detection tools. The configuration procedure is the same as for the primary tracker (see Setting up Tracker-based Scene Analytics detection tools(see page 260)).

> **Attention!**
>
> VMD-generated metadata does not include object type and color information.

> **Attention!**
>
> The abandoned objects detection tool works only with the primary tracker.

15.4.10.4.4 Examples of configuring neural tracker for solving typical tasks

Settings	Task: detection of moving people	Task: detection of moving vehicles
Main		
The number of frames processed per second	6	12
Minimum number of triggerings	6	6
Neural filter	No	No
Camera position	Wall	Wall
Recognition threshold	30	30
Neural network file	Path to the *.ann neural network file. You can also select **Object type** – in this case, this field should be left blank.	Path to the *.ann neural network file. You can also select **Object type** – in this case, this field should be left blank.
Advanced		
Hide static objects	Yes	Yes

> **Note**
>
> By default, the neural tracker is configured for detection of moving people.

15.4.11 Face detection tools

There are two types of face detection tools in *Axxon One*:

1. Face detection(see page 280).
2. Face detection (VL)(see page 285).

Attention!

You can install a *DetectorPack* add-on of only one of the given types.
It is forbidden to install both add-ons on the same system.

15.4.11.1 Functions of face detection tools

The **Face detection** basic object and the **Face detection (VL)** object are triggered every time a face is captured in the frame. Basic object is enough to perform a search for faces in the archive (see Search for similar face(see page 744)).

In addition, the following types of detection tools based on metadata from the face detection (see General information on metadata(see page 237)) are available in *Axxon One*:

1. Appearance in area – a detection tool is triggered by the appearance of an object and subsequent face capture in FOV.
2. Loitering in area – a detection tool triggered by the lengthy presence of an object and its face capture in FOV.
3. Mask detection – a detection tool is triggered by the face captured with or without a mask.

The *Axxon One* database stores all faces in binary form:

1. All captured face images are vectorized* and stored in the **t_face_vector** table, and their corresponding capture events are stored in the **t_json_event** table.
2. Reference images (see Face lists[104]) are stored in the **t_face_listed** table.

* Face vector is the mathematical representation of a face image created upon face capture.

Note

These detection tools require Add-on Face Recognition Pack to be installed (see Installing DetectorPack add-ons(see page 74)).

Attention!

With an increase in the number of faces in the database, the statistical error increases: the more faces in the database, the more often similar faces will be recognized when searching in the archive. Accordingly, the degree of similarity when comparing the reference face with the captured face will decrease.
This statistical error is relevant if:

1. The Requirements for face detection tools(see page 279) are met.
2. The database contains over a million faces.

An example of the error calculation results:

1. Face detection, mugshot dataset (good quality photo), 12 million faces in database, and false matching probability is 0.003%. With these initial data, the researchers obtained an identification error of 0.76%.
2. Face detection (VL), the initial data are the same. The identification error is 0.81%.

15.4.11.2 Requirements for face detection tools

Face detection works properly if video cameras are installed and set up as follows:

1. The frame rate should not be less than 12 FPS and not less than 6 FPS for face recognition at turnstiles.
2. The maximum angle of frontal perspective of the photos of people's faces received from video cameras should not exceed +/- 15°.
3. The distance between the pupils on the photos of people's faces received from video cameras should not be less than 32 pixels.
4. Mutual faces covering should be minimal.
5. Faces should be evenly illuminated with diffused light of at least 200 lux. Directional side lighting is not allowed.
6. The contrast of the photos of the captured faces should be over 64 grayscale. Insufficient or excessive lighting is not allowed.

104 https://docs.axxonsoft.com/confluence/display/anet/Face+lists

7. There should be no backlighting and sharp gradients of light and shade.
8. The photos of the captured faces received from video cameras should be clear. Image blurring caused by motion is not allowed.

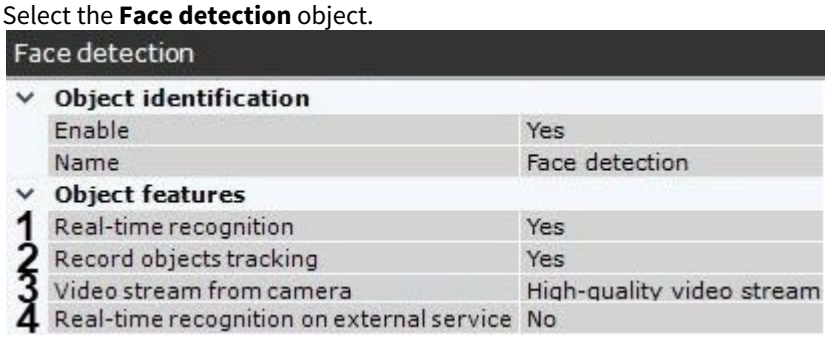
> **Note**
>
> The required distance between the camera and the face can be set using a lens with the required focal length.

15.4.11.3 Configuring Face detection

> **Attention!**
>
> You need to create a cache beforehand in order to start and correctly operate the basic Face detection tool on GPU (see Optimizing the operation of Face detection on GPU(see page 284)).

To configure the basic Face detection tool, do the following:

1. Select the **Face detection** object.



2. If you need to use this detection tool for real-time face recognition, set the corresponding parameter to **Yes** (**1**, see Configuring real-time face recognition(see page 301)).
3. If you need to record metadata, select **Yes** from the **Record objects tracking** list (**2**).
4. If the camera supports multistreaming, select the stream for which detection is needed (**3**). For the correct operation of the **Face detection**, it is recommended to use a High-quality video stream.
5. If you need to use this face detection tool in real-time together with FaceCube Recognition Server (see Configuring FaceCube integration(see page 307)), set **Yes** for the **Real-time recognition on external service** parameter (**4**).
6. If you need to save age and gender information for each captured face in the database, select **Yes** in the corresponding field (**1**).

   > **Note**
   >
   > The average error in age recognition is 5 years.

Face detection		
	Other	
1	Age and gender	No
2	Camera transform	No
3	Decoder mode	CPU
4	Face detection period (msec)	250
5	Face mask detection	No
6	Filter false alarms	Yes
7	Frame size change	1920
8	Maximum face height	100
	Maximum face width	100
	Minimum face height	5
	Minimum face width	5
9	Minimum threshold of face authenticity	90
10	Mode	CPU
11	Send face images	No
12	Track loss time	500

7. If you use a bi-spherical XingYun lens, the detector will analyze two 180° spherical images by default (see Configuring fish-eye cameras(see page 127)). This may decrease recognition quality. To dewarp the image before detection, select **Yes** for the **Camera transform** parameter (**2**). This parameter is relevant for other types of image transformation as well.
8. Select a processing resource for decoding video streams (**3**). 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.
9. Set the time (in milliseconds) between face search operations in a video frame in the **Face detection period (msec)** field (**4**). Acceptable values range is [1; 10000]. Increasing this value decreases the Server load, but can result in some faces being undetected.
10. If you plan to apply the masks detection tool, set **Yes** for the **Face mask detection** parameter (**5**, see Configuring Masks Detection(see page 291)).
11. In some cases, the detection tool may mistake other object for a face. Select **Yes** in the **Filter false alarms** field (**6**) to filter out non-face objects,while calculating the vector model of a face and its recording into the metadata DB. If the filtering is on, false results will appear in the detection feed (see Face recognition and search(see page 765)), but will be ignored during searches in the archive.
12. Analyzed framed are scaled down to a specified resolution (**7**, 1920 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.

13. Specify the minimum and maximum sizes of the captured faces as a percentage of the frame size (**8**).
14. In the **Minimum threshold of face authenticity** field, set the minimum level of face recognition accuracy for the creation of a track (**9**). You can set any value by trial-and-error. No less than 90 is recommended. The higher the value, the fewer faces are detected, while the recognition accuracy increases.
15. Select the processor for the face detection – CPU or NVIDIA GPU (**10**, see General Information on Configuring Detection(see page 234)).

> **Attention!**
>
> It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings.

16. If you use FaceCube integration (see Configuring FaceCube integration(see page 307)), activate the **Send face images** parameter (**11**).
17. Enter the time in milliseconds after which the face track is considered to be lost in the **Track loss time** field (**12**). Acceptable values range is [1; 10000]. This parameter applies when a face moves in a frame and gets hidden behind an obstacle for some time. If this time is less than the set value, the face will be recognized as the same.
18. If necessary, fine-tune the detection tool (see Fine-tuning the Face detection tool(see page 282)).
19. In the preview window, set the rectangular area of the frame in which you want to perform face detection. To select the area, move the anchor points .

20. Click the **Apply** button.

The basic Face detection tool is now configured.

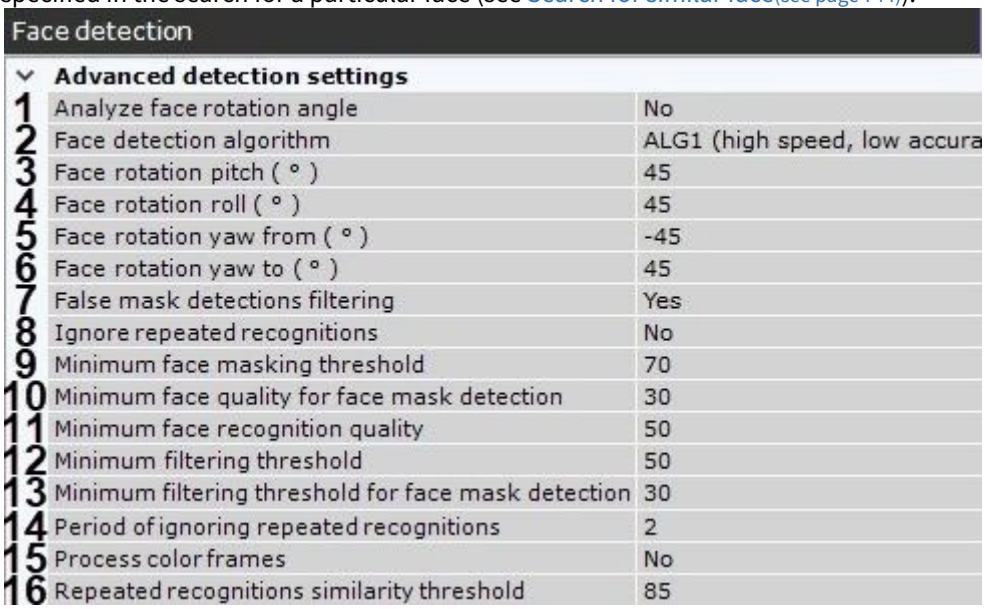
15.4.11.3.1 Fine-tuning the Face detection tool

> **Attention!**
>
> To fine-tune this detection tool, you will require assistance from AxxonSoft tech support.

To fine-tune the Face detection tool, do as follows:

1. Configure face rotation angle analysis:
   a. If it is necessary to determine the face rotation angle, then set **Yes** for the **Analyze face rotation angle** parameter (**1**). This setting allows you to filter out the results that have a rotation and tilt angle greater than the values

specified in the search for a particular face (see Search for similar face(see page 744)).



Face detection	
Advanced detection settings	
1 Analyze face rotation angle	No
2 Face detection algorithm	ALG1 (high speed, low accura
3 Face rotation pitch (°)	45
4 Face rotation roll (°)	45
5 Face rotation yaw from (°)	-45
6 Face rotation yaw to (°)	45
7 False mask detections filtering	Yes
8 Ignore repeated recognitions	No
9 Minimum face masking threshold	70
10 Minimum face quality for face mask detection	30
11 Minimum face recognition quality	50
12 Minimum filtering threshold	50
13 Minimum filtering threshold for face mask detection	30
14 Period of ignoring repeated recognitions	2
15 Process color frames	No
16 Repeated recognitions similarity threshold	85

   b. In the **Face rotation pitch (°)** field (**3**), set the allowable face tilt up/down angle in degrees. The value should be in the range [0; 90].
   c. In the **Face rotation roll (°)** field (**4**), set the allowable face tilt right/left angle in degrees. The value should be in the range [0; 90].
   d. In the **Face rotation yaw from (°)** field (**5**), set the minimum allowable angle of face rotation to the right or left. The value should be in the range [-90; 90].
   e. In the **Face rotation yaw to (°)** field (**6**), set the maximum allowable angle of face rotation to the right or left. The value should be in the range [-90; 90].
2. Select a face detection algorithm (**2**):
   a. **ALG1**—high speed, low accuracy.
   b. **ALG2**—average speed, average accuracy.
   c. **ALG3**—low speed, high accuracy.
3. Set up false mask detections filtering:
   a. To apply filters, set **Yes** for the **False mask detections filtering** parameter (**7**).
   b. Set the minimal percentage of probability which makes the additional algorithm identify a track as a masked face in the **Minimum filtering threshold for face mask detection** field (**13**). If the algorithm takes a decision that the track relates to a masked face with a probability value lower than the specified threshold, the track will be ignored. Set the value by trial-and-error, values over 30 are recommended.
4. Set the minimum threshold value for mask detection (**9**). Set a value by trial-and-error, values over 70 are recommended.
5. Set the minimum quality of a face image for recognition with a mask (**10**, see Configuring Masks Detection(see page 291)). Set the value by trial-and-error, values over 30 are recommended.
6. Set the minimum quality of a face image for recognition without a mask (**11**). Set the value by trial-and-error, values over 50 are recommended.
7. If it is necessary to filter out false positives, set the minimum percentage of probability which makes the algorithm identify a track as a human face in the **Minimum filtering threshold** field (**12**, see Configuring Face detection(see page 280)). If the algorithm takes a decision that the track relates to a face with a probability value lower than the specified threshold, the track will be ignored. Set the value by trial-and-error, values over 50 are recommended.
8. If it is necessary for the detection tool to use a color frame for processing, then set **Yes** for the **Process color frames** parameter (**15**). By default, a black and white frame is processed.
9. Configure the repeated face recognition ignoring:
   a. If it is necessary to ignore repeated recognition of the same face, then set **Yes** for the **Ignore repeated recognitions** parameter (**8**).
   b. In the **Repeated recognitions similarity threshold** field (**16**), set the similarity threshold of a face with the previous recognized ones in percentage from 0 to 100. If the similarity threshold is below the specified value, then the face will be recognized as a new one.
   c. In the **Period of ignoring repeated recognitions** field (**14**), set the period in minutes during which new recognized faces will be compared with the previous ones to identify similarities. The value should be in the range [0; 30].
10. Click the **Apply** button.

Fine-tuning the Face detection tool is now complete.

15.4.11.3.2 Optimizing the operation of Face detection on GPU

Configuring Face detection(see page 280)

Starting from *DetectorPack* 3.8, there is a utility in the Face Recognition Pack add-on (see Installing DetectorPack add-ons(see page 74)), which allows you to create GPU 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 basic Face detection on GPU.

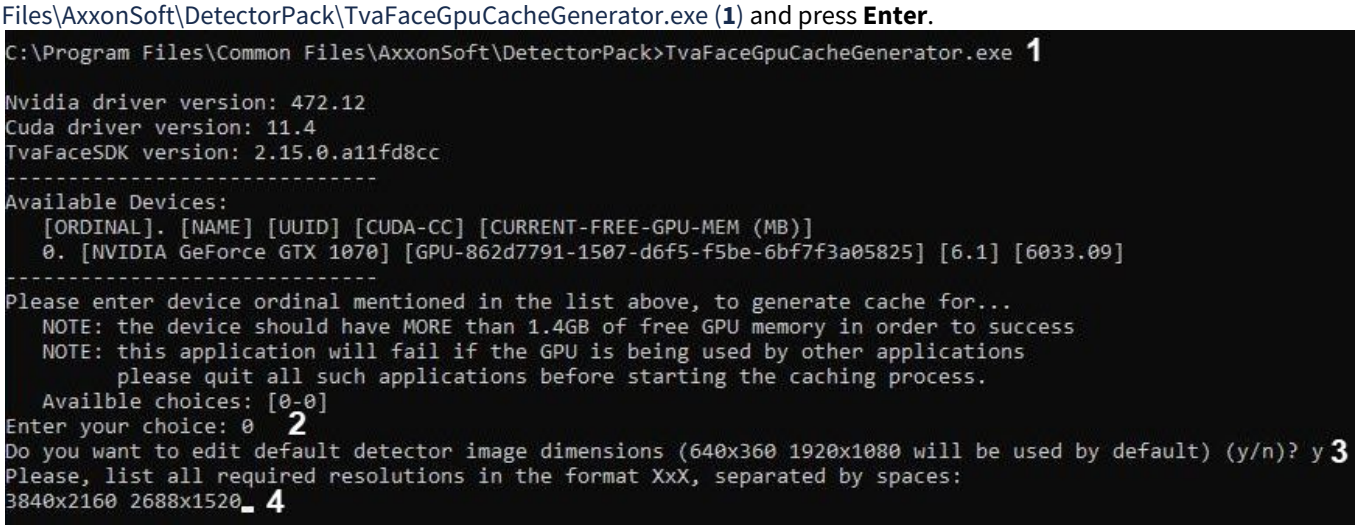
To optimize the operation of the Face detection on GPU, do the following:

1. Stop the Server (see Shutting down a Server(see page 100)).

   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(see page 951)) by specifying in the **Variable value** field the path to the cache location with an arbitrary folder name. For example, D:\AN_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\TvaFaceGpuCacheGenerator.exe (**1**) and press **Enter**.



4. Specify the ID of the required GPU (**2**, see General Information on Configuring Detection(see page 234)) and press **Enter**.
5. If you want to change the resolution of the video stream for the Face detection, enter **y** (**3**) and specify the required resolution (**4**).

   Note

   GPU uses the default video stream resolutions. Changing the resolution of the video stream will increase the percentage of face detection when using the resolutions from 1920*1080 and higher.

6. Press **Enter**. The cache creation process will start. The cache creation was successful, if the result value is “0”.

Optimizing the operation of Face detection on GPU is complete.

Attention!

The cache must be recreated in the following cases:

- if you update the Face Recognition Pack add-on (see Installing DetectorPack add-ons(see page 74)),
- if you change the NVIDIA GPU model,
- if you update the NVIDIA GPU drivers.

15.4.11.4 Configuring Face detection (VL)

To configure the Face detection (VL), do the following:

1. Select the **Face detection (VL)** object.

Face detection (VL)	
Object identification	
Enable	Yes
Name	Face detection (VL)
Object features	
1 Real-time recognition	No
2 Record objects tracking	Yes
3 Video stream from camera	Low-quality video stream

2. If you need to use this detection tool for real-time face recognition, set the corresponding parameter to **Yes** (**1**, see Configuring real-time face recognition[105]).
3. If you need to record metadata, select **Yes** from the **Record objects tracking** list (**2**).
4. If the camera supports multistreaming, select the stream for which detection is needed (**3**). For the correct operation of the **Face detection (VL)**, it is recommended to use a High-quality video stream.

Face detection (VL)	
Other	
4 Decoder mode	CPU
5 Face attributes recognition	No
6 Maximum face size	100
7 Medical mask detection	No
8 Minimum face size	10
9 Minimum image quality	50
10 Minimum threshold of face authenticity	60
11 Mode	CPU
12 Send face images	No

5. Select a processing resource for decoding video streams (**4**). 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.
6. In the **Face attributes recognition** field (**5**), select **Yes** if it is necessary to recognize gender and age.
7. Set the maximum size of the captured faces as a percentage of the frame size (**6**).
8. If necessary, set **Yes** for the **Medical mask detection** parameter (**7**, see Configuring masks detection[106]).
9. Set the minimum size of the captured faces as a percentage of the frame size (**8**).
10. Set the **Minimum image quality** of a person's face for face detection (**9**). A required value should be selected empirically, at least 50 is recommended.
11. In the **Minimum threshold of face authenticity** field (**10**), set the minimum level of face recognition accuracy for the creation of a track. A required value should be selected empirically, at least 90 is recommended. The higher the value, the higher the recognition quality will be.
12. Select the processor for the face detection – CPU or NVIDIA GPU (**11**, see General Information on Configuring Detection[107]).

> **Attention!**
>
> It may take several minutes to launch the algorithm on an NVIDIA GPU after you apply the settings.

13. If FaceCube integration is used (see Configuring FaceCube integration(see page 307)), enable the **Send face images** parameter (**12**).
14. If necessary, fine-tune the detection tool (see Fine-tuning the face detection (VL)(see page 286)).

105 https://docs.axxonsoft.com/confluence/display/next46en/Configuring+real-time+face+recognition
106 https://docs.axxonsoft.com/confluence/display/next46en/Configuring+masks+detection
107 https://docs.axxonsoft.com/confluence/display/next46en/General+Information+on+Configuring+Detection

15. In the preview window, set the rectangular area of the frame where faces should be detected. To select the area, move the anchor points .

16. Click the **Apply** button.

The Face detection (VL) is now configured.

15.4.11.4.1 Fine-tuning the face detection (VL)

> **Attention!**
>
> To fine tune this detection tool, you will require the assistance from AxxonSoft tech support.

To fine-tune the face detection tool, do as follows:

1. If necessary, set **Yes** for the **Advanced logging for SDK** parameter (**1**).

> **Attention!**
>
> Starting from *DetectorPack* 3.9.0, the **Advanced logging for SDK** parameter is absent.
> You can enable the advanced logging for SDK using the VL_SDK_VERBOSE_LOGGING=1 system variable (see Appendix 10. Creating system variable(see page 951)).

Face detection (VL)		
	Advanced detection settings	
1	Advanced logging for SDK	No
2	Analyze face rotation angle	No
3	Face recognition algorithm	Algorithm 2
4	Face rotation pitch (°)	45
5	Face rotation roll (°)	45
6	Face rotation yaw from (°)	-45
7	Face rotation yaw to (°)	45
8	Minimum number of detections	3
9	Number of frames between detections	7
10	Number of frames without detections	8
11	Number of threads	4
12	Track timeout	2

2. Select a face recognition algorithm (**3**):
   a. **Algorithm 1**—the recognition speed depends on the background and the number of faces in the frame. Works slower than **Algorithm 3**.
   b. **Algorithm 2**—high speed, low accuracy. The recognition speed depends on the number of faces in the frame.
   c. **Algorithm 3**—average speed, high accuracy. The recognition speed depends on the resolution of the image. Optimal for most scenes.
3. Configure the face rotation angle analysis:

   a. If it is necessary to determine the face rotation angle, then set **Yes** for the **Analyze face rotation angle** parameter (**2**). This setting allows you to filter out the results that have a rotation and tilt angle greater than the values specified in the search for a particular face (see Search for similar face(see page 744)).
   b. In the **Face rotation pitch (°)** field (**4**), set the allowable face tilt up/down angle in degrees. The value should be in the range [0; 90].
   c. In the **Face rotation roll (°)** field (**5**), set the allowable face tilt right/left angle in degrees. The value should be in the range [0; 90].
   d. In the **Face rotation yaw from (°)** field (**6**), set the minimum allowable angle of face rotation to the right or left. The value should be in the range [-90; 90].
   e. In the **Face rotation yaw to (°)** field (**7**), set the maximum allowable angle of face rotation to the right or left. The value should be in the range [-90; 90].
4. In the **Minimum number of detections** field (**8**), enter the time in milliseconds in the range [1; 10000], after which the track will be considered a detected face.
5. In the **Number of frames between detections** field (**9**), enter the time in milliseconds in the range [1; 10000]. The lower the value, the more likely the TrackEngine will detect a new face as soon as it appears in the selected area.
6. In the **Number of frames without detections** field (**10**), enter the time in milliseconds in the range [1; 10000]. If there is no face detection in the selected area, the TrackEngine will continue to process the specified number of frames before the track is considered lost.

   Note

   TrackEngine does not 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.

7. Specify the **Number of threads** per recognition channel (**11**). The value should be in the range [1; 256].
8. In the **Track timeout** field (**12**), enter the maximum time period in seconds in the range [1; 60], after which the event will be sent.
9. Click the **Apply** button.

Fine-tuning the face detection (VL) is now complete.

15.4.11.4.2 License activation for Face detection (VL)

To activate a license for Face detection (VL) (see Installing DetectorPack addons[108], Configuring Face detection (VL)(see page 285)), do the following:

1. Request EID and ProductID from technical support[109].

   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. Go to the website[110].

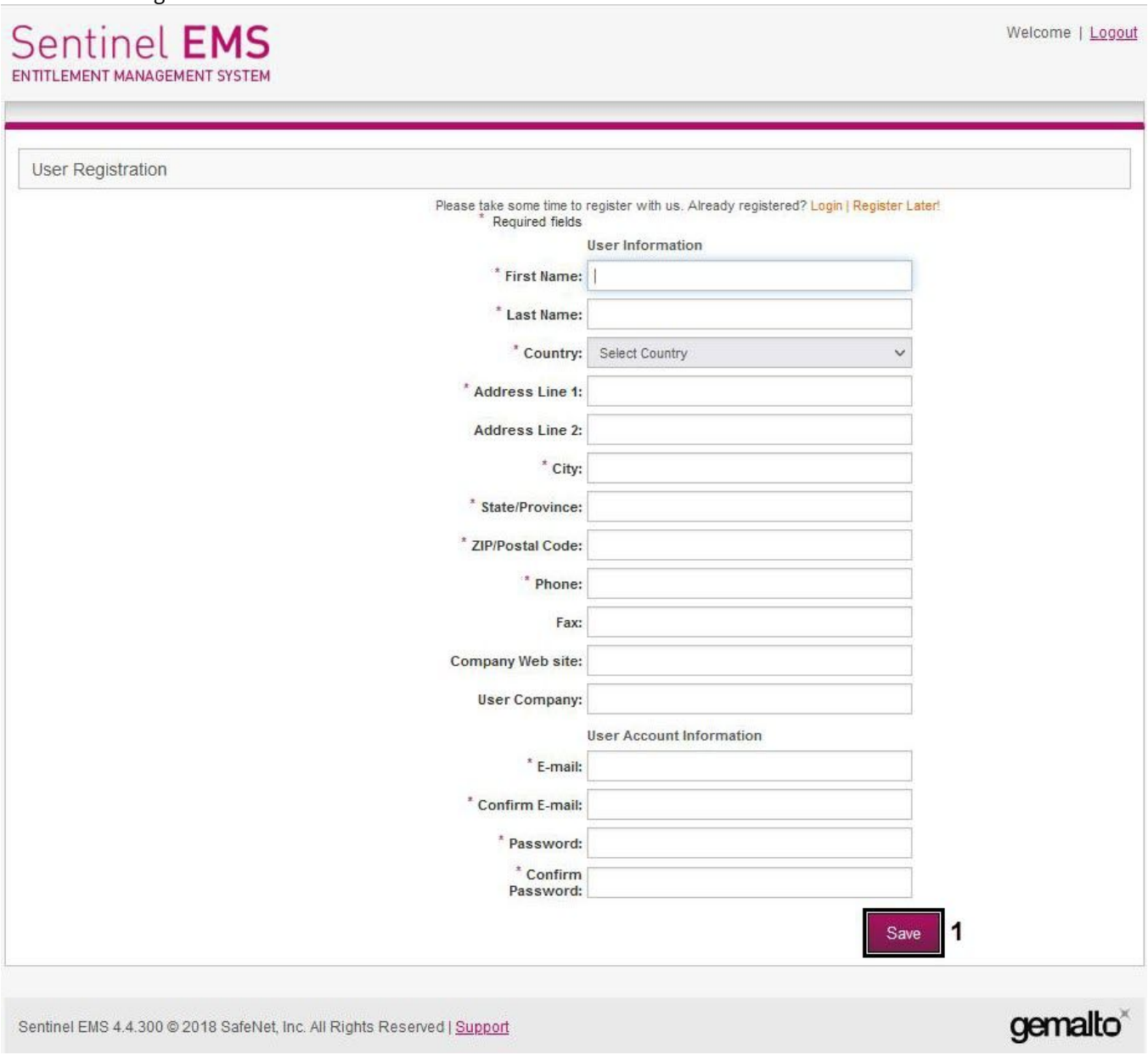
   Attention!

   If you fail to login to the website, please contact technical support[111].

3. Log in using the received EID.

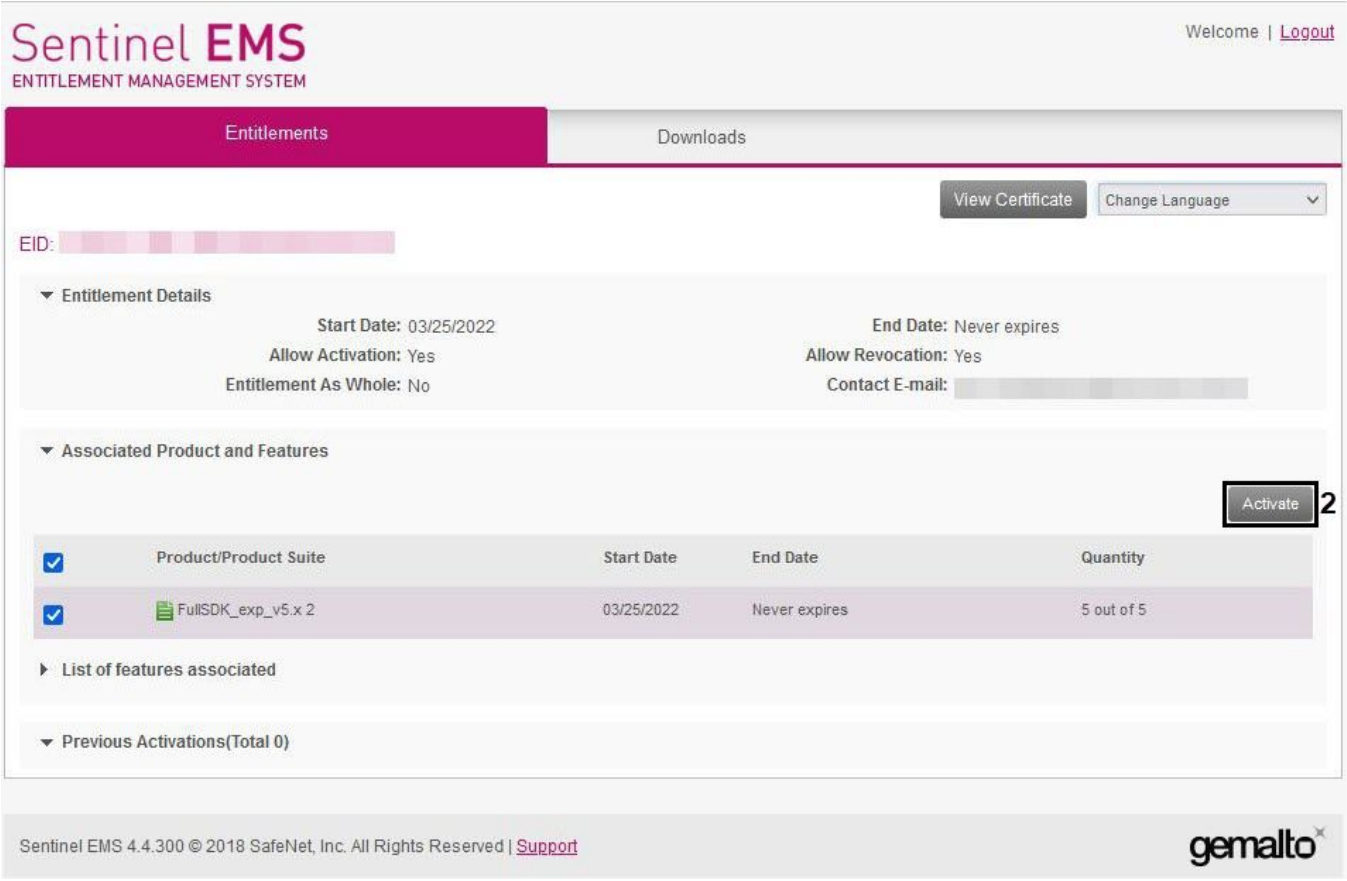
108 https://docs.axxonsoft.com/confluence/display/next46en/Installing+DetectorPack+addons
109 https://visionlabs.ru/contact-us?langChange=true
110 https://license.visionlabs.ai/ems/customerLogin.html
111 https://support.axxonsoft.com/jira/servicedesk/customer/portal/3

4. Fill in the user registration data.

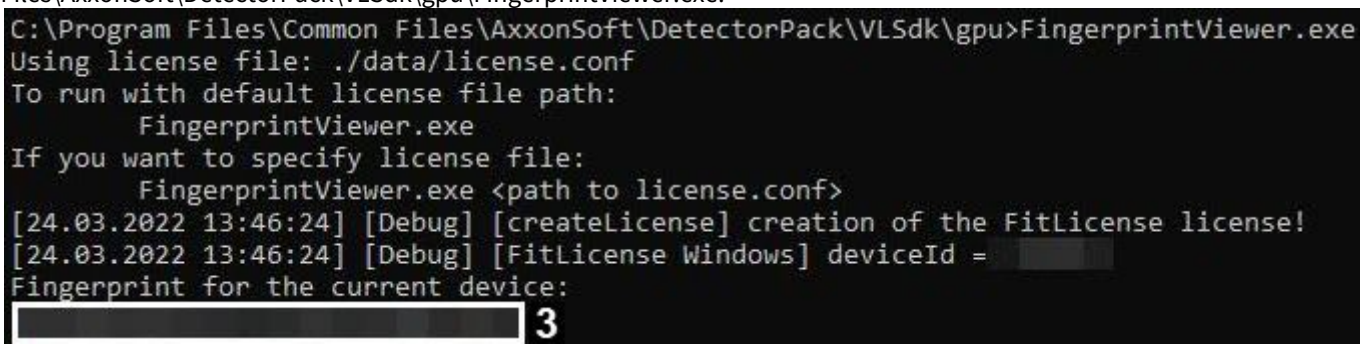


5. Click the **Save** button (**1**).

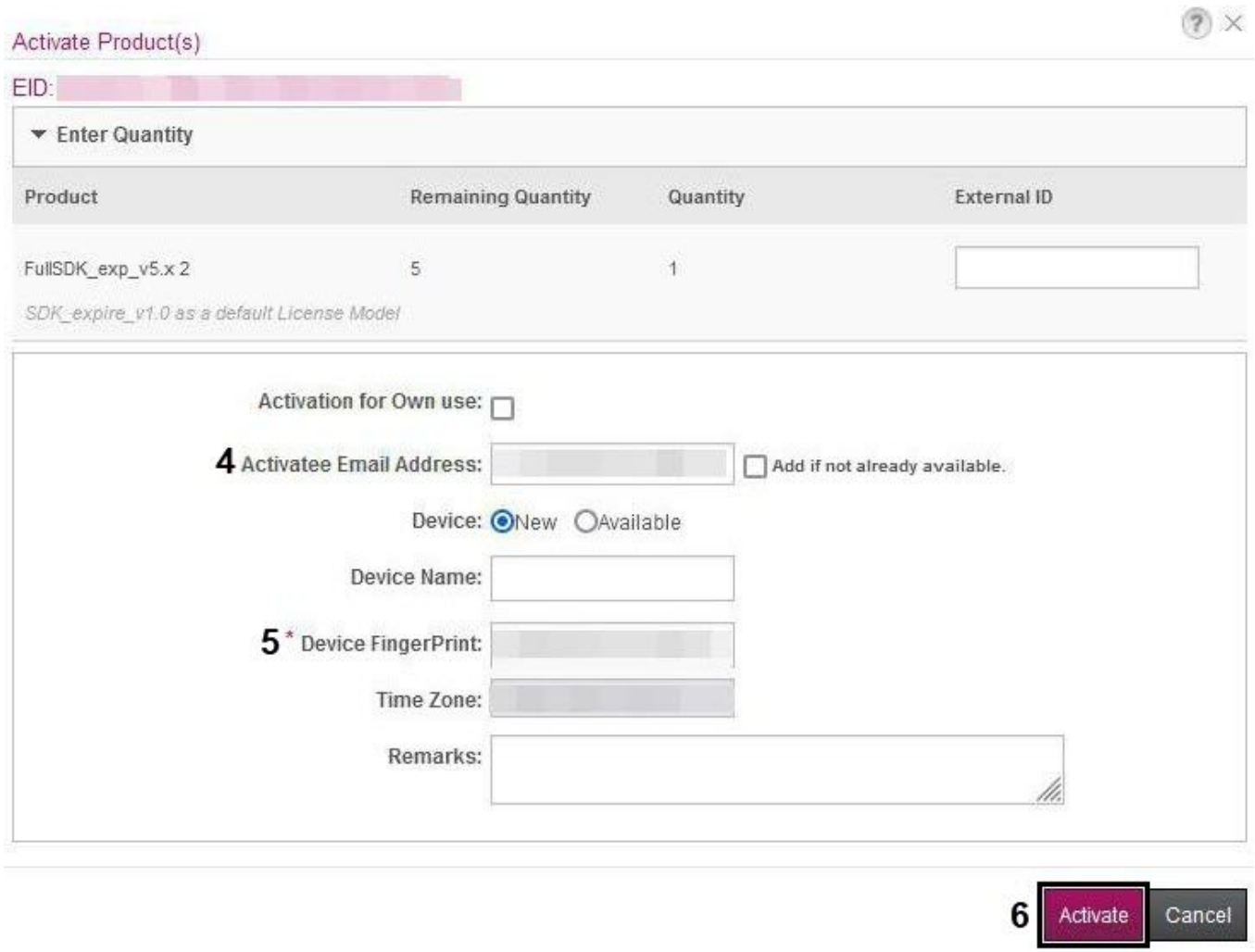
6. Click the **Activate** button (**2**) to activate the license.



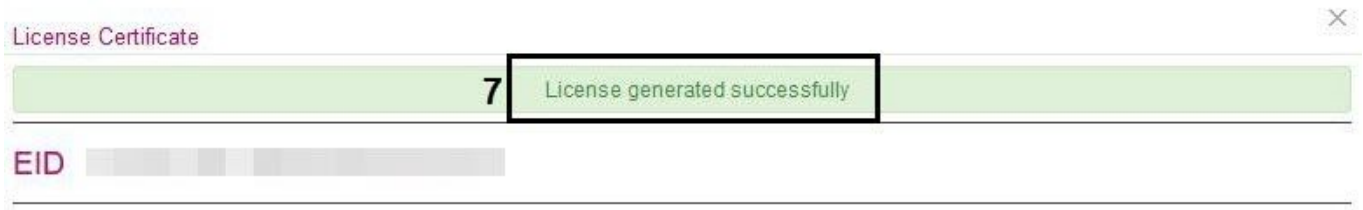
7. On the command line, run the following file as administrator: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\FingerprintViewer.exe.



8. To confirm the license activation, specify the Email address (**4**). The licenseFile.v2c file with license data will be sent to the specified Email address.



9. In the **Device FingerPrint** field (**5**) specify the FingerPrint data (**3**).
10. Click the **Activate** button (**6**).
11. Make sure the license is successfully activated (**7**).



12. Open the following file in a text editor: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.
13. Enter the received EID (**8**) and ProductID (**9**).

```
<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="                                    "/>   8
                <param name="ProductID" type="Value::String" text="                                    "/>   9
                <param name="Filename" type="Value::String" text="licenseFile.v2c"/>
                <param name="ContainerMode" type="Value::Int1" x="0"/>
        </section>
</settings>
```

14. Save the file: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\gpu\data\license.conf.

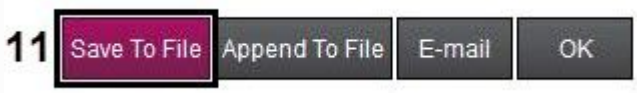
Face Detector (VL) license is activated.

Note

If the Server is connected to the Internet, the license will be checked automatically on the license server.
If the Server does not have an Internet connection, do the following:

1. Perform step 7, and steps 12—14 on the Server where the license will be used.
2. Perform steps 3—6, and steps 8—10 on any PC connected to the Internet.
3. Click the **View License** button (**10**).

4. Download the license file by clicking the **Save To File** button (**11**).



5. Place the downloaded licenseFile.v2c file on the Server to the folder: C:\Program Files\Common Files\AxxonSoft\DetectorPack\VLSdk\<licenseFile.v2c>.

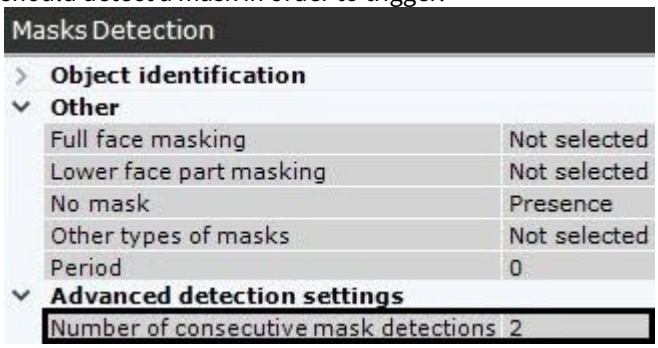
Face Detector (VL) license is activated on the Server with no Internet connection.

15.4.11.5 Configuring additional face detection tools

15.4.11.5.1 Configuring Masks Detection

To configure the Masks detection tool, do the following:

1. Enable the **Face mask detection** parameter in the Face detection tool settings (see Configuring Face detection(see page 280)).
2. In the **Number of consecutive mask detections** field, set the minimum number of frames in which the detection tool should detect a mask in order to trigger.



3. Depending on your particular task, set other parameters values according to the table.

Triggering event	Parameters values		
	Lower face part masking	**No mask**	**Full face masking**

No mask of any kind	Absence	Presence	Absence
No medical mask	Absence	Presence	Presence
No balaclava	Presence	Presence	Absence
Any mask present	Presence	Absence	Presence
Medical mask present	Presence	Absence	Absence
Balaclava present	Absence	Absence	Presence

Note

The **Other types of masks** parameter is not supported in this software version.

4. If required, you can set the advanced parameters (see Fine-tuning the Face detection tool(see page 282)).
5. Click the **Apply** button.

Configuring the Mask detection tool is complete.

15.4.11.5.2 Configuring Appearance in area and Loitering in area detection

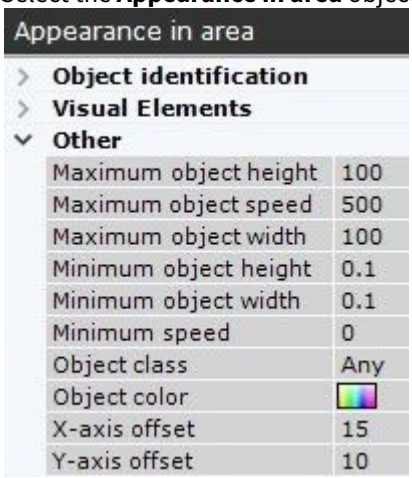
On this page:

- Appearance in area detection(see page 292)
- Loitering in area detection(see page 293)

15.4.11.5.2.1 Appearance in area detection

To configure the detection tool, do the following:

1. Select the **Appearance in area** object.



2. Configure the parameters of the captured face (just as with the detected objects, see Configuring detected objects(see page 266)).

Attention!

The object class should be either **Any** or **Face**.

Note

The metadata from the Face detection tool do not include color characteristics, so the color setting is not relevant for this detection tool.

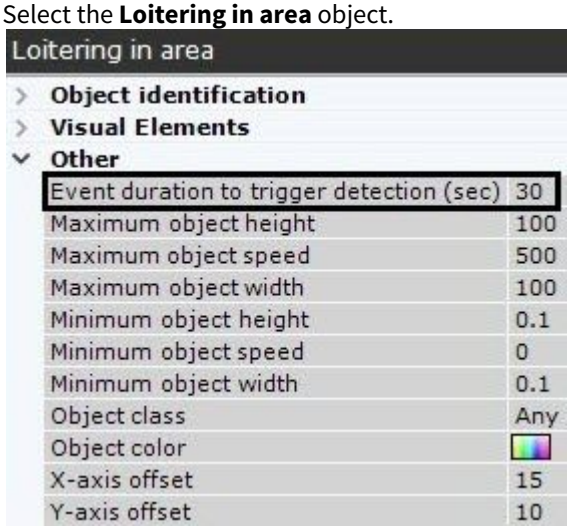
3. In the preview window, set an area inside the FOV where a person should appear. This is similar to the Scene analytics detection tools (see Configuring the Detection Zone(see page 266)).
4. Click the **Apply** button.

Configuring the Appearance in area detection tool is complete.

15.4.11.5.2.2 Loitering in area detection

To configure the detection tool, do the following:

1. Select the **Loitering in area** object.



2. In the **Event duration to trigger detection (sec)** field, set the maximum time in seconds of the object loitering in the analyzed area. When this time is exceeded, the detection tool will trigger. The value should be in the range [0; 86400].
3. Configure the parameters of the captured face (just as with the detected objects, see Configuring detected objects(see page 266)).

Attention!

The object class should be either **Any** or **Face**.

Note

The metadata from the Face detection tool do not include color characteristics, so the color setting is not relevant for this detection tool.

4. In the preview window, set an area inside the FOV where a person should loiter. This is similar to the Scene analytics detection tools (see Configuring the Detection Zone(see page 266)).
5. Click the **Apply** button.

Configuring the Loitering in area detection tool is complete.

15.4.11.5.3 Face Detection and Temperature Control with Mobotix M16 TR cameras

15.4.11.5.3.1 Functional parameters of the Face Detection and Temperature Control

When working with Mobotix M16 TR cameras, the standard face detection algorithm (see Functions of face detection tools(see page 279)) 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(see page 819)).

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(see page 411)).

15.4.11.5.3.2 Camera requirements for face detection and temperature control

Face detection with temperature control works properly if cameras are installed and set up as follows:

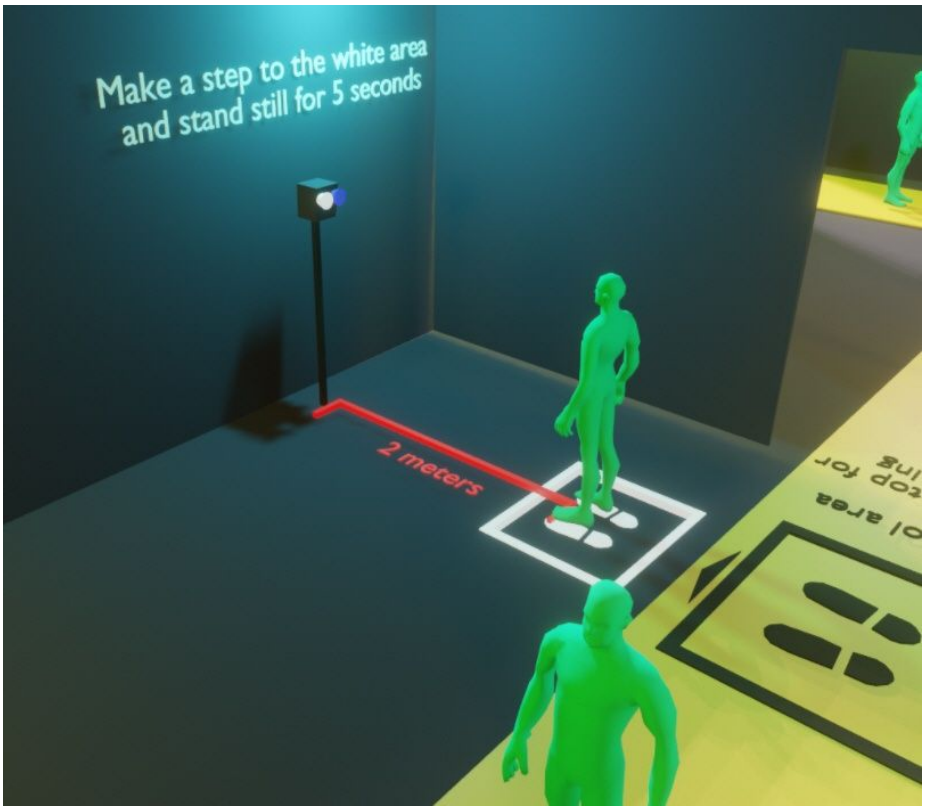
1. At least 8 frames per second.
2. Minimum resolution is at least 1280 x 960 pixels.
3. Indoor installation only.
4. To establish maximum measurement accuracy, avoid installing cameras near exits to street, in direct sunlight, and close to HVAC outlets.
5. Keep the distance from camera to the subject 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.

15.4.11.5.3.3 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.

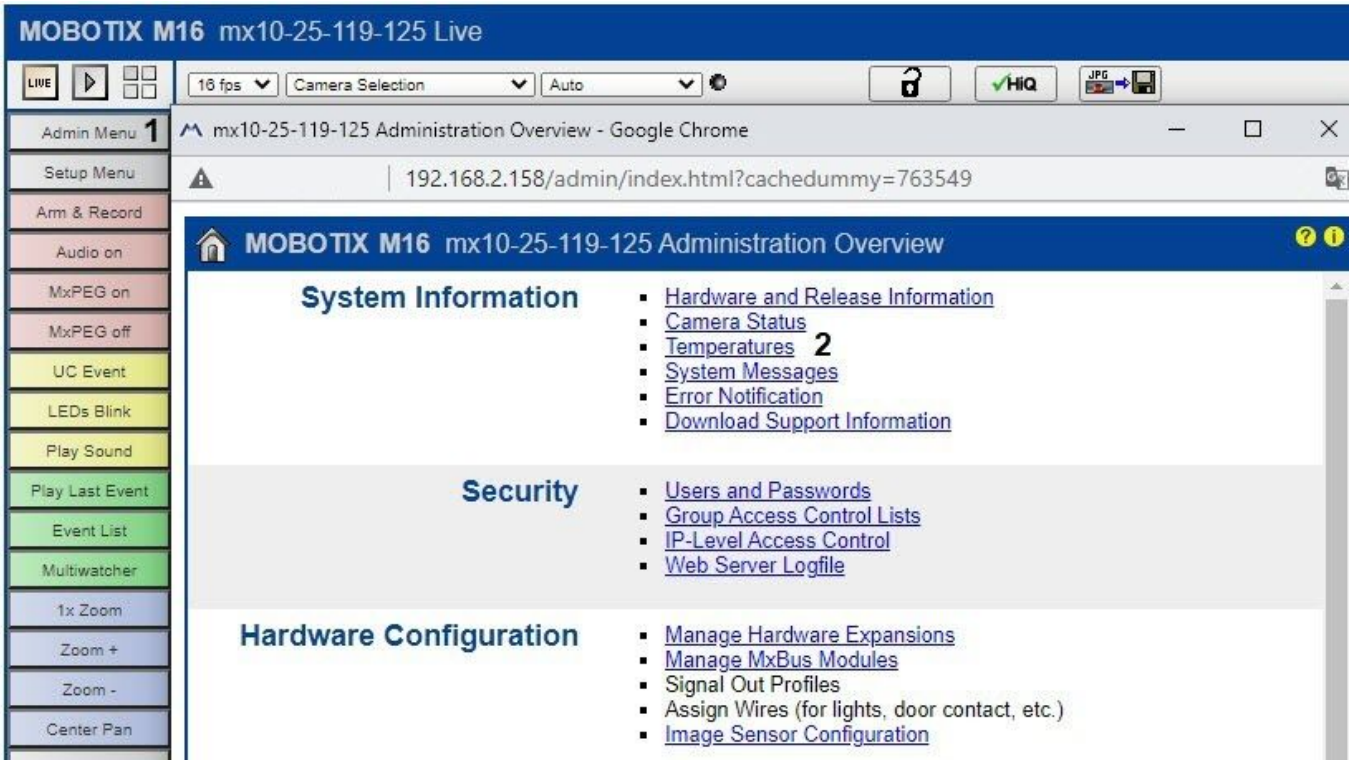


15.4.11.5.3.4 Pre-configuration of the Mobotix M16 TR camera

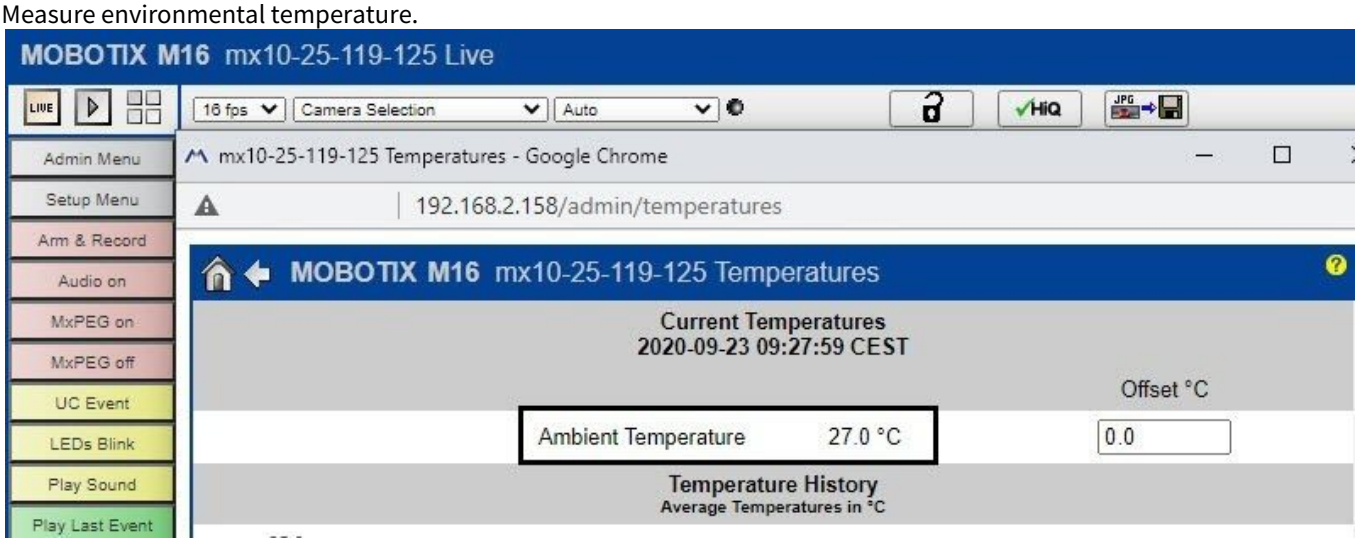
> **Attention!**
>
> Install MX-V5.2.6.7 (2020-06-16) or later firmware.
> For detailed configuration via the web interface, refer to manufacturer's instructions.

Before starting *Axxon One*, please configure the camera via the web interface:

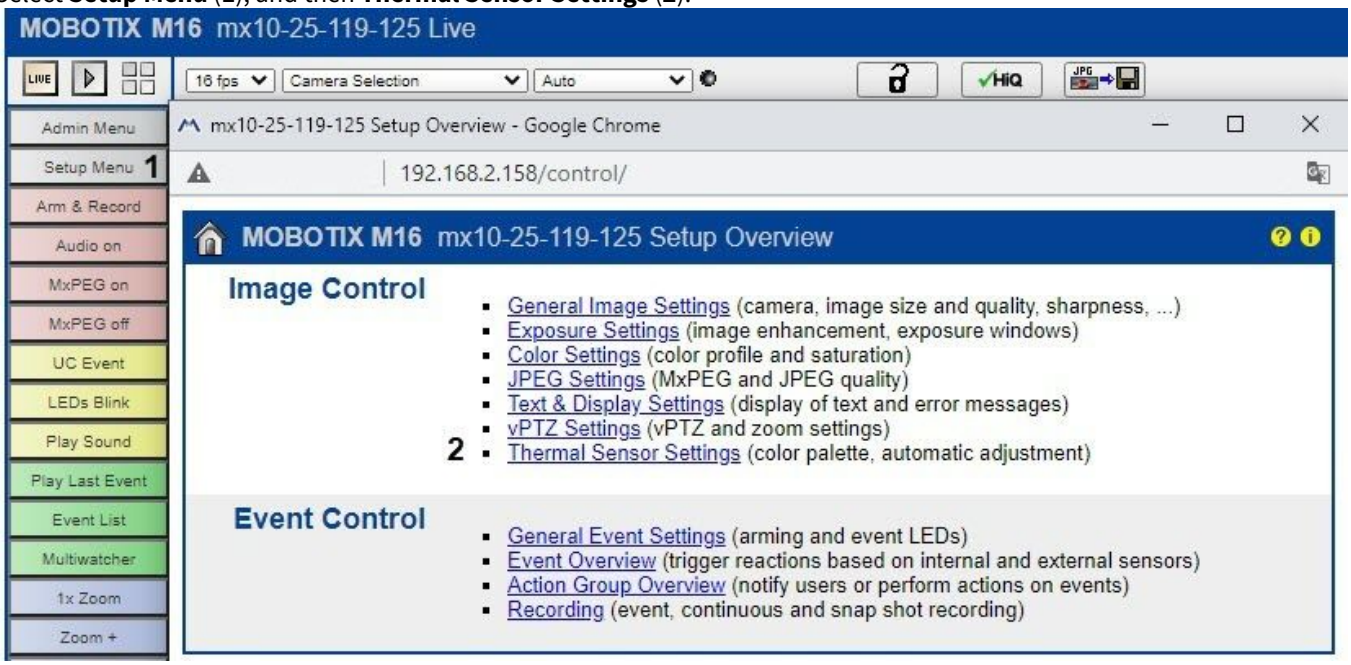
1. Proceed to admin menu (**1**), and select **Temperatures** (**2**).



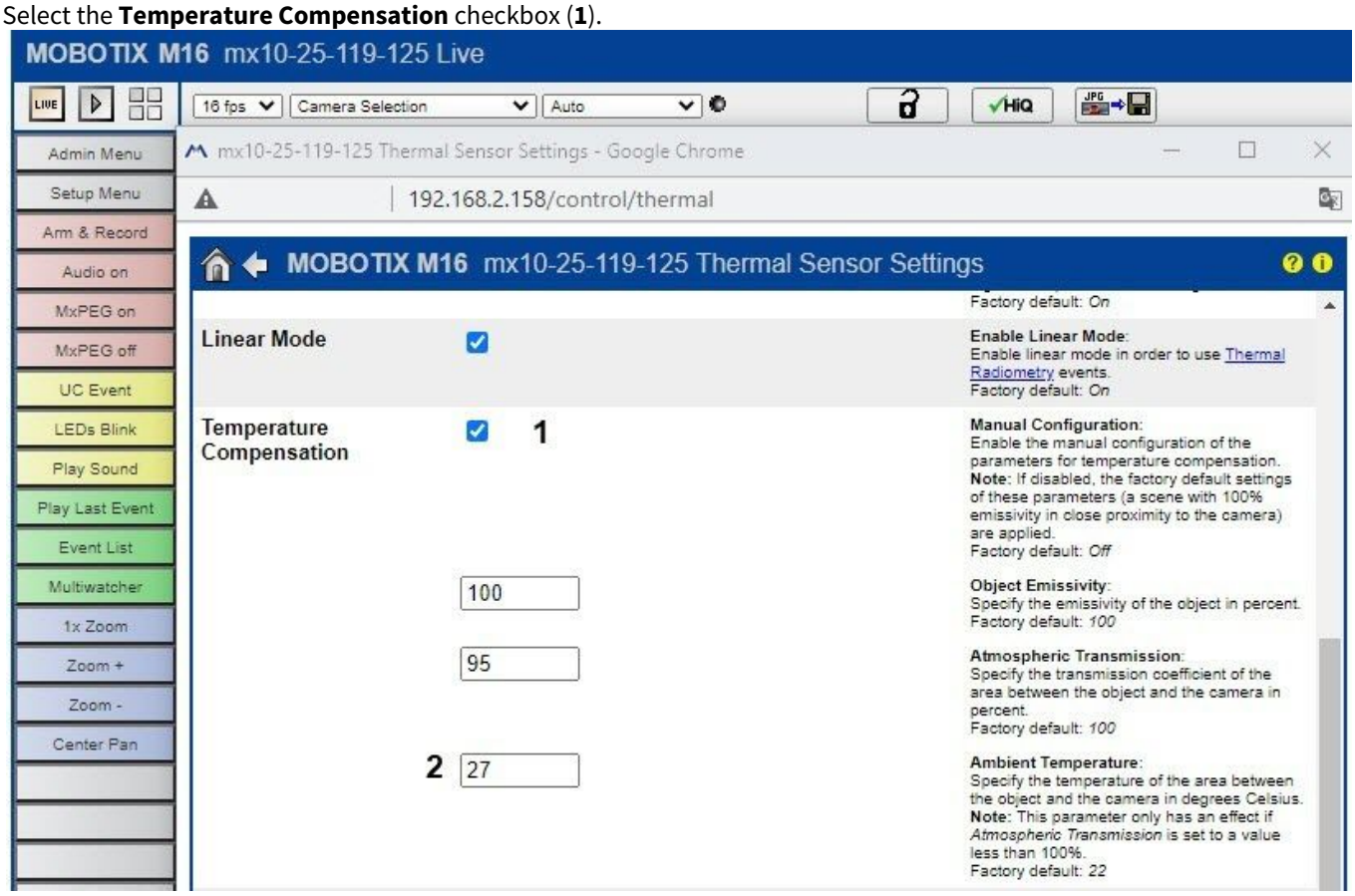
2. Measure environmental temperature.



3. Select **Setup Menu** (**1**), and then **Thermal Sensor Settings** (**2**).

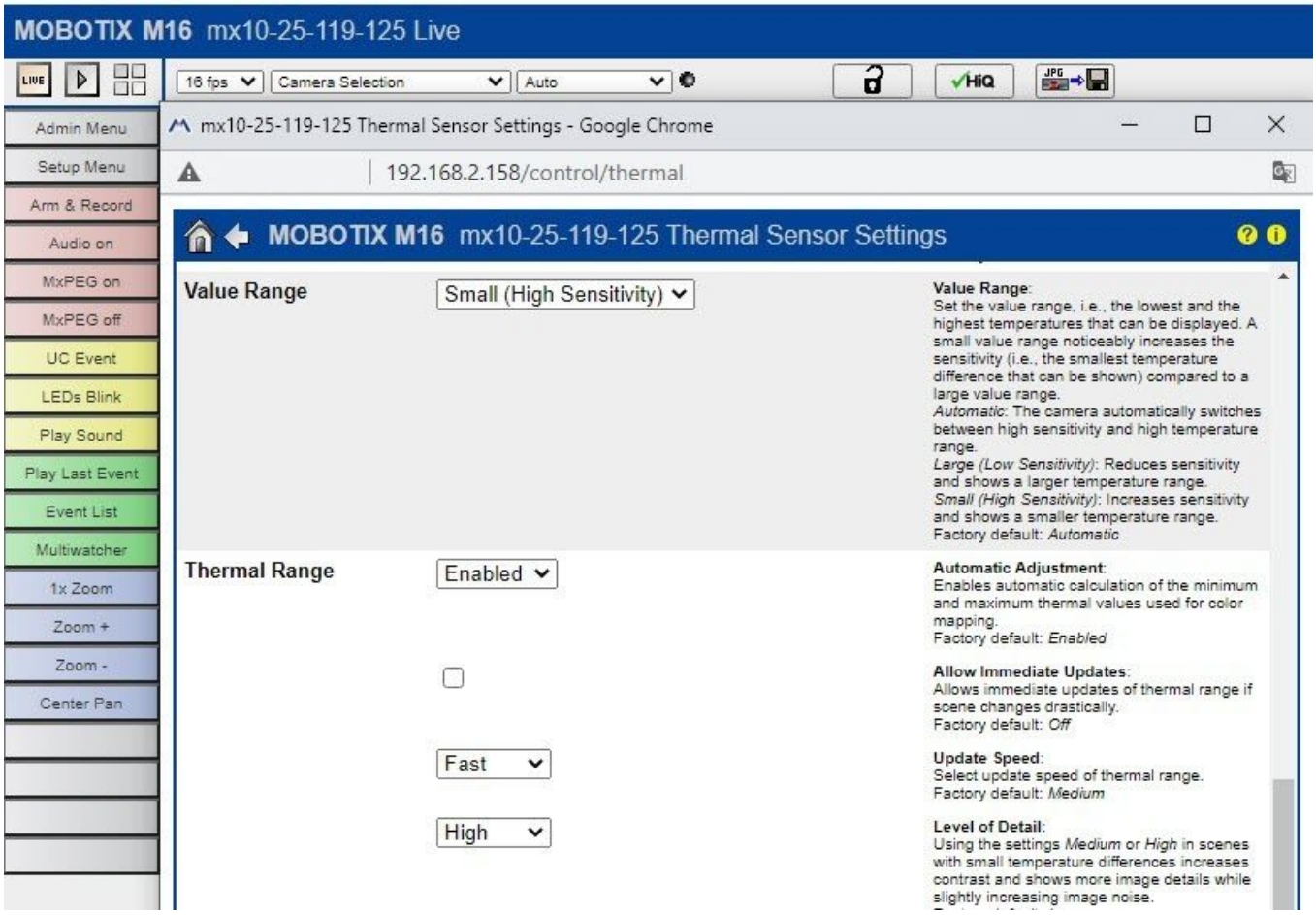


4. Select the **Temperature Compensation** checkbox (**1**).



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.

15.4.11.5.3.5 Configuring Face Detection and Temperature Control

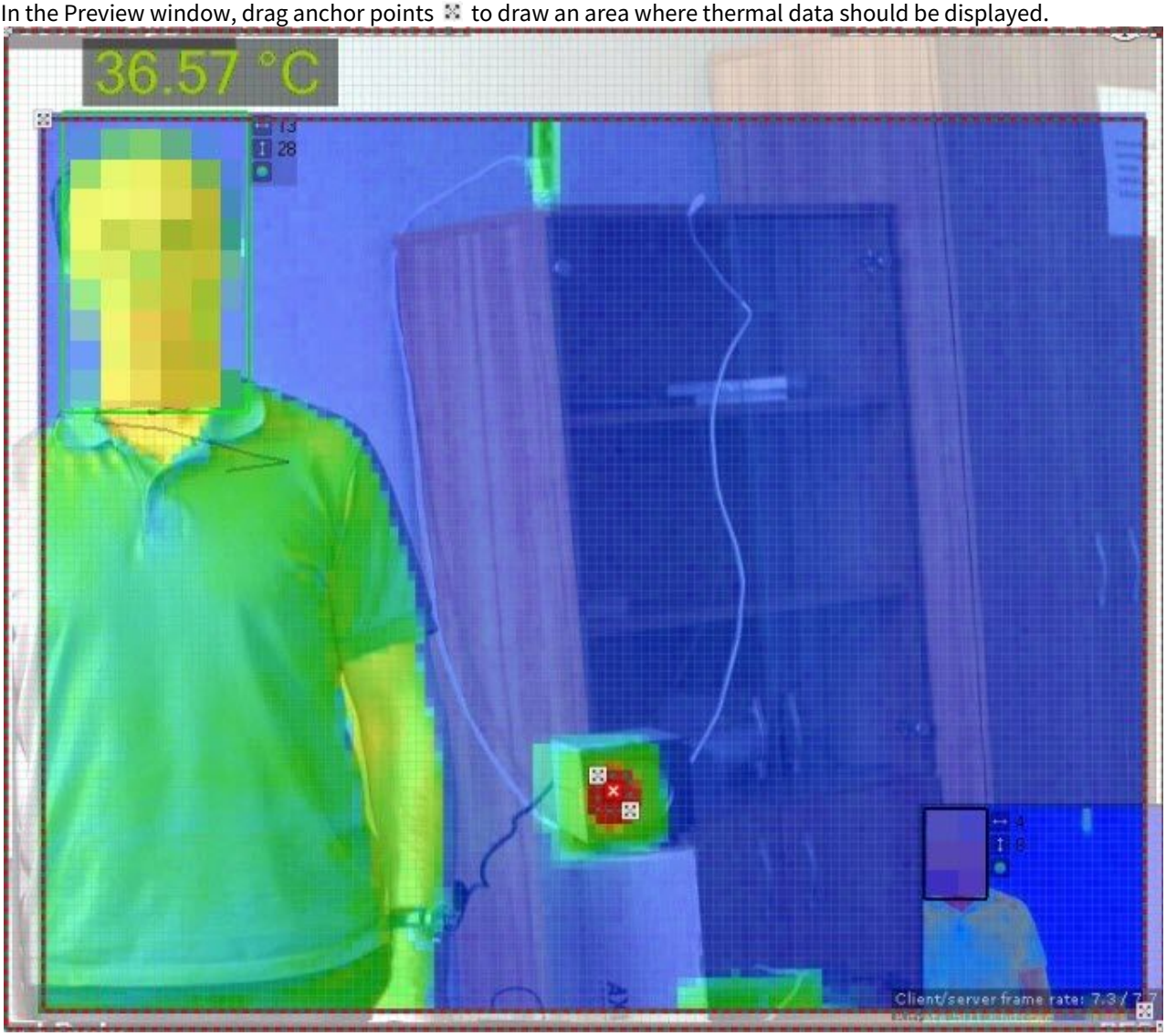
To configure face detection and temperature control, do the following:

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 Face detection(see page 280)).

7. Click the **Apply** button.

You have configured detection tool now.

15.4.11.6 Configuring real-time face recognition

In *Axxon One*, you can configure macros to run the automatic system reactions based on the created face lists (see Face lists[112]), 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* (see Connecting Axxon-domain to AxxonNet[113]).
2. Create one or more face lists in *AxxonNet* (see Face lists[114]).
3. Create a face detection tool (see Face detection tools(see page 278)).
4. Enable the **Real-time recognition** parameter in the face detection tool settings (see Configuring Face detection(see page 280), Configuring Face detection (VL)(see page 285)).
5. Select the condition to start the automatic system reaction (see Configuring filters for event-driven macros(see page 407), Configuring macros when working with face lists(see page 301)).
6. Select one or more actions for the automatic system reaction (see Settings specific to actions(see page 413)).
7. If necessary, configure information boards to display the information from the automatic system reaction (see Examples of macros used for working with face lists(see page 302), Configuring an Event Board(see page 490), Configuring a Dialog Board(see page 495)).

15.4.11.6.1 Configuring macros when working with face lists

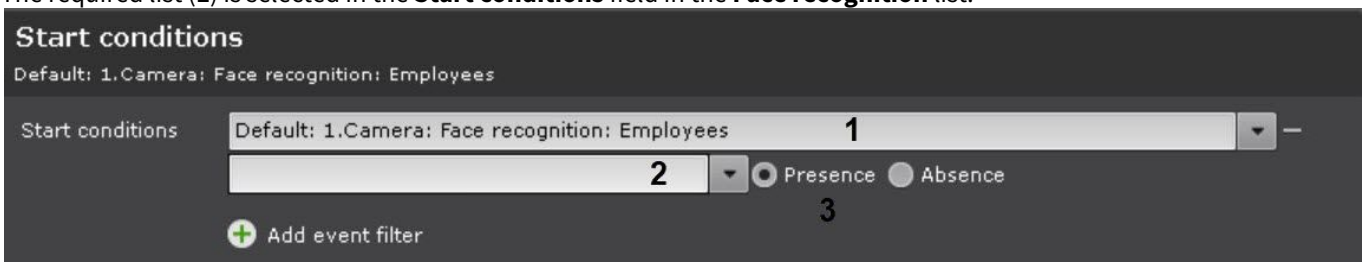
When working with face lists, you can configure the macro to trigger (see General information about the macros(see page 400)), when:

- 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.

15.4.11.6.1.1 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.



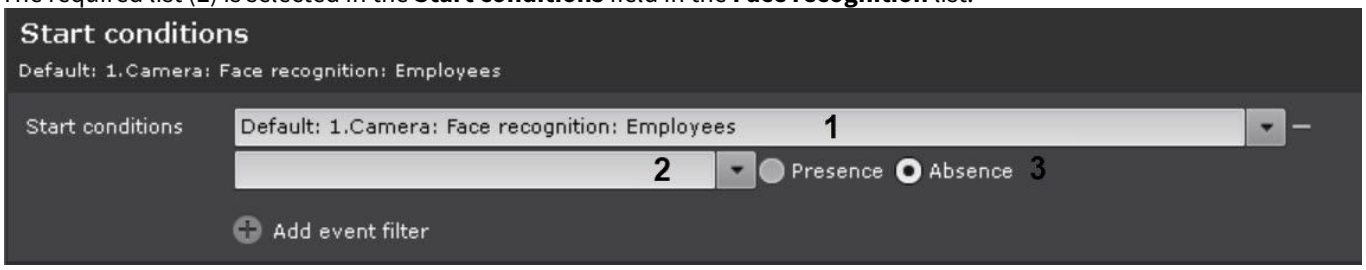
2. The field **2** is empty.
3. The **Presence** radio button is set (**3**).

15.4.11.6.1.2 Absence of the recognized face in the selected face list

In this case, the parameters for starting the macro are the following:

112 https://docs.axxonsoft.com/confluence/display/anet/Face+lists
113 https://docs.axxonsoft.com/confluence/display/anet/Connecting+Axxon-domain+to+AxxonNet
114 https://docs.axxonsoft.com/confluence/display/anet/Face+lists

1. The required list (**1**) is selected in the **Start conditions** field in the **Face recognition** list.

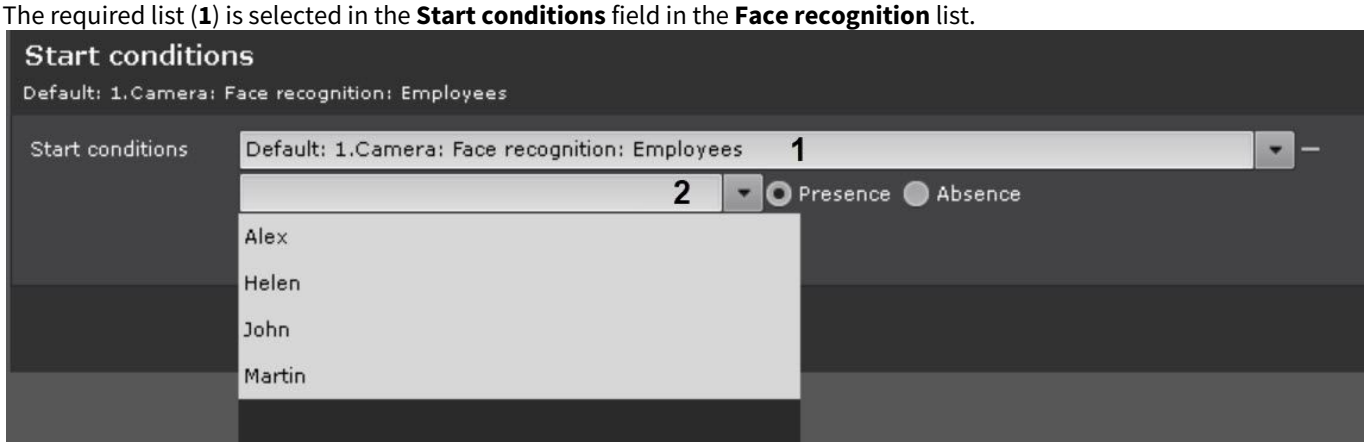


2. The field **2** is empty.
3. The **Absence** radio button is set (**3**).

15.4.11.6.1.3 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.

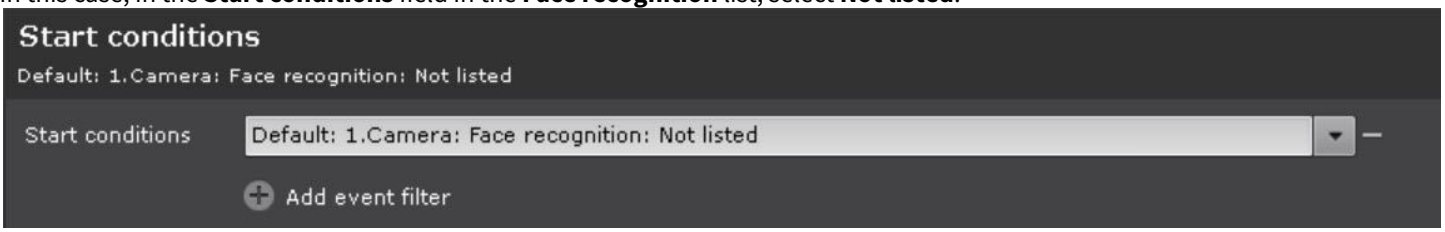


2. A specific person is selected in the field **2**.

> **Note**
>
> To select another person, clear the field **2** and re-open the list.

15.4.11.6.1.4 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**.



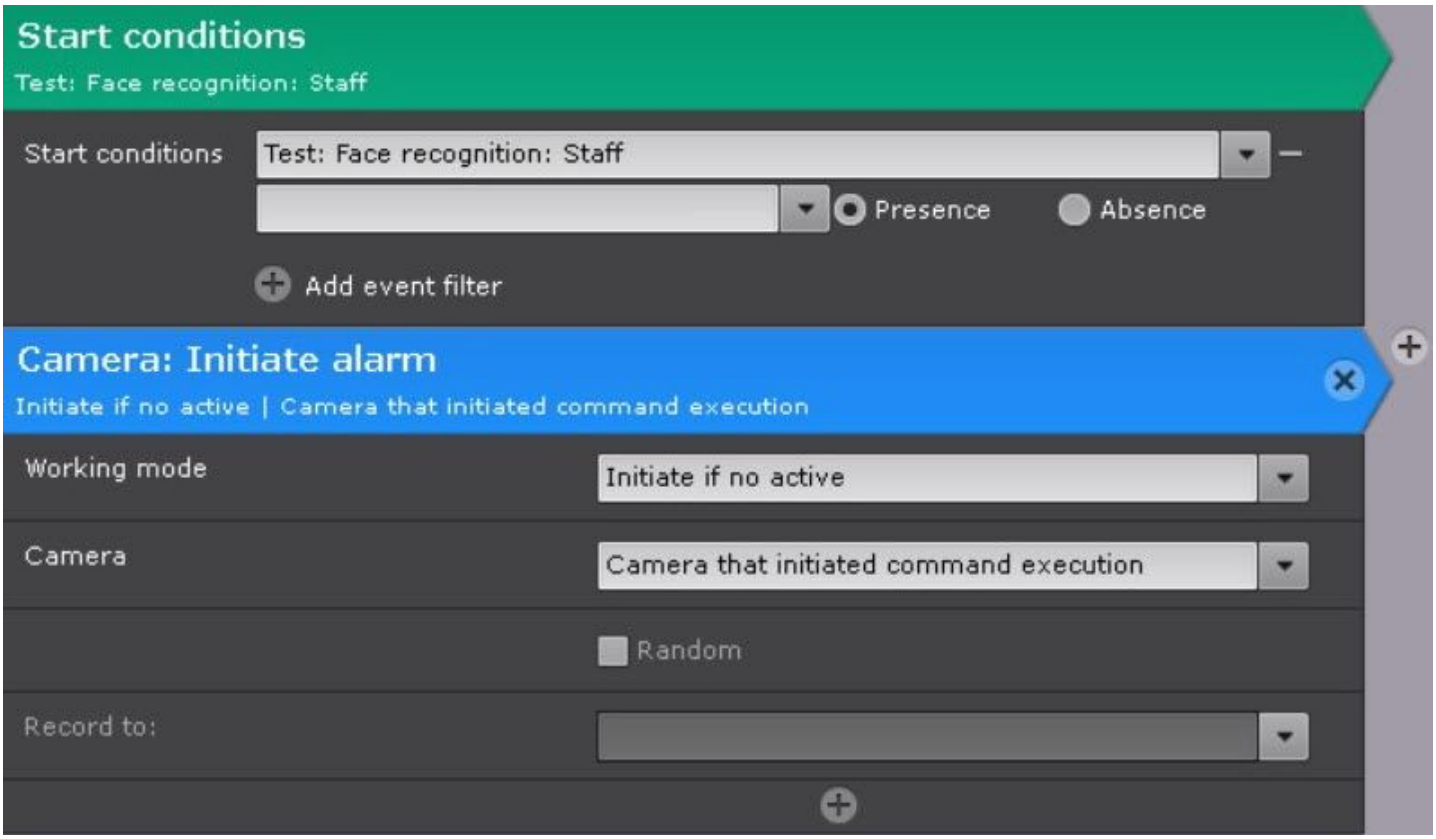
Examples of macros used for working with face lists(see page 302)

15.4.11.6.1.5 Examples of macros used for working with face lists

On this page:

- Alarm initiation(see page 303)
- Switching the output on for the authorized persons(see page 304)
- Sending an e-mail(see page 305)
- Starting export(see page 306)

Alarm initiation



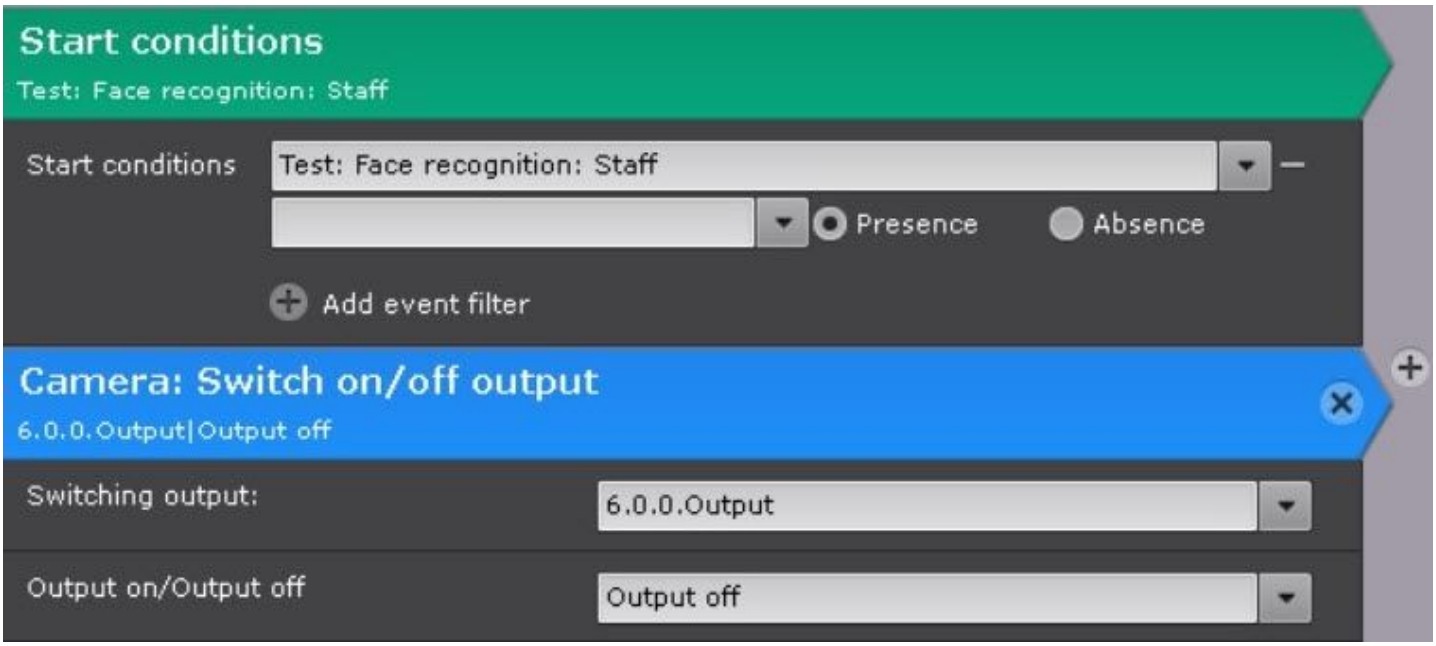
This macro can be used together with the Dialog Board (see Configure the Dialog Board(see page 495)).

If the Dialog Board is configured to display an alarm and linked with a video camera (see Linking cells(see page 481)), 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 Face lists[115]).

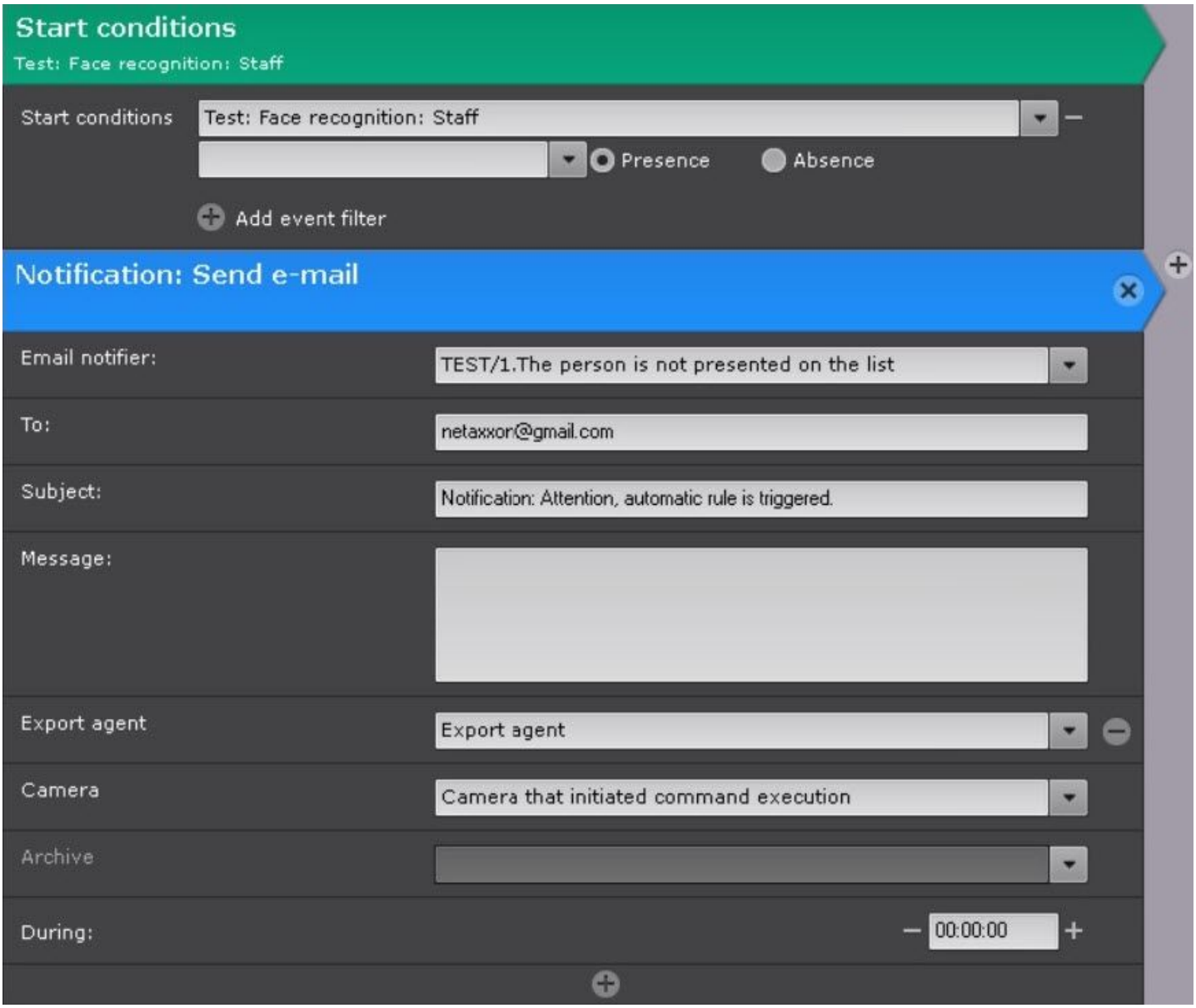
115 https://docs.axxonsoft.com/confluence/display/anet/Face+lists

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.

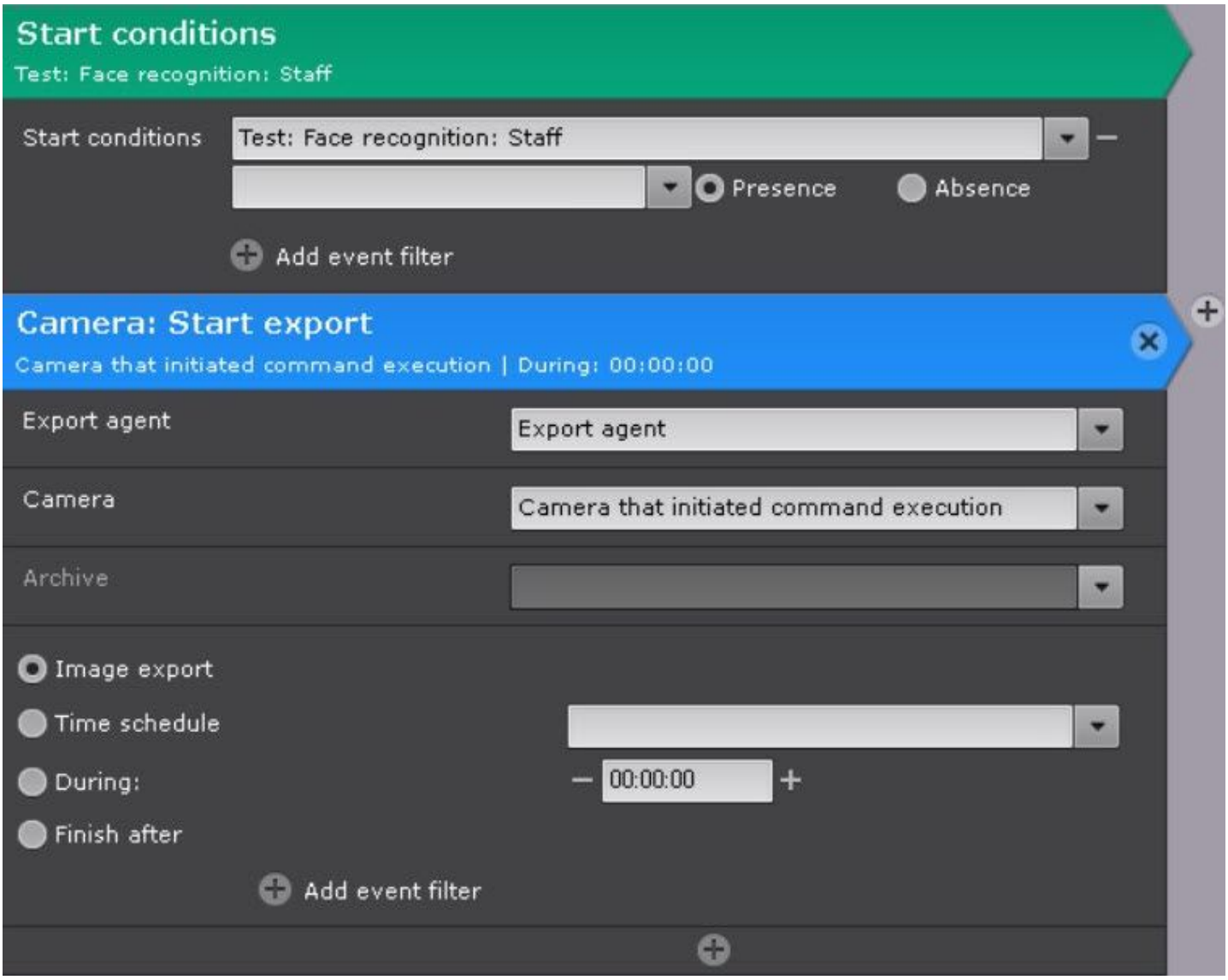
Sending an e-mail



If the e-mail is sent via the SMTP Server (see The E-mail notifier object(see page 435)), then 3 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.

15.4.11.6.2 Configuring FaceCube integration

Axxon One supports the FaceCube facial recognition server (see https://www.bio-cube.co.kr/vs-face).

Please see the FaceCube integration workflows below:

1. *Axxon One* captures and recognizes a face, then passes the facial image to the FaceCube facial recognition server.
2. FaceCube checks the facial image against the DB.
3. If a match is found, the *Axxon One* VMS receives the results (see Face recognition and search(see page 765)).

To configure FaceCube workflows, do as follows:

1. Configure the FaceCube facial recognition server and add Reference faces (see https://www.bio-cube.co.kr/).

2. Create a face list in *Axxon One* and enter the address of the FaceCube facial recognition server into the **List settings** field (see Face lists[116]).

3. Activate the **Real-time recognition on external service** parameter and **Send face images** in the facial recognition settings (see Configuring Face detection(see page 280)).
4. Configure automatic responses to positive identification against the list (see Configuring macros when working with face lists(see page 301)).

15.4.12 Automatic Number Plate Recognition (LPR/ANPR) tools

15.4.12.1 License plate recognition (VT)

15.4.12.1.1 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

116 https://docs.axxonsoft.com/confluence/display/anet/Face+lists

Proven installations	Tested
• Albania • Argentina • Azerbaijan • Belarus • Brazil • Colombia • Czech Republic • Georgia • Israel • Kazakhstan • Mexico • Moldova • Mongolia • Poland • Russia • Spain • Ukraine • United Kingdom • Uzbekistan • Bulgaria • Chile • Austria • Belgium • France • Guatemala • Hungary • Latvia • Lithuania • Netherlands • Paraguay • Taiwan • Uruguay • Iran • Jordan	• Armenia • Bolivia • Bosnia and Herzegovina • Denmark • Ecuador • El Salvador • Finland • Greece • Italy • Malta • Montenegro • Norway • Peru • Portugal • Philippines • Romania • Slovakia • Slovenia • Sweden • Tajikistan • Canada • Estonia • Germany • Honduras • India • Kyrgyzstan • Nicaragua • Panama • Serbia • Korea Republic • Switzerland • Turkmenistan • Croatia • Malaysia • New Zealand • Singapore • Turkey • Bahrain • Luxembourg • South Africa • Vietnam • Andorra • Kenya • Australia

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(see page 338)).
4. Determine the direction of the vehicle.

License plate recognition (VT) works in one of the following modes (see Configuring License plate recognition (VT)(see page 314)):

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(see page 74)).

15.4.12.1.2 Camera and image requirements for License plate recognition (VT)

On this page:

- General requirements(see page 310)
- Video camera requirements(see page 310)
- Camera installation requirements(see page 312)
- License plate image requirements(see page 313)
- Recommendations for highways(see page 314)

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.

15.4.12.1.2.1 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.

15.4.12.1.2.2 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.
   Expand the table with focal length settings

Distance to the object, m	Object width, m	Focal length, mm	Viewing angle, degrees	Sensor size, inches
3	4	4	85	1/3

Distance to the object, m	Object width, m	Focal length, mm	Viewing angle, degrees	Sensor size, inches
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.
   Expand the table with shutter speed settings

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

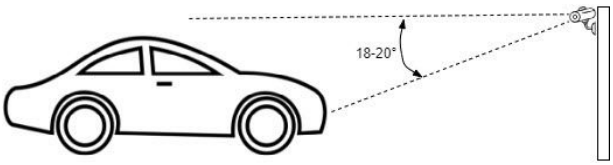
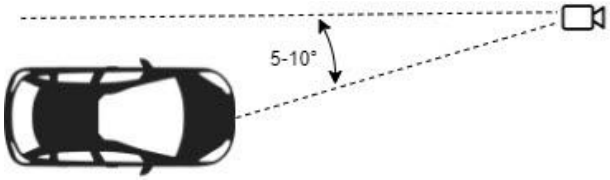
Sensor size	1/3 inch or more. During recognition, the physical size (area) of an individual pixel in a sensor is more important than the physical size (area) of the sensor itself. Larger pixel size provides better recognition in low light conditions
Pixel size	3.75 micrometers (µm) or more. The larger 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[117] 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.

15.4.12.1.2.3 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°	

117 https://www.emva.org/standards-technology/emva-1288/

Angle	Recommended value	Maximum value	Scheme
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 camera angle is checked by the "one-line rule": an imaginary horizontal line must cross both the first and last characters on the license plate.

15.4.12.1.2.4 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);

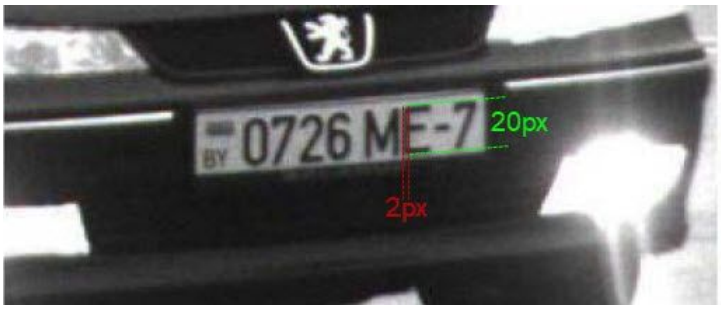
- interlaced;

- 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:



15.4.12.1.2.5 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.

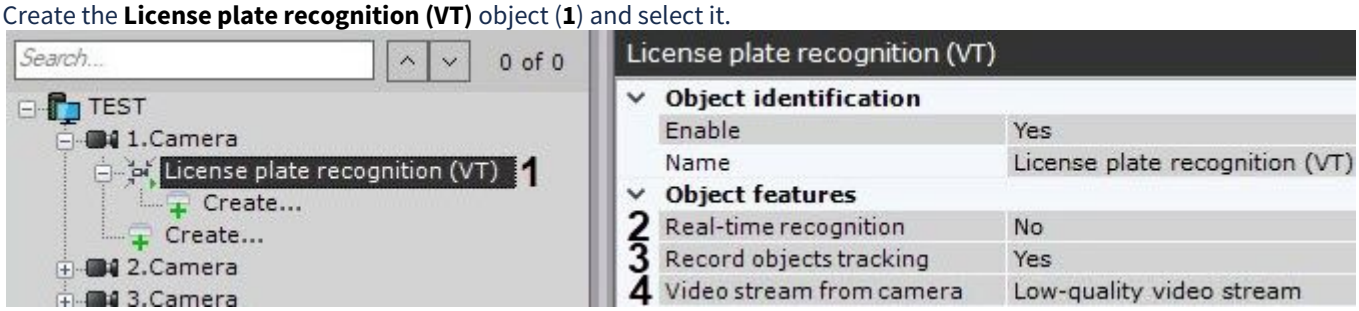
15.4.12.1.3 Configuring License plate recognition (VT)

Attention!

- The license plate recognition requires a CPU that supports the SSE4.1/SSE4.2 instructions.
- *Axxon One* ANPR/LPR is not compatible with *Auto PSIM*. Uninstall *Axxon One* VMS and *Auto PSIM*, then reinstall *Axxon One*.

To configure ANPR, do as follows:

1. Download ANPR (VT) from the website [118] and install it.
2. Create the **License plate recognition (VT)** object (**1**) and select it.



3. If you need to use this detection tool for real-time license plate recognition, set the corresponding parameter to **Yes** (**2**) (see Configuring real-time vehicle license plate recognition [119]).
4. If you need to enable recording of metadata to the database, select **Yes** from the **Record objects tracking** list (**3**).
5. 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 (**4**).
6. Select the **Algorithm for detecting vehicle direction** (**1**):

118 https://www.axxonsoft.com/support/downloads/detector-pack
119 https://docs.axxonsoft.com/confluence/display/one1en/Configuring+real-time+vehicle+license+plate+recognition

a. By LP coordinates—if the license plate coordinates shift from top to bottom, then the vehicle is moving towards the camera; if the license plate coordinates shift from bottom to top, then the vehicle is moving away from the camera;
b. By LP scale—if the license plate scale increases, then the vehicle is moving towards the camera; if it decreases, then the vehicle is moving away from the camera.

7. Select detection tool working mode: standard or neural (**2**).

License plate recognition (VT)	
Other	
Algorithm for detecting vehicle direction	By LP coordinates
Analysis mode	Standard (Morph)
Country 1 name	Albania
Country 2 name	Not used
Country 3 name	Not used
Country 4 name	Not used
Country 5 name	Not used
Decoder mode	CPU
Frame size change	1920
License type	Search in archive
Maximum LP width	20
Minimum LP width	5
Mode	CPU
Number of frames	6

8. In the appropriate fields, select one or more countries for ANPR (**3**).

> **Attention!**
>
> - The more countries you select, the slower the recognition works and the greater the likelihood of the recognition error.
> - To recognize the old USSR license plates, you need to select the corresponding country in the list.

9. Select a processing resource for decoding video streams (**4**) (see Hardware requirements for GPU based video decoding(see page 54)). 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.
10. Analyzed framed are scaled down to a specified resolution (**5**, 1920 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 (down to 512*384), as after the first division, the number of pixels on the longer side exceeds the limit (1024 > 1000).
> - If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.

11. Select the current license type (**6**).

License	Description
Search in archive	Basic ANPR Search License. **Attention!** This type of license provides a 30-sec delay between the number recognition and the corresponding event (see Vehicle number plate recognition and search[120]).

120 https://docs.axxonsoft.com/confluence/display/one1en/Vehicle+number+plate+recognition+and+search

License	Description
Standard (25 FPS or 6 FPS)	The 25 FPS license has a priority. The 6 FPS license is used only if you don't have 25 FPS license. You cannot use the license plate recognition function if you have not purchased both licenses.
Fast speed (25 FPS)	The "Fast" license allows you to process video feeds up to 25 FPS with a maximum vehicle speed of 150 km/h. You cannot use the license plate recognition function if you have not purchased the license.
Slow speed (6 FPS)	The "Slow" license allows you to process video feeds up to 6 FPS with a maximum vehicle speed of 20 km/h. You cannot use the license plate recognition function if you have not 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)(see page 320)). You can use a 60-day trial key (see Licensing of the software module for License plate recognition (VT)(see page 320)).
- You can use only a hardware key on virtual machines. To use a hardware key, select the **Standard** (25 FPS or 6 FPS) license type.

12. Set the maximum and minimum width of the vehicle license plate as a percentage of the FOV width (**7**, **8**).

Attention!

The **Minimum LP width** parameter affects the CPU load as follows: the higher the parameter is, the higher the load.

13. Choose a processor to run detection on (**9**, see Hardware requirements for License plate recognition (VT)(see page 55), General Information on Configuring Detection(see page 234)). In standard mode, detection runs on the CPU only. In neural network analysis mode, the algorithm runs on the NVIDIA GPU.

Attention!

Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

14. Set the number of frames required for LPR/ANPR (**10**). This is a necessary condition, but it is not sufficient for the first output. This condition delays the LPR output. This parameter allows increasing the reliability of the results, as well as hiding false positives.
15. If necessary, configure the advanced detection settings (see Fine-tuning the VT number plate detection tool(see page 317)).

16. You can configure the ANPR area in FOV. The area is resized by moving the anchor points.

> **Note**
>
> - For your convenience, you can click the button and configure the mask on a still frame. To undo, click this button again.
> - Detection area is displayed by default. You can click the button to hide the area. To undo, click this button again.

17. Click the **Apply** button.

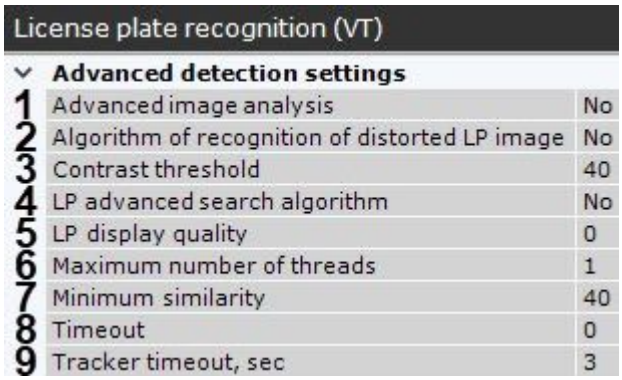
Configuration of ANPR is now complete.

15.4.12.1.4 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.

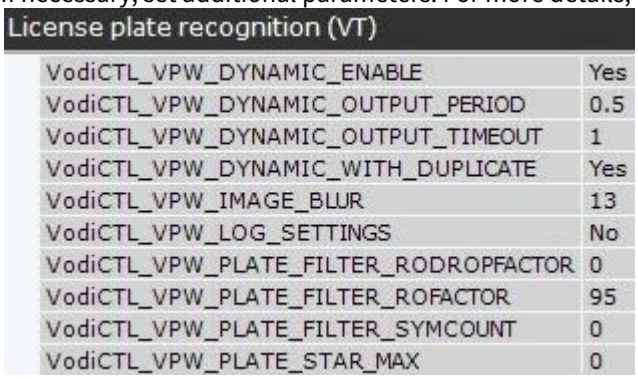
6. Specify the maximum number of recognition threads (**6**). If the value is **0**, the recognition process will occur in the same thread that starts it.

   > **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.



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 microseconds) 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 microseconds) 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.

15.4.12.1.5 Licensing of the software module for License plate recognition (VT)

On this page:

- Installing the license key environment(see page 320)
- Installing a demo license(see page 320)
- Installing a hardware key(see page 321)
- Installing a software key(see page 321)
- Activating and updating the license(see page 323)
- Removing a license(see page 324)
- Checking a license(see page 324)

15.4.12.1.5.1 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(see page 74)).

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.

15.4.12.1.5.2 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(see page 74)).

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(see page 768)).

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[121] web application, on the **Sentinel Keys** tab.

The installation of the demo license is now complete.

15.4.12.1.5.3 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[122] web application, on the **Sentinel Keys** tab.

The installation of the hardware key is now complete.

15.4.12.1.5.4 Installing a software key

Attention!

Before you install a software key, it is necessary to install the Sentinel LDK Run-time environment.

Attention!

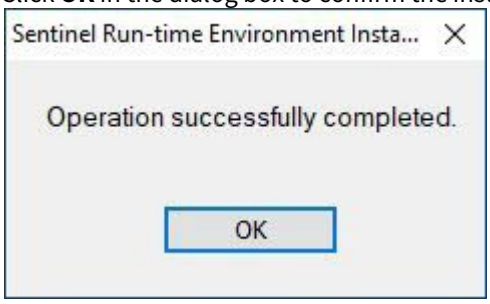
The License plate recognition (VT) license is not automatically transferred to a new node in a failover system (see Configuring Failover VMS(see page 587)).
To ensure the License plate recognition (VT) operation, it is necessary to manually activate the license on the computer where the node is running.

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.

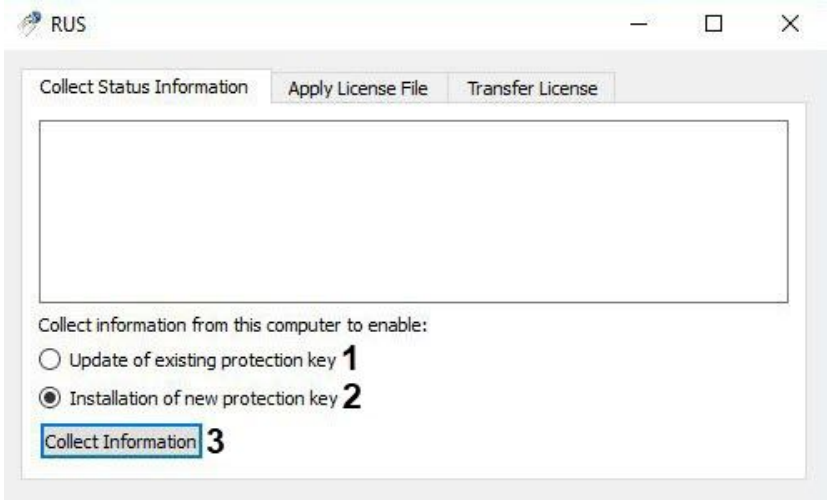
121 http://127.0.0.1:1947/
122 http://127.0.0.1:1947/

4. Click **OK** in the dialog box to confirm the installation is completed.

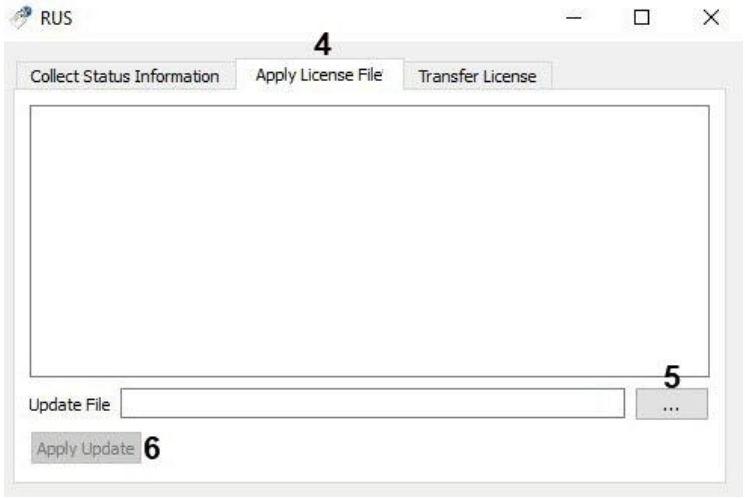


5. Run the RUS_EOAWT.exe file to start the Remote Update System. The **RUS** dialog box opens.

> **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[123] web application, on the **Sentinel Keys** tab.

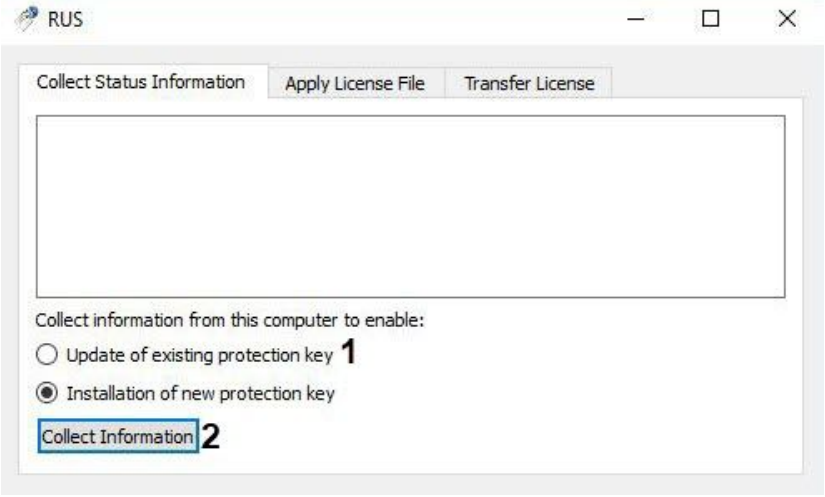
The installation of the software key is now complete.

15.4.12.1.5.5 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.

123 http://127.0.0.1:1947/

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[124] web application, on the **Sentinel Keys** tab.

The activation/update of the license is now complete.

15.4.12.1.5.6 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.

15.4.12.1.5.7 Checking a license

You can check the current license status on the Server. To do this, open the Sentinel Admin Control Center[125] web application. The license information is displayed on the **Features** tab.

15.4.12.2 License plate recognition (IV)

15.4.12.2.1 License plate recognition (IV) features and specifications

License plate recognition (IV) is designed to implement the following functions:

1. Recognize the license plate number of vehicles.

   List of supported countries: Australia, Belarus, Brazil, Canada, China, Czech Republic, Egypt, Finland, France, Germany, Great Britain, India, Indonesia, Israel, Italy, Japan, Kazakhstan, Mexico, Monaco, Mongolia, Pakistan, Poland, Qatar, Russia, Republic of South Africa, Saudi Arabia, Slovenia, South Korea, Spain, Sri Lanka, 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);

124 http://127.0.0.1:1947/
125 http://127.0.0.1:1947/

- 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 only for Brazil.

2. Write a recognized number to a database.
3. Check the recognized license plates of vehicles on the lists of license plates.

Note

Install the additional Addon IV LPR to work with License plate recognition (IV) (see Installing DetectorPack add-ons(see page 74)).

Attention!

Only a 64-bit version is available.

15.4.12.2.2 Camera requirements for License plate recognition (IV)

To ensure the recognition of the license plates with License plate recognition (IV), it is necessary to install and configure the cameras to meet the following requirements:

15.4.12.2.2.1 **Camera requirements**

1. The minimum video resolution is 640*480, the recommended resolution is 720p or 1080p.
2. The minimum frame rate is 15 FPS, the recommended frame rate is 25–30 FPS.
3. Autofocus and zoom would be useful for making small adjustments after configuring the detection tool.
4. Automatic white balance.
5. IR for night mode with good contrast of license plate images.
6. HDR or WDR.
7. In order to recognize state license plates on high-speed roads, the camera should have the Global Shutter mode

15.4.12.2.2.2 **Video requirements**

1. The video image should be clear, contrasting, without distortion, not blurred.
2. The video image should have minimum noise in low light conditions.
3. The size of the license plate should be 15–70% of the total size of the image.
4. The license plate must contain no more than two rows of characters.

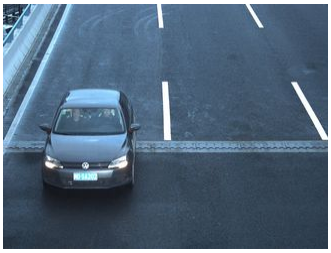
15.4.12.2.2.3 **Camera installation requirements**

1. The video camera should be mounted at 0.6–2.4 meters above the ground.
2. The angle formed by the lower line of the license plate and the horizon line should be from 0 to 20 degrees.

15.4.12.2.2.4 Examples of correct and incorrect video images

Video images that meet the video camera mounting and setup requirements for the Licence plate recognition (IV).

Video images that do not meet the video camera mounting and setup requirements for the Licence plate recognition (IV).



15.4.12.2.3 Configuring License plate recognition (IV)

To configure License plate recognition (IV), do as follows:

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 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(see page 100), Starting a Server(see page 94)).

4. Create the **License plate recognition (IV)** object and select it.

License plate recognition (IV)	
Object identification	
Enable	Yes
Name	License plate recognition (IV)
Object features	
1 Real-time recognition	No
2 Record objects tracking	Yes
3 Video stream from camera	Low-quality video stream
Visual Elements	
Visual Element	Detection area (rectangle)

5. If you need to use this detection tool for real-time license plate recognition, set the corresponding parameter to **Yes** (**1**, see Configuring online Vehicle License Plate recognition(see page 337)).
6. If you need to record metadata, select **Yes** from the **Record objects tracking** list (**2**).
7. If the camera supports multistreaming, select the stream for which detection is needed (**3**). Selecting a low-quality video stream allows reducing the load on the Server.
8. Select the **Algorithm for detecting vehicle direction** (**1**):
   a. By LP coordinates: if LP coordinates change position from top to bottom, the vehicle moves towards the camera. If LP coordinates change position from bottom to top, the vehicle moves away from the camera.
   b. By LP scale change: if LP scale increases, the vehicle moves towards the camera. If LP scale decreases, the vehicle moves away from the camera.

License plate recognition (IV)	
Other	
1 Algorithm for detecting vehicle direction	By LP coordinates
2 Country name	USA, medium CPU load
3 Decoder mode	CPU
4 Frame size change	1920
5 Frames processed per second	100
6 Maximal number of cores	0
7 Maximum LP width	10
8 Minimum LP width	1
9 Minimum recognition quality, in %	80
10 Processing unit	CPU

9. Select the country from the list for LPR and the level of recognition accuracy (**2**).
   a. High CPU load, high recognition accuracy—provides the maximum recognition accuracy, but creates a high load on the CPU and/or GPU.
   b. Medium CPU load, medium recognition accuracy—provides a high recognition accuracy, requires less computing resources than the maximum accuracy.
   c. Low CPU load, low recognition accuracy—provides the fastest recognition speed, but the recognition accuracy is low.
10. Select a processing resource for decoding video streams (**3**). 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.
11. By default, the analyzed framed are scaled down to a specified resolution (**4**, 1920 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).

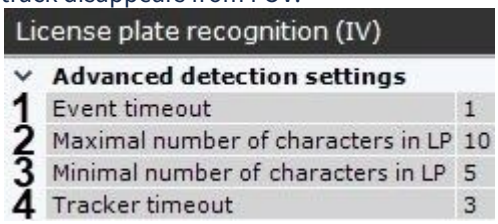
If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.

12. Set the number of frames processed per second by the detection tool (**5**). The value should be in the range [0,016; 100].
13. Set the maximum number of processor cores available for the detection tool. The **0** value means that all cores are used (**6**). The value should be in the range [−1; 1].
14. Set the maximum and minimum width of the license plate as a percentage of the frame width (**7**, **8**). The value should be in the range [1; 100].
15. Set minimum quality of LPR (**9**). The higher the minimum recognition quality, the fewer false positives will be detected. The value should be in the range [0; 100].
16. Select the processor for the detection tool—the CPU or one of NVIDIA GPUs (**10**, see General Information on Configuring Detection(see page 234)).

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 neural analytics on GPU(see page 240)).
If there are several GPUs in the system, a specific NVIDIA GPU value can be assigned to each License plate recognition (IV) tool.

17. In the **Event timeout** field (**1**) specify the time interval in seconds between the initial LP recognition and event registration. The value should be in the range [0; 3600]. The **0** value sets the event registration to the moment when the track disappears from FOV.



18. Specify the maximum and minimum number of characters in LP (**2**, **3**). The value should be in the range [1; 20].
19. In the **Tracker timeout** field (**4**), enter a time period in seconds after which the vehicle track is considered lost. The value should be in the range [0; 3600].

Note

This parameter should be used to prevent double detections that occur, for example, when the LP is recognized in the frame then gets hidden behind a visual obstacle and after that gets recognized by the detection tool again. If you set the timeout longer than the time of possible LP overlapping in the frame, the detection tool will trigger only once.

20. You can configure the LPR area in the FOV. The area is resized by moving the anchor points .

> **Note**
>
> For your convenience, you can click the button and configure the mask on a still frame. To undo, click this button again.
>
> Detection area is displayed by default. You can click the button to hide the area. To undo, click this button again.

21. Click the **Apply** button.

Configuration of License plate recognition (IV) is now complete.

15.4.12.3 License plate recognition (RR)

15.4.12.3.1 License plate recognition (RR) features and specifications

The License plate recognition (RR) is designed to implement the following features:

1. Recognize license plates.

   > **Note**
   >
   > List of supported countries: Armenia, Austria, Azerbaijan, Argentina (starting with *DetectorPack* 3.9.0), Belarus, Belgium, Brazil, Brunei, Bulgaria, Colombia (starting with *DetectorPack* 3.9.0), Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Ireland, Italy, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Moldova, Myanmar, Netherlands, Peru, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, 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, the *Axxon One* VMS offers three types of License plate recognition (RR) tools:

License plate recognition - Search in archive (RR)

License plate recognition - Parking (RR)

License plate recognition (RR)

1. **License plate recognition (RR)** – recognizes license plates in real time. Recognition is performed in the Fast mode (video stream processing at a speed of up to 30 FPS).
2. **License plate recognition** – **Parking (RR)** – recognizes license plates in real time. Recognition is performed in the Slow mode (video stream processing at a speed of up to 8 FPS).

   > **Note**
   >
   > The sampling rate for the detection tool is 150 milliseconds, all other frames are skipped.

3. **License plate recognition – Search in archive (RR)** – recognizes license plates in the archive. Recognition is performed in the Fast mode (video stream processing at a speed of up to 30 FPS).

   > **Note**
   >
   > This detection tool generates events with a 30 sec delay after the license plate recognition.

> **Note**

License plate recognition (RR) requires Add-on RR LPR to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.12.3.2 Camera requirements for License plate recognition (RR)

Type of requirements	Purpose	Requirements for the video image from the camera, which will be used for detection
Basic requirements	For the ANPR to operate using the detection tools	Character height is at least 10px, preferably 20px or more
		Minimum resolution is 1280*720. The recommended resolution is 1920*1080
		Minimum frame rate for the Slow mode is 5 FPS. Minimum frame rate for the Fast mode is 20 FPS
		Maximum horizontal angle is 30°
		Maximum vertical angle is 45°
		Expected image contrast: the contrast difference between characters of the LP and the background should be at least 20 units with the image brightness scale from 0 to 255
		In order to recognize state license plates on high-speed roads, the camera should have the Global Shutter mode
Additional requirements	To determine the vehicle driving direction	Camera installation height is at least 3 meters
		Maximum angle between the camera and the road direction is 30°
		Minimum camera tilt
	To recognize the make and the model of the vehicle	Visible width of the vehicle is from 100px
		Color or black and white image
	To recognize the color of the vehicle	Visible width of the vehicle is from 100px
		The scene illumination should 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 sudden 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

15.4.12.3.3 Configuring License plate recognition (RR)

To configure License plate recognition (RR), do as follows:

1. Download Add-on RR LPR from the website[126] and install it.

> **Note**
>
> To make the detection tool operate on Windows Server 2012 R2, make sure to install the Media Foundation component.

126 https://axxonsoft.com/resources/downloads/detector-pack.php

2. Create the required detection tool and select it.

License plate recognition (RR)	
Object features	
1 Real-time recognition	Yes
2 Record objects tracking	Yes
3 Video stream from camera	High-quality video stream

3. If you need to use this detection tool for real-time license plate recognition, set the corresponding parameter to **Yes** (**1**) (see Configuring real-time vehicle license plate recognition(see page 337)).
4. To record metadata to the database, select **Yes** from the **Record objects tracking** list (**2**).
5. 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 (**3**).

Other	
4 Algorithm for detecting vehicle direction	By LP coordinates
Country 1 name	Germany
Country 2 name	Not used
5 Country 3 name	Not used
Country 4 name	Not used
Country 5 name	Not used
6 Decoder mode	CPU
7 Frames processed per second	100
8 Minimum recognition quality, in %	80
9 Mode	CPU
10 Speed detection	Kmph
11 Speed detection area height	0
12 Speed detection area width	0
13 Vehicle recognition	Yes

6. Select the **Algorithm for detecting vehicle direction** (**4**):
   a. By LP coordinates—if the license plate coordinates shift from top to bottom, then the vehicle is moving towards the camera; if the license plate coordinates shift from bottom to top, then the vehicle is moving away from the camera;
   b. By LP scale—if the license plate scale increases, then the vehicle is moving towards the camera; if it decreases, then the vehicle is moving away from the camera.
7. In the corresponding fields, select from the list one or more countries for LPR (**5**).
8. Select the processor for decoding video streams (**6**). 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 be done with Intel Quick Sync Video technology. Otherwise, the CPU resources will be used for decoding.
9. Set the number of frames processed per second by the detection tool (**7**). The value should be in the range [0,016; 100].
10. Set the minimum quality of LPR (**8**). The value should be in the range [0; 100]. The higher the minimum recognition quality, the fewer false detections will occur.
11. Select the processor for the detection tool: the CPU or one of NVIDIA GPUs (**9**) (see General Information on Configuring Detection(see page 234)).

> **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 neural analytics on GPU(see page 240)).

12. From the **Speed detection** list, select the unit of measurement of vehicle speed (**10**).
13. Specify the speed detection area height and width in meters (**11**, **12**). The value should be in the range [0; 500].
14. If you need to search for the recognized LPs in the archive, set **Yes** for the corresponding parameter (**13**, see LPR search(see page 741)).
15. In the **Event timeout** field (**14**) specify the time interval in seconds between the initial LP recognition and event registration. The **0** value sets the event registration to the moment when the track disappears from FOV.

> **Note**
>
> Skip this step with **License plate recognition - Search in archive (RR).**

Advanced detection settings	
14 Force report timeout	0
15 Frame size change	1920
16 Maximum number of threads	4

16. By default, the analyzed frames are scaled down to a specified resolution (**15**, 1920 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, this resolution will be used further.
    c. If the resulting resolution still exceeds the specified value, it is divided by two, etc.

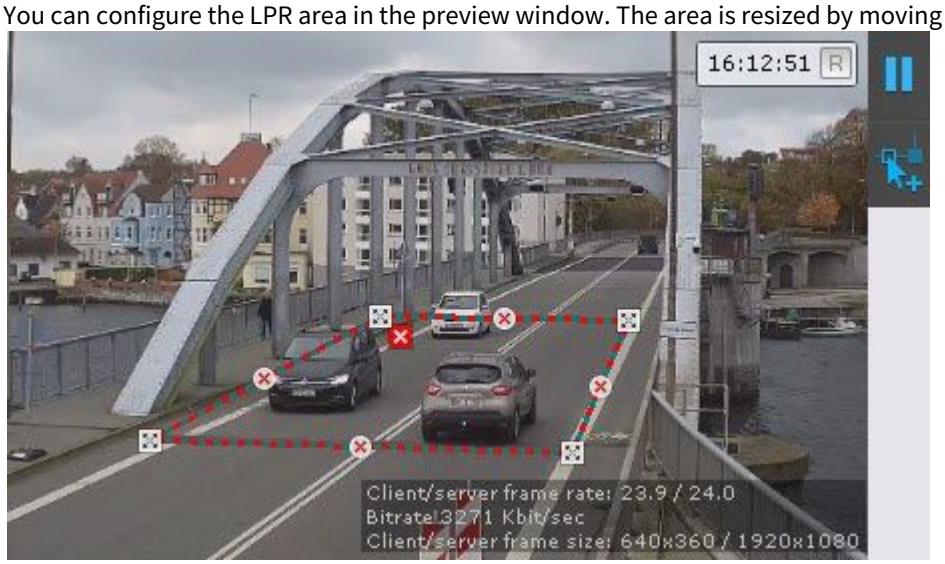
> **Note**
>
> For example, the source image resolution is 2048*1536, and the specified value is set to **1000**.
> In this case, the source resolution will be halved two times (512*384), as after the first division, the number of pixels on the longer side exceeds the limit (1024 > 1000).
> If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.

17. Specify the maximum number of recognition threads (**16**). If the value is **0**, the recognition process will occur in the same thread that starts it.

> **Attention!**
>
> The cumulative value of this parameters across all LPR detection tools should not exceed the number of CPU cores and is limited to **100**.

> **Attention!**
>
> Starting with *DetectorPack* 3.8.0.95 the **Maximum number of threads** parameter is not present.

18. You can configure the LPR area in the preview window. The area is resized by moving the anchor points .



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

Detection zone is displayed by default. You can click the button to hide the area. To undo, click this button again.

19. Click the **Apply** button.

Configuration of License plate recognition (RR) is now complete.

15.4.12.4 Optimizing the operation of the License plate (RR) and RR vehicles recognition on GPU

Starting from *DetectorPack* 3.10, a utility was added to the RR LPR add-ons (see Installing DetectorPack add-ons(see page 74)), which allows you to create GPU 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 the License plate recognition (RR) and RR vehicles on GPU, do the following:

1. Stop the Server (see Shutting down a Server(see page 100)).

   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(see page 951)) by specifying in the **Variable value** field the path to the cache location with an arbitrary folder name. For example, D:\AN_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[127] in the numeric or alphabetic form. After you select all required countries, enter the **-1** value.

127 https://support.axxonsoft.dev/jira/secure/attachment/1688337/1688337_LPR_RR_countries.txt

```
Please choose the countries...
0. AM          13. DK         26. KZ         39. RO
1. AR          14. EE         27. LT         40. RU
2. AT          15. EG         28. LU         41. SE
3. AZ          16. ES         29. LV         42. SI
4. BE          17. FI         30. MD         43. SK
5. BG          18. FR         31. MM         44. TJ
6. BN          19. GE         32. MT         45. TM
7. BR          20. GR         33. MX         46. UA
8. BY          21. HR         34. MY         47. UZ
9. CY          22. HU         35. NL         48. VN
10. CZ         23. IE         36. PE
11. DE         24. IT         37. PL
12. CO         25. KG         38. PT

   Enter the codes of the countries, separated by enter:
   Enter -1 when you are done
Enter your choice: 24
Enter your choice: FR
Enter your choice: 11
Enter your choice: -1
```

5. Specify the ID of the required GPU (see General Information on Configuring Detection(see page 234)) 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 a 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 the License plate recognition (RR) and RR vehicles on GPU is complete.

> **Attention!**
>
> If you update the RR LPR add-ons (see Installing DetectorPack add-ons(see page 74)) or change the NVIDIA GPU model, the cache must be recreated.

15.4.12.5 License plate recognition (BRS)

15.4.12.5.1 Camera requirements for License plate recognition (BRS)

To ensure the recognition of state license plates using the License plate recognition (BRS), it is necessary to install and configure video cameras in such a way that the requirements described below are met.

15.4.12.5.1.1 Camera requirements

1. The minimum video resolution is 640*480, the recommended resolution is 720p or 1080p.
2. The minimum frame rate is 15 FPS, the recommended frame rate is 25–30 FPS.
3. Autofocus and zoom would be useful for making small adjustments after configuring the detection tool.
4. Automatic white balance.
5. IR for night mode with good contrast of license plate images.
6. HDR or WDR.
7. In order to recognize state license plates on high-speed roads, the camera should have the Global Shutter mode.

15.4.12.5.1.2 **Video image requirements**

1. The video image should be clear, contrasting, without distortion, not blurred.

2. The video image should have minimum noise in low light conditions.
3. The size of the license plate should be 15–70% of the total size of the image.
4. The license plate must contain no more than two rows of characters.

15.4.12.5.1.3 Camera installation requirements

1. The camera should be mounted at 0.6–2.4 meters above the ground.
2. The angle formed by the lower line of the license plate and the horizon line should be from 0 to 20 degrees.

15.4.12.5.2 License plate recognition (BRS) features and specifications

License plate recognition (BRS) is designed to implement the following functions:

1. Recognize license plates. The list of supported countries: Hong Kong, China, Taiwan.
2. Write the recognized license plate to a database.
3. Check the recognized license plates on the lists of license plates.

> **Note**
>
> Install the additional Add-on BRS LPR to work with License plate recognition (BRS) (see Installing DetectorPack add-ons(see page 74)).

15.4.12.5.3 Configuring License plate recognition (BRS)

To configure License plate recognition (BRS), do the following:

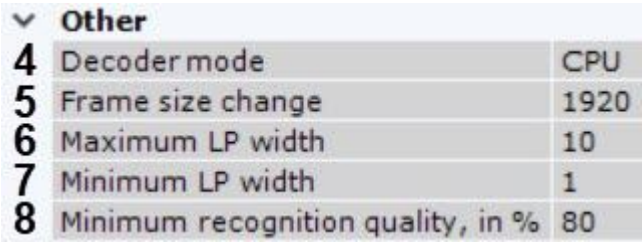
1. Submit to the AxxonSoft manager the MAC address of the Server where the detection tool will be used.

   > **Attention!**
   >
   > The detection tool will not operate on the Server with a different MAC address.

2. Copy the license received from the AxxonSoft manager into the C:\Program Files\Common Files\AxxonSoft\DetectorPack\BioirisSDK\License.txt file.
3. Restart the Server (see Shutting down a Server(see page 100), Starting a Server(see page 94)).
4. Create the **License plate recognition (BRS)** object and select it.

License plate recognition (BRS)		
	Object identification	
	Enable	Yes
	Name	License plate recognition (BRS)
	Object features	
1	Real-time recognition	No
2	Record objects tracking	Yes
3	Video stream from camera	High-quality video stream
	Visual Elements	
	Visual Element	Detection area (rectangle)

5. If you need to use this detection tool for real-time license plate recognition, set the corresponding parameter to **Yes** (**1**, see Configuring real-time vehicle license plate recognition(see page 337)).
6. If you need to record metadata to a database, select **Yes** from the **Record objects tracking** list (**2**).
7. If the camera supports multistreaming, select the stream for which detection is needed (**3**). Selecting a low-quality video stream allows reducing the load on the Server.
8. Select a processing resource for decoding video streams (**4**). When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips, see Hardware requirements for GPU based video decoding(see page 54)). If there is no appropriate GPU, the decoding will use the Intel Quick Sync Video technology or the CPU.

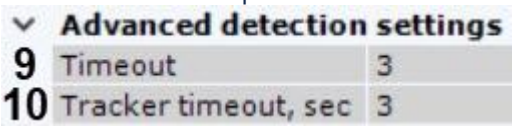


	Other	
4	Decoder mode	CPU
5	Frame size change	1920
6	Maximum LP width	10
7	Minimum LP width	1
8	Minimum recognition quality, in %	80

9. By default, the analyzed framed are scaled down to a specified resolution (**5**, by default, 1920 pixels on the longer side). The value should be in the range [640; 10000]. 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 is 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). If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.

10. Set the maximum and minimum width of the license plate as a percentage of the frame width (**6**, **7**). The value should be in the range [1; 100].
11. Set minimum quality of the license plate recognition (**8**). The higher the minimum recognition quality, the fewer false positives will be detected. The value should be in the range [0; 100].
12. In the **Timeout** field (**9**), specify the time in seconds after which the response should be generated after recognizing the license plate in the frame. The value should be in the range [0; 3600]. If you set the **0** value, the response will occur after the loss of the license plate track.

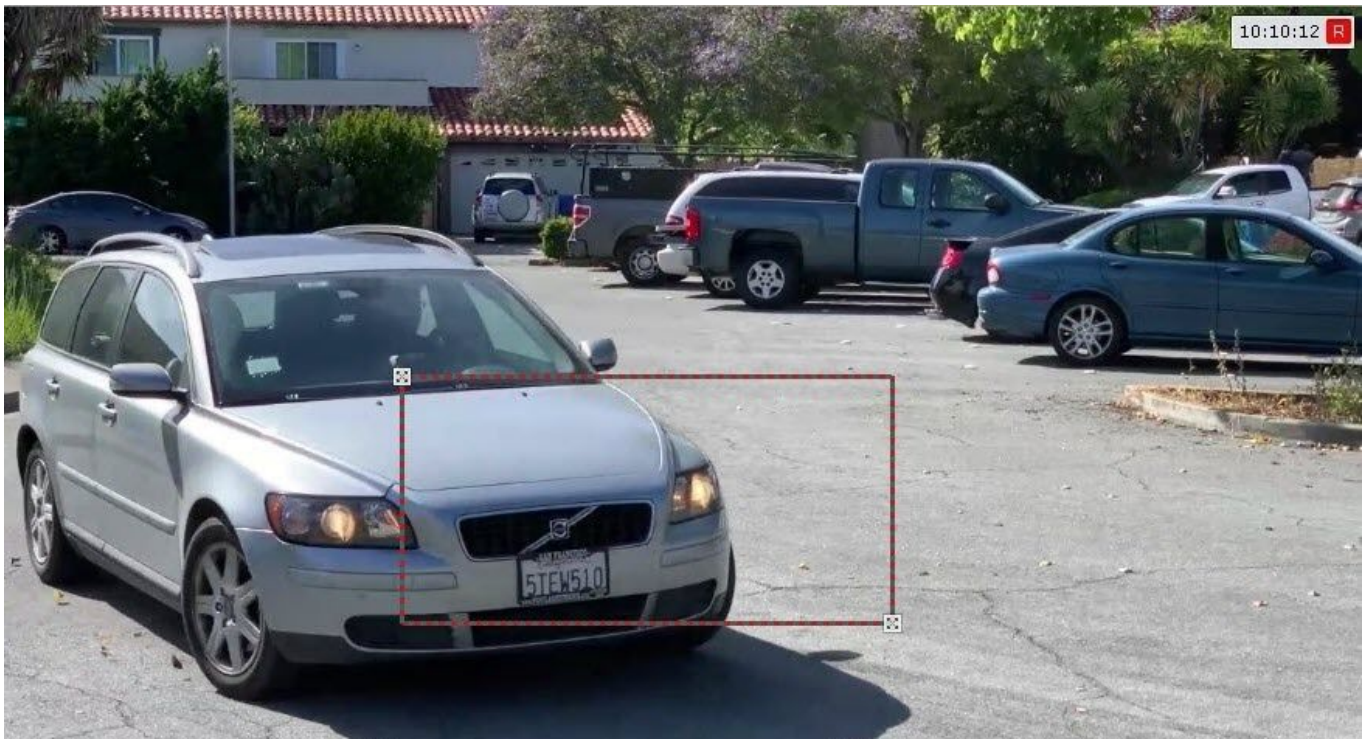


	Advanced detection settings	
9	Timeout	3
10	Tracker timeout, sec	3

13. In the **Tracker timeout, sec** field (**4**), specify the time in seconds after which the vehicle track is considered lost. The value should be in the range [0; 3600].

    > **Note**
    >
    > This parameter should be used to prevent double responses that occur, for example, when the license plate is recognized in the frame then gets hidden behind a visual obstacle and after that gets recognized by the detection tool again. If you set the timeout longer than the time of possible license plate overlapping in the frame, the detection tool will trigger only once.

14. In the camera FOV, set the area where the detection and license plate recognition will occur. You can configure the area by moving the anchor points .



Note

- For your convenience, you can click the button and configure the area on a freeze frame. To undo, click this button again.
- The detection area is displayed by default. You can click the button to hide the area. To undo, click this button again.

15. Click the **Apply** button.

Configuration of License plate recognition (BRS) is complete.

15.4.12.6 Configuring real-time vehicle license plate recognition

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[128]), 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* (see Connecting Axxon-domain to AxxonNet[129]).
2. Create one or more lists of license plates in *AxxonNet* (see Lists of vehicle numbers[130]).
3. Create a license plate recognition tool (see Automatic Number Plate Recognition (LPR/ANPR) tools(see page 308)).

128 https://docs.axxonsoft.com/confluence/display/anet/Lists+of+vehicle+numbers
129 https://docs.axxonsoft.com/confluence/display/anet/Connecting+Axxon-domain+to+AxxonNet
130 https://docs.axxonsoft.com/confluence/display/anet/Lists+of+vehicle+numbers

4. Enable the **Real-time recognition** parameter in the license plate recognition tool settings (see Configuring License plate recognition (VT)(see page 314), Configuring License plate recognition (IV)(see page 326), Configuring License plate recognition (RR)(see page 330)).
5. Select the condition to start the macro (see Configuring filters for event-driven macros(see page 407), Configuring macros when working with vehicles lists(see page 338)).
6. Select one or more actions to start the macro (see Settings specific to actions(see page 413)).
7. If necessary, configure information boards to display the information from the macro (see Examples of macros used when working with vehicles lists(see page 339), Configuring an Event Board(see page 490), Configuring a Dialog Board(see page 495)).

15.4.12.6.1 Configuring macros when working with vehicles lists

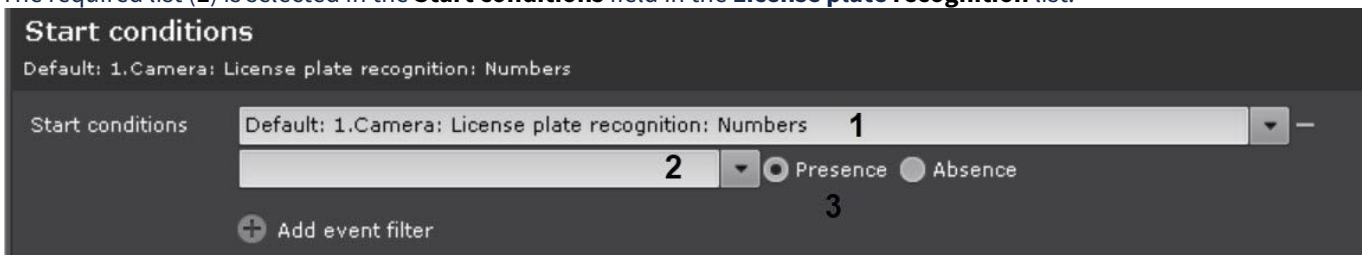
When working with vehicle license plate lists, you can configure the macro (see General information about the macros(see page 400)) to trigger when:

- 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.

15.4.12.6.1.1 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.

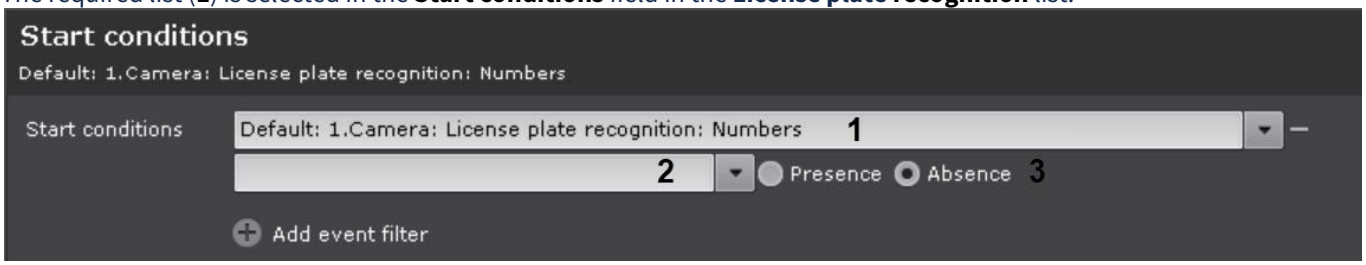


2. The field **2** is empty.
3. The **Presence** radio button is set (**3**).

15.4.12.6.1.2 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.

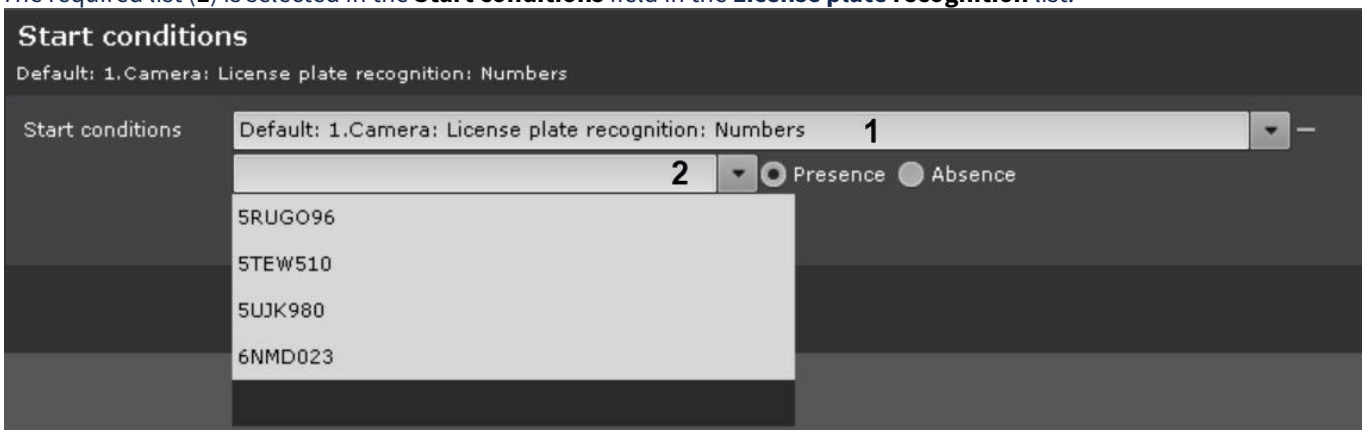


2. The field **2** is empty.
3. The **Absence** radio button is set (**3**).

15.4.12.6.1.3 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.

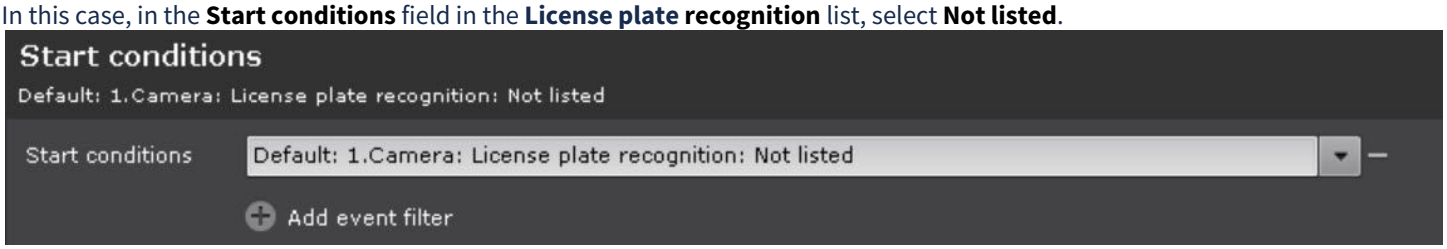


2. A specific license plate is selected in the field **2**.

> **Note**
>
> To select another license plate, clear the field **2** and re-open the list.

15.4.12.6.1.4 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**.



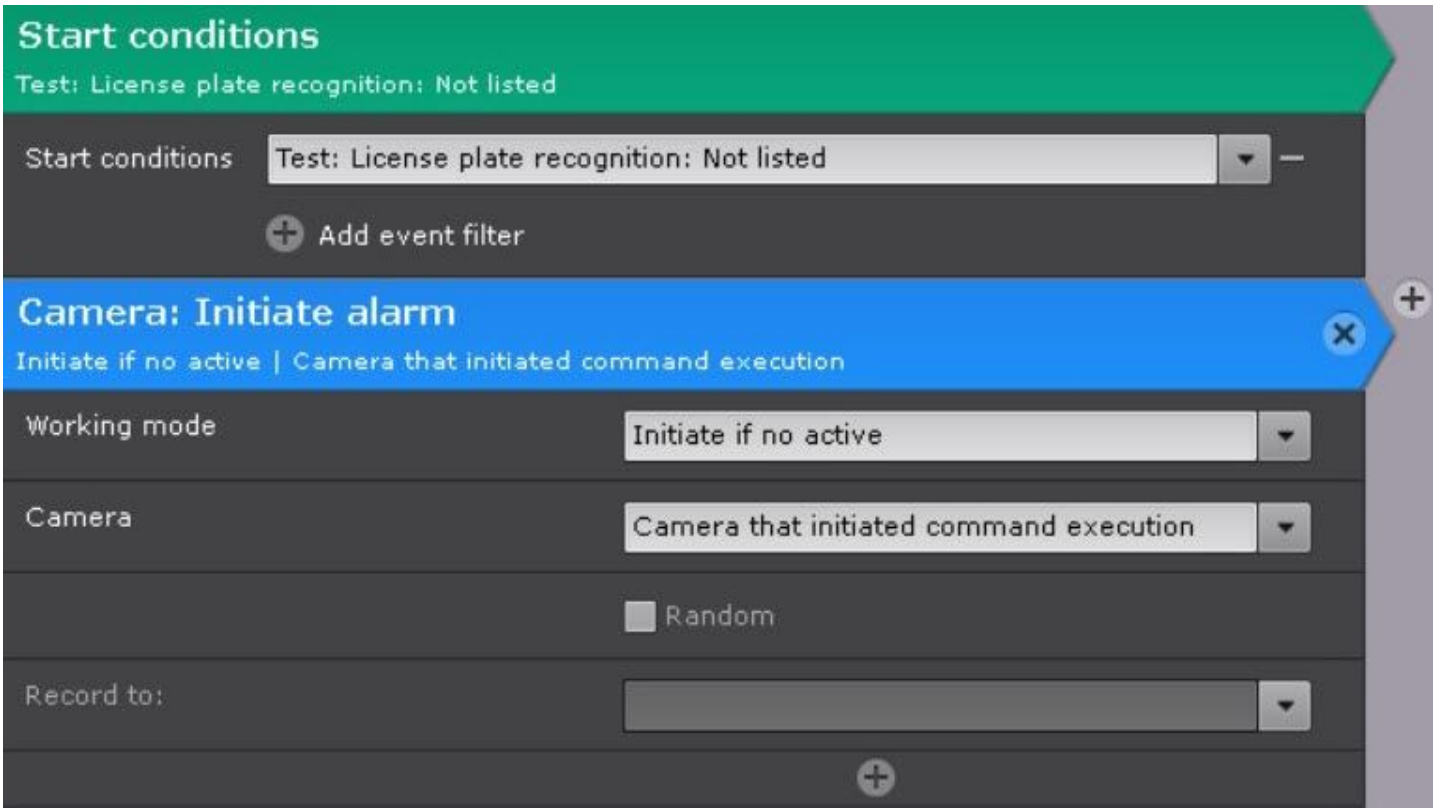
Examples of macros used when working with vehicles lists(see page 339)

15.4.12.6.1.5 Examples of macros used when working with vehicles lists

On this page:

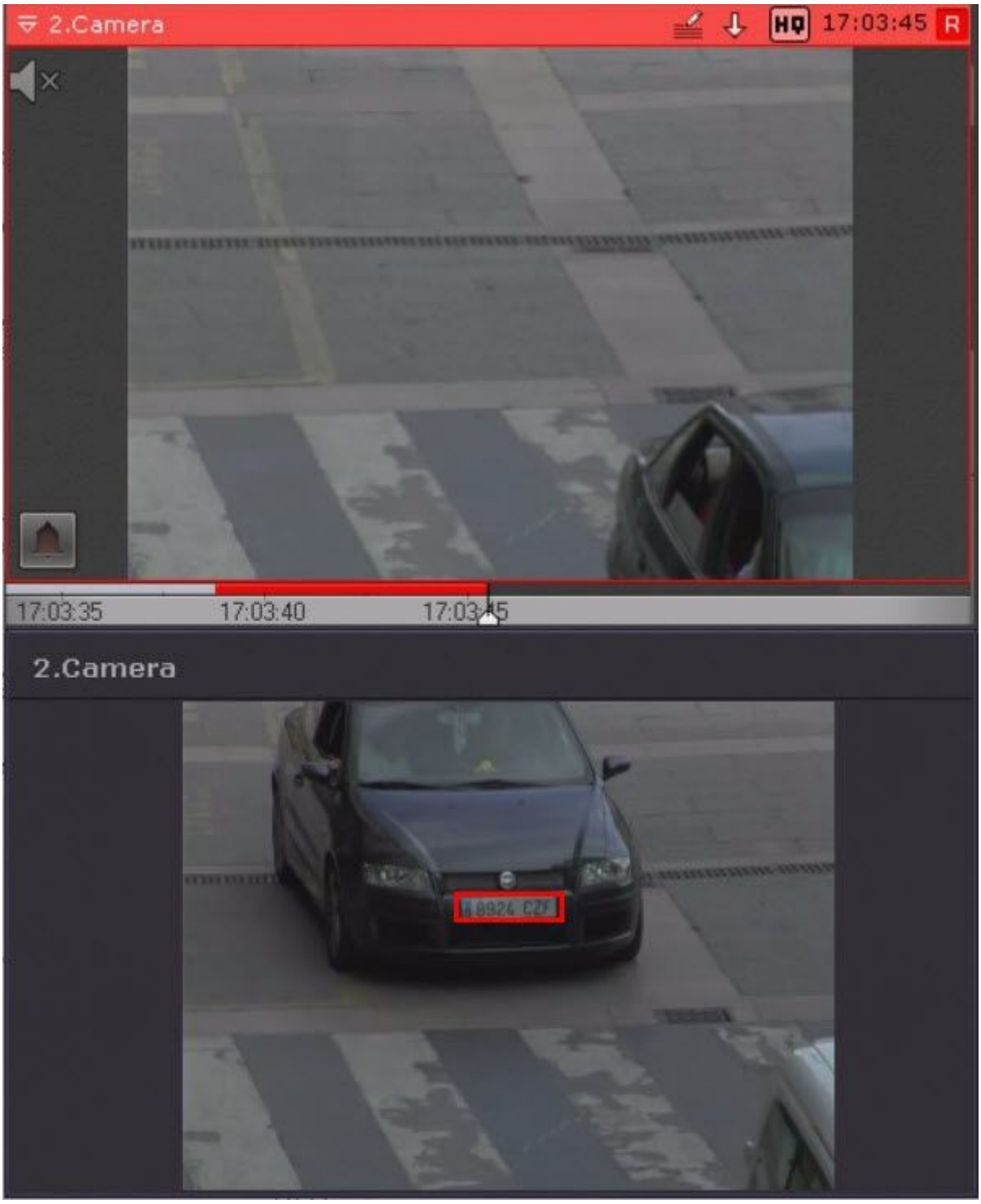
- Alarm initiation(see page 339)
- Switching the output on for the authorized license plates(see page 341)
- Sending an E-mail(see page 342)
- Starting export(see page 343)

Alarm initiation

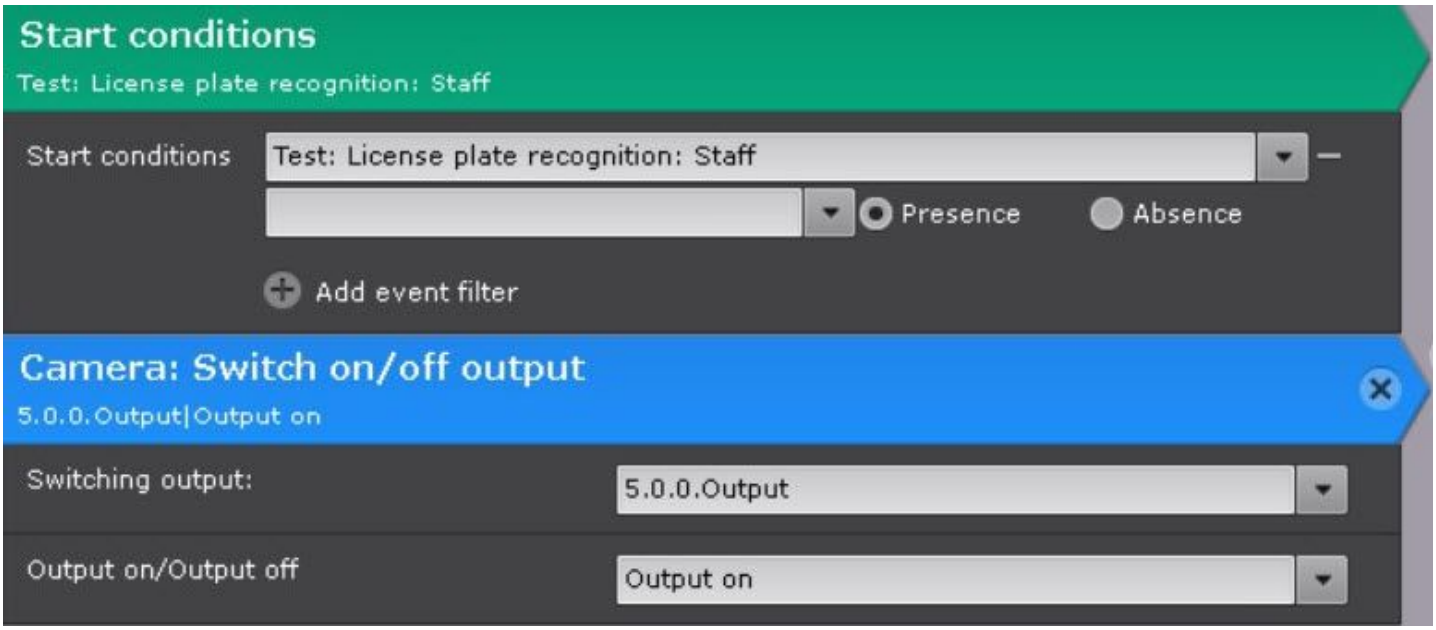


This macro can be used together with the Dialog Board (see Configuring a Dialog Board(see page 495)).

If the Dialog Board is configured to display an alarm and linked with a video camera (see Linking cells(see page 481)), then when not listed license plate is recognized, the board will display the recognized license plate highlighted in a red frame.

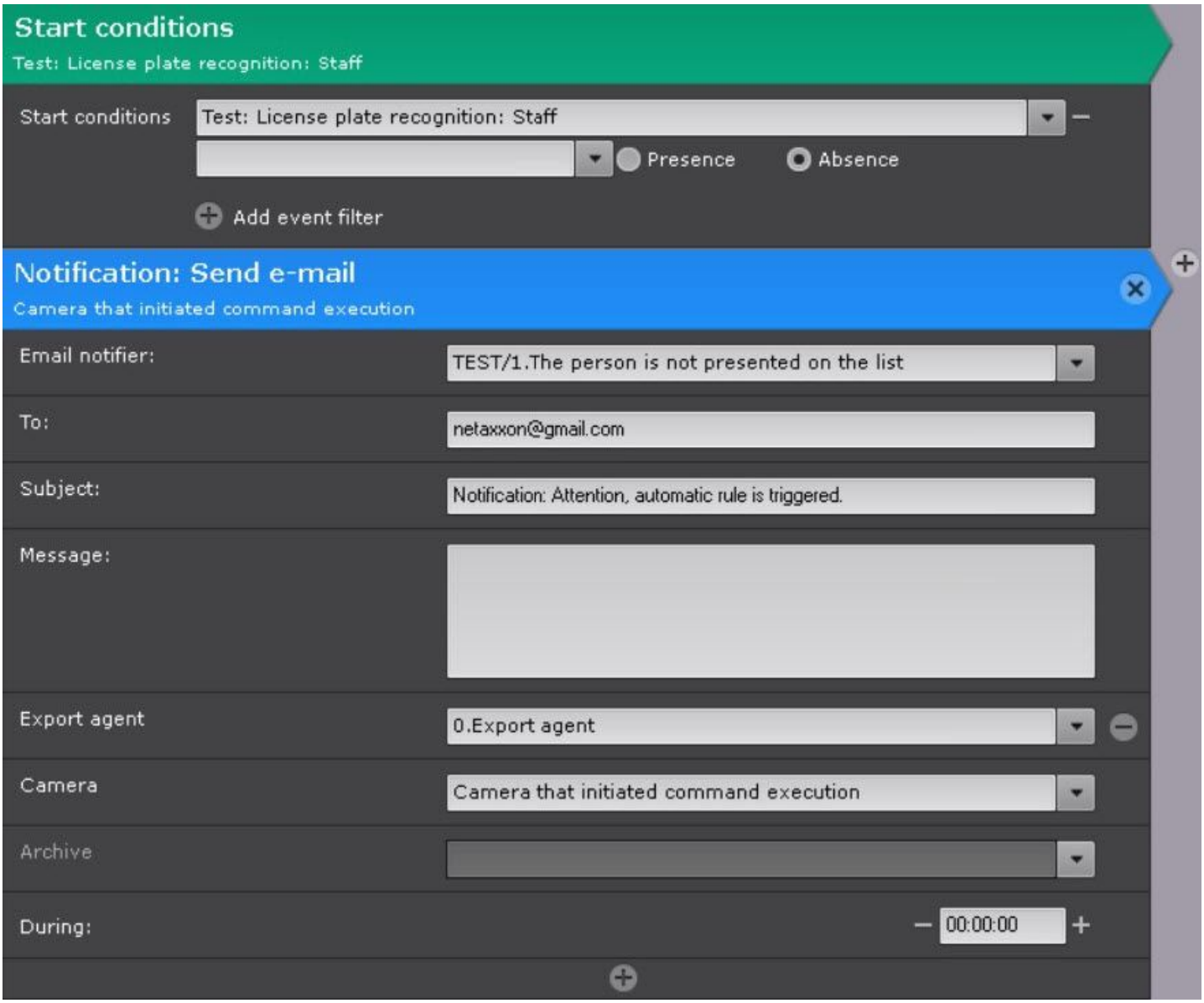


Switching the output on for the authorized license plates



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.

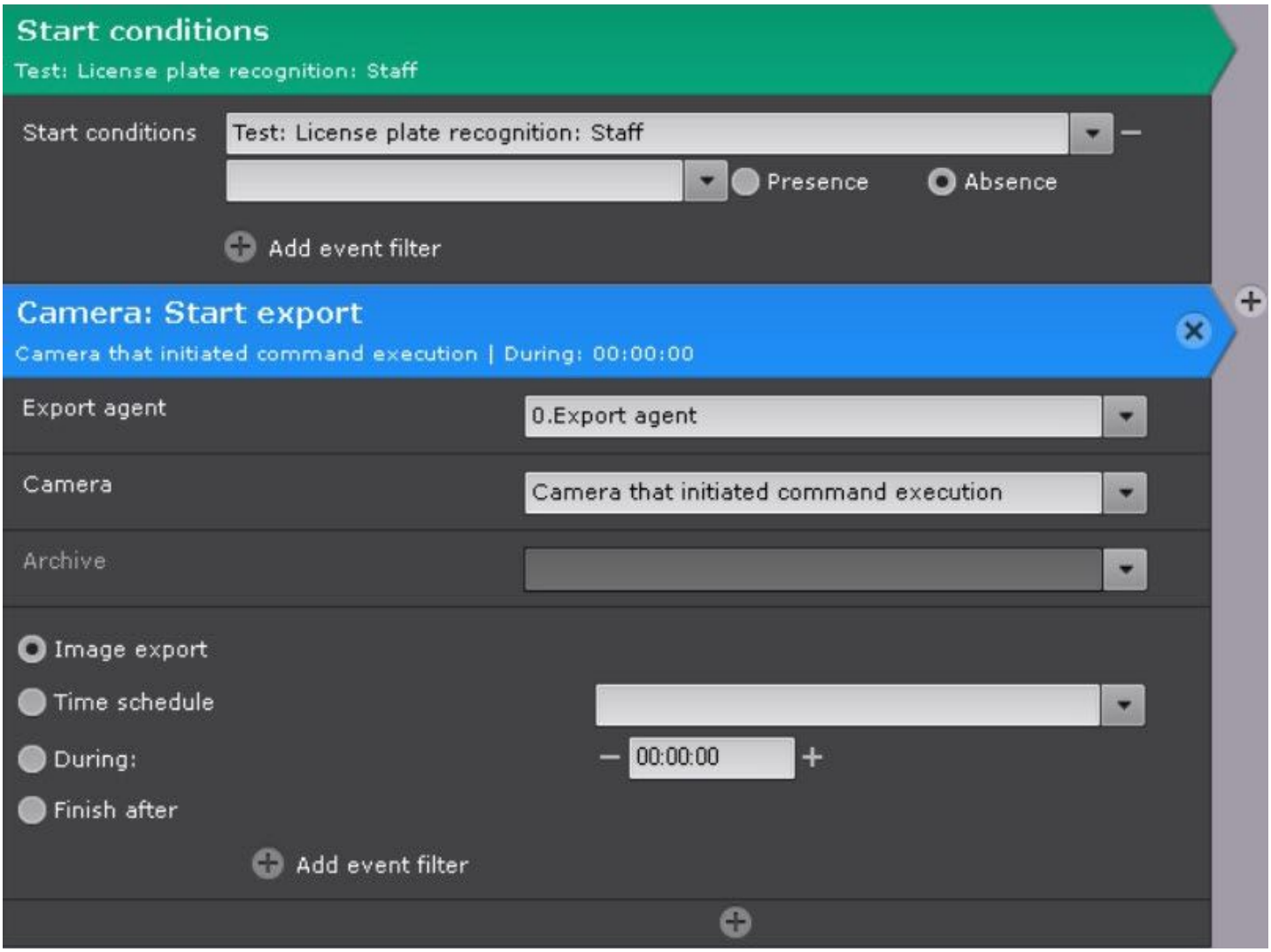
Sending an E-mail



If the E-mail is sent via the SMTP Server (see The E-mail notifier object(see page 435)), 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.

15.4.13 Neural Counter

15.4.13.1 Video stream and scene requirements for neural counter operation

The neural counter operation imposes the following requirements:

1. To the video stream from the camera:
   a. The resolution is at least 640x360 pixels. It is also not recommended to use a resolution higher than 1920×1080, since higher resolution does not increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720 (see Example of configuring neural counter for solving typical task(see page 349)).
   b. The frame rate per second in the video stream from the camera is at least 8 for solving typical task.
   c. Both colorless (gray) and color images.
2. To lighting:
   a. 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 video analytics is not guaranteed.
   b. There are no abrupt changes in lighting.
3. To the scene and camera angle:
   a. Moving objects are visually separable from each other.

b. The background is mostly static and does not change abruptly.
c. Moving objects are minimally obscured by static objects in the scene (columns, trees, etc.).
d. The analyzed scene does not have reflective surfaces and sharp shadows from moving objects. If present, they should be masked.
e. Camera shake does not result in image offsets greater than 1% of the frame size.

Attention!

Correct operation of the neural counter is not guaranteed when using a fish-eye lens.

Hardware requirements for neural analytics operation(see page 52)
Objects image requirements for neural counter(see page 349)

15.4.13.2 Functions of the neural counter

The neural counter relies on a neural network to work out the number of objects in the zone.

A detection event that can be used to launch a macro is generated when the number of objects in FoV matches the pre-defined conditions (see Configuring filters for event-driven macros(see page 407)).

Note

Unlike the Multiple objects detection tool (see Settings specific to Multiple objects(see page 272)), the neural counter generates events of one type, namely – triggering.
The neural counter is less resource-intensive than Multiple objects detection tool based on Neural Tracker.

Note

For the neural counter to work, install Addon Neuro Pack (see Installing DetectorPack add-ons(see page 74)).

15.4.13.3 Configuring a Neurocounter

Video stream and scene requirements for neural counter operation(see page 344)
Hardware requirements for neural analytics operation(see page 52)

To configure a Neurocounter, do the following:

1. To record mask (highlighting of recognized objects) to the archive, select **Yes** for the corresponding parameter (**1**).

Neurocounter	
Object features	
1 Record mask to archive	Yes
2 Video stream	Second stream

2. If the camera supports multistreaming, select the stream for which detection is needed (**2**).

Neurocounter	
Advanced settings	
3 Decoder mode	CPU
4 Number of frames processed per second	1
5 Detection threshold	30
6 Mode	CPU
7 Number of alarm objects	5
8 Object type	Human
9 Trigger upon count	Greater than or equal

3. Select a processing resource for decoding video streams (**3**). 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.
4. Set the frame rate value for the detection tool to process per second (**4**). This value should be in the range [0; 100].

> **Note**
>
> The default values (three output frames and 1 FPS) indicate that Neurocounter will analyze one frame every second. If Neurocounter detects the specified number of objects (or more) on three frames, then it triggers.

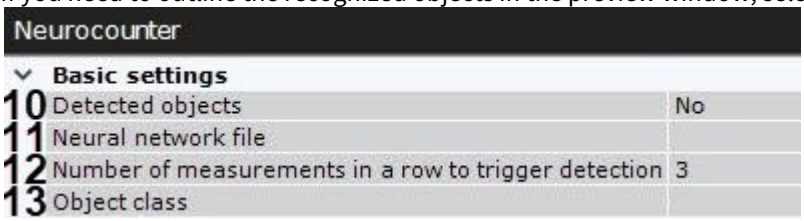
5. Set the recognition threshold for objects in percent (**5**). If the recognition probability falls below the specified value, the data will be ignored. The higher the value, the higher the recognition accuracy, but some triggers may not be considered. This value should be in the range [0.05; 100].
6. Select the processor for the neural network—CPU, one of NVIDIA GPUs or one of Intel GPUs (**6**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

> **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 Neurocounter.
> - 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(see page 240)).
> - Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

7. Set the triggering condition for Neurocounter:
   a. In the **Number of alarm objects** field (**7**), set the threshold value for the number of objects in the frame. This value should be in the range [0; 100].
   b. In the **Trigger upon count** field (**9**), select when you want to generate a trigger—when the number of objects in the detection area is:
      i. Greater than or equal to threshold value.
      ii. Less than or equal to threshold value.

> **Note**
>
> Neurocounter will generate a trigger from the specified threshold (**9**).

8. In the **Object type** field (**8**), select the object for counting:
   a. Human.
   b. Human (top view).
   c. Vehicle.
   d. Human and Vehicle (Nano)—low accuracy, low processor load.
   e. Human and Vehicle (Medium)—medium accuracy, medium processor load.
   f. Human and Vehicle (Large)—high accuracy, high processor load.
9. If you need to outline the recognized objects in the preview window, select **Yes** for the **Detected objects** parameter (**10**).



10. If you use a unique neural network, select the corresponding file (**11**).

> **Attention!**
>
> - To train your neural network, contact AxxonSoft (see Data collection requirements for neural network training(see page 239)).

- A trained neural network for a particular scene allows you to detect only objects of a certain type (e.g. person, cyclist, motorcyclist, etc.).
- If the neural network file is not specified, the default file will be used, which is selected automatically depending on the selected object type (**8**) and the selected processor for the neural network operation (**7**). 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.
- For correct neural network operation in Linux, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

11. Set the minimum number of frames on which Neurocounter should detect objects in order to trigger (**12**). The value should be in the range [2; 20].
12. If necessary, specify the class/classes of the detected object (**13**). 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 view), **10**—Vehicle.
    a. If you leave the field blank, the tracks of all available classes from the neural network will be displayed (**8**, **11**).
    b. If you specify a class/classes from the neural network, the tracks of the specified class/classes will be displayed (**8**, **11**).
    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 (**8**, **11**).
    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 (**8**, **11**).

    > **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 (**8**, **11**).

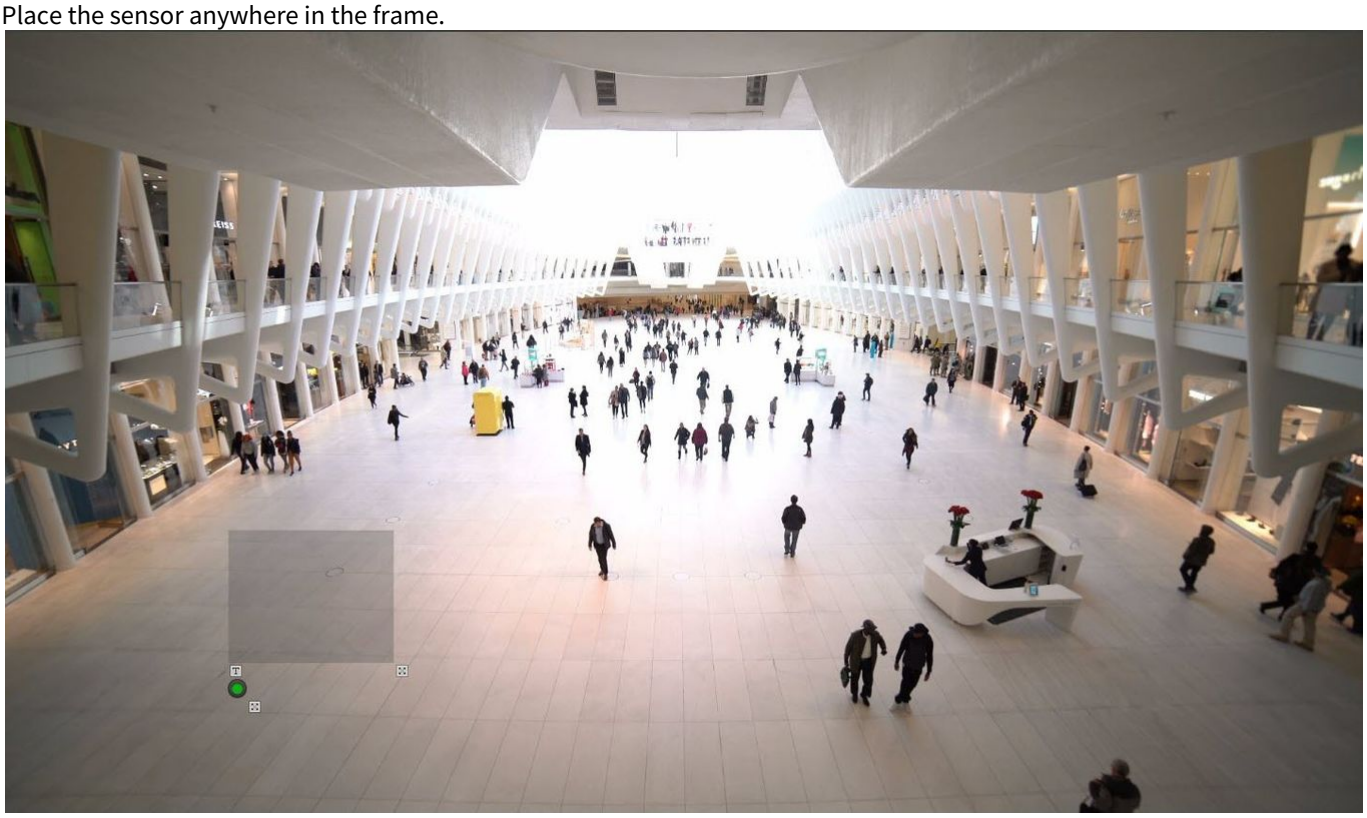
13. In the preview window, you can set the detection areas with the help of anchor points much like privacy masks in Scene Analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)). By default, the entire frame is a detection area.

14. Click the **Apply** button.

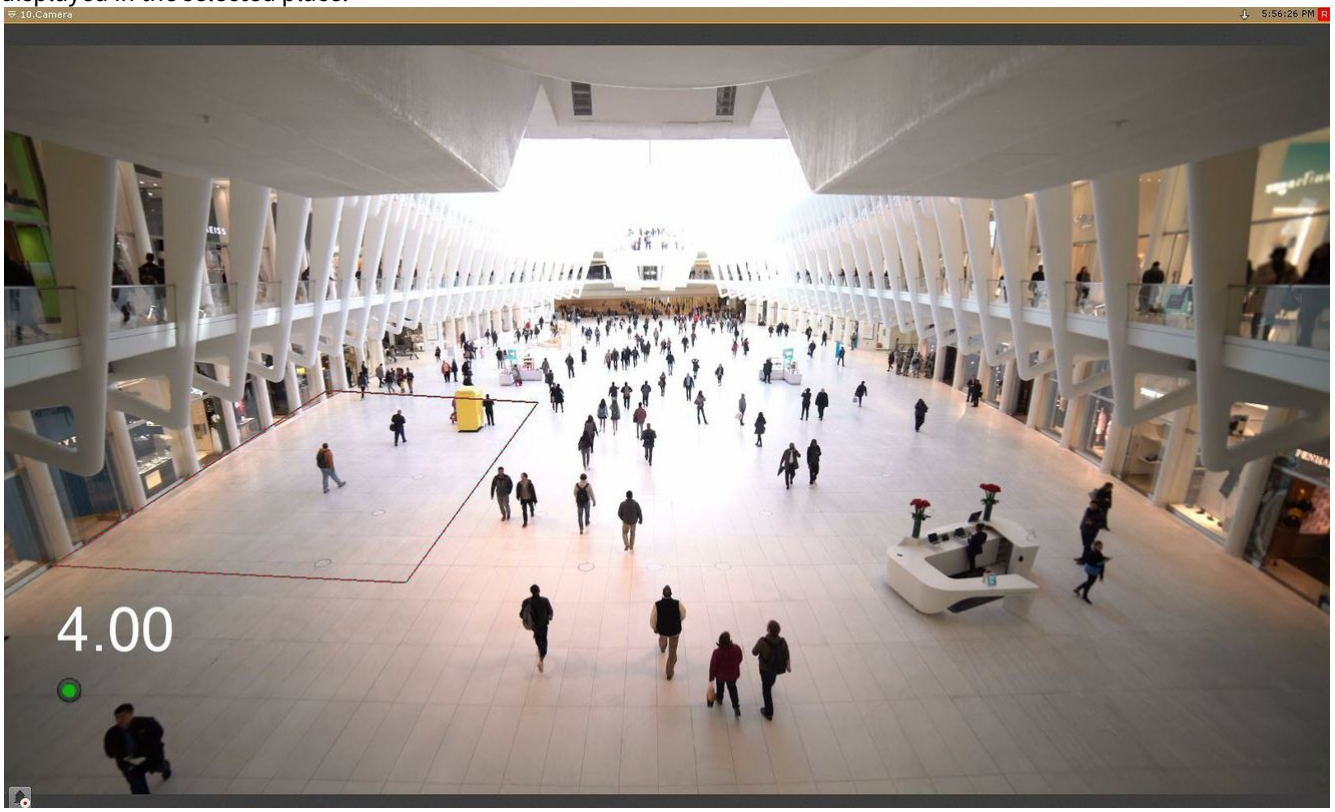
Configuring a Neurocounter is complete.

It is possible to display the sensor and the number of objects in the controlled area in the **Surveillance window** on the layout. To configure this option, do the following:

1. Go to the Layout Editing mode (see Switching to layout editing mode(see page 474)).
2. Place the sensor anywhere in the frame.



3. Customize the font. To do this, click the T button.
4. Save the layout (see Exiting Layout Editing mode(see page 499)). As a result, the sensor and the number of objects will be displayed in the selected place:



15.4.13.4 Example of configuring neural counter for solving typical task

To detect objects with a speed less than 0,3 m/s, the following settings are recommended:

1. **The number of frames for analysis and output**: 3.
2. **The number of frames processed per second**: 1.
3. **Neural filter**: No.
4. **Recognition threshold**: 30.
5. **Neural network file**: Path to the *.ann neural network file. You can also select **Object type** — in this case, this field should be left blank.

> **Note**
>
> By default, the neural counter is configured for detection of objects with a speed less than 0,3 m/s.

To solve tasks in which the speed of the object is greater than 0,3 m/s, it is necessary to increase the number of processed frames and/or reduce the number of frames for analysis and output. The values are selected by trial-and-error method depending on the conditions of the task.

15.4.13.5 Objects image requirements for neural counter

To ensure the correct operation of neural counter, the following image requirements should be met:

1. The object to be detected is clearly distinguishable by the human eye.
2. The width or height of the objects does not exceed 75% of the frame size.
3. The image is not noisy and not distorted by compression algorithm artifacts.
4. The duration of the object's visibility is at least 6 frames.
5. The object moves in the certain direction between two adjacent frames at a distance which does not exceed the object's size. This condition is necessary for the correct calculation of the trajectory of the object (track).
6. 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%

Video stream and scene requirements for neural counter operation(see page 344)

15.4.14 Fire and Smoke Detection Tools

15.4.14.1 Functions of Fire and Smoke detection

> **Important!**

Unlike standard smoke/fire detection systems, smoke and fire software detection tools face many issues with the scene and the background mage. We cannot warrant 100% smoke/fire detection. The smoke and fire detection tools are meant to increase the likelihood of detecting smoke/fire. However, there may be both false alarms and failures to detect actual fire/smoke events in the camera's FoV.
We keep improving smoke and fire detection and use machine learning based on a Neural network[131].
If the fire/smoke detection tools does not respond to actual fire/smoke events, please record a video clip and send it to AxxonSoft[132]. We will update *Axxon One* to refine detection. Help us train the neural network with video feeds from you scene to deliver best results for your fire security.

Note

These detection tools require Addon Neuro Pack to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.14.2 Camera requirements for Fire and Smoke Detection

Please follow these recommendations for proper fire and smoke detection:

1. Use color cameras. With black and white cameras, the detection quality can be noticeably worse.
2. The video resolution must be at least 640x360.
3. FPS directly affects detection efficiency: in most cases, the default value (1 detection per 10 seconds) is sufficient to detect smoke or fire which develops in more than one minute.
4. The minimal recognized fire/smoke area depends on the particular neural network used. For a standard neural network (see Configuring Fire and Smoke Detection Tools(see page 350)), the fire/smoke area must occupy at least 10% of the frame.

   Note

   In some cases, when fire is expected to be clearly visible, the fire area may be sufficient at 1-3% of the FoV width/ height.

5. Fire/smoke should be visually separated from the background.

Attention!

If you set a rectangular recognition area for the detection tool, the limitations apply to this area rather than to the entire frame (see Configuring Fire and Smoke Detection Tools(see page 350)).

Hardware requirements for neural analytics operation(see page 52)

15.4.14.3 Configuring Fire and Smoke Detection Tools

Camera requirements for Fire and Smoke Detection(see page 350)
Hardware requirements for neural analytics operation(see page 52)

To configure smoke (fire) detection tool:

1. To record the sensitivity scale of the detection tool to the archive (see Displaying information from a detection tool (mask) (see page 672)), select **Yes** for the **Record mask to archive** parameter (**1**).

131 https://en.wikipedia.org/wiki/Artificial_neural_network
132 https://support.axxonsoft.com/

Fire detection		
	Object features	
1	Record mask to archive	No
2	Video stream from camera	Low-quality video stream
	Other	
3	Decoder mode	CPU
4	Frames processed per second	0.1
5	Mode	CPU
6	Neural network file	
7	Number of measurements in a row to trigger detection	5
8	Scanning mode	No
9	Sensitivity	33
	Advanced detection settings	
10	Ignore black and white image	No

2. If the 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.
3. Select a processing resource for decoding video streams (**3**). 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.
4. Set the frame rate value for the detection tool to process per second (**4**). The value should be in the [0,016; 100] range.

> **Note**
>
> The default values (five frames for output and 0,1 FPS) indicate that the tool will analyze frame over 50 seconds span. The detection tool analyzes one frame every 10 seconds. If it detects smoke/fire on five consecutive fames, the detection tool will trigger an alert.

5. Select the processor for the neural network—CPU, one of Nvidia GPUs or one of Intel GPUs (**5**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

> **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(see page 240)).
> - 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.

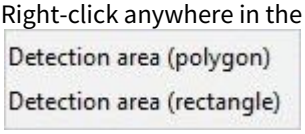
6. Select a neural network file (**6**). The standard neural networks for different processor types are located in the C:\Program Files\Common Files\AxxonSoft\DetectorPack\NeuroSDK directory. You don't need to select the standard neural networks in this field, the system will automatically select the required one. If you use a custom neural network, enter a path to the file.

> **Note**
>
> For correct neural network operation on Linux, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

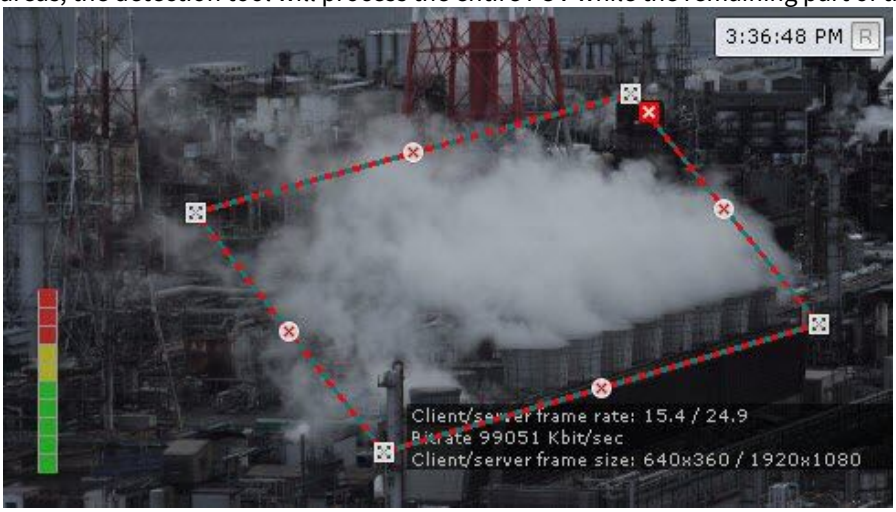
7. Set the minimum number of frames with smoke (fire) for triggering the tool (**7**). The value should be in the [5; 20] range.
8. To detect the objects without changing the frame size, select **Yes** in the **Scanning mode** field (**8**).
9. Set the sensitivity of the tool by trial and error (**9**). The value should be in the [1; 99] range. The preview window displays the sensitivity scale of the detection tool that relates to the sensitivity parameter. If the scale is green, smoke (fire) is not detected. If the scale is yellow, smoke (fire) is detected, but not enough to trigger the tool. If the scale is red, smoke (fire) is detected and the detection tool will trigger, if the scale is red through the sampling period (50 seconds by default, see item 4).
   Example. The sensitivity parameter value of 40 implies that the alert is triggered when the scale has at least 4 divisions full over the entire detection time span. The triggering will stop when the scale has less than 2 divisions full over the detection

time span. The alert will trigger again if the scale has at least 4 divisions full over the entire detection time span.

10. Select **Yes** for the **Ignore black and white image** parameter (**10**), if it is necessary that the detection tool does not trigger when the image is black and white.
11. By default, the detection is performed over full image area. In the preview window, you can set several detection areas using the anchor points as follows:
    a. Right-click anywhere in the preview window.

    b. Select **Detection area (rectangle)** to set one or several rectangular areas. If you specify a rectangular area, the detection tool will work only within its limits. The rest of the FOV will be ignored.
    c. Select **Detection area (polygon)** to set one or several polygonal areas. If you specify one or several polygonal areas, the detection tool will process the entire FOV while the remaining part of the FOV will be blacked out.



> **Attention!**
>
> You can configure detection areas similarly to privacy masks in Scene analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)).
> You can use trial and error method to decide which type of detection area (rectangular or polygonal) is more effective in your case. Some neural networks give better detection with rectangles while others are better with polygons.

15.4.15 Object presence detection tool

15.4.15.1 Functions of the object presence detection tool

The object presence detection tool triggers when the required type of object appears in the camera field of view.

> **Attention!**
>
> The object presence detection tool is based on a neural network[133], the basic principle of which is learnability.
> In order for the object presence detection tool to respond to the required type of object in the camera field of view, it is necessary to record a video and send it to AxxonSoft[134]. In *Axxon Next*, the detection tool will be refined (neural network training) based on the video data for the optimal operation in the specified conditions.

> **Note**

133 https://en.wikipedia.org/wiki/Artificial_neural_network
134 https://support.axxonsoft.com/

The object presence detection tool requires Addon Neuro Pack to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.15.2 Camera requirements for the object presence detection tool

When working with the object presence detection tool, the following camera requirements should be met:

1. It is recommended to use color cameras. If you use black and white cameras, the recognition quality may be noticeably worse.
2. The video resolution should be at least 640x360 pixels.
3. The frame rate: the FPS determines the speed of the detection tool reaction. In most cases, the default value (1 time per 10 seconds) is enough to detect the appearance of an object, which lasts more than 1 minute.
4. The minimum area of the object in the frame depends on the used neural network.
5. The object must be visually separated from the background.

Attention!

If you set a rectangular recognition area for the detection tool, the above requirements apply to this area, not to the entire frame (see Configuring the object presence detection tool(see page 353)).

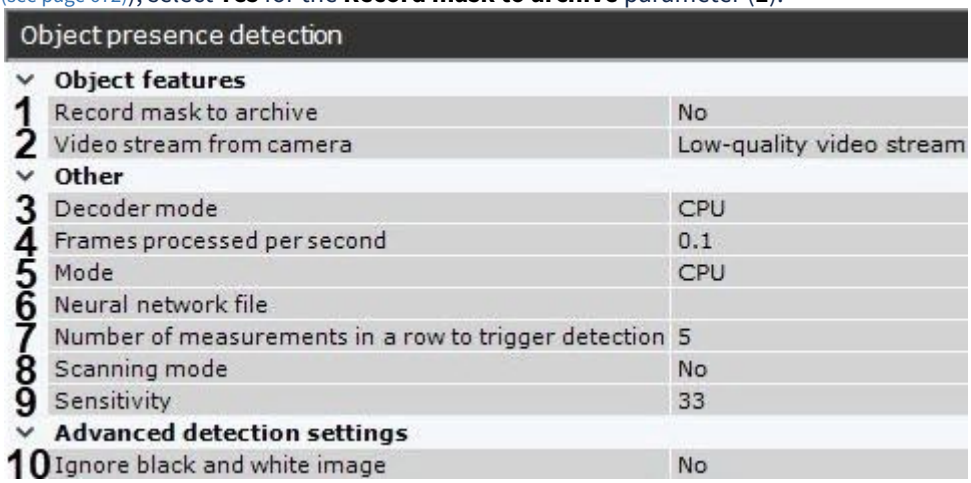
Hardware requirements for neural analytics operation(see page 52)

15.4.15.3 Configuring the object presence detection tool

Camera requirements for the object presence detection tool(see page 353)
Hardware requirements for neural analytics operation(see page 52)

To configure the object presence detection tool, do the following:

1. To record the sensitivity scale of the detection tool to the archive (see Displaying information from a detection tool (mask) (see page 672)), select **Yes** for the **Record mask to archive** parameter (**1**).



2. If the 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.
3. Select a processing resource for decoding video streams (**3**). 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.
4. Set the frame rate value for the detection tool to process per second (**4**). The value should be in the [0.016; 100] range.
5. Select the processor for the neural network operation—CPU, one of NVIDIA GPUs or one of Intel GPUs (**5**, see Hardware(see page 52) requirements (see page 52)for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)). 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.

Attention!

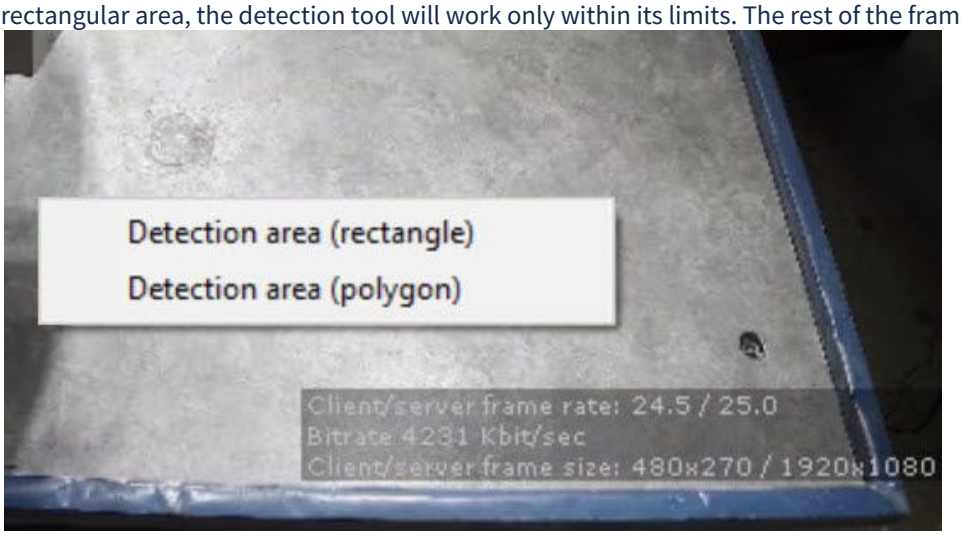
- It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU(see page 240)).
- If you specify other processing resource than the CPU, this device will carry the 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.

6. Select a neural network file (**6**). 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.

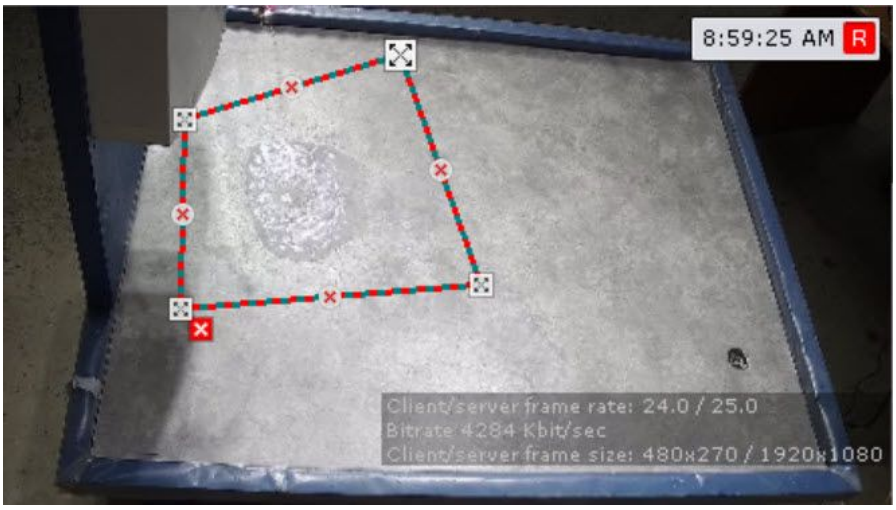
   Note

   For correct neural network operation on Linux, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

7. Set the minimum number of frames with the object present for triggering the tool (**7**). The value should be in the [5; 20] range.
8. To detect the objects without changing the frame size, select **Yes** in the **Scanning mode** field (**8**). To work in the scanning mode, the neural network must support the scanning mode.
9. Set the sensitivity of the detection tool by trial and error (**9**). The value should be in the [1; 99] range. The preview window displays the sensitivity scale of the detection tool that relates to the sensitivity parameter. If the scale is green, the object is not detected. If the scale is yellow, the object is detected, but not enough to trigger the tool. If the scale is red, the object is detected and the detection tool will trigger, if the scale is red through the analysis period (50 seconds by default, see item 4).
   Example. The sensitivity parameter value of 40 means that the detection tool will trigger when the scale has at least 4 divisions full over the entire analysis period. The triggering will stop when the scale has less than 2 divisions full over the analysis period. The detection tool will trigger again if the scale has at least 4 divisions full over the entire analysis period.
10. Select **Yes** for the **Ignore black and white image** parameter (**10**), if it is necessary that the detection tool does not trigger when the image is black and white.
11. By default, the entire frame is a detection area. If necessary, in the preview window, you can set detection areas using the anchor points:
    a. Right-click in the preview window.
    b. If you want to set the detection area by one or more rectangles, select **Detection area (rectangle)**. If you specify a rectangular area, the detection tool will work only within its limits. The rest of the frame will be ignored.



    c. If you want to set the detection area by one or more polygons, select **Detection area (polygon)**. If you specify one or several polygonal areas, the detection tool will process the entire frame, but the part of the frame that is not included in the specified polygons will be blacked out.



Attention!

You can configure detection areas similarly to exclude areas in Scene analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)).
You can use trial and error method to decide which type of detection area (rectangular or polygonal) is more effective in your case. Some neural networks give better detection with rectangles, while others are better with polygons.

15.4.16 Personal protective equipment detection tools

15.4.16.1 PPE detection (VL)

15.4.16.1.1 Functions of the PPE detection tool (VL)

The PPE detection tool (VL) locates individuals wearing no necessary personal protective equipment at the entrance or within the area where it's required, and also individuals wearing improperly applied PPE.

Attention!

It is recommended to use the detector in a "gateway" environment: at the entrance to an area in which equipment or PPE is required, the employee is delayed for 5—10 seconds, during which the detection tool determines the presence of the necessary equipment.

The PPE detection tool (VL) uses a built-in neural network that detects the following types of personal protective equipment:

1. Helmet.
2. Hood.
3. Gloves.
4. Vest.

Note

The PPE detection tool (VL) requires an additional Neuro Pack to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.16.1.2 Video stream and scene requirements for PPE detection tool (VL) operation

The PPE detection tool (VL) operation imposes the following requirements:

1. To the video stream from the camera:

   a. The resolution is at least 640x360 pixels. It is also not recommended to use a resolution higher than 1920×1080, since higher resolution does not increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1920x1080.
   b. The frame rate per second in the video stream from the camera is at least 13 for solving typical tasks.
   c. Color image only.
2. To lighting:
   a. Lighting in the scene is at least 200 lux per square meter. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the video analytics is not guaranteed.
   b. There are no abrupt changes in lighting.
3. To the scene and camera angle:
   a. Moving objects are visually separable from each other.
   b. The background is mostly static and does not change abruptly.
   c. There are no products made of rods in the detection area.
   d. Moving objects are minimally obscured by static objects in the scene (columns, trees, etc.).
   e. Avoid large obstructions in the camera FOV (columns, tower cranes, stacked materials, etc.). They will obscure the detected objects and cause track breaks. If obstructions cannot be avoided, it is recommended not to place them in the center of the frame.
   f. The analyzed scene does not have reflective surfaces and sharp shadows from moving objects. If present, they should be masked.
   g. The analyzed scene does not have strong light flashes (spotlights, active welding zones).
   h. Camera shake does not result in image offsets greater than 1% of the frame size.
   i. Shooting angle without a strong camera tilt.
   j. To improve the quality of the video stream, the camera lens should be cleaned of heavy dirt. It is not recommended to locate cameras above the material unloading area or near ventilation shafts.

Attention!

Correct operation of the detection tool is not guaranteed when using a fish-eye lens.

Hardware requirements for neural analytics operation(see page 52)
Objects image requirements for PPE detection tool (VL)(see page 356)

15.4.16.1.3 Objects image requirements for PPE detection tool (VL)

To ensure the correct recognition of personal protective equipment, the following image requirements should be met:

1. The object to be detected (PPE) is clearly distinguishable by the human eye.
2. Color image, not noisy and not distorted by compression algorithm artifacts.
3. Linear dimensions of PPE must not exceed 65% of the corresponding frame size.
4. The duration of the object's visibility is at least 10-13 frames. The minimum number depends on the current task.
5. There are no visible physical barriers between the camera lens and the analyzed object.
6. 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%.
7. The minimum height of the equipment on body areas in pixels is observed:
   a. Vest—at least 50 pixels.
   b. Helmet/Hood—at least 20 pixels.
   c. Gloves—at least 20 pixels.
8. PPE must have a standard look and shape, and have the following colors:
   a. Vest: green, yellow, orange.
   b. Helmet/Hood: white, yellow, orange, red, blue, green.
   c. Gloves: white, gray, black.
9. 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

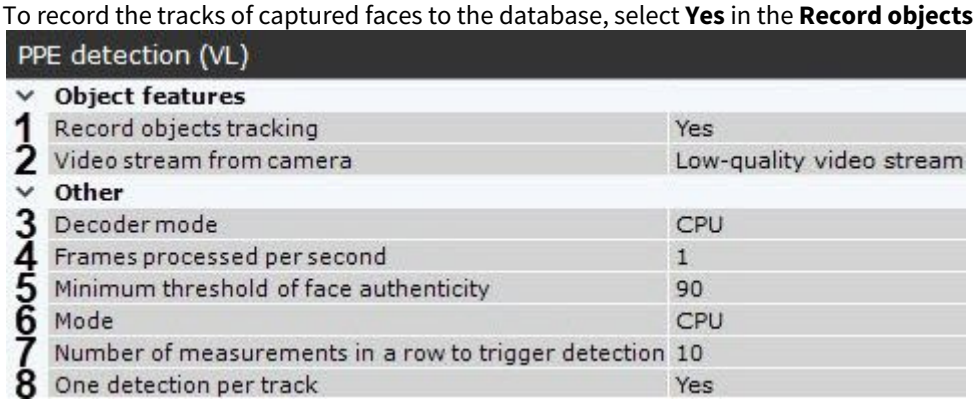
Image resolution	Minimum pixel density per meter (ratio of the object height in pixels to the object height in meters)	Minimum object height in pixels
1280x720	60	100
640x360	60	100

Video stream and scene requirements for PPE detection tool (VL) operation(see page 355)

15.4.16.1.4 Configuring PPE detection tool (VL)

To configure the PPE detection tool (VL), do the following:

1. To record the tracks of captured faces to the database, select **Yes** in the **Record objects tracking** parameter (**1**).



2. If the camera supports multistreaming, in the **Video stream from camera** field select the stream for which detection is needed (**2**).
3. In the **Decoder mode** field, select a processor for video decoding (**3**). 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 (see General Information on Configuring Detection(see page 234)).
4. Set the frame rate value for the detection tool to process per second (**4**). This value should be in the range [0.016; 100].
5. In the **Minimum threshold of face authenticity** field, set the minimum level of face recognition accuracy for creating a track (**5**). The value should be in the range [1; 100].

> **Note**
>
> An appropriate value should be selected empirically; at least 90 is recommended. The higher the value, the higher the recognition quality will be.

6. In the **Mode** field, select a processor for the neural network operation: CPU, one of GPUs, or one of Intel processors (**6**, see Hardware requirements for neural analytics operation(see page 52)).

> **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 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.
> 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(see page 240)).

7. In the **Number of measurements in a row to trigger detection** field, set the minimum number of frames on which the detection tool should detect a violation in order to generate a trigger (**7**). The value should be in the range [1; 20].
8. By default, a detection tool trigger for each item of equipment will be generated once within the existence of a person's track. If it is necessary to generate a trigger for each equipment violation, then select **No** in the **One detection per track** parameter (**8**).

The PPE detection tool (VL) is configured.

15.4.16.2 Equipment detection tool (PPE)

15.4.16.2.1 Functions of the Equipment detection tool (PPE)

The Equipment detection tool (PPE) locates individuals wearing no personal protective equipment within the area where it's required, and also individuals wearing improperly applied PPE.

Attention!

It is recommended to use the detector in a "gateway" environment: at the entrance to an area in which equipment or PPE is required, the employee is delayed for 5-10 seconds, during which the detection tool determines the presence of the necessary equipment (see Examples of configuring Equipment detection tool (PPE) for solving typical tasks(see page 362)).

For detection tool operation, at least two separate neural networks are used:

- segmenting network – it structures up an image of a human body (locates head, shoulders, arms, hands, thighs, legs and feet);
- classifying network – it detects equipment (PPE) on a specified body part, and checks if it's properly applied.

Attention!

To train a classification neural network, it is necessary to provide a list of equipment (see Example of providing a list of valid equipment at the facility(see page 363)).

Note

The equipment detection tool (PPE) requires an additional Neuro Pack to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.16.2.2 Video stream and scene requirements for Equipment detection tool (PPE) operation

The Equipment detection tool (PPE) operation imposes the following requirements:

1. To the video stream from the camera:
   a. The resolution is at least 640x360 pixels. It is also not recommended to use a resolution higher than 1920×1080, since higher resolution does not increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720.
   b. The frame rate per second in the video stream from the camera is at least 3 for solving typical tasks.
   c. Color image only.
2. To lighting:
   a. Lighting in the scene is at least 200 lux per square meter. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the video analytics is not guaranteed.
   b. There are no abrupt changes in lighting.
3. To the scene and camera angle:
   a. Moving objects are visually separable from each other.
   b. The background is mostly static and does not change abruptly.
   c. There are no products made of rods in the detection area.
   d. Moving objects are minimally obscured by static objects in the scene (columns, trees, etc.).
   e. The analyzed scene does not have reflective surfaces and sharp shadows from moving objects. If present, they should be masked.
   f. Camera shake does not result in image offsets greater than 1% of the frame size.

Attention!

Correct operation of the detection tool is not guaranteed when using a fish-eye lens.

Hardware requirements for neural analytics operation(see page 52)
Objects image requirements for Equipment detection tool (PPE)(see page 359)

15.4.16.2.3 Objects image requirements for Equipment detection tool (PPE)

To ensure the correct recognition of personal protective equipment, the following image requirements should be met:

1. The object to be detected (PPE) is clearly distinguishable by the human eye.
2. The image is not noisy and not distorted by compression algorithm artifacts.
3. The width or height of the equipment does not exceed 75% of the frame size.
4. The duration of the object's visibility is at least 3-8 frames. The minimum number of frames depends on the task.
5. There are no visible physical barriers between the camera lens and the analyzed object.
6. 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

7. The minimum dimensions of the equipment on the body areas in pixels are observed. An example of equipment dimensions for a resolution of 1920x1080:
   a. upper body (torso) 75*100,
   b. legs 75*105,
   c. head 60*65,
   d. hands 65*60,
   e. feet 45*40,
   f. set of equipment 165*295.

Video stream and scene requirements for Equipment detection tool (PPE) operation(see page 358)

15.4.16.2.4 Configuring equipment detection tool (PPE)

Video stream and scene requirements for Equipment detection tool (PPE) operation(see page 358)
Objects image requirements for Equipment detection tool (PPE)(see page 359)
Hardware requirements for neural analytics operation(see page 52)

To configure the Equipment detection tool (PPE), do the following:

1. To record mask (body-based segmentation) to the archive (see Displaying information from a detection tool (mask)(see page 672)), select **Yes** in the corresponding parameter (**1**).

Equipment detection (PPE)		
	Object features	
1	Record mask to archive	No
2	Record objects tracking	Yes
3	Video stream from camera	Low-quality video stream
	Other	
	Classification network 1 file	
	Classification network 2 file	
4	Classification network 3 file	
	Classification network 4 file	
	Classification network 5 file	
5	Decoder mode	CPU
6	Frames processed per second	1
7	Min person height	0.01
8	Min person width	0.01
9	Mode	CPU
10	Segmenting network file	
	Advanced detection settings	
11	Mask	No
12	Number of measurements in a row to trigger detection	3
13	One event per PPE element	Yes

2. By default, metadata is not recorded to the database. To enable metadata recording, select **Yes** in the **Record objects tracking** parameter (**2**).
3. If the camera supports multistreaming, select the stream for which detection is needed (**3**).
4. 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 (**9**). To initialize only one item of equipment, select the required classification neural network file (**4**). There should 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 (**4**).

   > **Note**
   >
   > To ensure the correct operation of the neural network on Linux OS, the corresponding file should be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

5. 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 (see General Information on Configuring Detection(see page 234)).
6. Set the frame rate value for the detection tool to process per second (**6**). This value should be in the range [0,016; 100].

   > **Attention!**
   >
   > To apply detection in gateway mode (see Examples of configuring Equipment detection tool (PPE) for solving typical tasks(see page 362)), we recommend that you use the detection tool standard settings: 1 FPS and 3 frames for output (see step 10).
   > To apply detection in continuous mode for busy scenes, set the delay to no less than 4 FPS, and the number of frames for output to no less than 6.

7. Set the minimum height and width of a person (**7**, **8**) in the frame as a percentage of the frame height/width (0,15 = 15%). Objects which are smaller than the specified size will not be detected. The value should be in the range [0; 1].
8. Select the processor for the neural network—CPU, one of Nvidia GPUs or one of Intel GPUs (**9**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

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(see page 240)).
- 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 classifying neural networks.
- Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

9. By default, the Segmenting neural network is initialized according to the selected processing device (**9**). 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 (**10**).

   Note

   To ensure the correct operation of the neural network in Linux OS, the corresponding file should be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

10. Enable the **Mask** parameter to display body segments in the preview window (**11**).
11. Set the minimum number of frames containing people with no PPE for the tool to trigger (**12**). The value should be in the range [1; 20].
12. By default, each equipment element triggering occurs once during a continuous tracking of a person. You can set triggering to multiple by setting the **One event per PPE element** parameter to **No** (**13**).

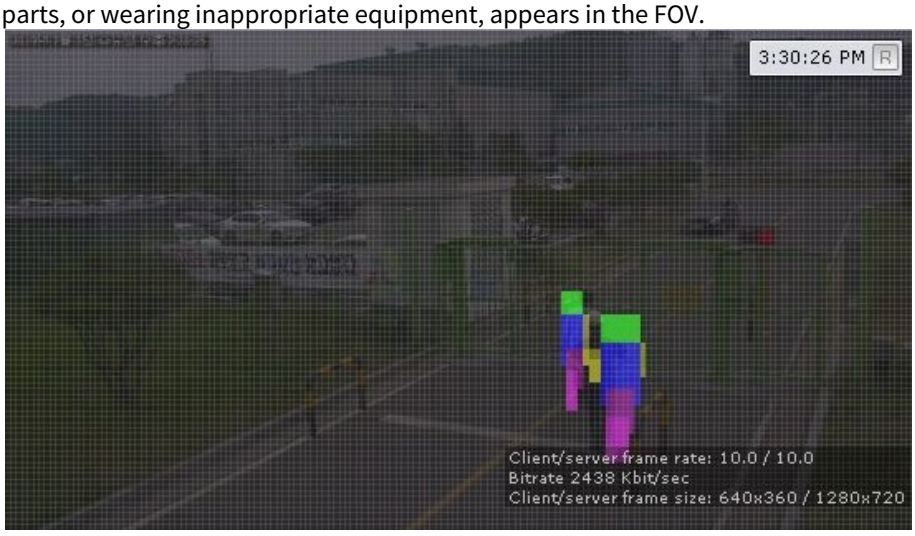
    Note

    Example. An individual not wearing a helmet appears in the FOV, 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.

13. In the preview window, you can set the detection zones with the help of anchor points much like privacy masks in Scene Analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)). By default, the entire FOV is a detection area.
14. Click the **Apply** button.

The Equipment detection tool (PPE) is now configured.

The Equipment detection tool (PPE) triggers an alarm when a person not wearing required equipment (PPE) on specified body parts, or wearing inappropriate equipment, appears in the FOV.



The Equipment detection tool (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(see page 433)) after the Equipment detection tool (PPE) is triggered, it is necessary to set up a separate macro command with an E-mail message for each item of equipment.

15.4.16.2.5 Examples of configuring Equipment detection tool (PPE) for solving typical tasks

Typical tasks for detecting personal protective equipment are the following:

1. Detection in gateway conditions. A gateway is a border, which can be either 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 PPE is required.
   b. The person poses in a way that it is possible to check the presence of all items of equipment (the item is not overlapped by the person himself, other items of equipment, items of clothing).

   c. Human screening. There should 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 tool (PPE) is configured for detection in gateway conditions.

The recommended settings for solving typical tasks are as follows:

Settings	Equipment detection in gateway conditions	Equipment detection in production conditions
Main		
The number of frames processed per second	1	3
Minimum person height	0,01	0,09
Minimum person width	0,01	0,03
Advanced		
Number of frames for analysis and output	3	7
Mask	No	No
One event per item of equipment	Yes	Yes

15.4.16.3 Example of providing a list of valid equipment at the facility

Data collection requirements for neural network training(see page 239)

For correct detection, it is important to understand exactly what items of equipment are used at the facility.

A complete list of equipment should be provided regardless of the current season of the year. This will help to reduce the number of false events from the Personal protective equipment detection tools and get the most positive experience from using this analytics.

Below are examples of lists in the form of a table:

Gloves #1

Gloves #2

Gloves #3

Gloves #4

Helmet #1:
Helmet #2:
Helmet #3:
Helmet #4:
Helmet #5 (#4 screen:)
Helmet #6 (#4 earmuffs):
UpperBody+Shoes
Helmets
Gloves

15.4.17 Person-based privacy masking

15.4.17.1 Person-based privacy mask functions

The privacy mask hides selected parts of a human body from viewing on video.

A segmenting network structures up an image of a human body: locates head, shoulders, arms, hands, thighs, legs and feet.

> **Note**
>
> Person-based privacy masking requires the Add-on Neuro Pack to be installed.

15.4.17.2 Camera requirements for person-based privacy masking

For person-based privacy masking operation, a camera must match the following requirements:

1. Frame rate is no less than 12 FPS.
2. Pixel density must be at least 170 pixels per meter.
3. Average illumination in scenes with privacy masking must not drop below 200 lux.

Attention!

We cannot guarantee normal operation with a fisheye camera.

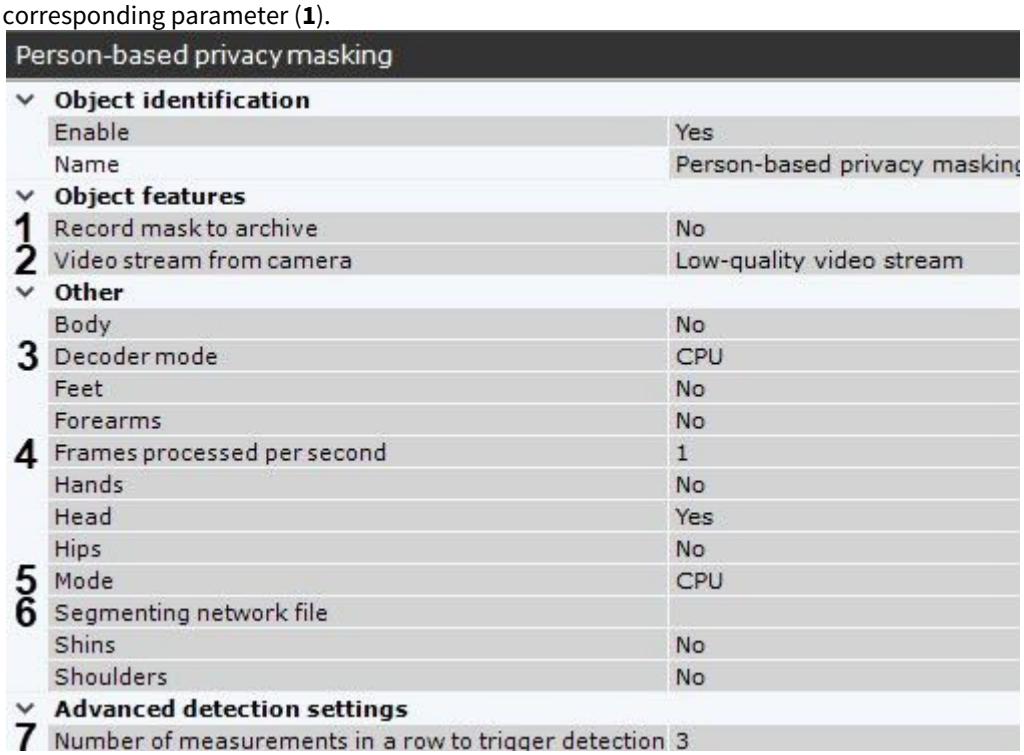
Hardware requirements for neural analytics operation(see page 52)

15.4.17.3 Person-based privacy masking configuration

Camera requirements for person-based privacy masking(see page 367)
Hardware requirements for neural analytics operation(see page 52)

To configure Person-based privacy masking, do the following:

1. To record mask to the archive (see Displaying information from a detection tool (mask)(see page 672)), set **Yes** for the corresponding parameter (**1**).



Person-based privacy masking		
	Object identification	
	Enable	Yes
	Name	Person-based privacy maskin
	Object features	
1	Record mask to archive	No
2	Video stream from camera	Low-quality video stream
	Other	
	Body	No
3	Decoder mode	CPU
	Feet	No
	Forearms	No
4	Frames processed per second	1
	Hands	No
	Head	Yes
	Hips	No
5	Mode	CPU
6	Segmenting network file	
	Shins	No
	Shoulders	No
	Advanced detection settings	
7	Number of measurements in a row to trigger detection	3

2. If the camera supports multistreaming, select the stream for which detection is needed (**2**).
3. Select a processing resource for decoding video streams (**3**). 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.
4. Set the frame rate value for the detection tool to process per second (**4**). This value should be in the range [0,016; 100].
5. Select the processor for the neural network—CPU, one of NVIDIA GPUs, or one of Intel GPUs (**5**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

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(see page 240)).
- Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

6. Select the segmenting neural network file (**6**). 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.

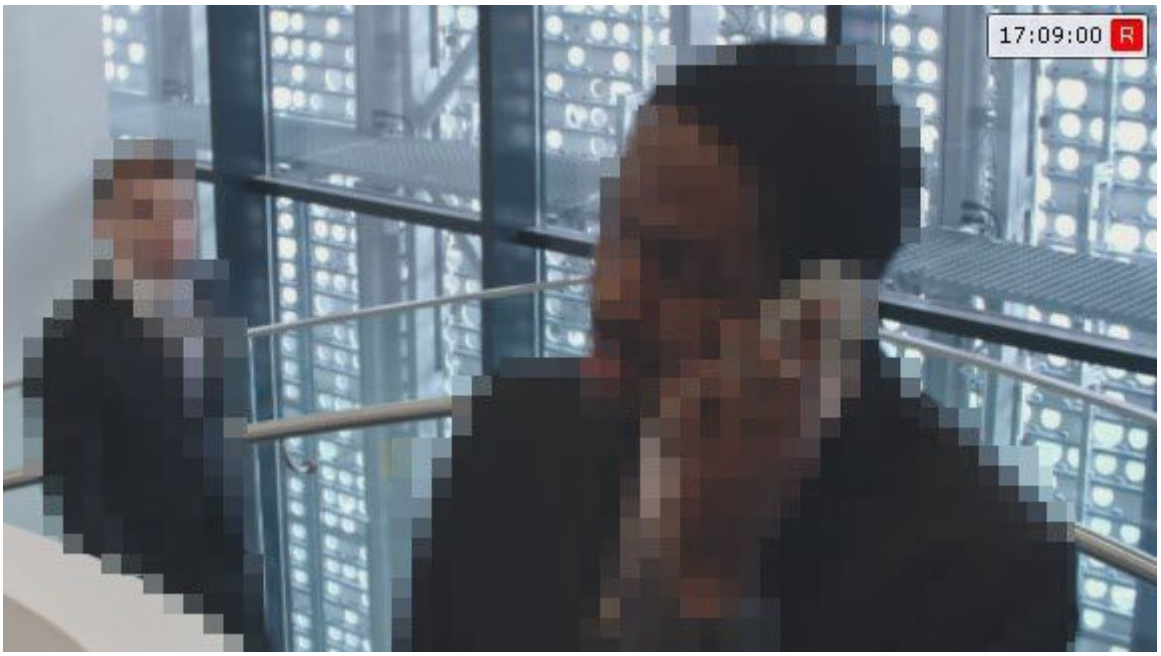
   Note

   For correct neural network operation on Linux, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

7. Set the minimum number of frames in which the detection tool should detect objects in order to trigger (**7**). The value should be in the range [1; 20].
8. Select **Yes** for all body parts that should be masked within FOV.
9. Click the **Apply** button.

Privacy mask configuration is now complete.

Selected body parts of all individuals within FOV will be hidden from view. For a user group with limited rights to view masked video (see Creating and configuring roles(see page 452)), 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(see page 809)).



15.4.18 Privacy masking detection tool

15.4.18.1 Functions of the Privacy masking detection tool

The Privacy masking detection tool hides moving objects in the video image.

When you use a neural network in the Privacy masking detection tool operation, it improves the accuracy of working with moving objects and hides stationary objects.

Note

The Privacy masking detection tool requires Neuro Pack add-on to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.18.2 Camera requirements for the Privacy masking detection tool

Make sure the following requirements are met for the correct operation of the Privacy masking detection tool:

1. Camera requirements:
   a. Resolution is at least 320x240 pixels.
   b. Frame rate is at least 1 FPS.
   c. Camera shake shouldn't cause image shift greater than 1% of the frame size.
2. Lighting requirements:
   a. Moderate lighting. The quality of analytics performance can be lower in conditions of low lighting (night) or excessive lighting (overexposure).
   b. No sudden changes in lighting.
3. Scene and camera angle requirements:
   a. Moving objects must be visually separable from each other in the image.
   b. Background is mostly static and without sudden changes.
   c. Moving object should be minimally obscured by the stationary objects in the scene (columns, trees, etc.).
   d. Analytics may not work correctly on reflective surfaces and when there are sharp shadows from moving objects.
   e. Analytics may not work correctly on long, one-colored objects.
4. Object images requirements:
   a. The digital noise and compression-related artifacts are minimal.
   b. The width and height of the objects in the image must not be less than 1% of the frame size (if resolution is at least 1920x1080 pixels) or 15 pixels (at lower resolutions).
   c. The width and height of the objects in the image must not exceed 75% of the frame size.
   d. The movement speed of the objects in the image must not be less than 1 pixel per second.
   e. To detect an object, the duration of its visibility must be at least 8 frames.

15.4.18.3 Configuring the Privacy masking detection tool

Camera requirements for the Privacy masking detection tool(see page 369)
Hardware requirements for neural analytics operation(see page 52)

To configure the Privacy masking detection tool, do the following:

1. To record mask to the archive (see Displaying information from a detection tool (mask)[135]), set **Yes** for the corresponding parameter (**1**).

135 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=202671400

Privacy masking		
	Object features	
1	Record mask to archive	Yes
	Video stream	Second stream
	Other	
	Enable	Yes
	Name	Privacy masking
	Decode key frames	No
2	Decoder mode	CPU
3	Detection threshold	15
4	Mode	CPU
5	Neural network	No
6	Neural network file	
7	Number of frames processed per second	25

2. Select a processing resource for decoding video streams (**2**). 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.
3. Set the detection threshold (**3**). The value should be selected empirically in the range [5, 100]. The higher the value, the higher the sensitivity to object recognition and masking.
4. Select the processor for the neural network—CPU, one of NVIDIA GPUs, or one of Intel GPUs (**4**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

   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(see page 240)).
   - Starting with *Detector Pack* 3.11, Intel HDDL and Intel NCS aren't supported.

5. If the detection tool cannot correctly identify the object in the frame, you should use the **Neural network** (**5**):
   a. If **No** is selected, the detection tool will operate on the basis of the algorithm without using a neural network, ignoring the value specified in the **Neural network file** field.
   b. If **Yes** is selected, and in the **Neural network file** field a custom neural network is selected that is a privacy masking neural network, a detection tool with a neural network algorithm based on this network will be created.
6. Select the neural network file (**6**). 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, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

7. Set the frame rate value for the detection tool to process per second (**7**). This value should be in the range [0.016; 100].
8. If you want to exclude complex areas (foliage, water, etc.) from the analysis of the camera FOV, set one or more exclude areas similar to the **Object Tracker** (see Setting General Zones for Scene analytics detection tools(see page 262)) inside which the detection won't be performed.

Configuring the Privacy masking detection tool 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.

15.4.19 Pose detection tools

15.4.19.1 Functions of Pose detection tool

The Pose detection tool uses a neural network and add-on detection tools to determine each person's skeleton and detect poses that could indicate a potentially dangerous situation.

The following detection tools can be created on the basis of the Pose detection tool:

Detection Tool	Detection tool description
Sitting person detection(see page 375)	Detection tool triggers when there is a sitting human in the frame
Man down detection(see page 376)	Detection tool triggers when there is a prostrate human in the frame
Hands up detection(see page 378)	Detection tool triggers when there is a human raising one or two hands in the frame. A hand is considered raised if the forearm is parallel to the back
Handrail holding detection(see page 378)	Detection tool triggers when there is a human in the specified part of the frame who does not hold any of specified handrails
People counter detection(see page 379)	Detection tool counts objects in the specified area. Detection tool triggers when the number of objects reaches or exceeds the specified limit
Close-standing people detection(see page 381)	Detection tool triggers when the distance between people in the frame exceeds the specified minimum value
People masking detection(see page 382)	Detection tool masks people in the video image. Detection tool does not trigger

Note

Pose detection tools require Addon Neuro Pack to be installed (see Installing DetectorPack add-ons(see page 74)).

15.4.19.2 Video stream and scene requirements for Pose detection tools

The Pose detection tools operation has the following requirements:

1. To the video stream from the camera:
   a. The resolution is at least 640x360 pixels. It is also not recommended to use a resolution higher than 1920x1080, since higher resolution does not increase the detection quality, but significantly increases the consumption of resources. The optimal resolution for solving typical tasks is 1280x720.
   b. The frame rate per second in the video stream from the camera is at least 8.
   c. Color image only.
2. To the lighting:
   a. Scene lighting is at least 50 lux per square meter. In conditions of insufficient or excessive lighting (night or light-striking), stable operation of the analytics is not guaranteed.
   b. There are no abrupt changes in lighting.
3. To the scene and camera angle:
   a. Moving objects are visually separable from each other in the image.
   b. The background is mostly static and does not change abruptly.
   c. Moving objects are minimally obscured by the static objects in the scene (columns, trees, etc.).
   d. The analyzed scene does not have reflective surfaces and sharp shadows from moving objects. If present, they should be masked.
   e. Camera shake does not result in image offsets greater than 1% of the frame size.

Attention!

Correct operation of the Pose detection tools is not guaranteed when using fish-eye cameras and other cameras with strong image distortion.

Hardware requirements for neural analytics operation(see page 52)
Objects image requirements for Pose detection tool(see page 372)

15.4.19.3 Objects image requirements for Pose detection tool

To ensure the correct recognition of a person's posture, the following image requirements should be met:

1. The detected object is clearly distinguishable by the human eye.
2. The detected object is completely within the frame.
3. The image is not noisy and not distorted by the compression algorithm artifacts.
4. The duration of the object visibility is at least 2 frames.
5. 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 sub-detection tools			
1920x1080	Human	170	~102x309
1280x720	Human	128	~77x233
640x360	Human	80	~48x145
For classical Pose sub-detection* tools			
1920x1080	Human	100	~45x187
1280x720	Human	68	~31x134
640x360	Human	35	~15x65

Video stream and scene requirements for Pose detection tools(see page 372)

* see information about classical Pose sub-detection tools here: Functions of Scene Analytics detection tools(see page 255)

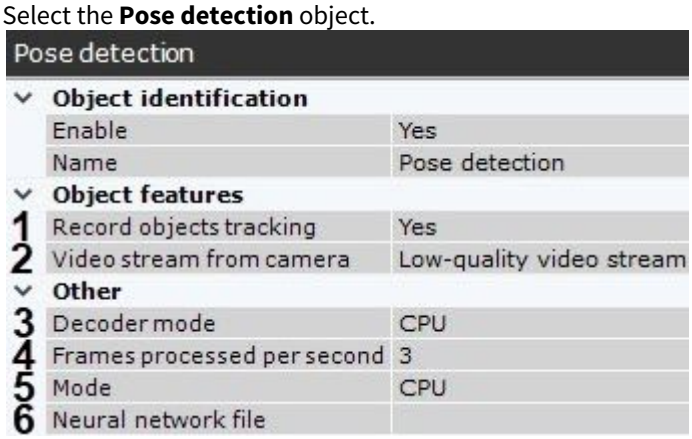
15.4.19.4 Configure Pose detection tools

15.4.19.4.1 Setting up common parameters for Pose detection tools

Video stream and scene requirements for Pose detection tools(see page 372)
Objects image requirements for Pose detection tool(see page 372)
Hardware requirements for neural analytics operation(see page 52)

To configure the common parameters for Pose detection tools, do as follows:

1. Select the **Pose detection** object.



2. By default, video stream metadata are recorded to the database. You can disable it by selecting **No** in the **Record objects tracking** list (**1**).
3. If the 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.
4. Select a processing resource for decoding video streams (**3**). 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.
5. Set the frame rate value for the detection tool to process per second (**4**). This value should be in the range [0,016; 100].

   Attention!

   With static individuals in scene, set the FPS to no less than 2. With moving individuals in scene, the FPS should be set to 4 and above.
   The higher the FPS value, the higher the accuracy of pose detection, but the load on the CPU 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.

6. Select the processor for the neural network—CPU, one of NVIDIA GPUs or one of Intel GPUs (**5**, see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

   Attention!

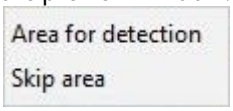
- It may take several minutes to launch the algorithm on NVIDIA GPU after you apply the settings. You can use caching to speed up future launches (see Optimizing the operation of neural analytics on GPU(see page 240)).
- If you specify other processing resource than the CPU, the selected device will 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.
- Man down or sitting pose detection accuracy may depend on the particular processor. If another selected processor gives less accurate results, set the detection parameters empirically, and configure scene perspective (see Specific settings for the Man down detection tool(see page 376), Specific settings for the Sitting person detection tool(see page 375)).

7. Select a neural network file (**6**). 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

   To ensure the correct operation of the neural network on Linux OS, the corresponding file should be located in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

8. By default, the entire FOV is an area for detection. If necessary, you can specify the areas for detection and skip areas in the preview window. To set an area for detection, right-click on the image, and select the required area.

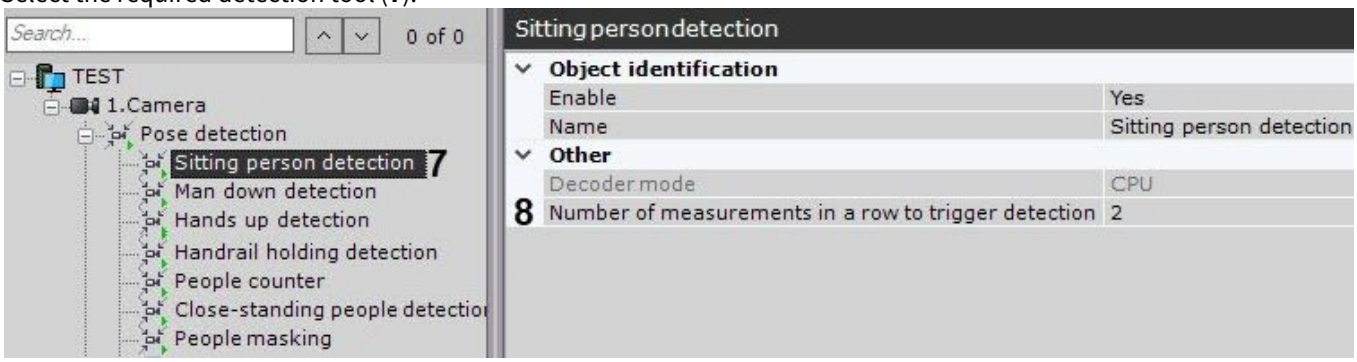
   Note

   The areas are set the same way as for the Scene Analytics detection tools (see Configuring the Detection Zone(see page 266)).

   This is how it works:

   a. if you specify areas for detection only, no detection will be performed in the rest of FOV.
   b. if you specify skip areas only, the detection will be performed in the rest of FOV.

9. Select the required detection tool (**7**).



10. Set the minimum number of frames with a relevant pose or behavior for the tool to trigger (**8**).

> **Note**
>
> The default values (2 frames and 1000 milliseconds) indicate that the tool will analyze one frame every second. When a pose is detected in two subsequent frames, the tool will trigger.
> This parameter is not used when configuring people masking.

11. Click the **Apply** button.

Setting up the common parameters for the Pose detection tools is complete.

15.4.19.4.2 Specific settings for the Sitting person detection tool

Setting up common parameters for Pose detection tools(see page 373)

To detect a sitting pose, you should configure frame perspective first.

To do this, do the following:

1. Select a detection tool, and click the button in the preview window.
2. Set the size of the same person in different areas of the FOV. To create a leveling rod, left-click on the video image to add two anchor points. You should set at least three leveling rods. The size of the leveling rod should be about the average height of a person at this point in the frame. You can resize the rod by stretching its anchor points . You can move it on screen by dragging and dropping[136].

136 https://ru.wikipedia.org/wiki/Drag-and-drop

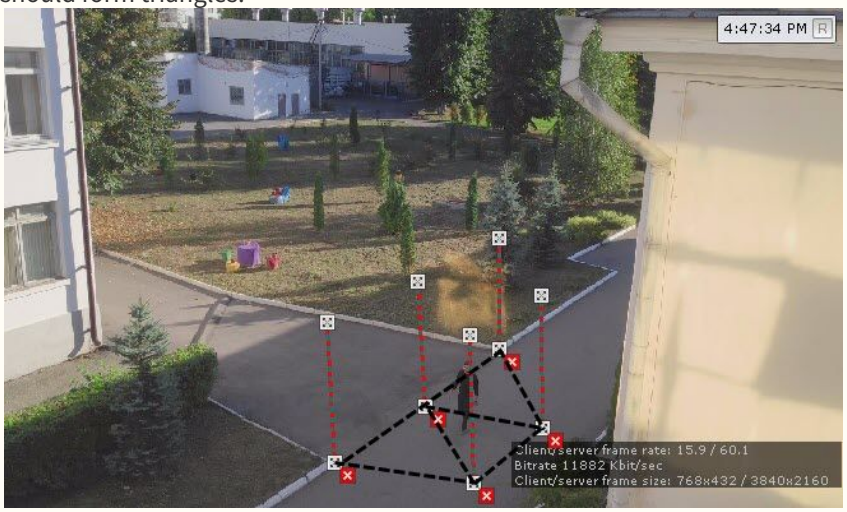
Attention!

When setting up the leveling rods, the following conditions should be met:

a. The rods that are located at the same distance from the video camera lens, should be of the same size.
b. The feet of the rods should be located on the same surface (e.g. floor).
c. In complex scenes, it is recommended to add 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 should be parallel to the nearest vertical objects (e.g. door, wardrobe).

Attention!

For portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, etc.), the arrangement of the rods should form triangles.



Note

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

Note

To delete the rod, click the button.

3. Click the **Apply** button.

Configuring the Sitting person detection tool is complete.

15.4.19.4.3 Specific settings for the Man down detection tool

Setting up common parameters for Pose detection tools(see page 373)

To detect a recumbent pose, you should configure the frame perspective first.

To do this, do the following:

1. Select a detection tool, and click the button in the preview window.

2. Set the size of the same person in different areas of the FOV. To create a leveling rod, left-click on the video image to add two anchor points. You should set at least three leveling rods. The size of the leveling rod should be about the average height of a person at this point in the frame. You can resize the rod by stretching its anchor points . You can move it on screen by dragging and dropping[137].

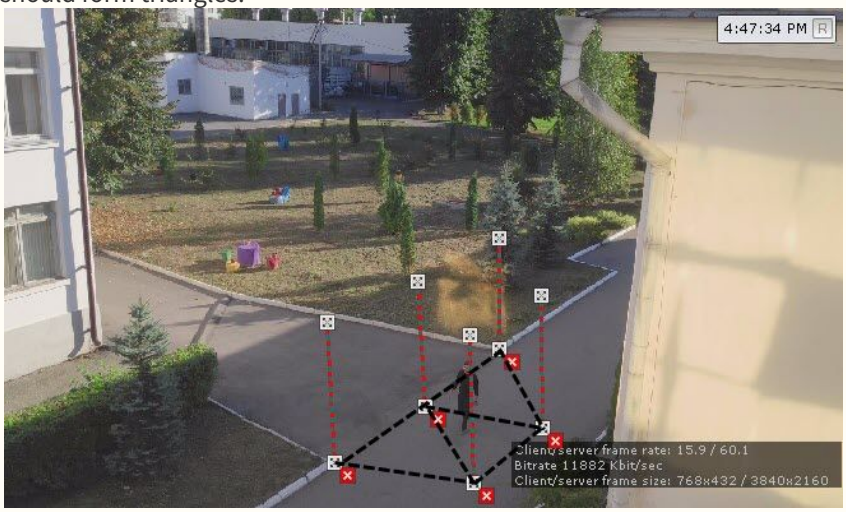
Attention!

When setting up the leveling rods, the following conditions should be met:

a. The rods that are located at the same distance from the video camera lens, should be of the same size.
b. The feet of the rods should be located on the same surface (e.g. floor).
c. In complex scenes, it is recommended to add 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 should be parallel to the nearest vertical objects (e.g. door, wardrobe).
e. If only three leveling rods are added to the scene, they cannot be removed from the scene, only their size and position can be changed.
f. If more than three leveling rods are added to the scene, you can change their position, size, and also remove them from the scene.

Attention!

For portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, etc.), the arrangement of the rods should form triangles.



137 https://ru.wikipedia.org/wiki/Drag-and-drop

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

> **Note**
>
> To delete the rod, click the button.

3. Click the **Apply** button.

Configuring the Man down detection tool is complete.

> **Attention!**
>
> In cases when the recumbent person is facing the camera or facing away from the camera, the correct operation of the detection tool isn't guaranteed.

15.4.19.4.4 Specific settings for Hands up detection tool

The Hands up detection tool triggers if a person with one or both hands raised is detected in a specified area.

To configure the Hands up detection tool, do the following:

1. Configure general settings (see Setting up common parameters for Pose detection tools(see page 373)).
2. Set the detection tool operation **Mode** (**1**):
   a. Both hands: triggers only if the person has both hands raised.
   b. One hand: triggers only if the person has one hand raised.
   c. Only left hand or Only right hand: triggers only if one selected hand is raised.
   d. Left or Right hand: triggers only if the selected hand is raised.

Hands up detection	
Object identification	
Enable	Yes
Name	Hands up detection
Other	
Decoder mode	CPU
1 Mode	Both hands
2 Number of measurements in a row to trigger detection	2

3. Set the minimum number of frames in which the counter should detect a person with a raised hand/hands in order to trigger (**2**). The value should be in the range [1; 20].

> **Note**
>
> The Hands up detection tool works in the areas for detection and skip areas specified in the Pose detection tools (see Setting up common parameters for Pose detection tools(see page 373)).

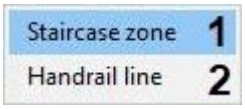
Configuring the Hands up detection tool is complete.

15.4.19.4.5 Specific settings for Handrail holding detection tool

To configure the Handrail holding detection tool, do the following:

1. Set common parameters (see Setting up common parameters for Pose detection tools(see page 373)).
2. Click anywhere in the Preview window.

3. Mark one or several handrails with lines (**1**).



> **Attention!**
>
> - If lens distortion makes the handrail non-linear, use several lines.
> - The presence of a person in the staircase zone is determined by their lower limbs.

4. Set anchor points to specify the area where a person should hold the handrail (**2**).

Configuring the Handrail holding detection tool is complete.

15.4.19.4.6 Specific settings for People counter detection tool

The People counter detection tool counts the number of people in the specified area using the pose detection metadata.

A macro triggers when the number of individuals in FOV matches the predefined conditions (see Configuring filters for event-driven macros(see page 407)).

> **Note**
>
> Unlike the Multiple objects detection tool (see Settings specific to Multiple objects(see page 272)), the counter generates events of just one type, namely triggering.
> As opposed to Neurocounter (see Configuring a Neurocounter(see page 345)), People counter detection tool counts only people.

To configure the People counter detection tool, do the following:

1. Set common parameters (see Setting up common parameters for Pose detection tools(see page 373)).

2. To record mask to the archive, set **Yes** for the corresponding parameter (**1**).

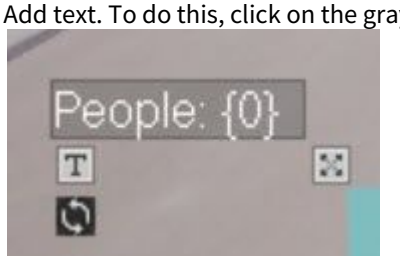
	People counter	
	Object identification	
	Enable	Yes
	Name	People counter
	Object features	
1	Record mask to archive	No
	Other	
2	Alarm when value	In range
	Decoder mode	CPU
3	End value of alarm range settings	100
4	Event interval	1
5	Number of measurements in a row to trigger detection	3
6	Start value of alarm range settings	5

3. Set the People counter detection tool triggering condition:
   a. Set the condition polarity, i.e. triggering when the number of people in the specified area is within the set range, or out of the range (**2**).
   b. Set the range of the number of people in FOV (**3**, **5**). The value should be in the range [0; 100].
4. Set an interval in seconds between two consecutive triggering of the counter when the number of individuals in FOV continuously matches the condition(s) (**4**). The value should be in the range [1; 10000].
5. Set the minimum number of frames in which the counter should detect the specified number of people in order to trigger (**6**). The value should be in the range [1; 20].
6. In the preview window, you can set the detection areas with the help of the anchor points much like privacy masks in the Scene analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)). By default, the entire FOV is a detection area.

Configuring the People counter detection tool is complete.

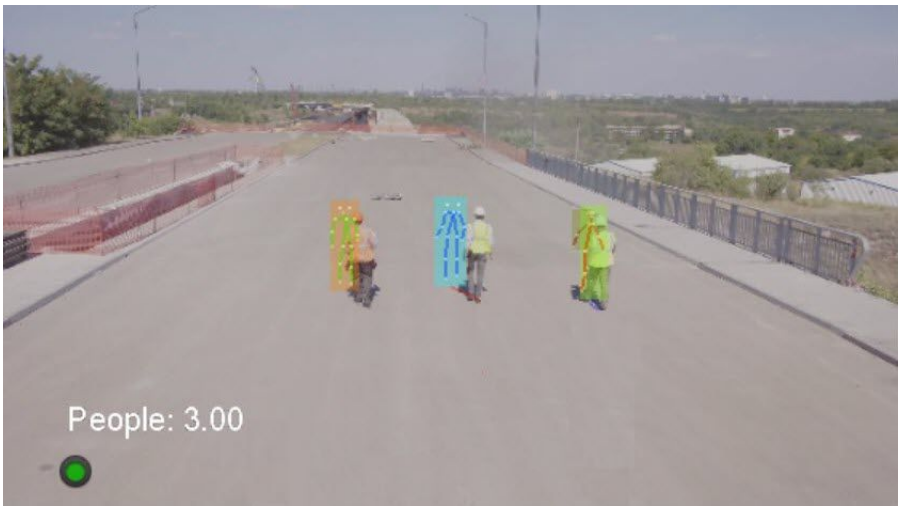
To display the counter and the number of counted people, do the following:

1. Switch to layout editing mode (see Switching to layout editing mode(see page 474)).
2. Place the counter icon anywhere within the layout cell.
3. Customize the font. To do this, click the T button.
4. Add text. To do this, click on the gray area and enter the required text.



5. Save the layout (see Exiting Layout Editing mode(see page 499)).

As a result, the text and the number of people counted by the detection tool will be displayed next to the counter icon.



15.4.19.4.7 Specific settings for Close-standing people detection tool

Setting up common parameters for Pose detection tools(see page 373)

By default, the Close-standing people detection tool triggers when "skeleton" bounding boxes around individuals collide.

Note

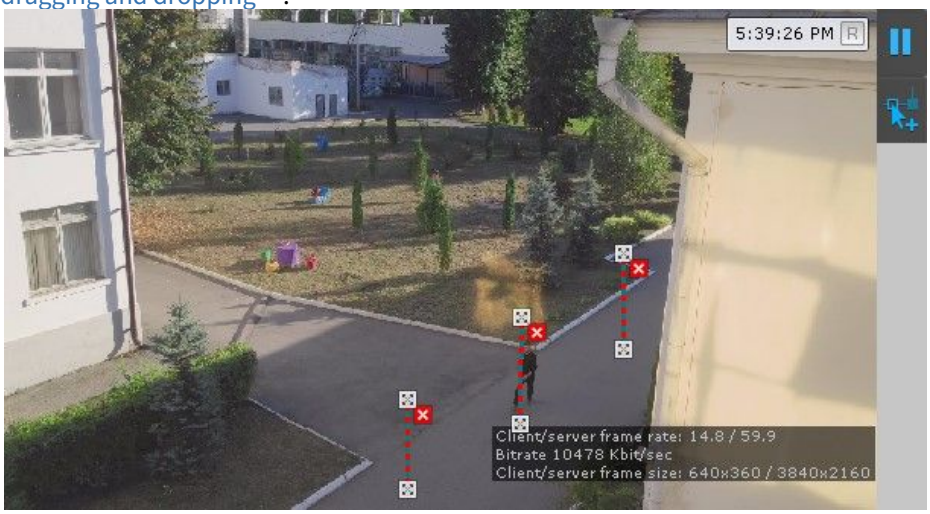
Bounding boxes are not displayed in the interface. They are usually a bit larger than the "skeletons" dimensions.

You can set another triggering distance by adjusting the frame perspective:

Attention!

For portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, etc.) perspective adjustment is a must.

1. Select a detection tool, and click the button in the preview window.
2. Set the size of the same object in different areas of the frame. To create a leveling rod, left-click on the video image and add two anchor points. Set at least three leveling rods. The size of the leveling rod should be about the average height of a person at this point in the frame. You can resize the rod by stretching its anchor points . You can move it on screen by dragging and dropping[138].



138 https://ru.wikipedia.org/wiki/Drag-and-drop

Attention!

When setting up the leveling rods, the following conditions should be met:

a. The rods that are located at the same distance from the video camera lens, should be of the same size.
b. The feet of the rods should be located on the same surface (e.g. floor).
c. In complex scenes, it is recommended to add 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 should be parallel to the nearest vertical objects (e.g. door, wardrobe).

Attention!

For portrait-oriented scenes (such as corridor, shopping aisle, warehouse aisle, etc.), the arrangement of the rods should form triangles.

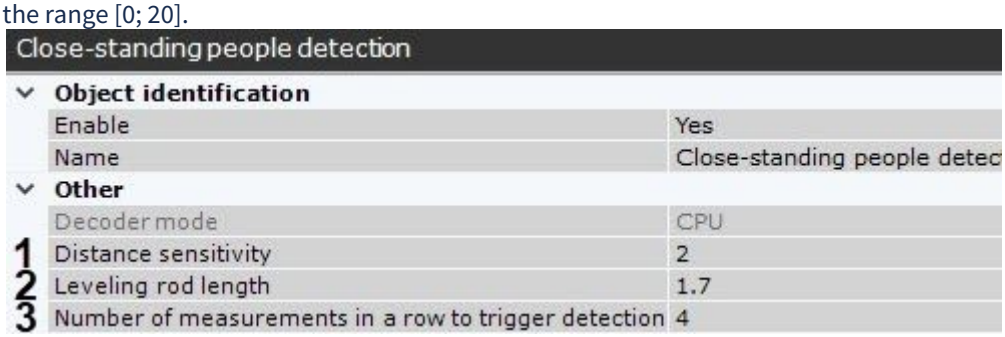
Note

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

Note

To delete the rod, click the button.

3. In the **Distance sensitivity** field (**1**) enter a triggering distance value in meters between people. The detection tool will trigger if the distance between people in the frame becomes equal or less than the specified value. The value should be in the range [0; 20].



4. In the **Leveling rod length** field (**2**) enter the average height of a person (in meters), according to which the leveling rods are set. The value should be in the range [0; 3].
5. Set the minimum number of frames in which the detection tool should detect close-standing people in order to trigger (**3**). The value should be in the range [1; 100].

Configuring the frame perspective for the Close-standing people detection tool is complete.

15.4.19.4.8 Specific settings for People masking detection tool

This detection tool does not trigger. It uses the Pose detection tools metadata to mask people on the video image:

- on live video;
- in the archive;
- when exporting from the archive.

Attention!

Masking function works only for those users who have the **View masked video** parameter disabled in the role settings (see Creating and configuring roles(see page 452)).

15.4.20 Retail Analytics

15.4.20.1 Functions of retail analytics

Name of a Detection Tool object	**Detection description**
Queue detection	Triggers if the specified number of people in the queue is exceeded.
Visitors counter	This detector monitors the number of visitors within the protected area, and triggers if the specified count is exceeded.

15.4.20.2 Camera requirements for Queue detection

The following table contains the requirements for the cameras used by the queue detection tool:

Camera	• Resolution: 720 x 576 (CIF4), 360 x 288 (CIF1) is also allowed to use. Increasing the resolution above CIF4 does not improve the operating quality of the recognition algorithm. • Frames per second: 6 or more. • Color: color or greyscale. • No camera jitter is allowed.
Illumination	• Best recognition results are achieved under moderate illumination. If the scene is under- or over-illuminated, the recognition accuracy may drop down. • Sharp changes in illumination may lead to improper operation of analytics.

Scene and camera angle	• Vertically downward position of the camera is the best for the purpose. The closer to vertical, the more accurate the estimation. • Camera FOV dimensions: minimum 3x3 m (6x6 humans), optimal 4x4 m (8x8 humans), maximum 8x8 m (16x16 humans). • The background should be primarily static and should not undergo sudden changes. • Reflective surfaces and harsh shadows from moving objects can affect the quality of analytics. • Analytics may not work correctly if there are periodic movements of the background objects in the camera FOV (leafage, TV screens, etc.).
Images of objects	• Image quality: the image should be clear, with no visible compression artifacts. • Dimensions of a human in scene: bounding rectangle has to occupy from 0,25% to 10% of the frame area.

15.4.20.3 Camera requirements for Visitors counter operation

The following table contains the requirements for cameras to enable the effective operation of the Visitors counter:

Camera:	• resolution: 720 x 576 (CIF4) or 360 x 288 (CIF1) pixel resolution. Using pixel resolutions higher than CIF4 do not lead to higher recognition accuracy; • frames per second: 25; • color: color camera is obligatory; • no camera jitter is allowed.
Illumination:	• best recognition results are achieved under moderate illumination. If the scene is under- or over-illuminated, the recognition accuracy may drop down; • sharp changes in illumination may lead to improper operation of analytics.
Scene and viewing angle:	• vertically downward position is the best for the purpose. The closer to vertical, the more accurate counting; • camera FOV dimensions: min. 2 x 2m, optimal 4 x 4m; • the background must be primarily static and not undergo sudden changes; • the counting area must not contain any moving objects except for humans; • reflective surfaces and harsh shadows from moving objects can affect the quality of analytics; • leafage, TV screens or any periodic object movement in the background may cause analytics glitches; • if possible, avoid obstruction of the humans by static objects such as pillars, trees, etc.
Images of objects within the scene:	• image quality: the image must be clear and sharp with no visible compression artifacts; • the allowable size of a person is described in the Requirements for the person size in the frame(see page 385).

Other requirements:	• the visitors must not move in a continuous flow; smaller groups of humans are counted correctly.

15.4.20.3.1 Requirements for the person size in the frame

The person size is the area of the rectangle circumscribed around the person, as a percentage of the frame area. To ensure the correct operation of the detection tool, the it is necessary to select the size of a person in the range from the minimum value, depending on the frame width, to 75% of the frame width.

> **Note**
>
> Frame width means not the original resolution of the video image, but the compressed size that depends on the **Frame size change** parameter (see Configuring the Visitors counter detection tool(see page 388)).

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

Frame width, px	Minimum size of a person in %
2560	2,4
2732	2,2
2800	2,2
3200	1,9
3840	1,6
4096	1,5
6400	1
8192	0,8

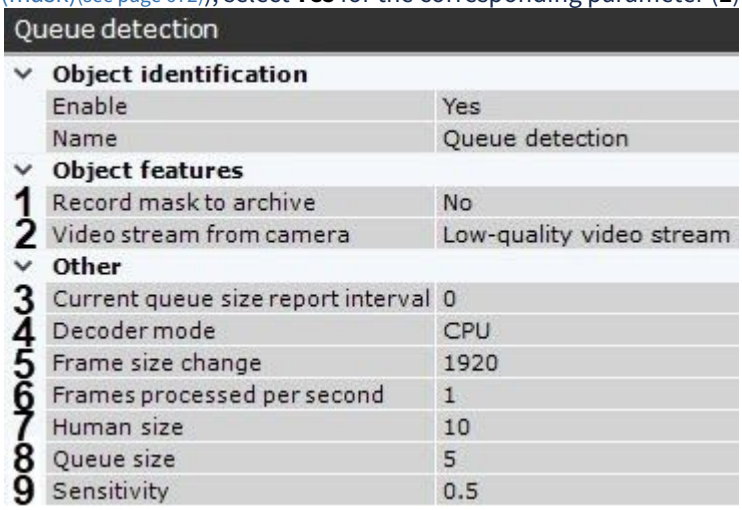
15.4.20.4 Configuring retail analytics detection tools

15.4.20.4.1 Configuring the Queue detection tool

Camera requirements for Queue detection(see page 383)

To configure the Queue detection tool, do the following:

1. To record mask (highlighting the queue on the video) to the archive (see Displaying information from a detection tool (mask)(see page 672)), select **Yes** for the corresponding parameter (**1**).



2. If the 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.
3. Set the event transmission interval in seconds for sending the data to the AxxonData report subsystem (see Queue length report[139]), if the queue length exceeds the set limit (**3**). If **0** value is selected, no events will be transmitted.
4. Select a processing resource for decoding video streams (**4**). 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.
5. Analyzed framed are scaled down to a specified resolution (**5**, 1920 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.

139 https://docs.axxonsoft.com/confluence/display/anet/Queue+length+report

> **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.

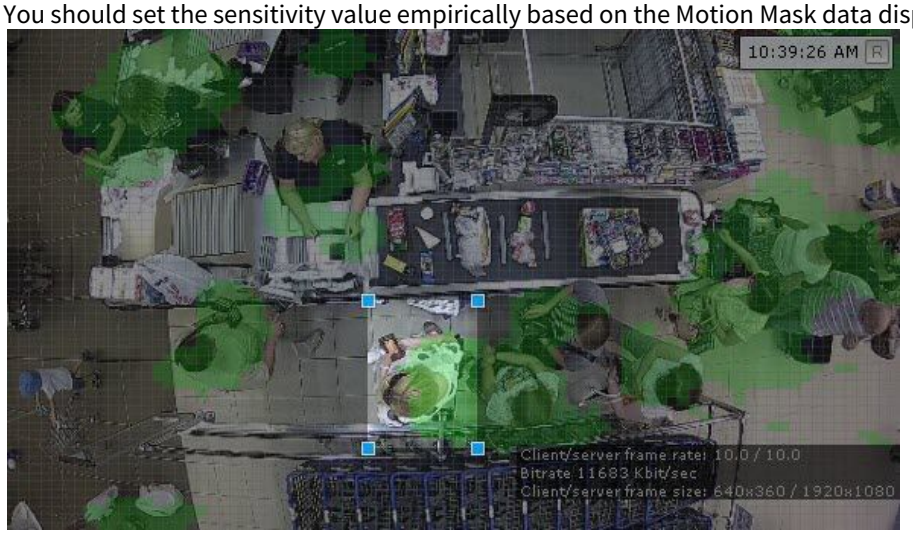
6. Set the frame rate value for the detection tool to process per second (**6**). This value should be in the range [0,016; 100]. The higher the value of this parameter, the higher the CPU load.
7. Click the

button and set the minimum size of a human (**7**). You can do so by dragging the anchor points of the rectangular area.

> **Note**
>
> It is recommended to set the minimum size of a human graphically. The number in the **Human size** field is a conventional value.

8. Specify the number of people in the queue above which the detection tool triggers (**8**). The value should be in the range [2; 20].
9. Specify the detection tool sensitivity in standard units from 0 to 1 (**9**). The higher the sensitivity, the smaller the disturbances will be attribute to the queue, i.e. the algorithm will react to more insignificant movement. If you specify the lowest sensitivity value, the detection tool will process only significant changes in the scene.

You should set the sensitivity value empirically based on the Motion Mask data displayed in the preview window.



10. In the preview window, you can set the detection areas with the help of the anchor points much like privacy masks in Scene Analytics detection tools (see Setting General Zones for Scene analytics detection tools(see page 262)).
11. Click the **Apply** button.

The Queue detection tool is now configured. When the detection tool is triggered, the following events are generated:

```
Camera. Detection "Queue detection" triggered, queue (min.: 10, max.: 10)
```

where min. and max. is estimated queue length.

15.4.20.4.2 Configuring the Visitors counter detection tool

Camera requirements for Visitors counter operation(see page 384)

Attention!

- The Visitors counter detection tool may have a margin of error and is suitable for counting the average number of visitors.
- We cannot guarantee the correct operation of the Visitors counter detection tool with fish-eye video cameras.

To configure the Visitors counter detection tool, do the following:

1. Enable the detection tool—select **Yes** for the corresponding parameter (**1**).

Visitors counter		
	Object identification	
1	Enable	Yes
2	Name	Visitors counter
	Object features	
3	Video stream from camera	High-quality video stream
	Visual Elements	
4	Visual Element	Detection area (polygon)
5	Visual Element	Visitors entrance/exit areas
	Visual Element	Visitors entrance/exit areas

2. Enter the detection tool name or leave the default name (**2**).
3. If the camera supports multistreaming, select the stream for which detection is needed. Select a low-quality video stream to reduce the Server load (**3**).

4. Click the

button and specify the size of a human (**4**). You can do this by dragging the anchor points of the rectangular area. You can also specify the size of a human manually by entering into the **Human size** field (**9**) the area of the rectangle around a human as a percentage of the frame area. Consider that to calculate the size, the size of the compressed frame is taken into account (**7**) and not the original size of the video stream. The value should be in the range [1; 75].

   > **Attention!**
   >
   > When specifying the size of a human, consider the Requirements for the person size in the frame(see page 385).

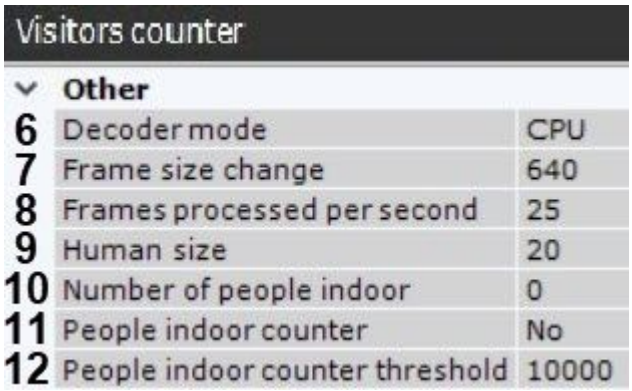
5. In the preview window, set the detection area (**5**). The detection area is divided into two sectors—area 1 and area 2. The transition from area 1 to area 2 is the visitor's passage in the "Exit" direction. The transition from area 2 to area 1 is the visitor's passage in the "Entrance" direction.
   If the **People indoor counter** parameter (**11**) is enabled:
   a. Transition from area 1 to area 2—minus one to the visitors counter.
   b. 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. To display/hide sectors in the preview window, click the button.

6. Select a processing resource for decoding video streams (**6**). When you select a GPU, a stand-alone graphics card takes priority (when decoding with NVIDIA NVDEC chips). If there's no appropriate GPU, the decoding will use the Intel Quick Sync Video technology. Otherwise, CPU resources will be used for decoding.
7. By default, during analysis the frame is compressed to the specified size (**7**, the default size is 640 pixels on the larger side). The value should be in the range [640; 10000]. The following algorithm is used:

a. If the original resolution on the larger side of the frame is greater than the one specified in the **Frame size change** field, then it is divided in half.
b. If the resulting resolution is less than the specified one, then the algorithm stops and this resolution is used.
c. If the resulting resolution is still greater than the specified one, then it is divided in half until it becomes less.

> **Note**
>
> For example, the original video image resolution is 2048*1536, the specified value is **1000**. In this case, the original resolution will be halved 2 times (512*384), because after the first division, the value on the larger side of the frame will be greater than the specified value (1024 > 1000). If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.



8. Set the number of frames for the detection tool to process per second (**8**). This value should be in the range [0.016; 100].
9. By default, the detection tool generates the *Camera. Visitor access in the direction of "Entrance"* and *Camera. Visitor access in the direction of "Exit"* events. If you also want to count visitors at the facility, and it is necessary to trigger an alarm when the threshold value is exceeded, do the following:
   a. Select **Yes** for the **People indoor counter** parameter (**11**).
   b. Enter the number of visitors in the area at the time of the detection tool configuration (**10**). The value should be in the range [0; 100000].
   c. Set the threshold value for the number of visitors, above which the event will be generated (**12**). The value should be in the range [0; 100000].
10. Click the **Apply** button.

Configuration of the Visitors counter detection tool is now complete.

15.4.21 Water Level Detection

15.4.21.1 Camera requirements for Water level detection

To establish accurate results, please ensure the following:

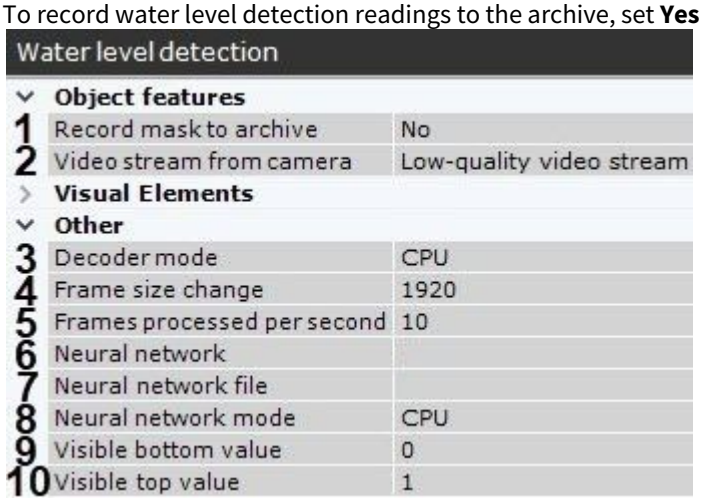
1. Only color cameras are used.
2. Video resolution is no less than 640x360.
3. No glares or shadows are cast over the measurement scale.

15.4.21.2 Configuring Water level detection

Camera requirements for Water level detection(see page 390)

To configure Water level detection, do the following:

1. To record water level detection readings to the archive, set **Yes** for the **Record mask to archive** parameter (**1**).



2. If the camera supports multistreaming, select the stream for which detection is needed. Select a low-quality video stream to reduce the Server load (**2**).
3. Select a processing resource for decoding video streams (**3**). 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 or the CPU.
4. Analyzed framed are scaled down to a specified resolution (**4**, 1920 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). If detection is performed on a higher resolution stream and detection errors occur, it is recommended to reduce the compression.

5. Set the frame rate value for the detection tool to process per second (**5**). The value should be in the range [0.016; 100].
6. If the water in the frame is transparent and the detection tool cannot correctly identify its level, use **Neural network** (**6**):
    a. If **No** 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.
    b. If **Yes** is selected:
        i. 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.
        ii. 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 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.

7. Select the neural network file (**7**). 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, place the corresponding file in the /opt/AxxonSoft/DetectorPack/NeuroSDK directory.

8. Select the processor for the neural network—CPU, one of GPUs, or one of Intel processors (**8**) (see Hardware requirements for neural analytics operation(see page 52), General Information on Configuring Detection(see page 234)).

   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(see page 240)).
   - 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.

9. On the measurement scale (**9**, **10**), set the top and bottom visible values in normal conditions. The value should be in the range [0; 19].
10. Move the anchor points in the preview window:
    a. Set the measurement scale in the frame.

   Attention!

   Top and bottom values of the measurement scale should match the actual settings (see step 9).

   Note

   Water level sensor is shown in the lower left corner. If the sensor is blue, the water level is below high and critical marks. If the sensor is yellow, the water level is at high mark, but below critical mark. A red sensor means that water level is above critical mark.

    b. Draw a line to set the top limit for water level upon reaching which the detection tool triggers an alarm.
    c. Draw a line to set the top limit for water level upon reaching which the detection tool highlights the sensor icon in the video surveillance window with yellow color.
11. Click the **Apply** button.

Configuring Water level detection tool is complete.

When you have created a detection tool, you can see a sensor on the layout in the video surveillance window.

If the sensor icon is green , the water level is lower than both critical and high marks. If the icon is yellow , 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 video surveillance window (see Configuring display of water level detection(see page 487)).

15.4.22 Embedded Detection Tools

By the date the documentation in created, the *Axxon One* software package includes integrated analytics for multiple video cameras (see Drivers Pack release notes[140]).

If *Axxon One* supports built-in analytics for a device, then detectors can be created (see Creating detection tools(see page 243)).

> **Note**
>
> Some devices may have issues with interdependent embedded analytics. If there is already a relevant detection tool in *Axxon One*, you can add another one, but it will not work.

15.4.22.1 Embedded Temperature Detection Tool

Axxon One supports selected models of thermal cameras with an embedded temperature detection tool (the Drivers Pack documentation[141], **body temperature detection**). This detection tool recognizes human faces on video, and performs temperature measurement on them.

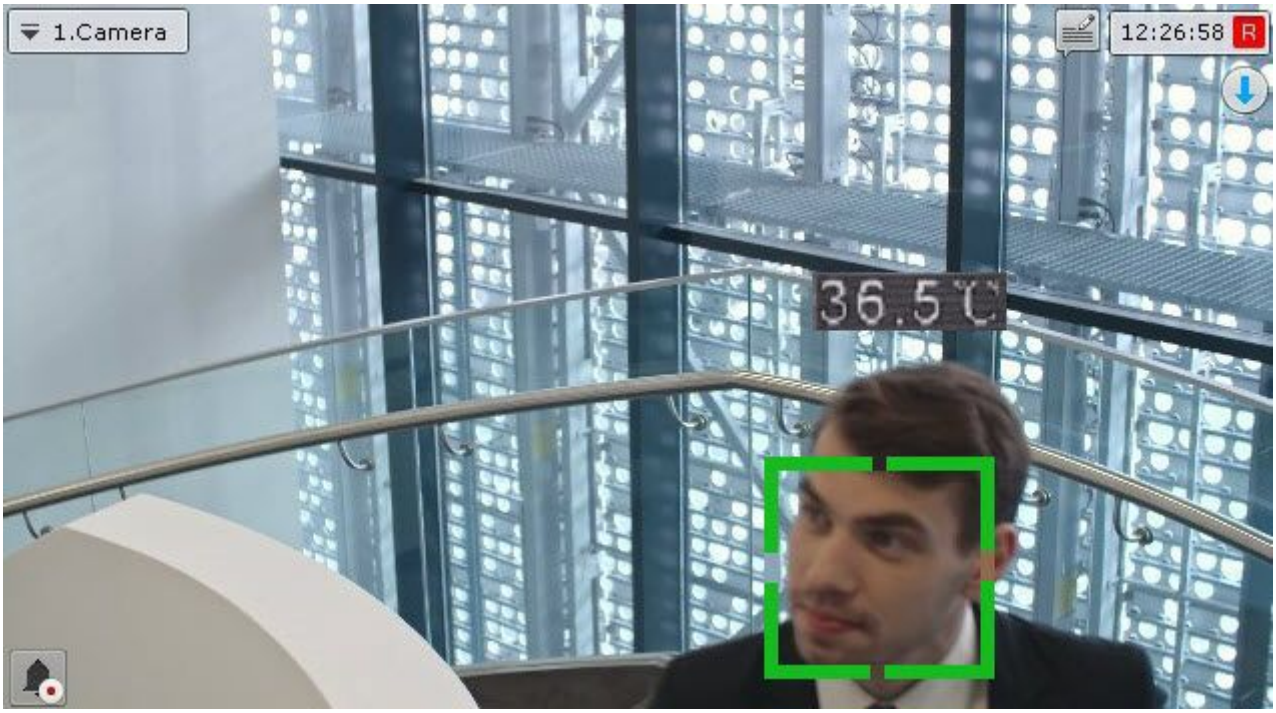
Normally, you should set up a detection tool as follows:

1. Create a detection tool (see Creating detection tools(see page 243)).
2. Using the camera manufacturer's documentation, set up the detection tool in the *Axxon One* VMS.

   > **Attention!**
   >
   > As a rule, a camera requires specifying the temperature threshold, upon reaching which the detection tool would trigger an alarm.

3. If required, set up macros to perform pre-defined actions upon triggering the detector (see Configuring macros and counters(see page 400)).

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.

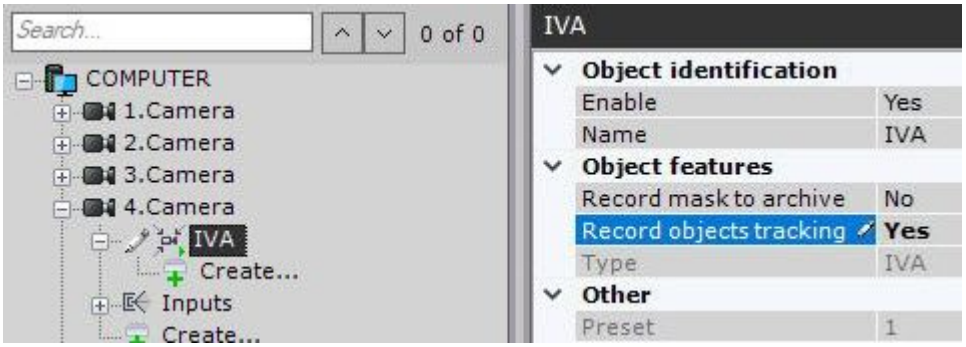


140 https://docs.axxonsoft.com/confluence/display/DDP/Release+Notes+Drivers+Pack+3.72
141 https://docs.axxonsoft.com/confluence/display/DDP/Documentation+Drivers+Pack

15.4.22.2 Obtaining metadata

Axxon One is also able to obtain metadata directly from certain video cameras. For example, metadata can be received from a Bosch IVA system.

To receive metadata from a Bosch IVA, you need to create an **IVA** object and select **Yes** in the **Record objects tracking** list.



15.4.22.3 ANPR

The VMS can process ANPR data from some cameras' on-board analytics.

> **Note**
>
> Please contact technical support https://support.axxonsoft.com/ for a list of cameras with this feature.

Generally, when configuring the embedded analytics you must follow official documentation for the corresponding video camera or parameter description in the *Axxon One* interface.

Motion Mask

If the camera supports Motion Mask, then when you configure VMD, it will be displayed in the preview window.

If there is motion, but it does not exceed the threshold value (because of the detection sensitivity), the mask cells are colored green. If motion triggers VMD, the cells turn red.

15.4.22.4 AxxonSoft tracking in Axis devices

You can use analytics from AxxonSoft (Configuring Scene Analytics Detection Tools(see page 260)) on Axis devices.

Note

This option is available for all Axis devices on the following hardware platforms:

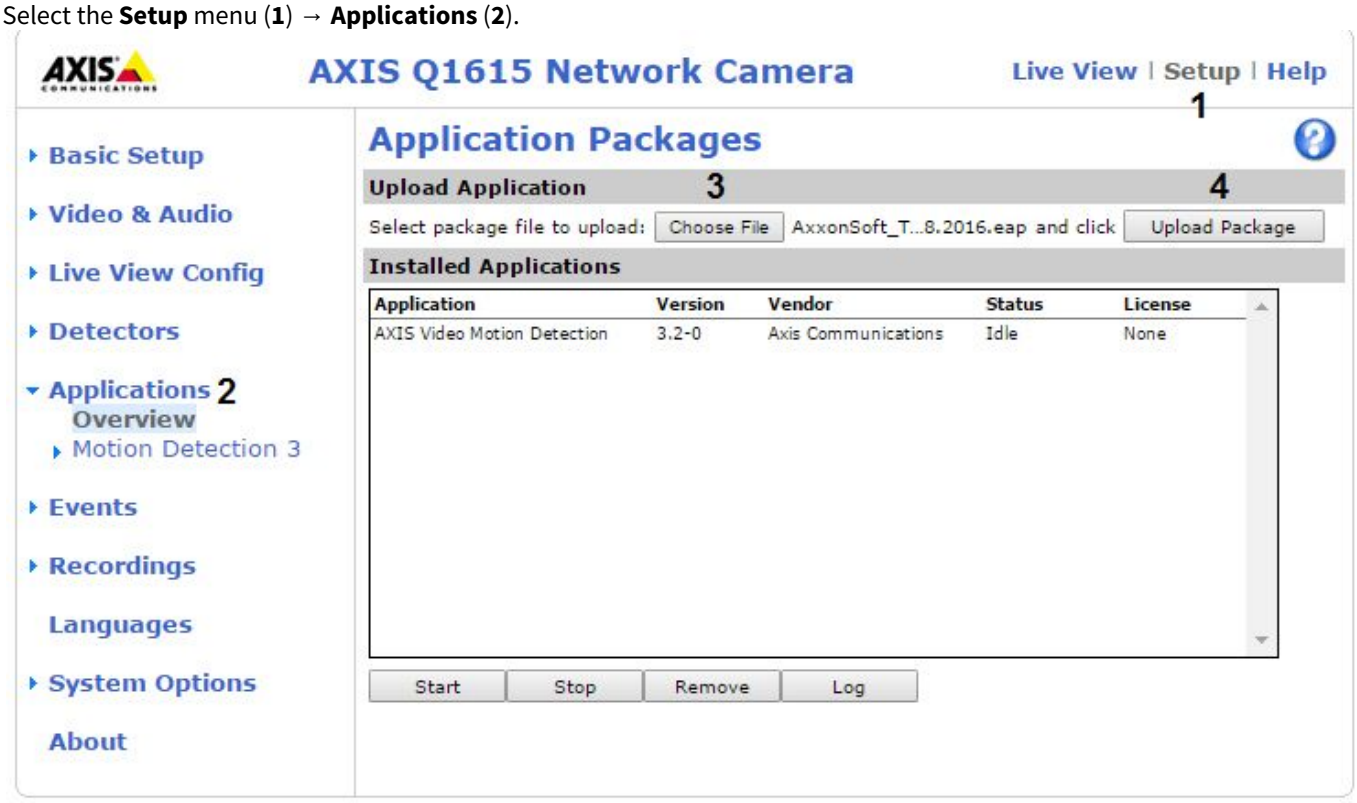
- MIPS (ARTPEC-4 and ARTPEC-5 CPUs),
- ARMv7 (ARTPEC-6 and ARTPEC-7 CPUs).

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**).



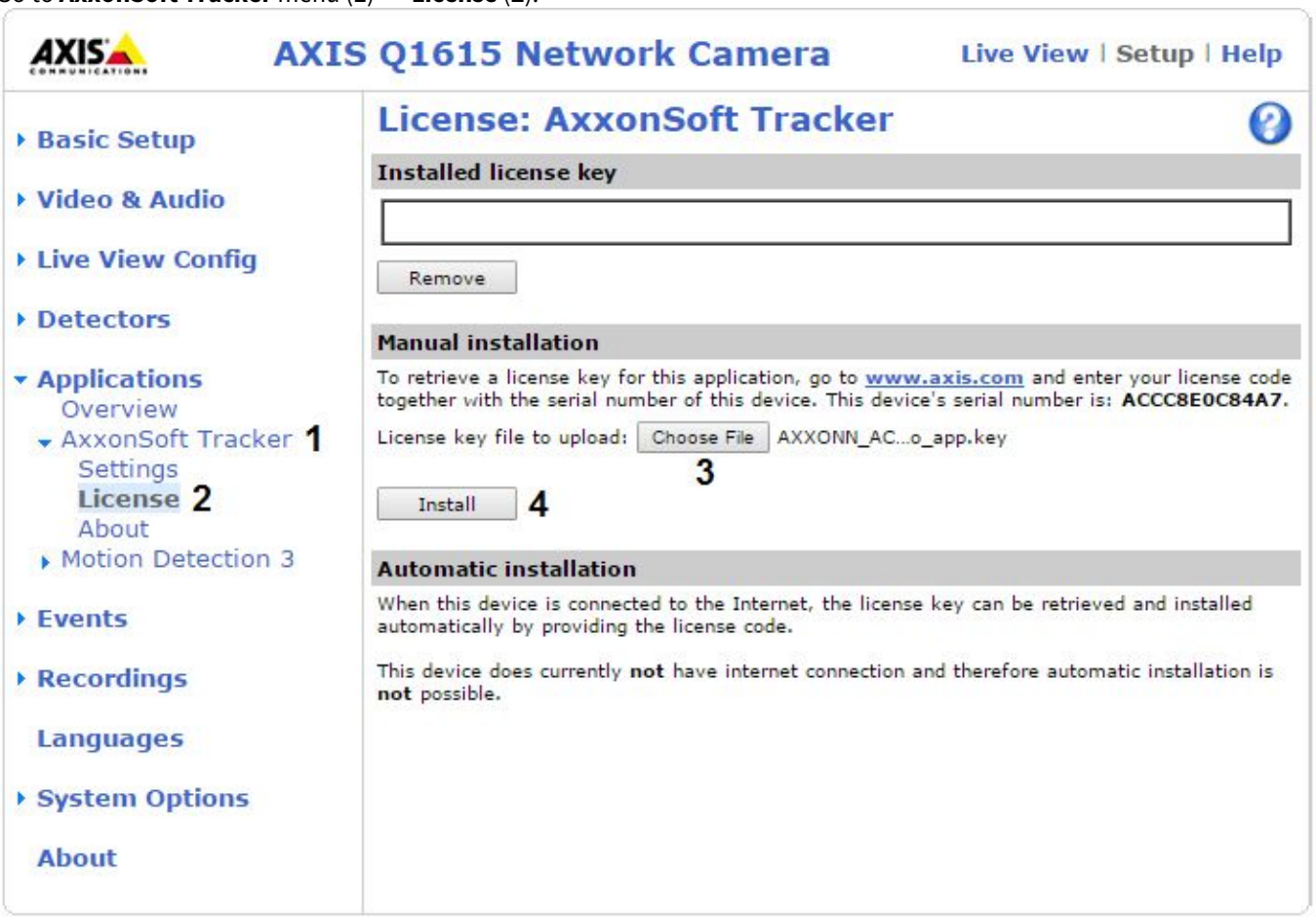
3. Select the ACAP[142] application (**3**) and click **Upload Package** (**4**).

Important!

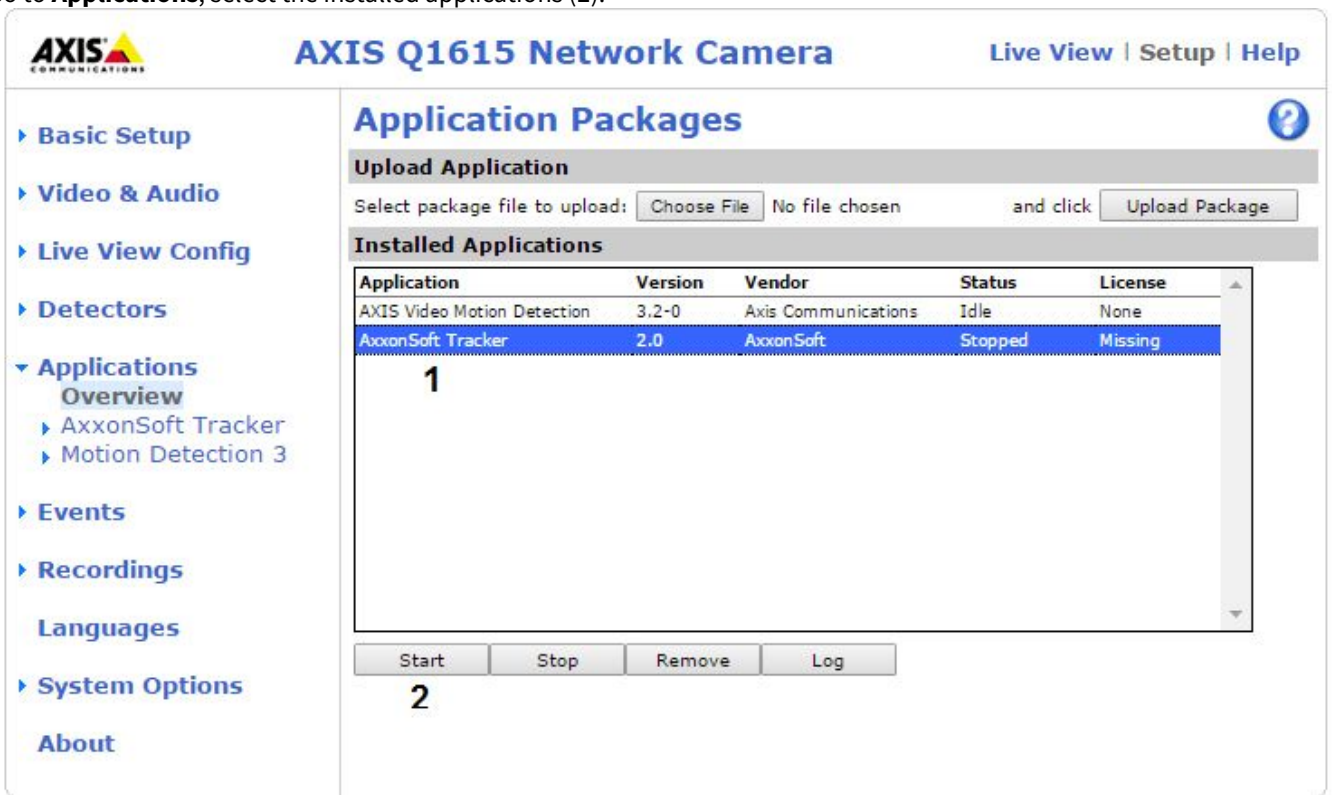
For application, contact AxxonSoft help-desk[143]. You will be given a license code that is to be registered along with camera's MAC address on Axis website[144] in order to get the license file.

142 http://www.axis.com/us/en/support/developer-support/axis-camera-application-platform
143 https://support.axxonsoft.com
144 https://auth.axis.com/authn/authentication/html-experimental

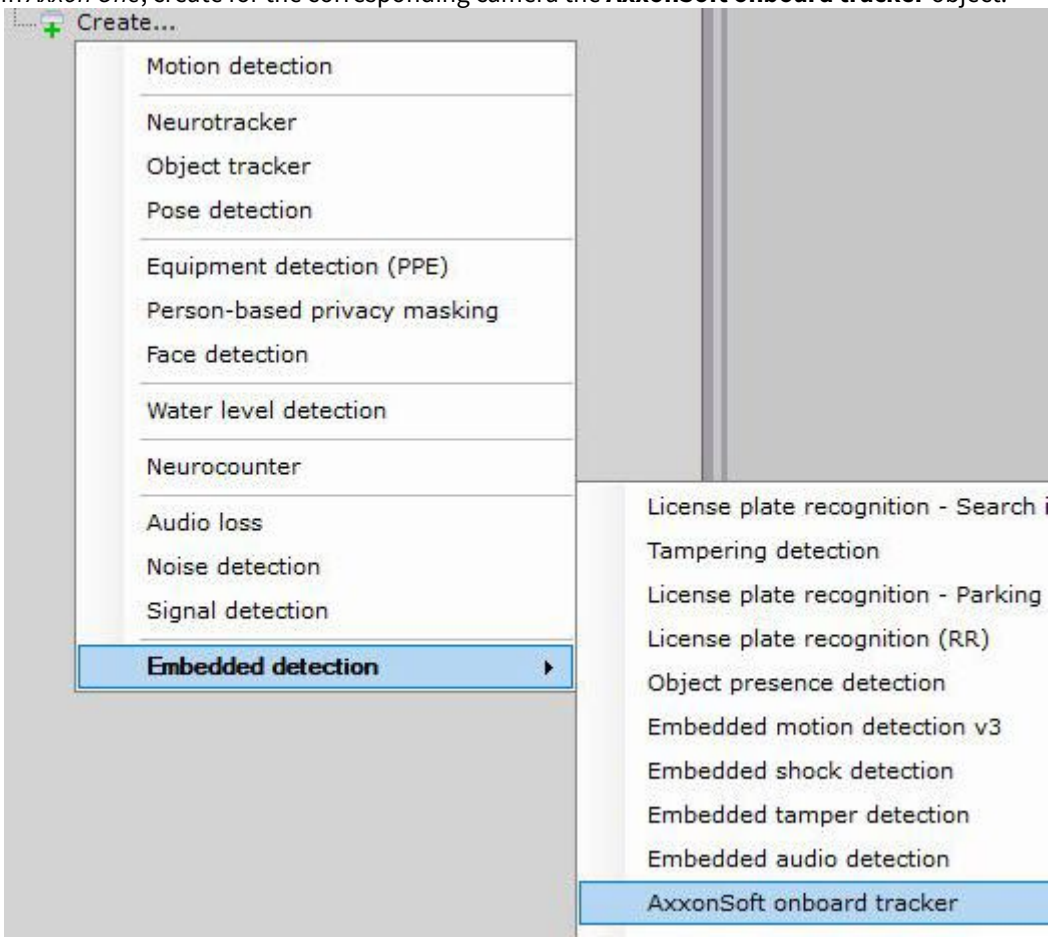
4. Go to **AxxonSoft Tracker** menu (**1**) → **License** (**2**).



5. Select the license file (**3**).
6. Click **Install** (**4**).
7. Go to **Applications**, select the installed applications (**1**).



8. Click **Start** (**2**).
9. In *Axxon One*, create for the corresponding camera the **AxxonSoft onboard tracker** object.



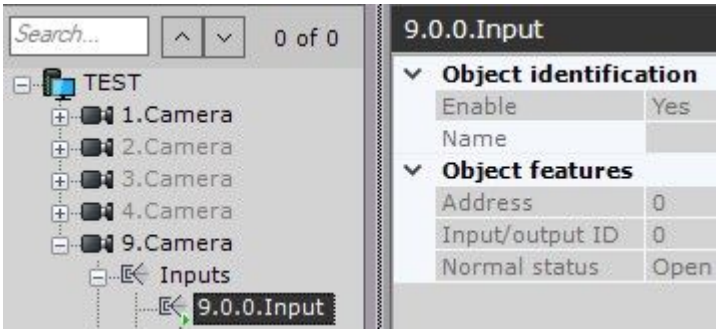
10. Configure the tracker and create the required detection tools.

> **Note**
>
> You can configure the **AxxonSoft onboard tracker** object similar to the General information on Scene Analytics detection tools(see page 254).
> You cannot configure perspective for solution based on Axis devices.

15.4.23 Configuring Inputs

After becoming enabled on the **Devices** tab, the **Input** object appears on the **Detection Tools** tab (see the section The Input Object(see page 166)**).**

Check the functioning of the Input in the **Devices** tab (see the section The Input Object(see page 166)). The **detection properties** field in the **Detection 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(see page 398)).
2. Set the rules to be automatically executed when the detection tool is triggered (see the section titled Automatic Rules(see page 399)).

15.4.24 Checking the Triggering of a Detection Tool

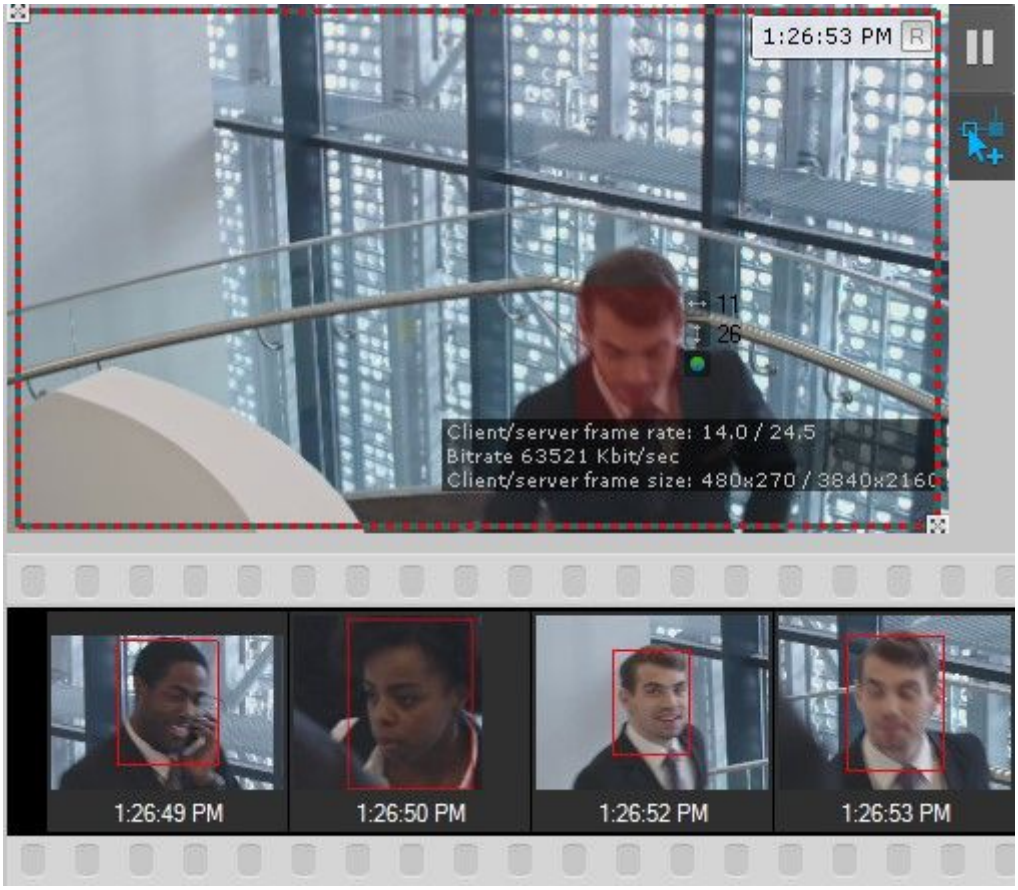
You can check the triggering of detection tools in the **Detection Tools tab**.

To use this option you must perform the following steps:

1. In the Detection Tools list, highlight the detection tool object whose triggering you need to check.

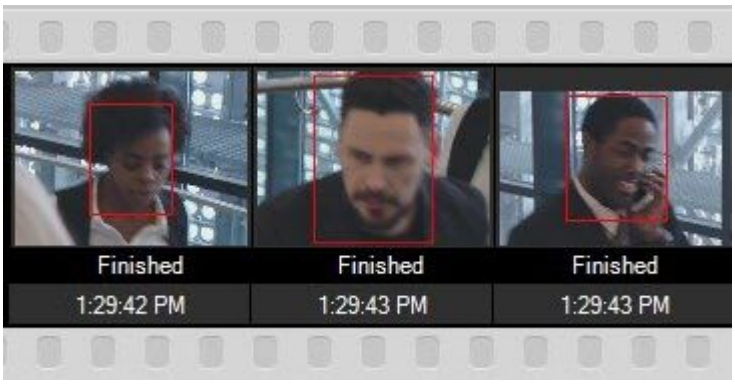
   > **Attention!**
   >
   > The Detection Tool object should be enabled and configured.

2. Produce an event whose occurrence should trigger the detection tool: motion in the frame, turning the video camera, providing sound to an audio device, etc.
3. If the detection tool is configured correctly, video image frames from the video camera corresponding to the detection tool will be displayed on the trigger ribbon with the time they were received indicated.



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, you get the **Finished** message**.**

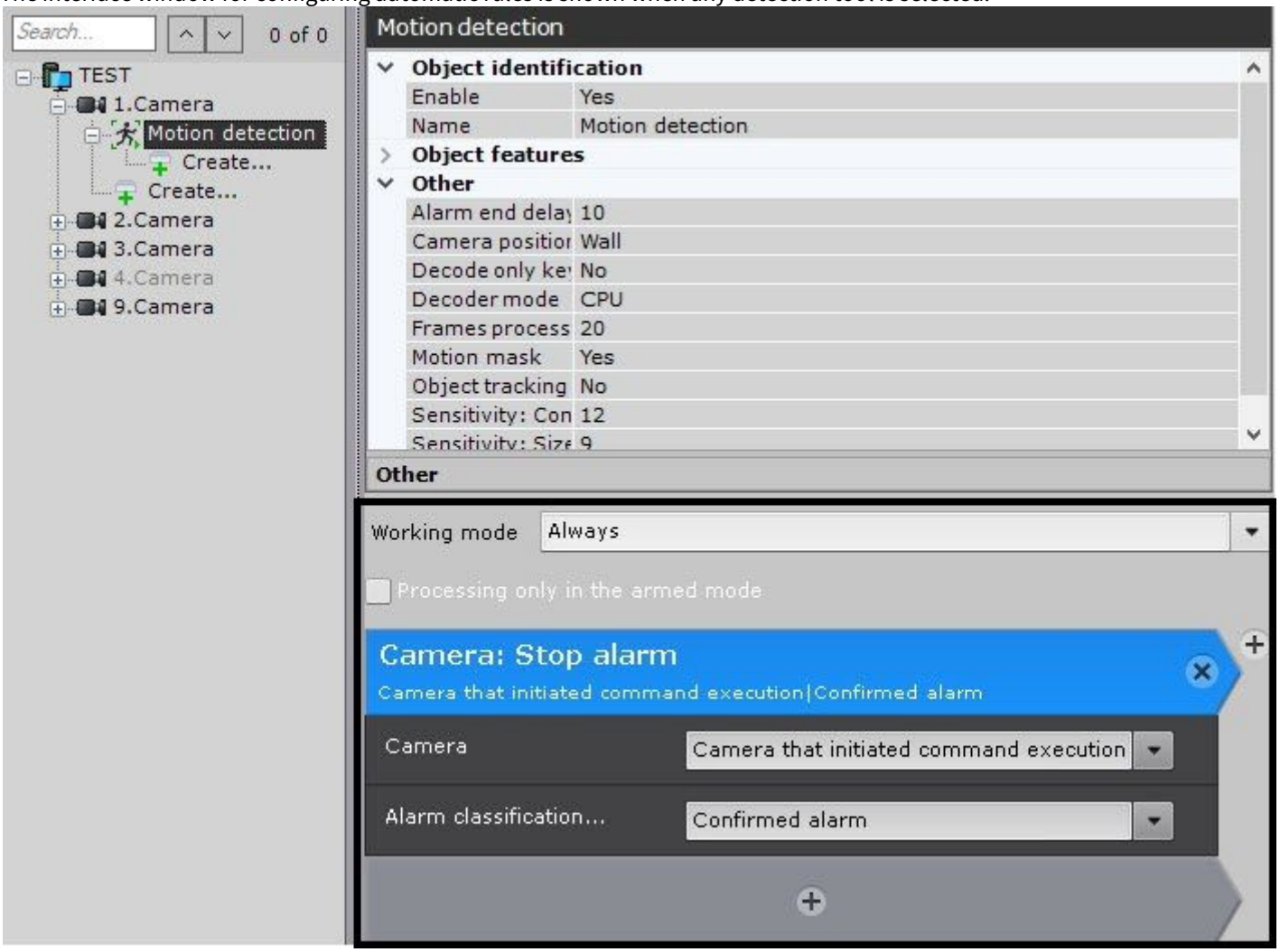


Checking the triggering of a detection tool is now complete.

15.4.25 Automatic Rules

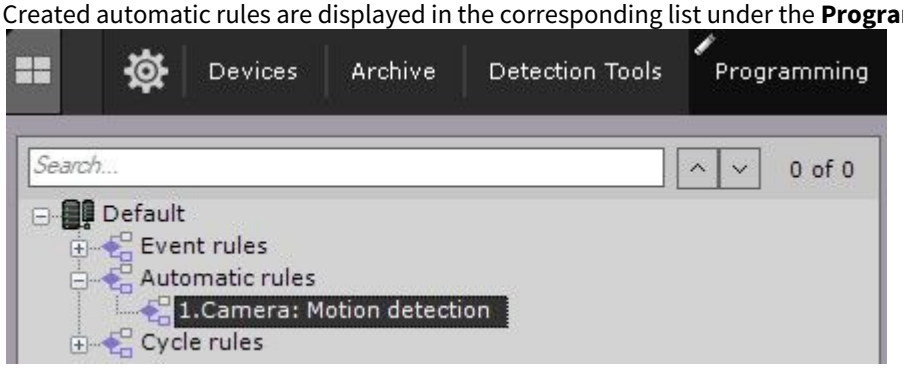
Automatic rules are basic macros: particular actions that are performed when a detection tool is triggered (see Configuring macros and counters(see page 400)). One or multiple automatic rules can be set for each detection tool.

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 and counters(see page 400)).

Created automatic rules are displayed in the corresponding list under the **Programming** tab.



Note

When you create the Record to archive(see page 418) automatic rule, the recording stops when VMD (see Configuring Scene Analytics Detection Tools(see page 260)) triggering stops.

15.5 Configuring macros and counters

15.5.1 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.

15.5.1.1 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(see page 399) (**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(see page 403)). 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.

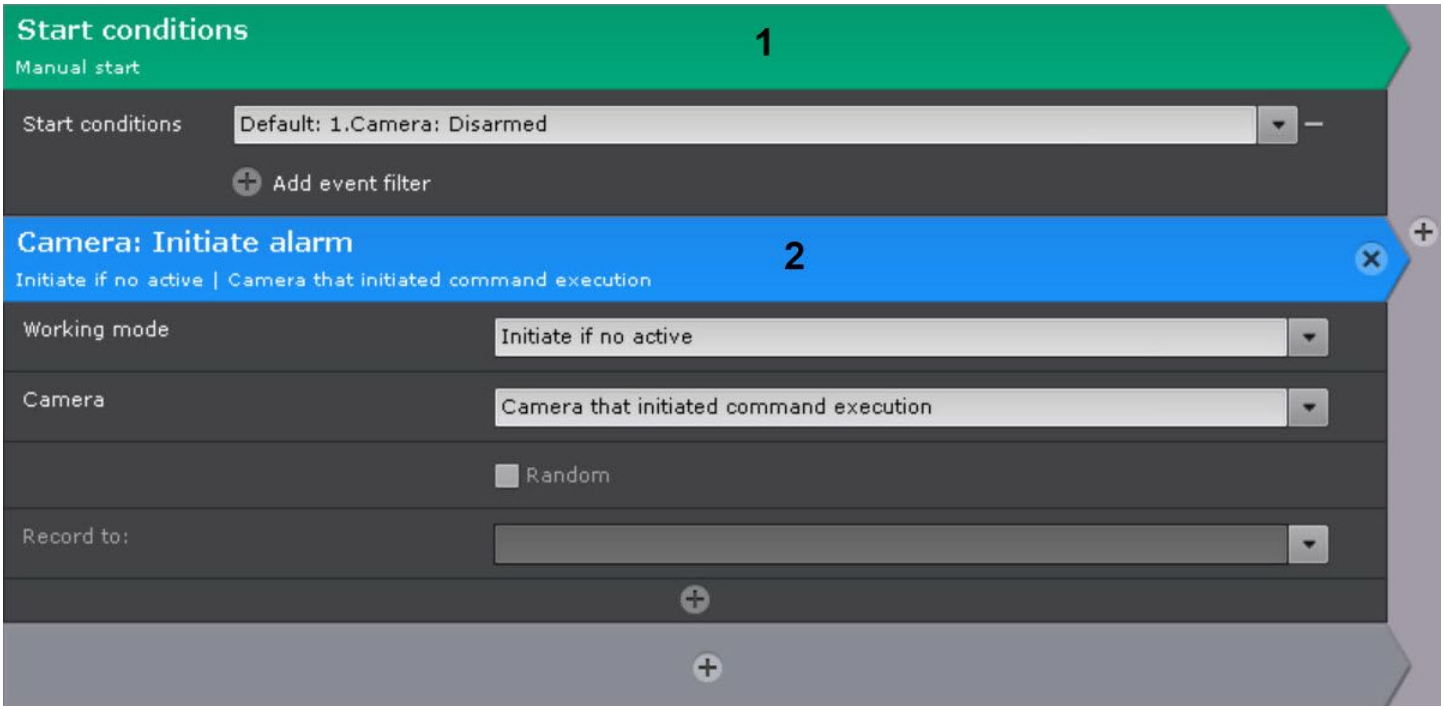
Unless the macro has standby commands (see Wait for event(see page 413), Wait for timeout(see page 414), Wait till previous action finishes(see page 415)), all actions are performed simultaneously.

Macros control(see page 817)

15.5.1.2 Configuring macros

You can create and configure macros on the **Programming** tab (see Create Macros(see page 403)).

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 filters for event-driven macros(see page 407)).
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(see page 413)). 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(see page 448).

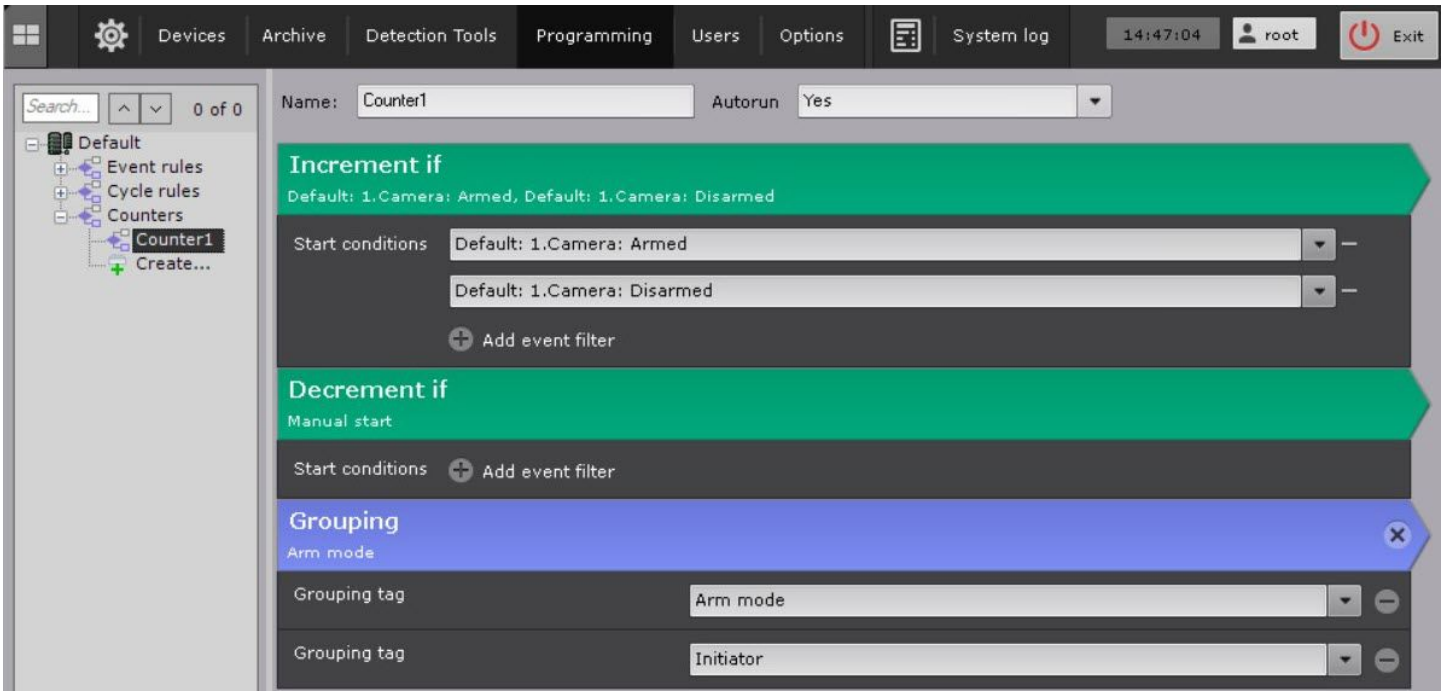
You can find examples of macros on these pages: Configuring macros when working with vehicles lists(see page 338), Examples of macros used for working with face lists(see page 302).

15.5.2 General information about the counters

A counter is a tool that allows you to count any values based on events. You can create and edit counters in the **Programming** tab.

Attention!

The counters work only within a single Axxon-domain. The objects belonging to another Axxon-domain cannot be used in the Increase conditions and Decrease conditions.



When creating a counter, select one or more events that increase the value of the counter, and one or more events that decrease the value (see Creating and configuring counters(see page 405)).

By default, the counter value is 0, each selected event increases or decreases it by 1.

Attention!

The counter value is reset to 0 when:

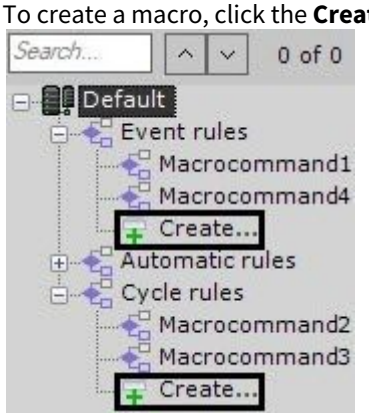
- Server restarts;
- Counter settings change.

In practical terms, counters can be used, for example, to count visitors at a site or facility. In this case, counting is based on faces captured by cameras with facial recognition installed at the entrance and exits.

Counters can be added to the map (see Adding counters(see page 513)), and managed both from the map (see Controlling devices from the map(see page 803)) and using a macro (see Managing the counter(see page 447)).

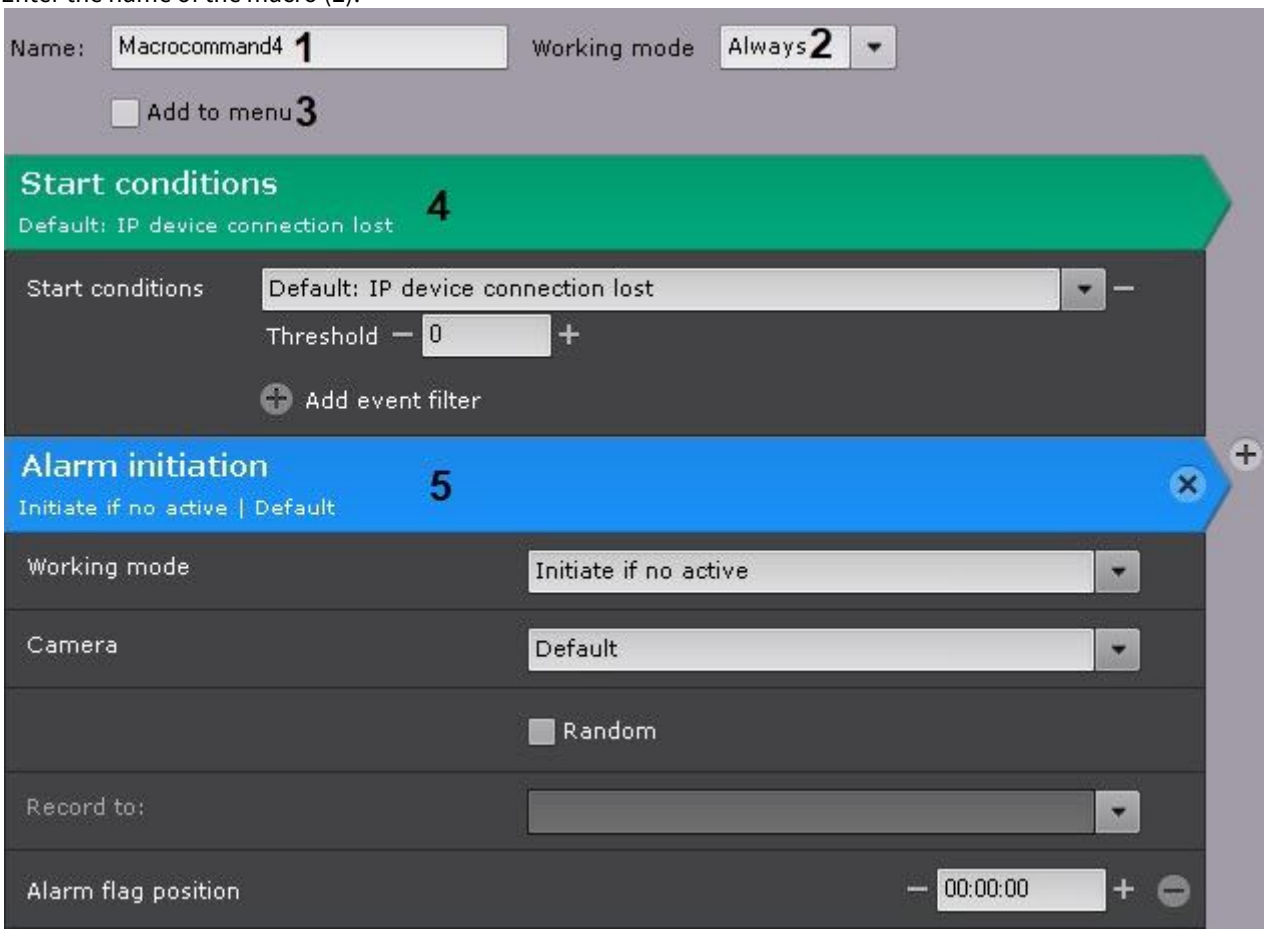
15.5.3 Create Macros

To create a macro, click the **Create** button in the required list.



Then do as follows:

1. Enter the name of the macro (**1**).

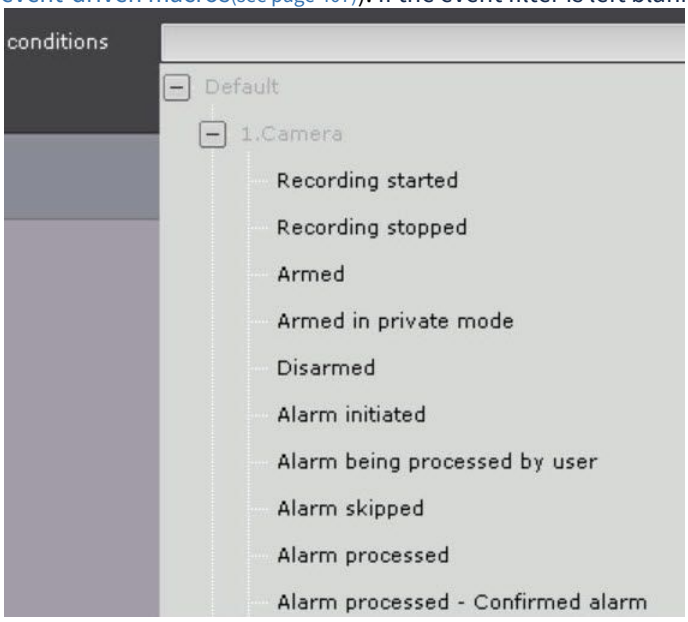


2. Select the macro working mode (**2**):

Mode	Event-driven	Cyclic
Never	Manual execution only (see Working with Dialog Board(see page 782), Macros control(see page 817))	Disabled, manual execution is possible (see Macros control(see page 817))
Always	Always on	Always on
Time schedule	Runs within the selected time schedule (see Creating schedules(see page 541)). 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(see page 817)), set the corresponding checkbox (**3**).
4. To configure event-driven macros, click the button and select one or more trigger events (**4**, see Configuring filters for event-driven macros(see page 407)). If the event filter is left blank, the macro can be executed only manually.



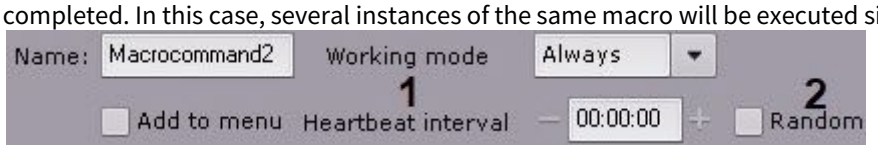
> **Note**
>
> To delete an event from the filter, click the button.

5. Add one or more actions to the macro (**5**, see Settings specific to actions(see page 413)). 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(see page 203)).

> **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.



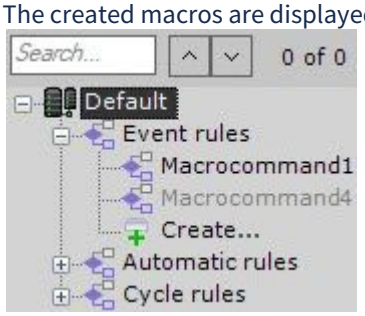
   b. Set the **Random** checkbox (**2**), if you need to launch the macro at a random moment set by the **Heartbeat interval** parameter. For example, if the interval is set to 8 hours, then once every 8 hours at a random moment, the macro will be launched.

> **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(see page 452)).

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.

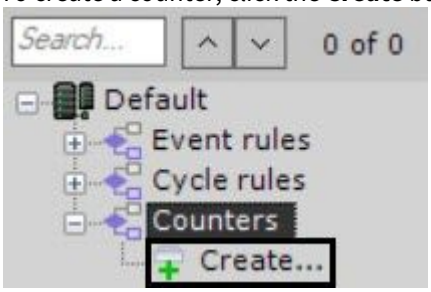
A new macro with the similar parameter will be created.

> **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.

15.5.4 Creating and configuring counters

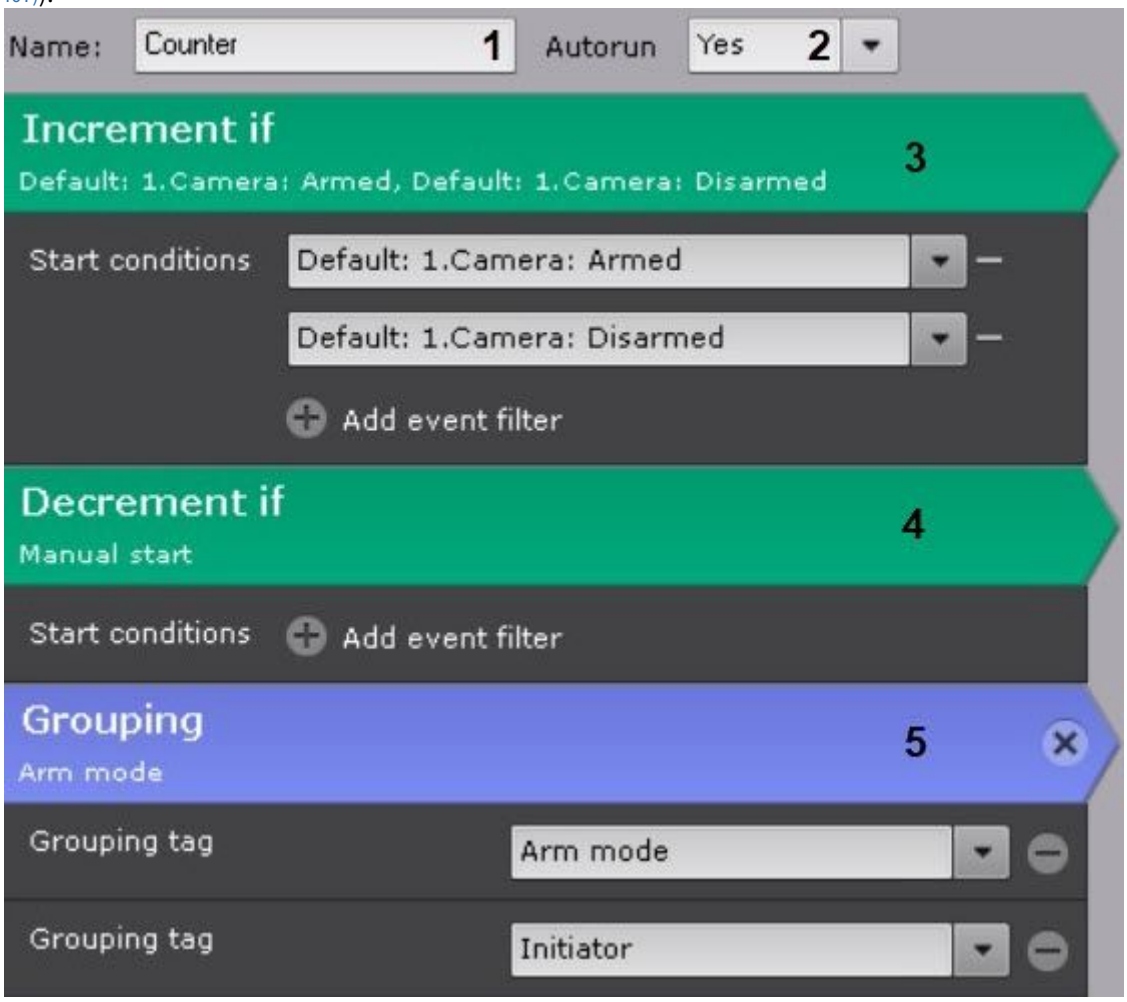
To create a counter, click the **Create** button in the Counters list.



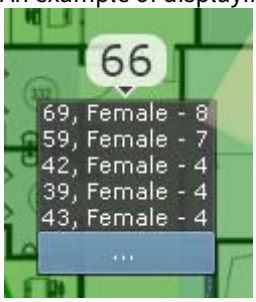
Then do as follows:

1. Specify the name of the counter (**1**).
2. Select the autorun mode (**2**):
    a. **Yes** — the counter starts working from the moment the server starts.
    b. **No** — the counter does not start working when the server starts, it it necessary to start it manually.

3. Select one or more events that will increase the counter value (**3**, see Configuring filters for event-driven macros(see page 407)).



4. Select one or more events that will decrease the counter value (**4**, see Configuring filters for event-driven macros(see page 407)).
5. Select one or several properties by which the counting results will be grouped (**5**). Grouping is available for camera arming and disarming events, as well as for face detection and license plate recognition events.

> **Note**
>
> If you select several properties, then the resulting groups will be formed by the consolidation of these properties. An example of displaying the counting results with the **Gender** and **Age** properties selected:
>
> 
>
>
> where **69** in the first line is the age, **Female** is the gender, and **8** is the number of women at the age of 69. The same goes for the rest of the lines.
> The order in which the properties are set does not affect the result.

6. Click **Apply**.

You can copy counters. Please follow the steps below:

1. Select the counter to copy.
2. Click **Create**.

This creates a new identical counter.

> **Note**
>
> To create an empty counter, select the **Counter** group and click **Create**.

To remove a counter, select it in the list and click **Remove**.

15.5.5 Configuring filters for event-driven macros

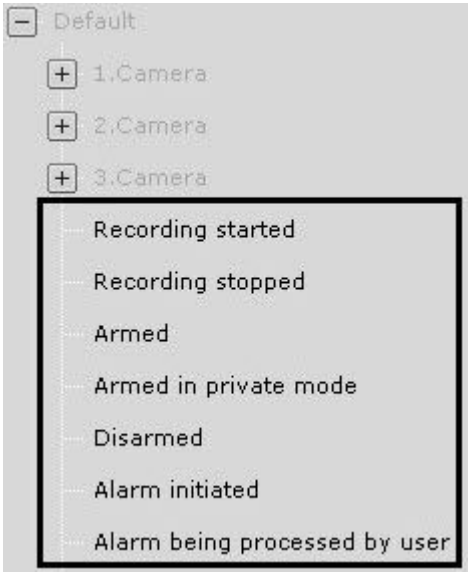
When creating event macros, you can select one or more events which will trigger the macro.

In addition, the macros can be triggered when specified statistical conditions are met (see Triggering macros by statistical data(see page 412)).

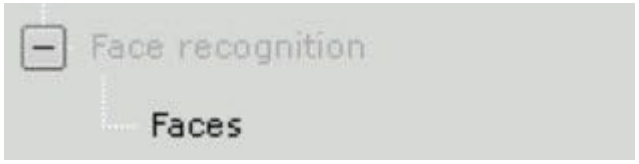
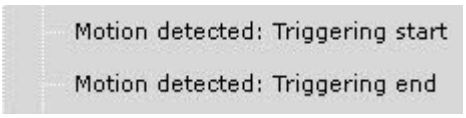
If several conditions are set, the macro will be triggered when any of these conditions are met.

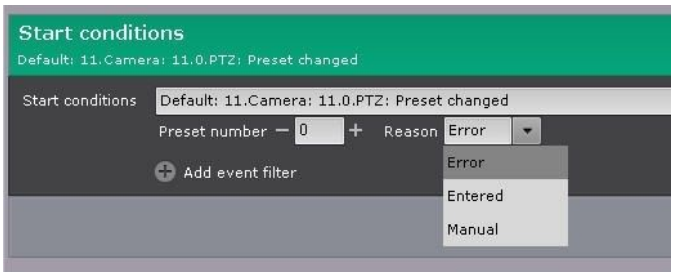
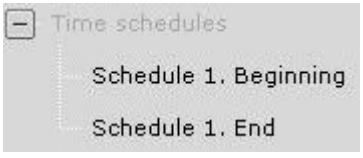
You can also filter events:

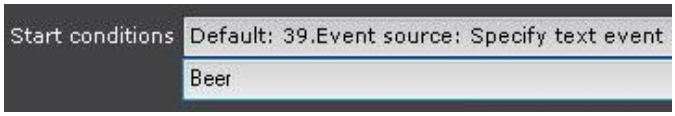
The following events are available for selection:

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	

<table>
<tr><th>Object</th><th>Event</th><th>Image</th></tr>
<tr><td rowspan="5"></td><td>Motion: Triggering start</td><td rowspan="2"></td></tr>
<tr><td>Motion: Triggering end</td></tr>
<tr><td>Signal lost</td><td rowspan="2">

You can set a threshold for these type of events: the time in seconds (0 to 100) 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</td></tr>
<tr><td>Signal restored</td></tr>
<tr><td>Face recognition
It is necessary to select the list from which the macro will be triggered when recognizing a face</td><td> 
</td></tr>
<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 rowspan="3">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.</td><td rowspan="3"> 
</td></tr>
<tr><td>Triggering end</td></tr>
<tr><td>Triggering (for detection tools, which do not have the start and end of the triggering, see Checking the Triggering of a Detection Tool(see page 398))</td></tr>
</table>

Object	Event	Image
	Specified Triggering (for face detection only, see Specific parameters for triggering a face recognition macro(see page 411))	
	Preset switch	 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(see page 678)) with the selected number while controlling the camera (see Controlling a PTZ Camera(see page 675)). 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(see page 681))
Neurocounter	Triggering	
Archive	Archive partition error Archive partition restored	
Time schedules	Beginning End	

Object	Event	Image
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}	

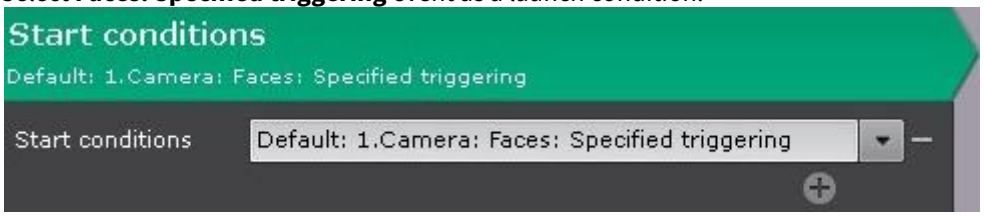
15.5.5.1 Specific parameters for triggering a face recognition macro

You can set a number of specific parameters which affect triggering a face recognition macro:

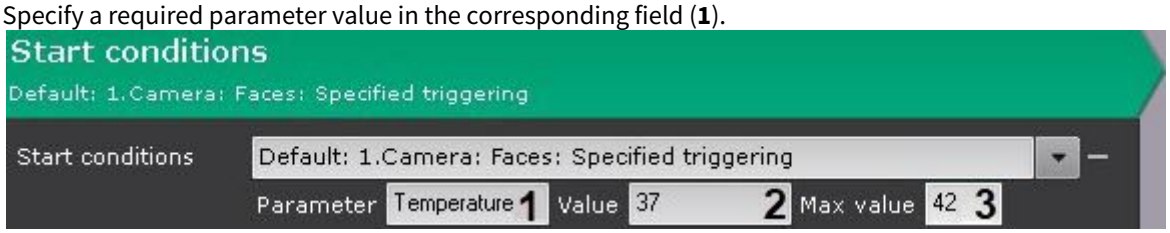
1. **Age** of the individual (requires activation of the **Gender and Age** parameter, see Configuring Face detection(see page 280)).
2. **Gender** of the individual (requires activation of the **Gender and Age** parameter, see Configuring Face detection(see page 280)). Value: **1** = female, **2** = 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(see page 293)).

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(see page 413)).

6. Click the **Apply** button.

15.5.5.2 Triggering macros by statistical data

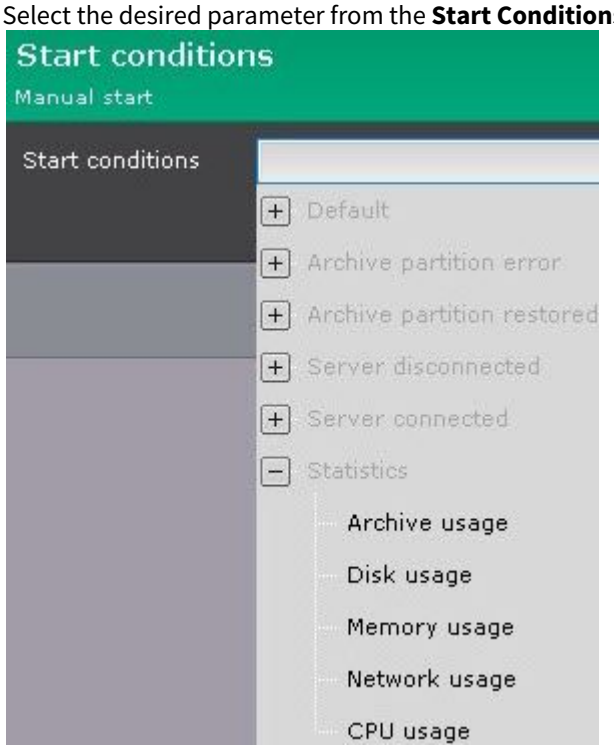
Event-triggered macros can be launched not only by events of particular type (see Configuring Filters for Event-driven Macros(see page 407)) but also by statistical parameters.

A macro can be initiated by the following parameters reaching pre-defined criteria:

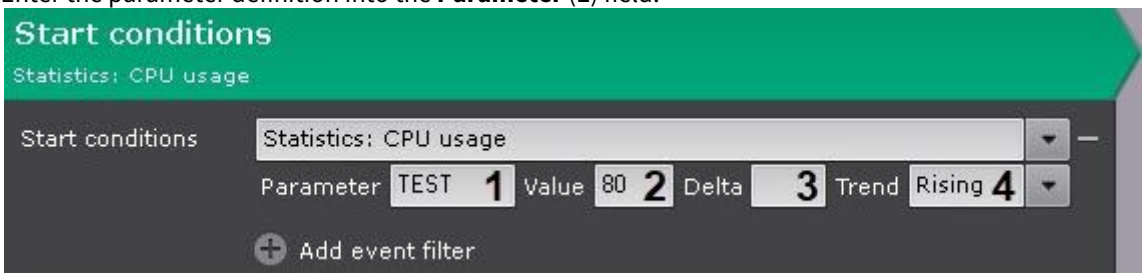
1. The percentage of used space in Archive.
2. The percentage of used space on a volume.
3. The percentage of used RAM on a Server.
4. The percentage of used network bandwidth on a Server.
5. The percentage of CPU load on a Server.

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.

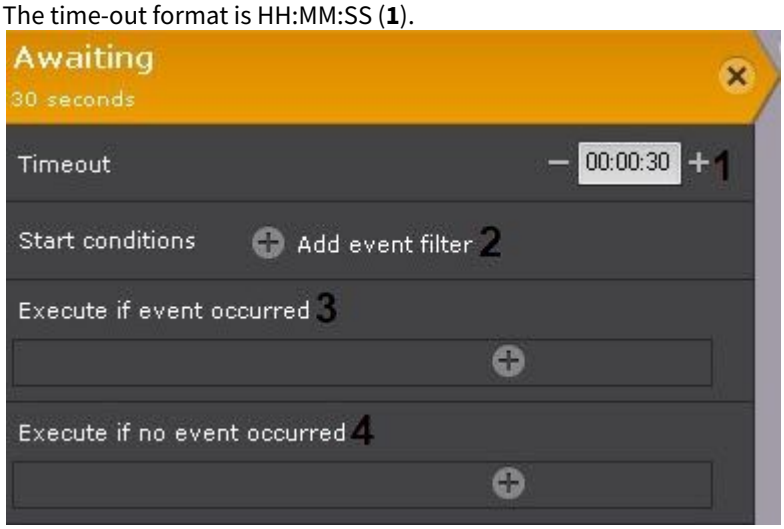
15.5.6 Settings specific to actions

15.5.6.1 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(see page 407)).

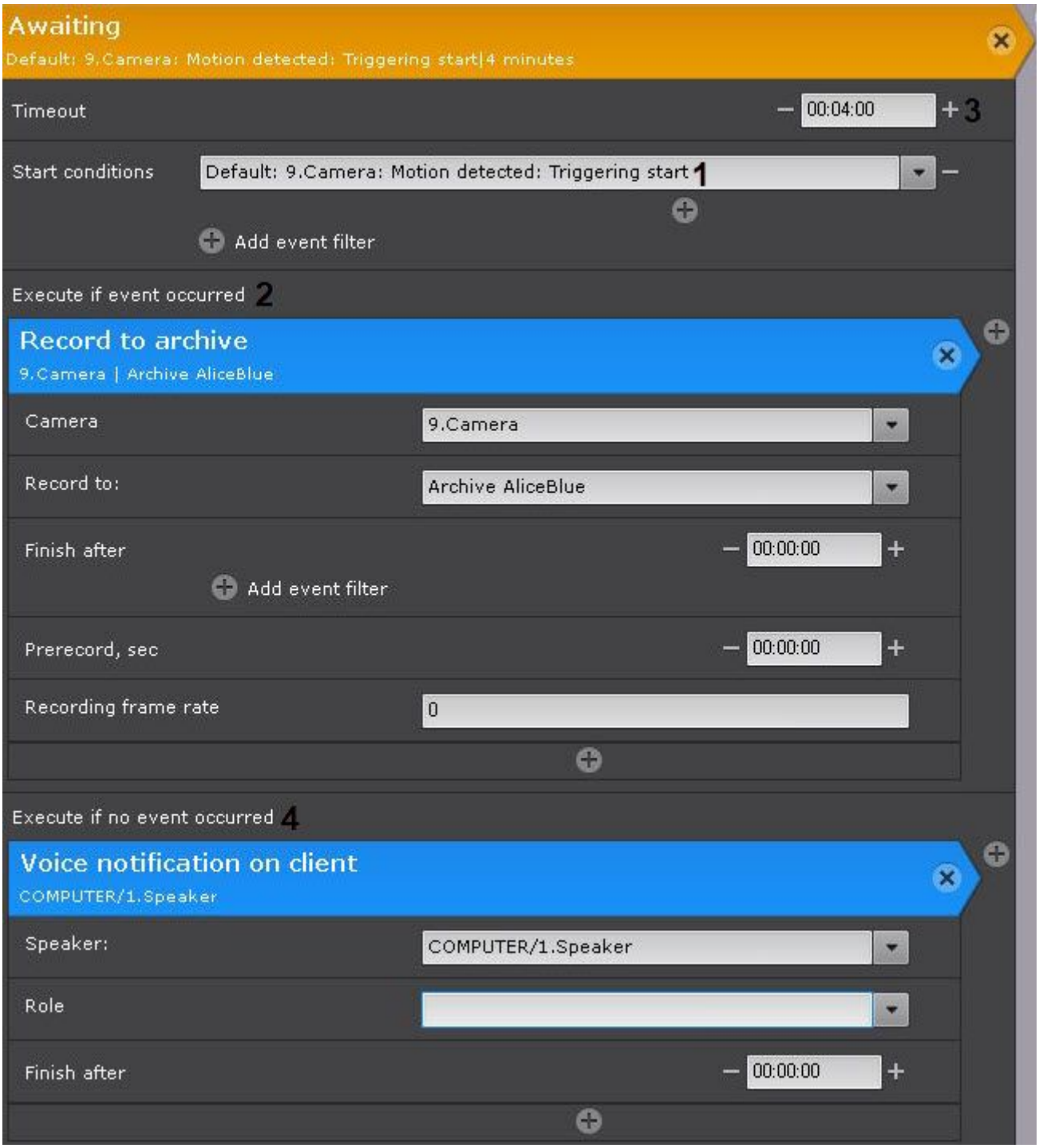
You can enter the following parameters in the **Awaiting** command:

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**)**.**

For example, this 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.

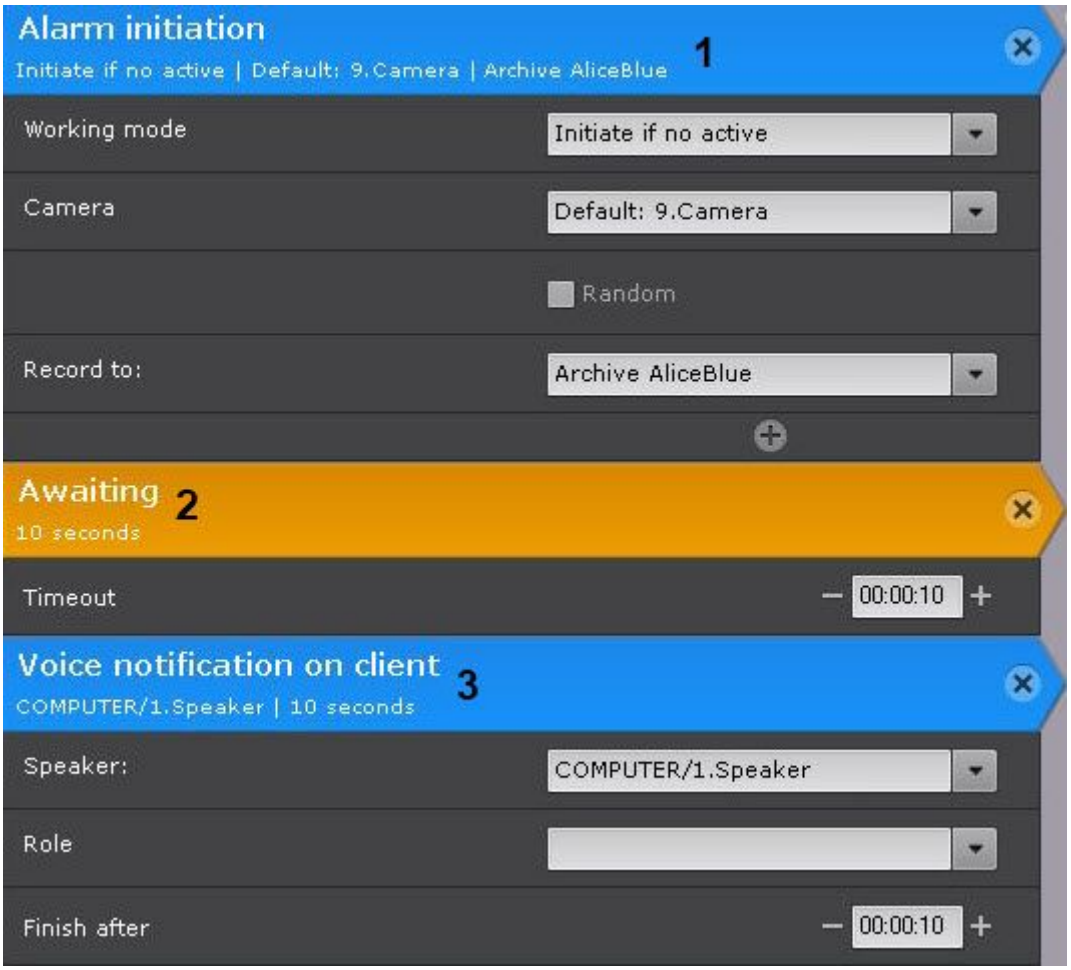
> **Attention!**
>
> The **Awaiting** command does not affect the commands below (outside of) it.

15.5.6.2 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(see page 407))

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**).



15.5.6.3 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).

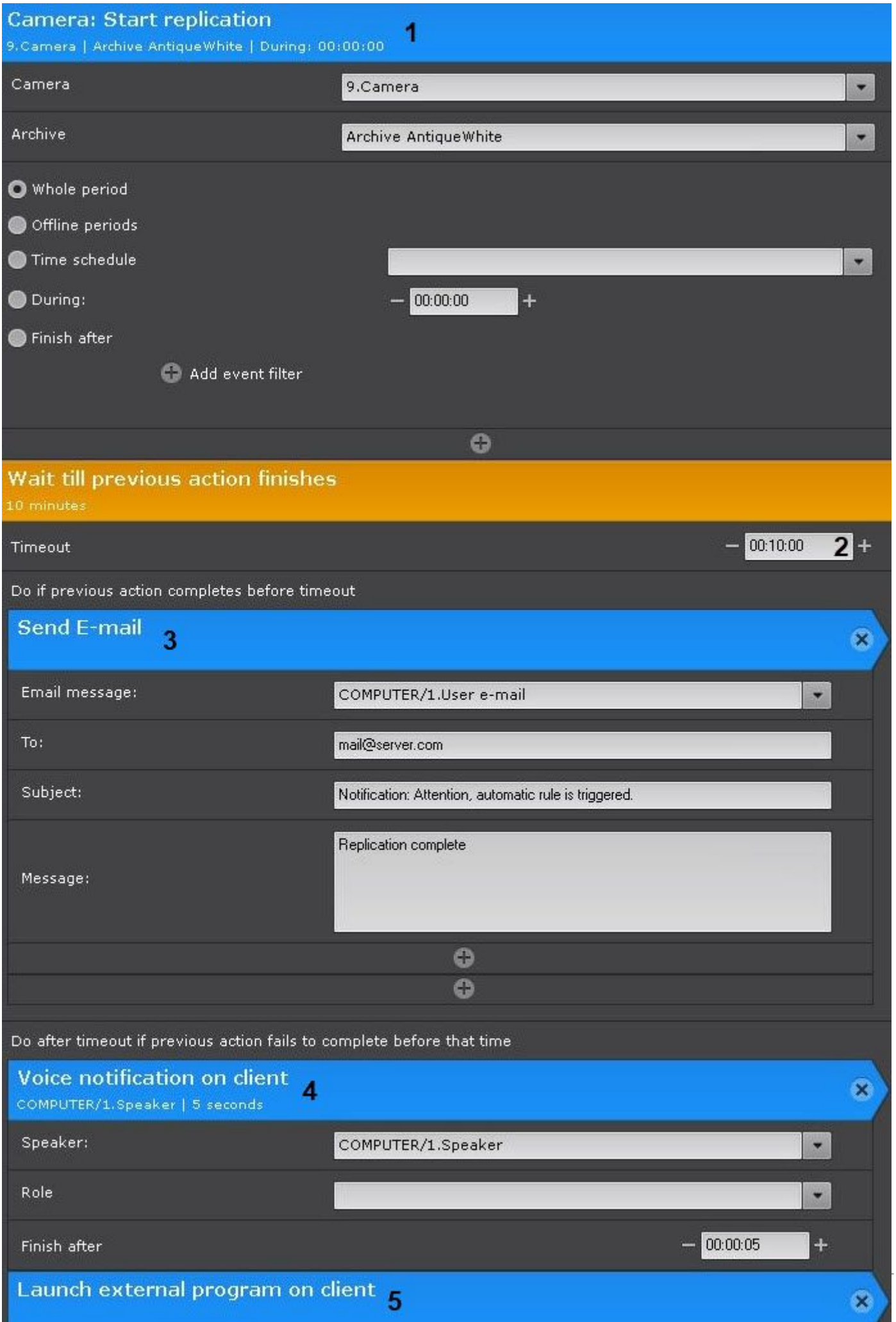
To configure, set up the following parameters:

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.

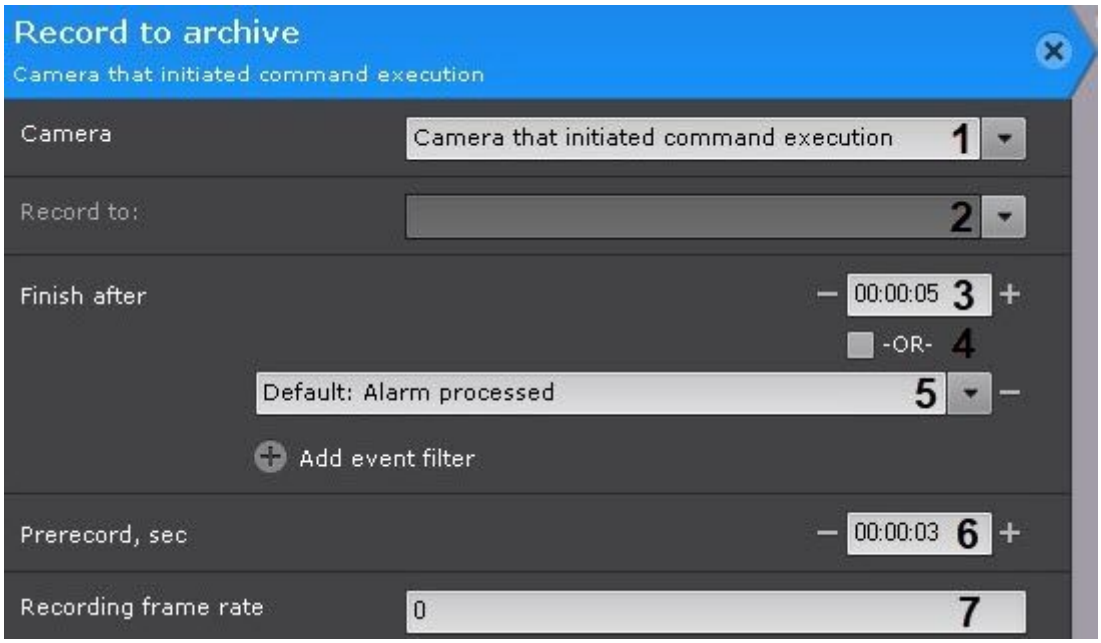
Example: In this macro, replication (**1**) and the program on the Client (**5**) start at the same time. If replication is completed within 10 minutes (**2**), an Email message (**3**) is sent. Otherwise, a voice alert (**4**) is played.


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

15.5.6.4 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 filters for event-driven macros(see page 407)) 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.

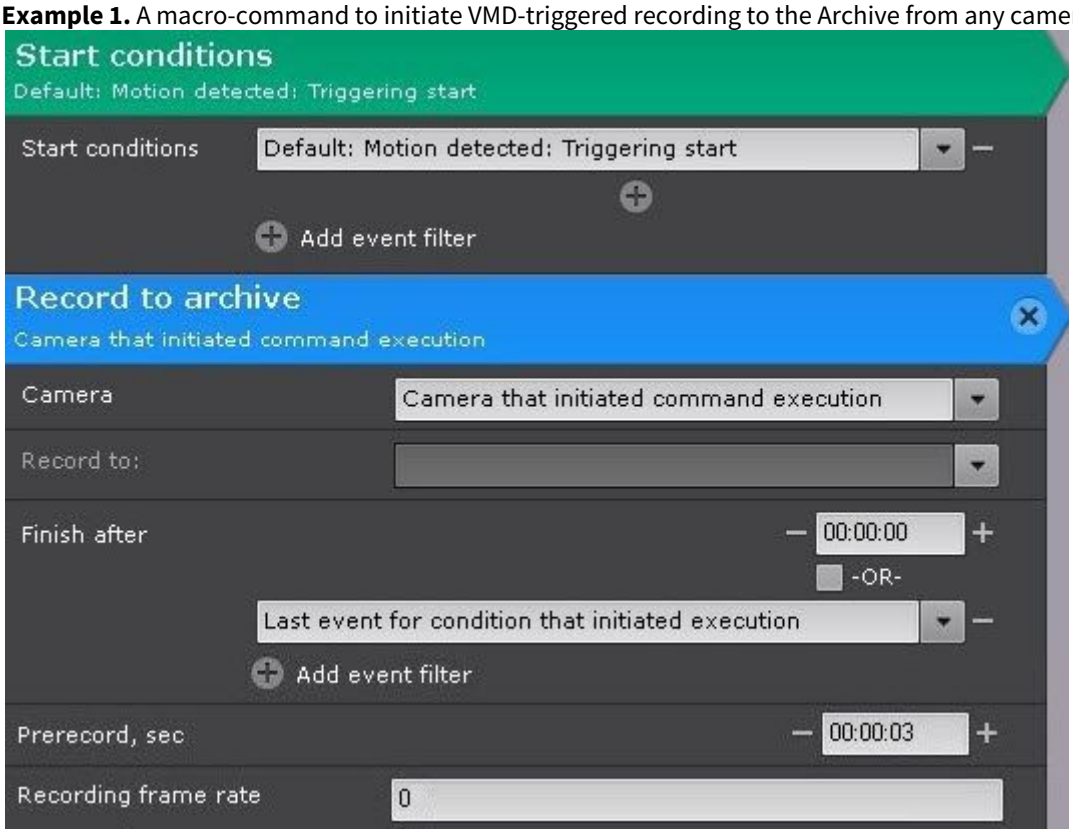
> **Attention!**
>
> By default, the pre-alarm recording time interval is set to the value specified in Archive settings (see Configuring recording to an archive(see page 224)).
> The longest pre-alarm recording time available in the Archive settings is used.
> Changing this value in a specific macro does not affect the Archive settings.

5. If you have cameras in continuous recording mode (see Configuring recording to an archive(see page 224)) 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.

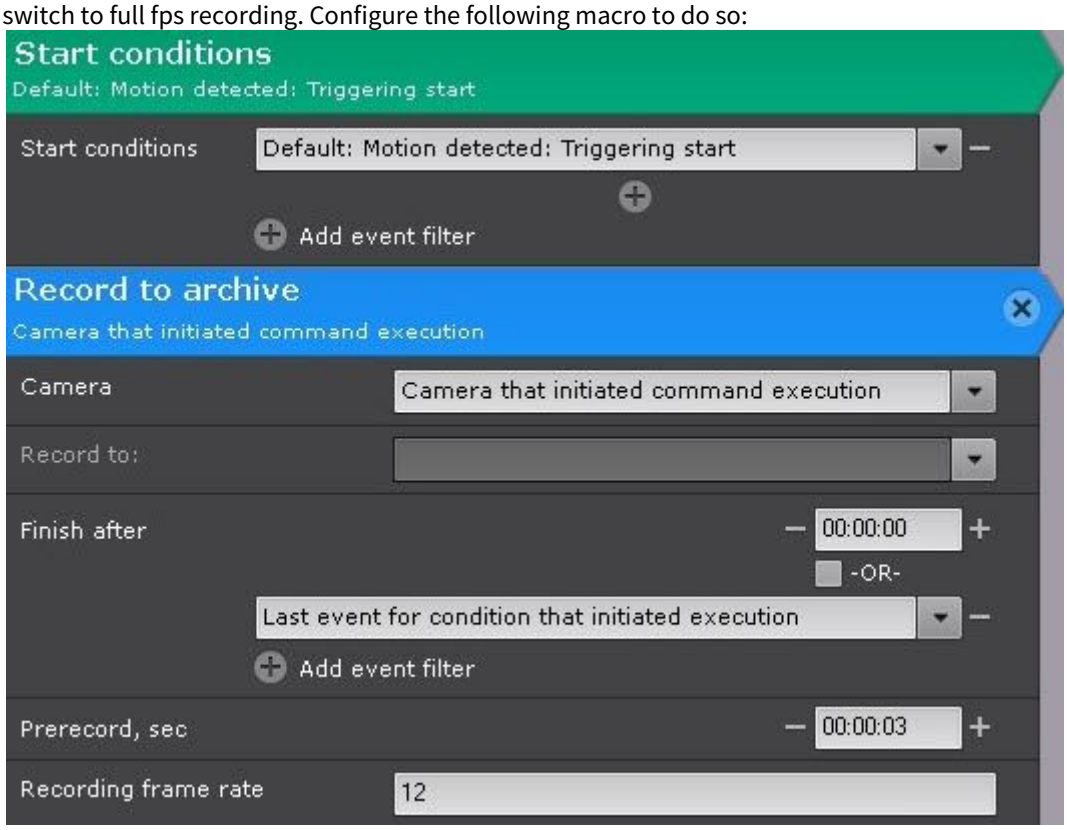
> **Attention!**
>
> Fps for pre-recording will not change.
> If the macro command is set to complete some time after a specified event has been received (see p. 3), the frame rate will change for this Check-in Event-time.

> **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 I-frames (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(see page 224)). When you have a motion detection event, you need to switch to full fps recording. Configure the following macro to do so:

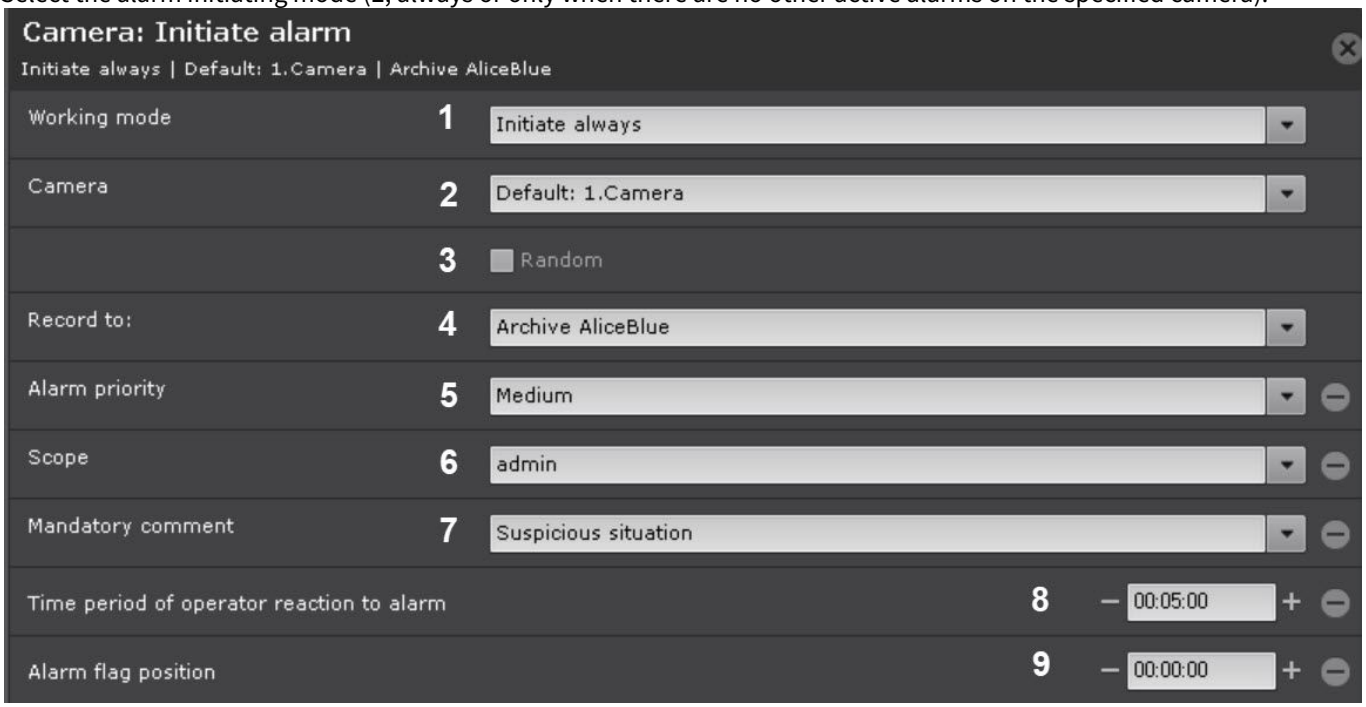


15.5.6.5 Initiating an alarm in the system

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(see page 407)).
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 filters for event-driven macros(see page 407)).

   Attention!

   If the start of the macro was triggered by the activation of input or output (see Configuring filters for event-driven macros(see page 407)) 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(see page 540)). 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.

15.5.6.6 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(see page 407)).
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 filters for event-driven macros(see page 407)) 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**).

15.5.6.7 Switch output

This action switches a output to a pre-selected state.

To configure this action, do as follows:

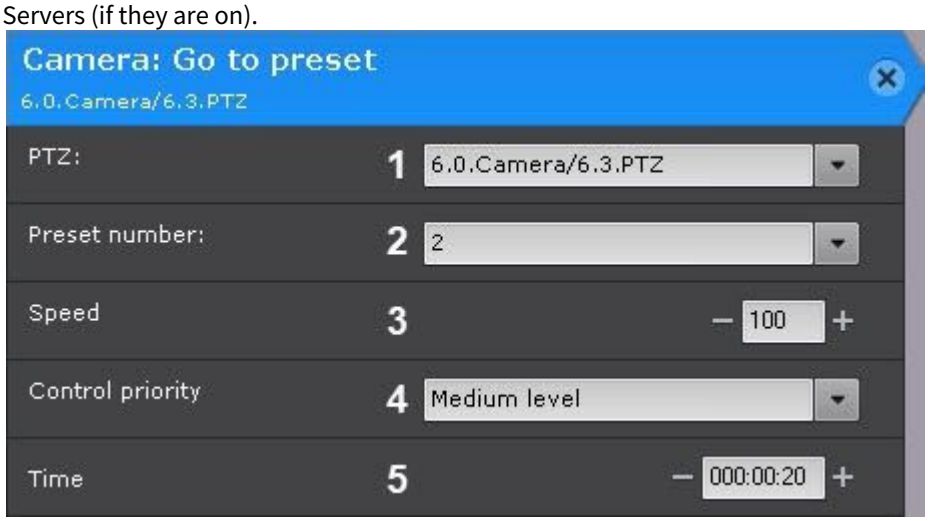
1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407)).
2. Select a output to switch by the macro (**1**). You can select any active output within your system, including outputs linked to another Server.

3. Outputs switch back after On-time (**2**), or after Check-in Event-time for any specified events**.**

15.5.6.8 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(see page 407)).
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(see page 452)) 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(see page 415) between the switching actions. You can also set Wait for timeout(see page 414). In this case, the switching between the presets will take place after the timeout time.

15.5.6.9 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(see page 407)).

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 filters for event-driven macros(see page 407)) 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.

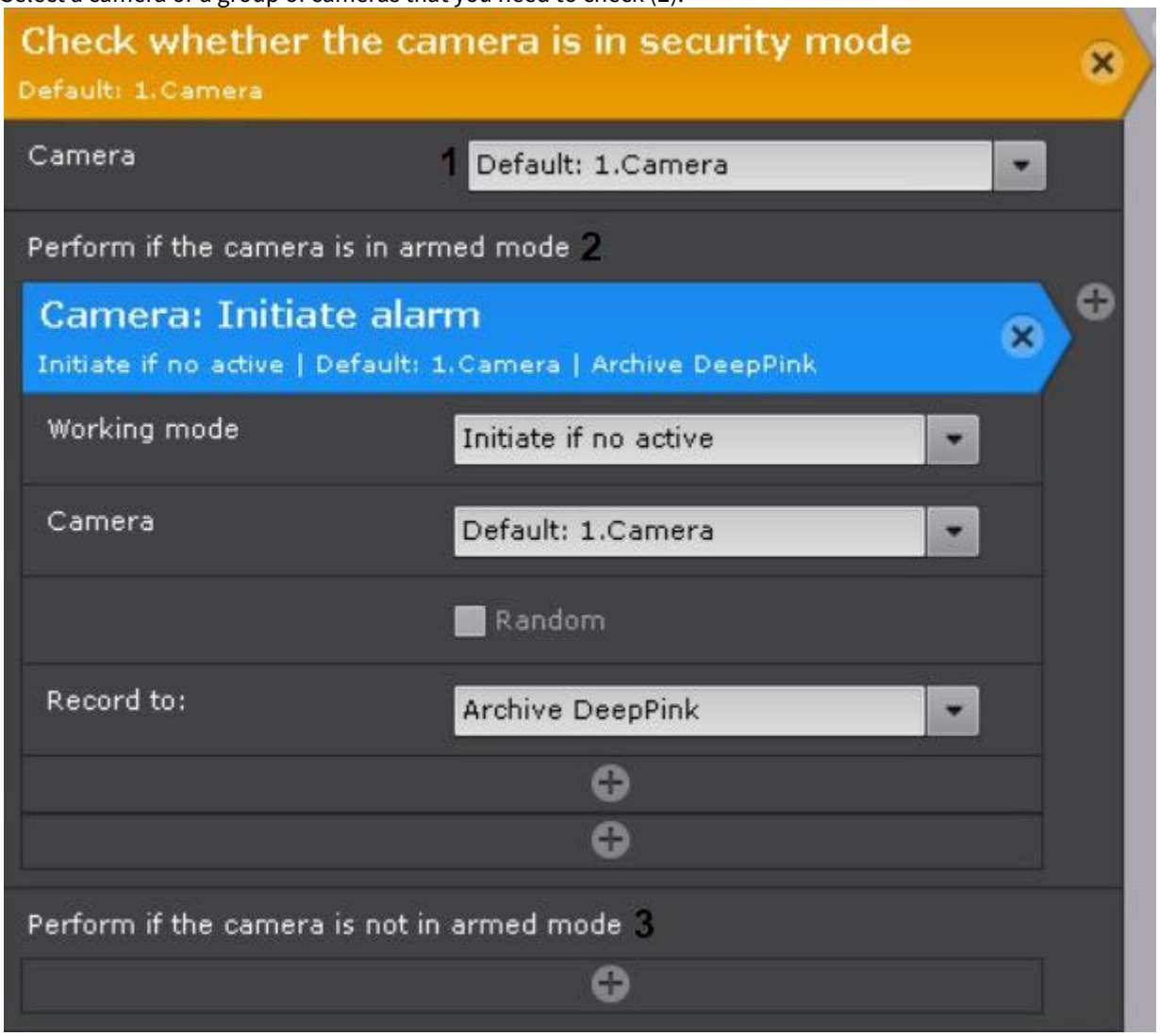
15.5.6.10 Checking whether the camera is in armed mode

This command allows you to check whether a camera or a group of cameras is armed (see Arming and Disarming a Video Camera(see page 674)).

To configure this command, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407).

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**).

15.5.6.11 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(see page 407)).
2. Select the camera to be displayed (**1**) or **Camera that initiated command execution** (see Configuring filters for event-driven macros(see page 407)). 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 filters for event-driven macros(see page 407)) 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(see page 802) 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(see page 501))
Unmark camera	The camera is deleted from the **Marked cameras** layout (see Creating special layouts(see page 501))

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.

15.5.6.12 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:

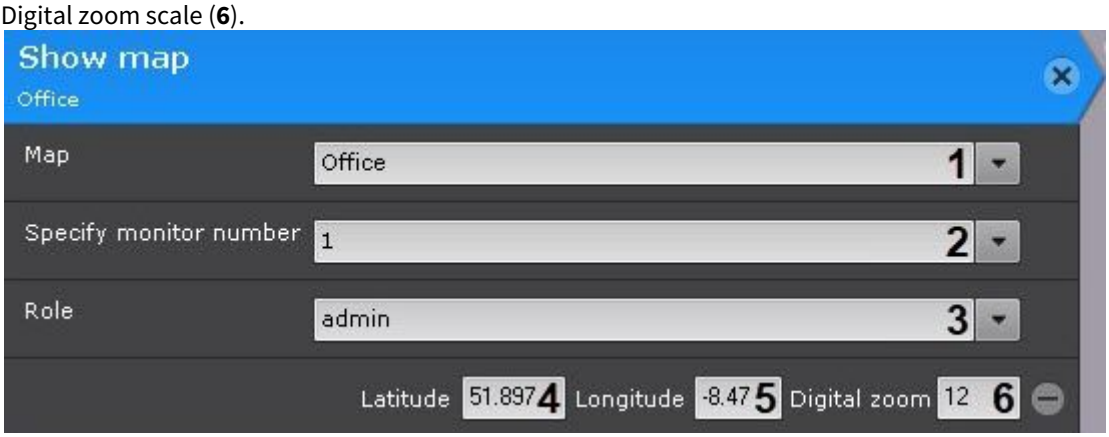
1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407)).
2. Select the layout (**1**).
3. Specify the number of the monitor on which you want to open the selected layout (**2**).
4. Select the role of users who can access this macro (**3**).

15.5.6.13 Show map

You can display any map added to the system on the required monitor (see Adding a new map(see page 510)).

To configure the **Show map** macro, do the following:

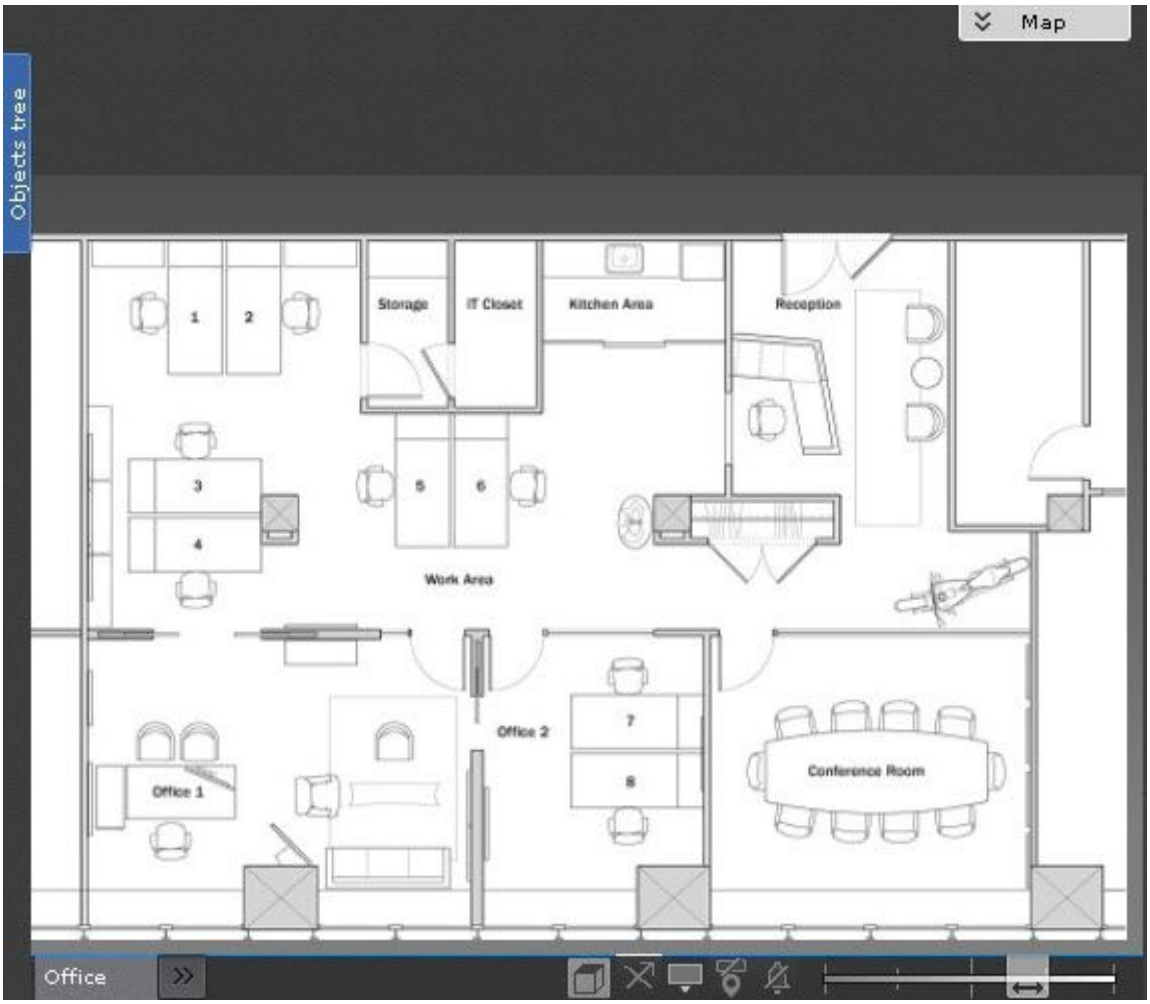
1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407)).
2. Select the map (**1**). When selecting a geomap, it is necessary to specify the following parameters to display the required area:
   a. Latitude (**4**).
   b. Longitude (**5**).
   c. Digital zoom scale (**6**).



3. Specify the number of the monitor on which you want to display the selected map (**2**).
4. Select the role of users who can access this macro (**3**).
5. Click the **Apply** button.

The **Show map** macro is now configured.

The selected map will be displayed on the specified monitor.

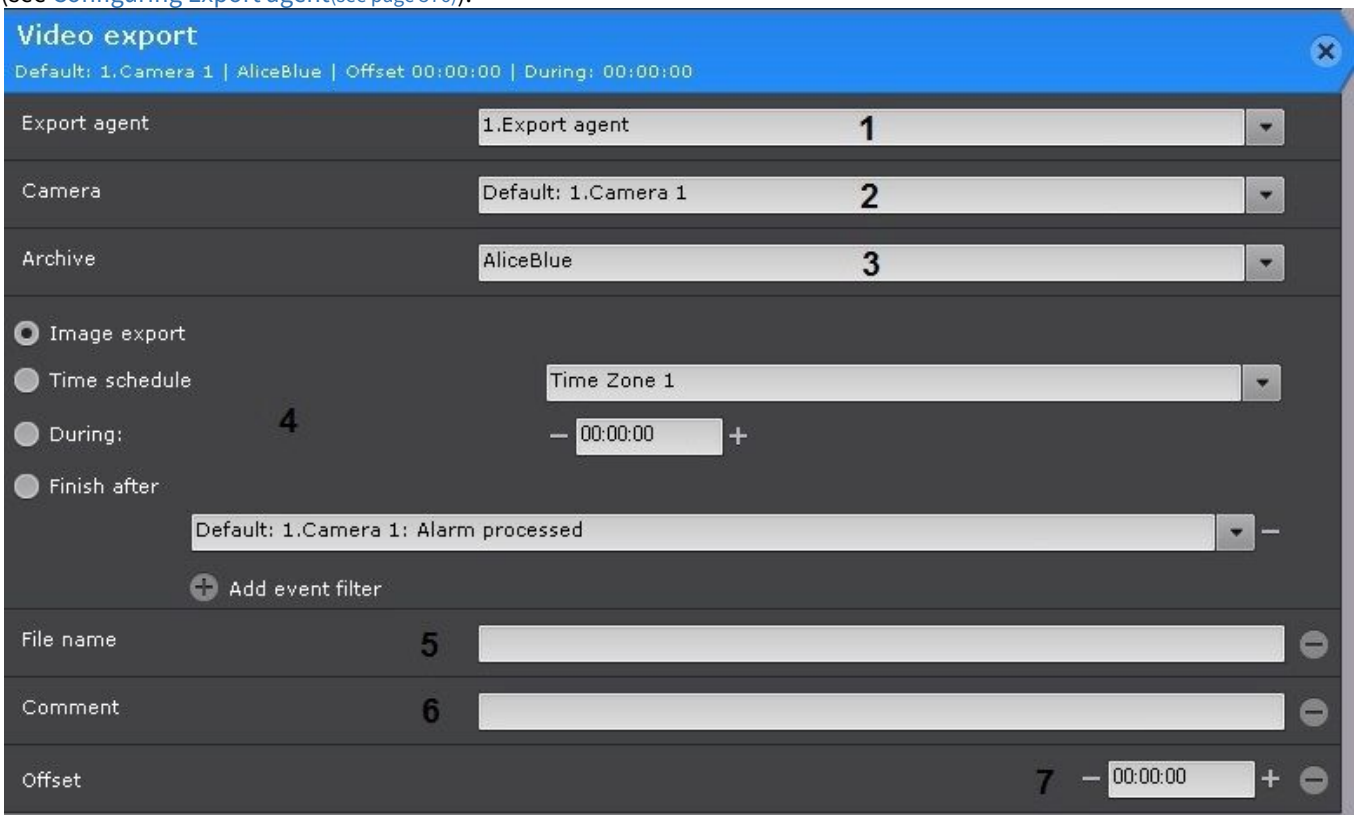


15.5.6.14 Starting export

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(see page 407)).

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(see page 576)).



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 filters for event-driven macros(see page 407)) 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**).

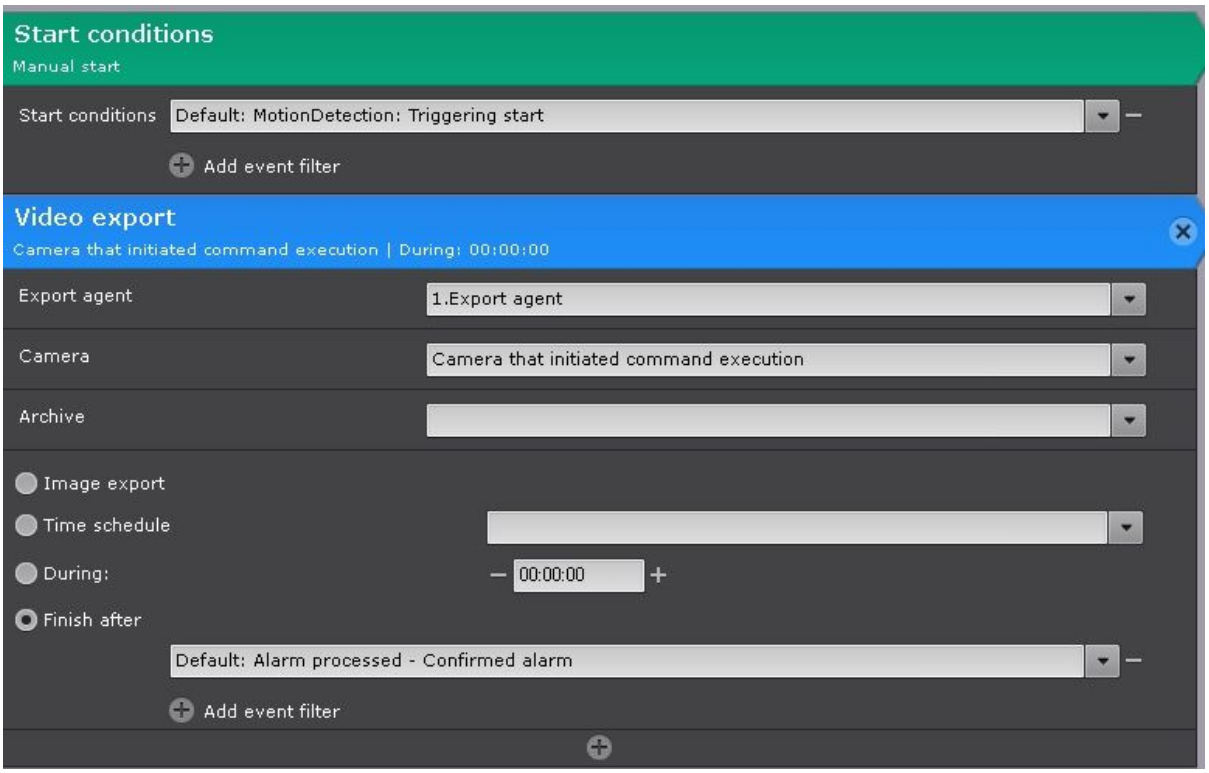
> **Attention!**
>
> You can use the following templates for file names and text comments:

- **%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 filters for event-driven macros(see page 407)):
- **%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".



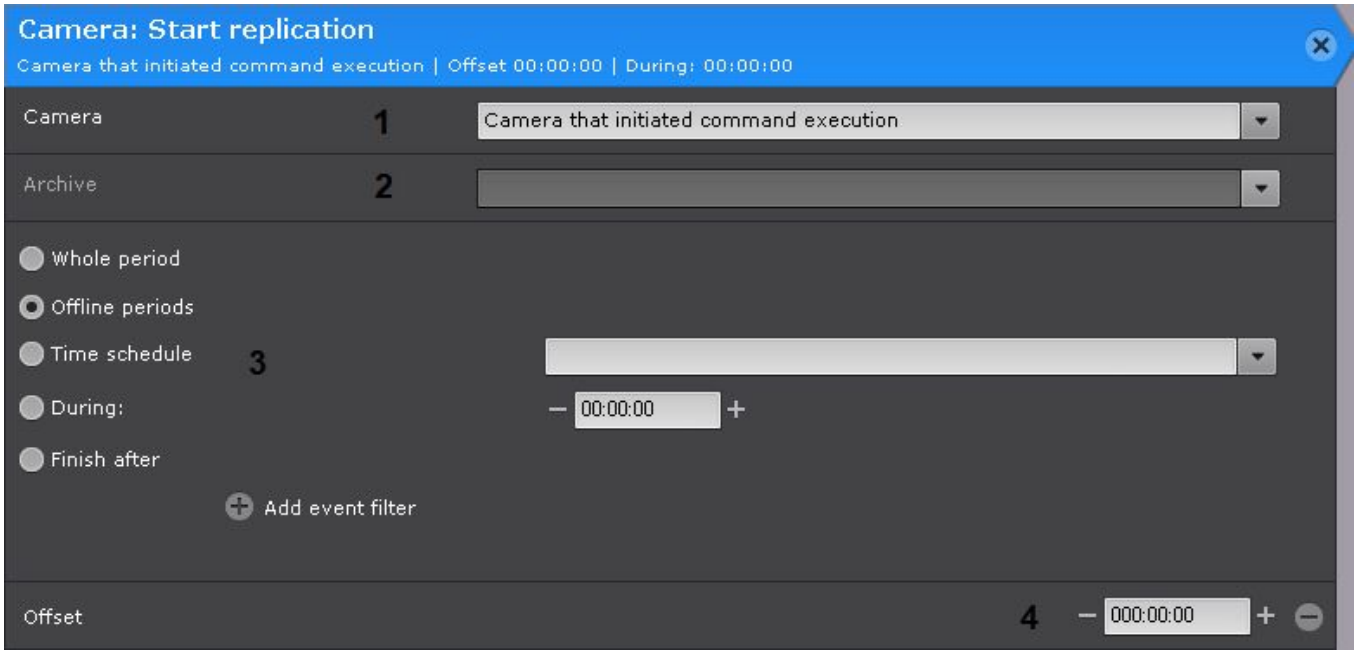
15.5.6.15 Start replication

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(see page 226)). 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(see page 174)).

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**.



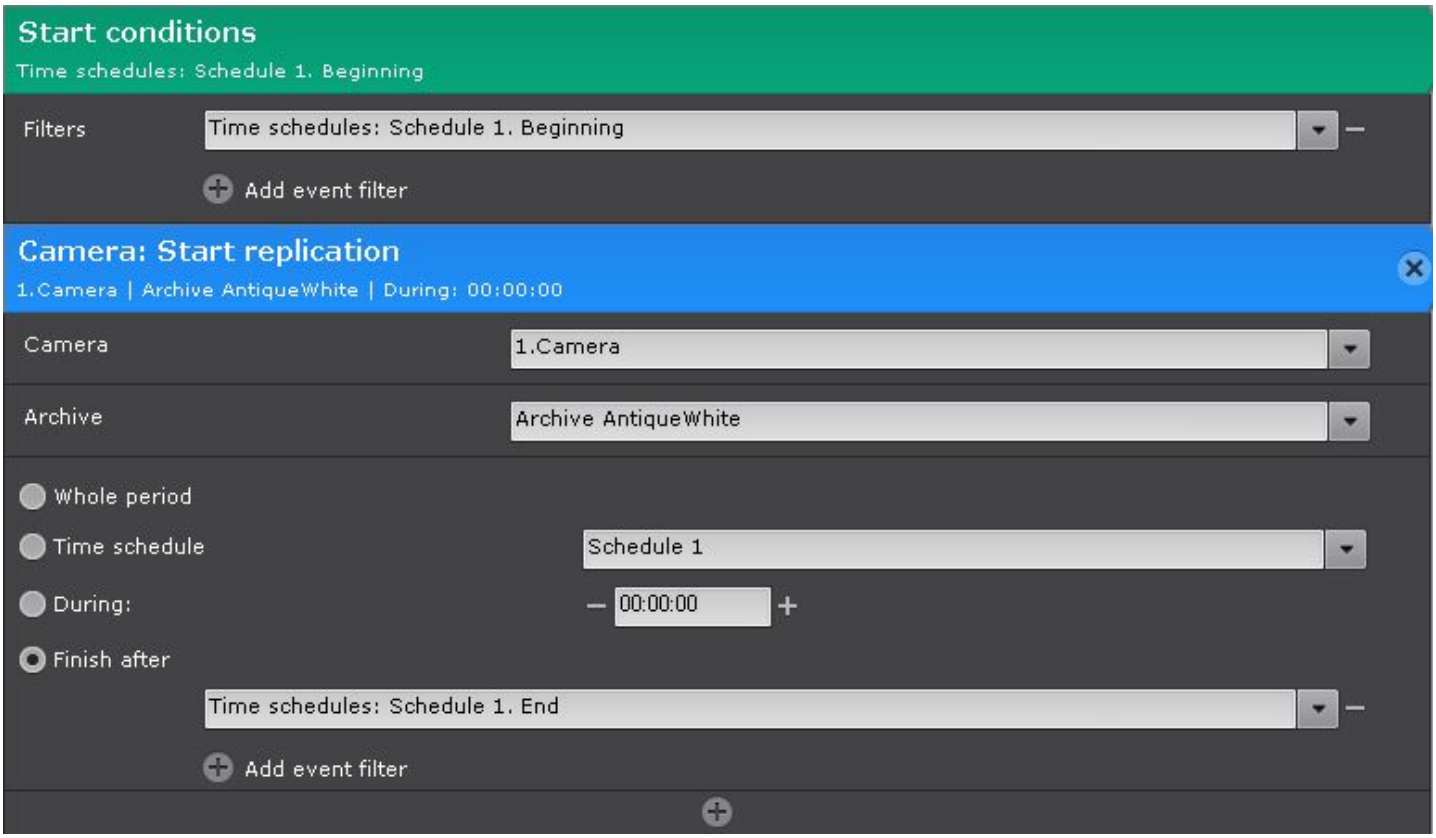
> **Attention!**
>
> If the start of the macro was triggered by the activation of input or output (see Configuring filters for event-driven macros(see page 407)) that is not connected to any camera, you need to select a specific camera here. If you select a group of cameras or a camera that triggered 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(see page 541)). 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:



15.5.6.16 Notifications

15.5.6.16.1 Audio notification on Client

You can playback audio via Client's speakers.

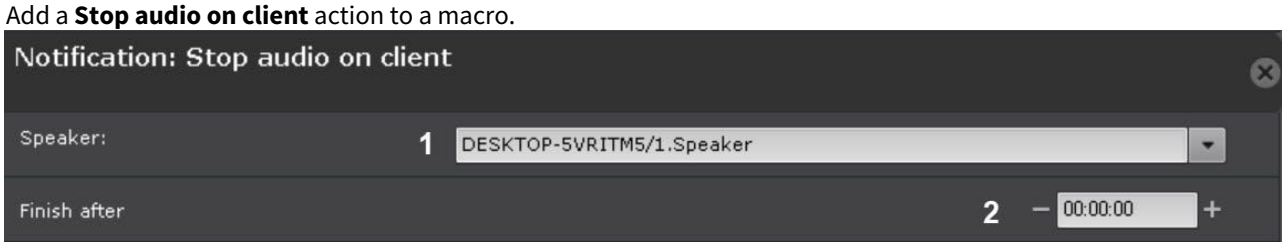
> **Attention!**
>
> To make the Client-side audio playback possible, you have to create a **Speaker** object allowing **Play on client** playback mode (see The Speaker Object(see page 170)).

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407)).
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(see page 403), Configuring filters for event-driven macros(see page 407)).
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**).

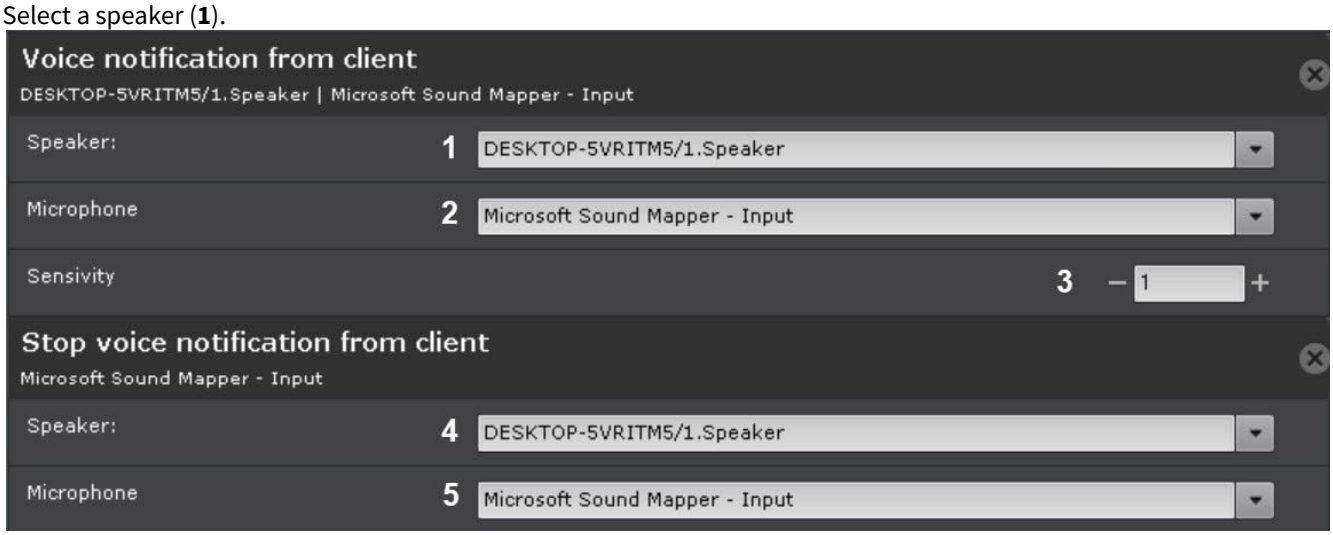
15.5.6.16.2 Voice notification from Client

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(see page 899)).

To configure this action, do as follows:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407)).
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**).

15.5.6.16.3 Play audio on Server

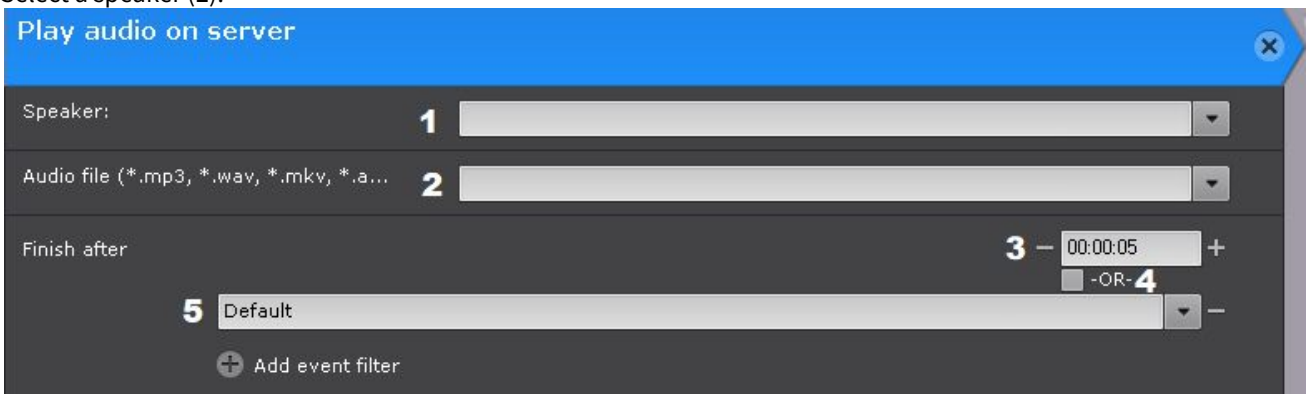
This action allows you to play audio on a Server speaker.

> **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(see page 170)).

To configure the action, set up the parameters:

1. Configure the conditions to start a macro (see Configuring filters for event-driven macros(see page 407)).

2. Select a speaker (**1**).



3. In the **Audio file** field (**2**), enter the full path to 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

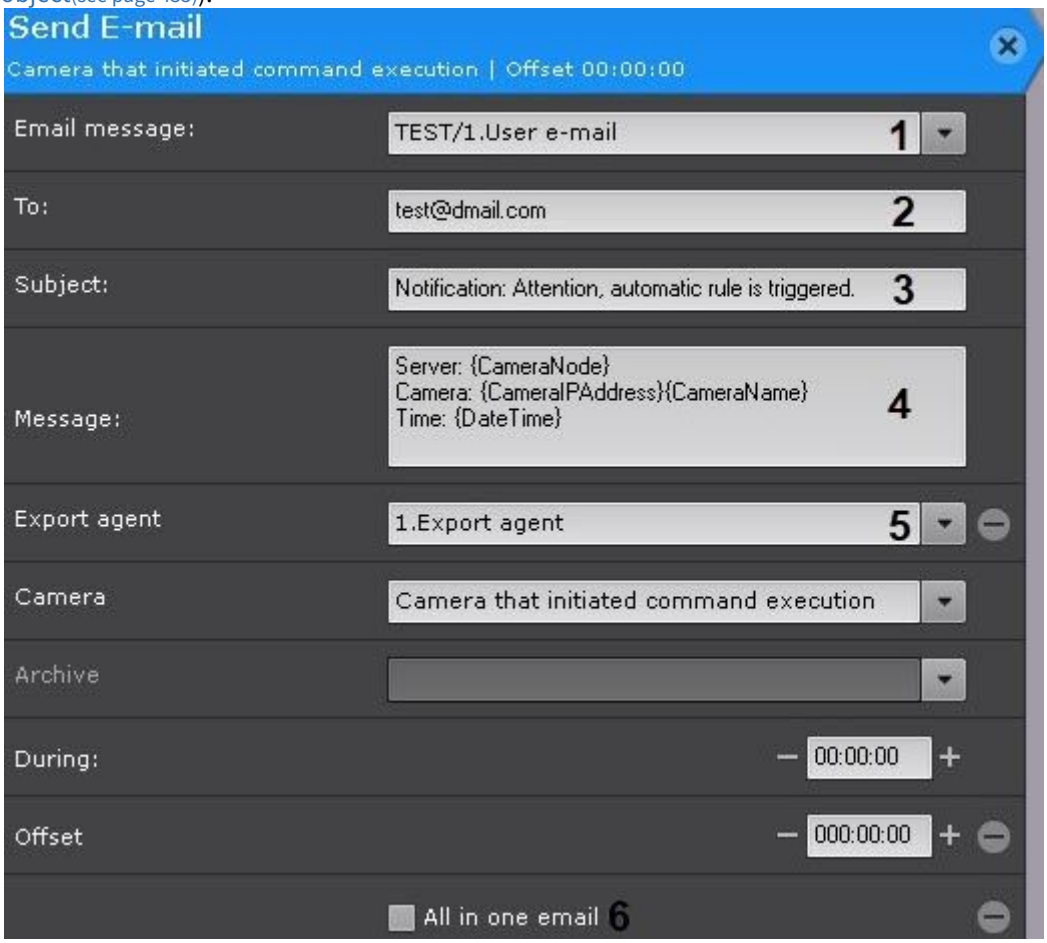
The **OR** checkbox can be set only if the timer setting is not 00:00:00.
An implicit selection of an event is allowed—**Last event for condition that initiated execution** (see Configuring filters for event-driven macros(see page 407)).
For example, if the event that triggered the execution of the command 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.

15.5.6.16.4 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(see page 407)).

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 E-mail notifier object(see page 435)).



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 E-mail notifier object(see page 435)).

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(see page 445)).

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(see page 427)).

> **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(see page 576)).

6. If a macro is launched from a group of cameras (see Configuring filters for event-driven macros(see page 407)), 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.

15.5.6.16.4.1 The E-mail notifier object

On this page:

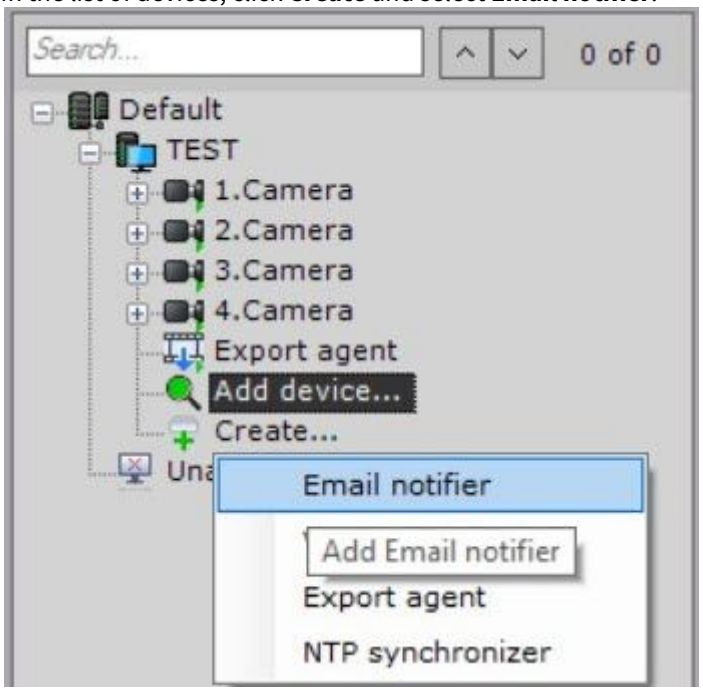
- Creating the E-mail notifier object(see page 435)
- Configuring the E-mail notifier object(see page 435)
- Checking E-mail notification(see page 436)

The **E-mail 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 E-mail notifier object

To create the **E-mail notifier** object, do the following:

1. In the list of devices, click **Create** and select **Email notifier**.



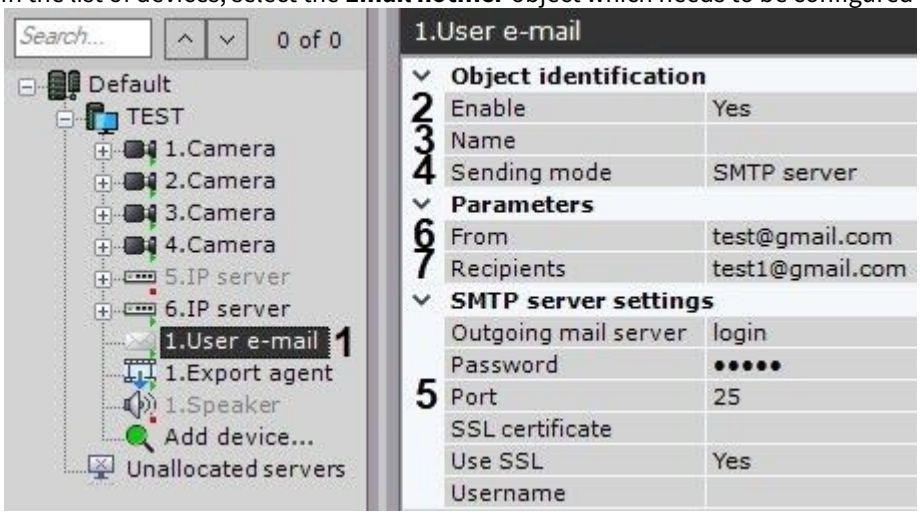
2. Click the **Apply** button.

The **E-mail notifier** object will appear in the list of devices.

Configuring the E-mail notifier object

To configure the **E-mail 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 **E-mail notifier** object.
4. Select the mode for sending the E-mail notifications: through *AxxonNet* or through the specified SMTP Server (**4**).

> **Attention!**
>
> To send notifications through *AxxonNet*, you should connect to it (see Connecting Axxon-domain to AxxonNet[145]). *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 E-mail SMTP Server.
   b. In the **Password** field, enter the password of the user account on the outgoing E-mail Server.
   c. In the **Port** field, enter the number of the port used by the outgoing E-mail 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 E-mail Server certificate will be used.
   e. If you need to use SSL-encrypted connection when connecting to the outgoing E-mail 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 E-mail Server.
6. In the **From** field, enter the E-mail address from which the messages will be sent (**6**).

> **Attention!**
>
> When using email notification, E-mail 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.

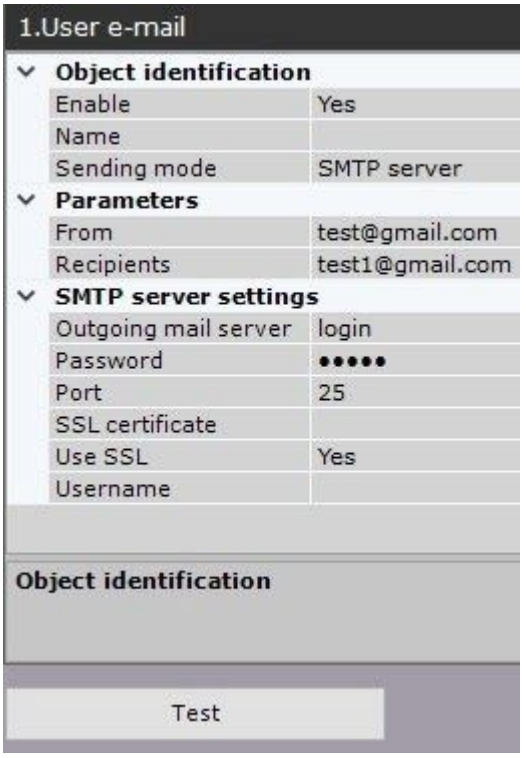
7. In the **Recipients** field (**7**), enter one or several E-mail addresses to which messages will be sent.
8. Click the **Apply** button.

Configuration of the **E-mail notifier** object is now complete.

Checking E-mail notification

145 https://docs.axxonsoft.com/confluence/display/anet/Connecting+Axxon-domain+to+AxxonNet

To check the E-mail 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 E-mail address specified in the **Recipients** field (see Configuring the E-mail notifier object[146]): "Test message".

15.5.6.16.5 Push notification

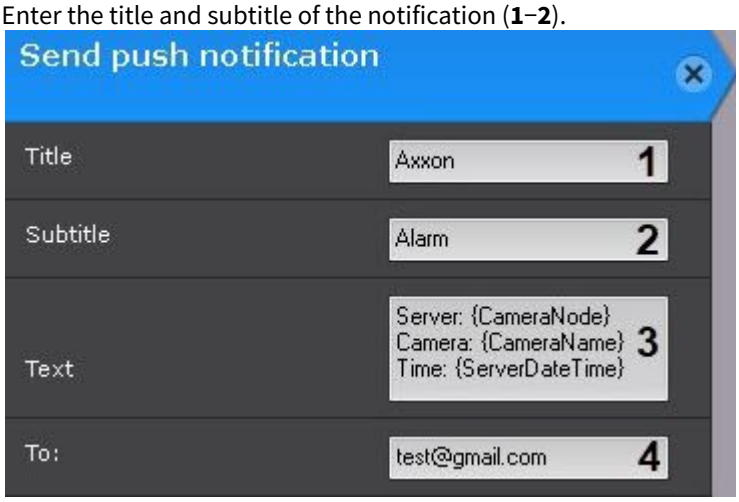
This action sends a push notification to the device with the *AxxonNet* app installed.

To run the action, make sure the following requirements are met:

- the Axxon-domain must be connected to *AxxonNet* (see Connecting Axxon-domain to AxxonNet[147]);
- 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(see page 407)).
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(see page 445)).
4. Enter the e-mail address of the user who will be notified (**4**). Only one address is allowed.

146 https://docs.axxonsoft.com/confluence/display/next46en/The+Email+notifier+object#TheEmailnotifierobject-ConfiguringtheEmailnotifierobject
147 https://docs.axxonsoft.com/confluence/display/anet/Connecting+Axxon-domain+to+AxxonNet

15.5.6.16.6 Telegram bot notification

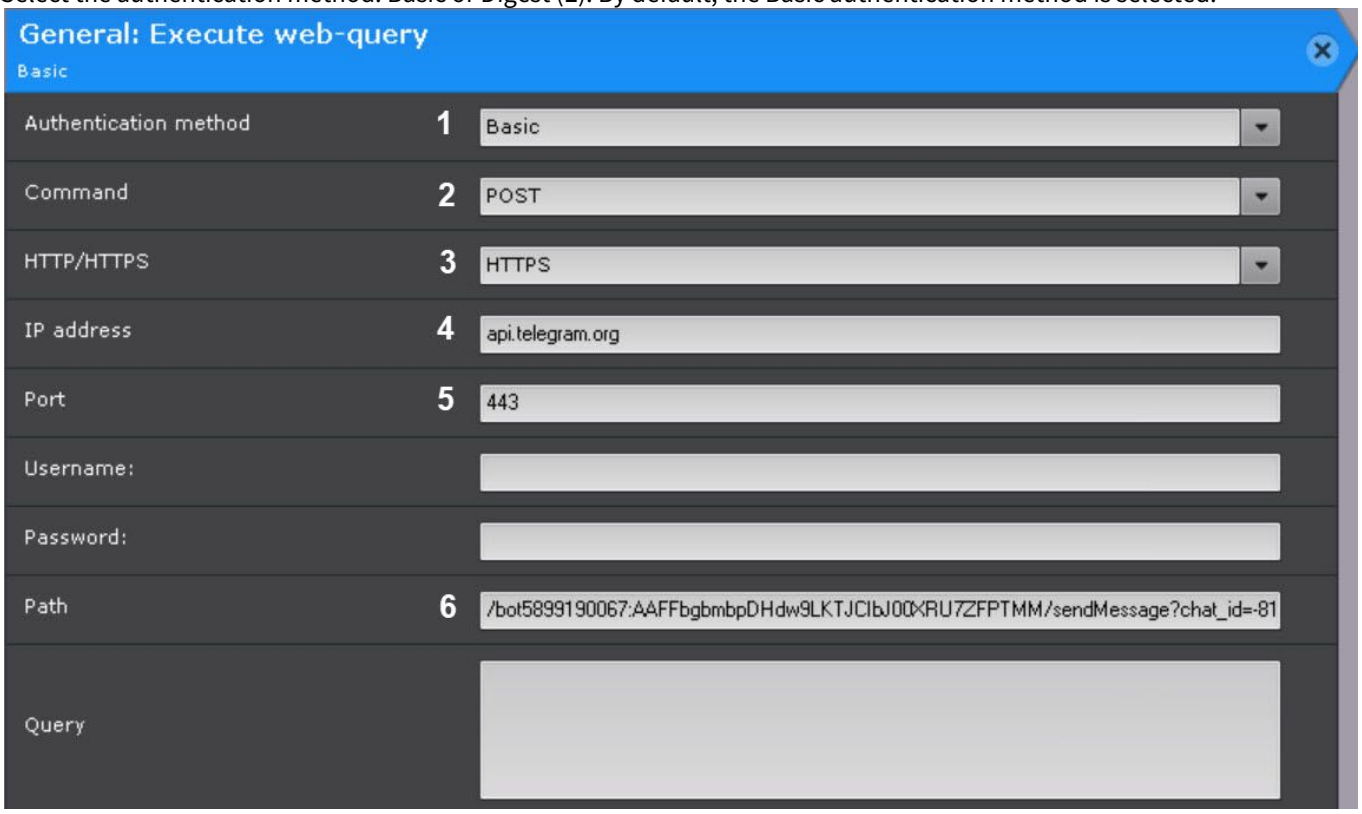
Axxon One allows you to send text notifications to Telegram chat when any event occurs from the objects registered in the *Axxon One* objects tree. Once configured, the notification sending is initiated by the *Axxon One* macro.

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[148].

> **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 filters for event-driven macros(see page 407)).
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**

148 https://telegram.org/?setln=en

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[149] 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(see page 444)). However, the **Username, Password** and **Query** fields are not required for sending a notification via Telegram bot.

15.5.6.17 Starting an external program on Clients

This starts an external program on your *Axxon One* client.

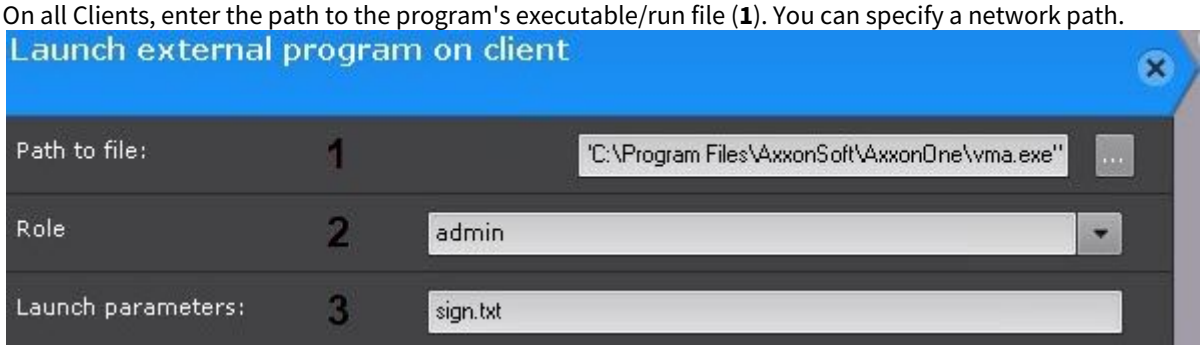
The external program is started on all Clients that are connected to the domain.

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(see page 407)).
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 OS Windows Server 2012 versions, 8, 8.1 and you need to edit the registry[150]), or start *Axxon One* with administrator rights.

15.5.6.18 Starting an external program on Servers

This starts an external program on your Axxon domain.

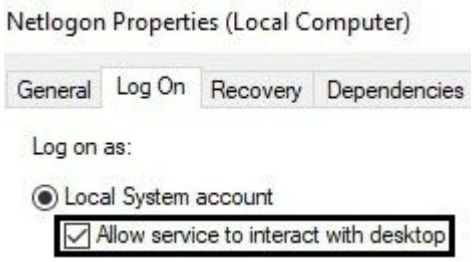
Attention!

149 https://tools.ietf.org/html/rfc3986
150 http://winaero.com/blog/how-to-turn-off-and-disable-uac-in-windows-10/

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[151] 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(see page 62)), you have to allow the **NGP RaFT supervisor service** to interact with desktop.

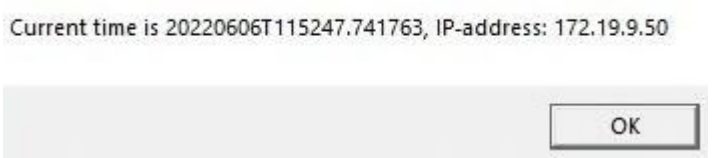
2. Add to folder <Directory where *Axxon One* is installed>\UserScripts\ one or more .bat files with the application startup command.
   The command should include a path to the executable file. You can specify a network path and command-line options (see Starting an external program on Clients(see page 439)).
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:

151 https://docs.microsoft.com/en-us/windows/desktop/Services/interactive-services

```
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
```

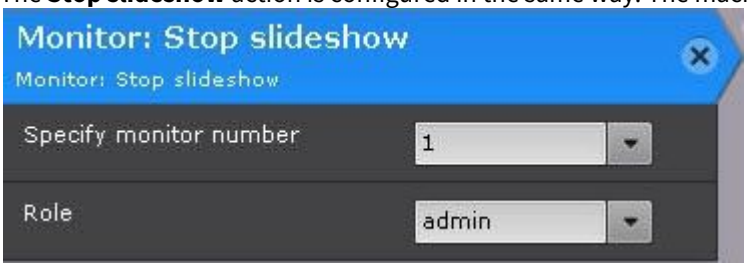
15.5.6.19 Start/stop slideshows of layouts

These actions start and stop a specific layout slideshow (see Selection and Slideshow of Layouts(see page 786)) 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(see page 407)).

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.



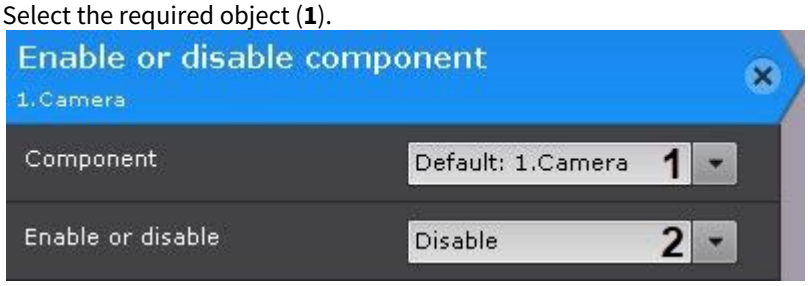
To stop the slideshow of the layouts, you can also select any video surveillance window by clicking the left mouse button. After restarting the Client, the slideshow resumes.

15.5.6.20 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(see page 407)).
2. Select the required object (**1**).



3. Select the required command (**2**).

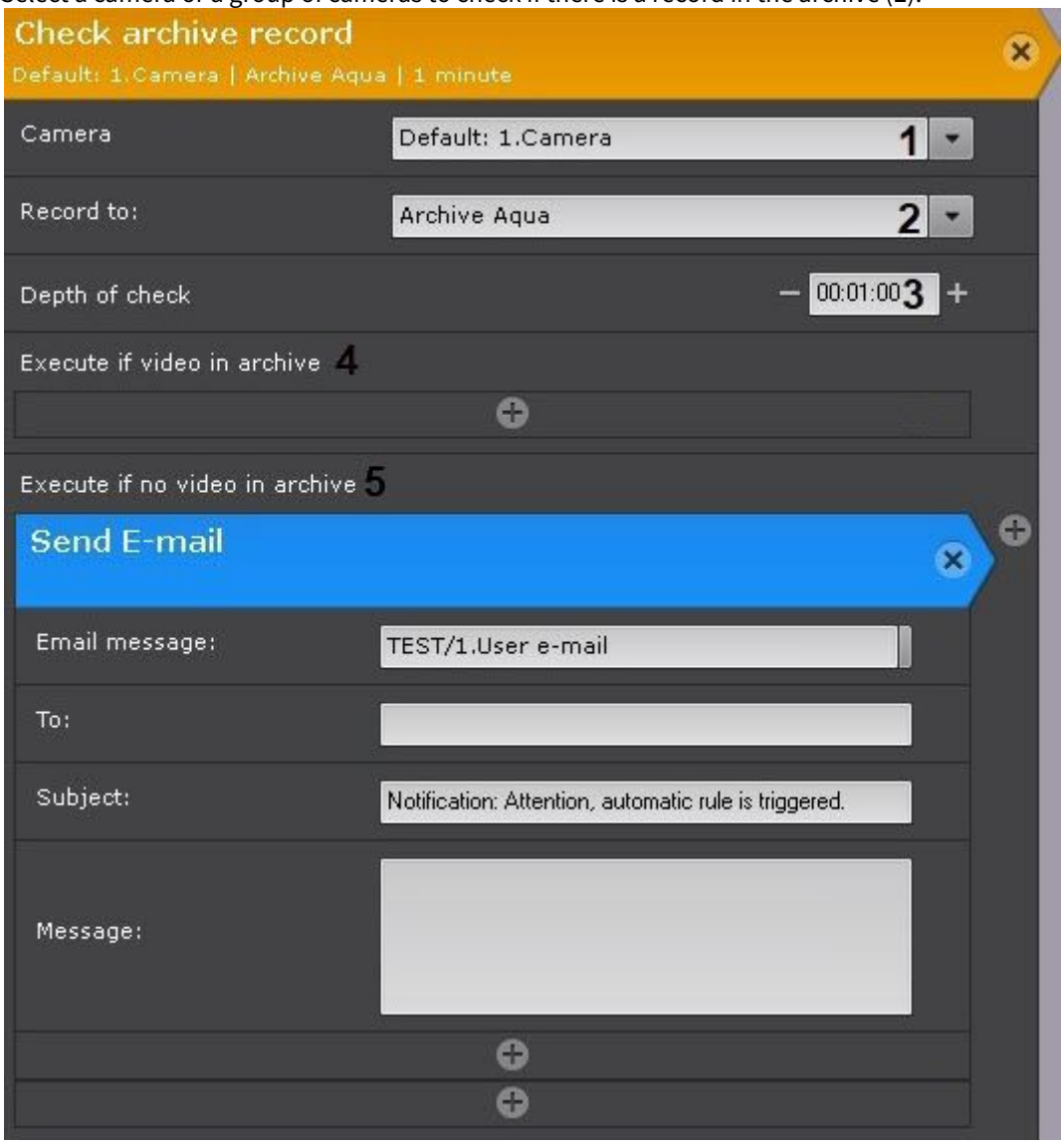
15.5.6.21 Checking for archive video recordings

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(see page 407)).

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 filters for event-driven macros(see page 407)) 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(see page 433) 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).

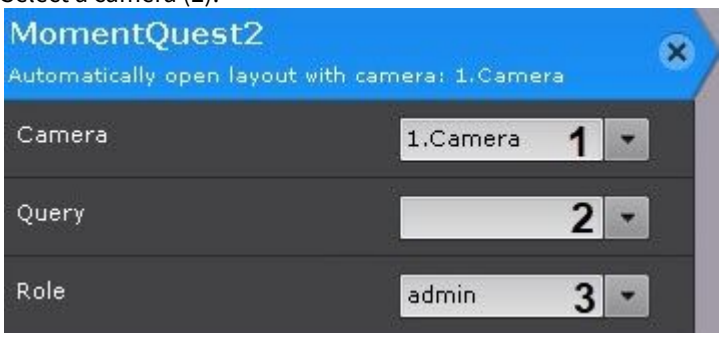
Attention! For the correct execution of the macro, synchronize the time across all Servers within the Axxon-domain.

15.5.6.22 Switching to MomentQuest2 search results in archive

This action allows you to open the results of a previously saved MomentQuest2 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(see page 407)).
2. Select a camera (**1**).



3. Select a previously saved search query (**2**, see Saving search queries(see page 749)).
4. Select a role for users of which this action must be performed (**3**).

15.5.6.23 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(see page 407)).
2. Select the necessary macro.

Attention!

This action launches only event-related macros.

15.5.6.24 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(see page 228)). To configure this action, see Setting up a macro for automatic copying of protected records(see page 229).

15.5.6.25 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(see page 407)).
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(see page 445)).

15.5.6.26 Text templates in macros

You can use message templates in commands (see E–mail notification(see page 433), Executing a Web-query(see page 444)) 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:

a. The **Gender and Age** parameter is activated in facial detection tool settings (see Configuring Face detection(see page 280)).
b. 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 Triggering macros by statistical data(see page 412)).

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:

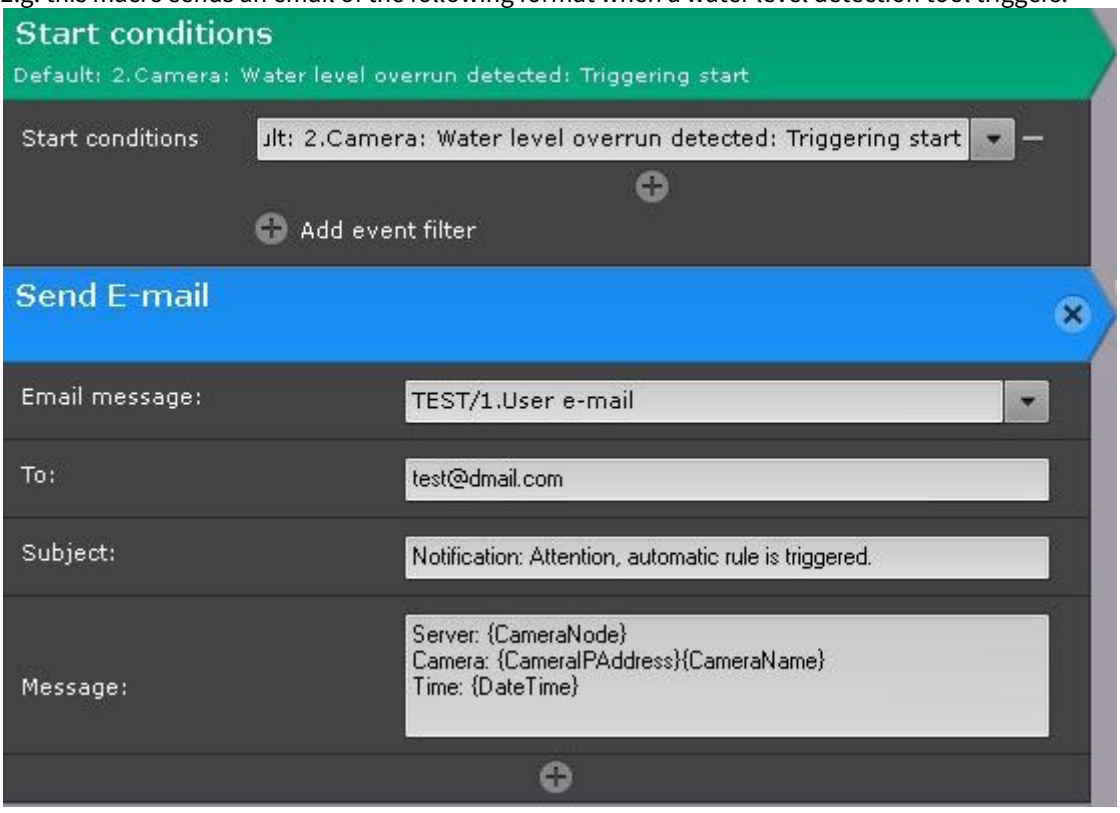
Parameter	Description
%a	Abbreviation for the day of the week
%A	Full name of the day of the week
%b	Abbreviation for the month
%B	Full name of the month
%y	Last two digits of the year
%Y	Full number of the year
%m	Month of the year
%d	Day of the month

Parameter	Description
%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:



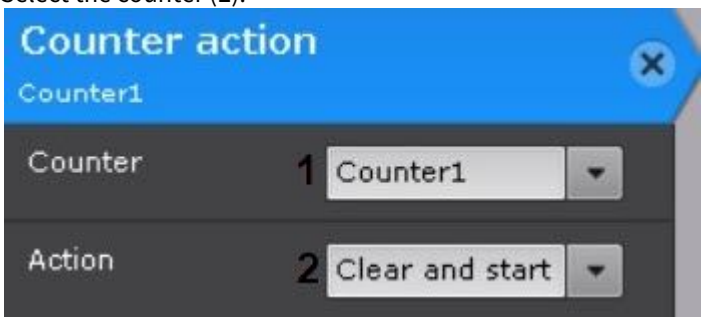

```
Subject: Notification: Attention, water level detection is triggered.

Server: Server1
Camera: 10.0.11.36 34.Camera
Time: 20190812T085517.926430
```

15.5.6.27 Managing the counter

This command allows you to run various operations with counters (see General information about the counters(see page 401)).

To configure this command, do as follows:

1. Select the counter (**1**).



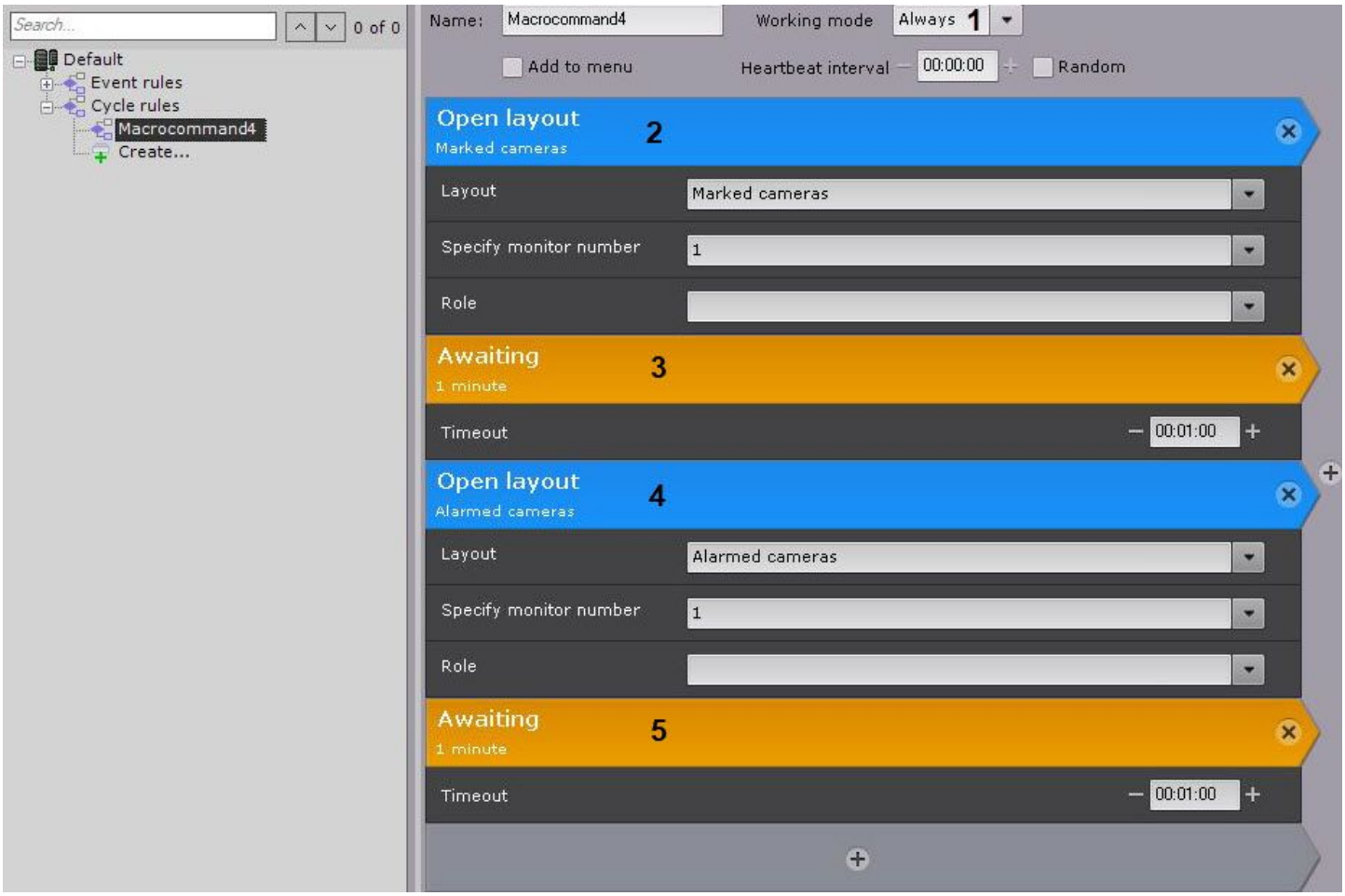
2. Select the desired command (**2**).

Command	Description
Start	Starting the counter. If the counter is running, its value changes as specified.
Stop	Stopping the counter. If the counter is on pause, its value does not change.
Clear	Resets the counter value to 0.
Clear and start	Resetting the counter value to 0 and starting it.
Stop and clear	Stopping the counter and resetting its value to 0.

15.5.7 Cyclical macros

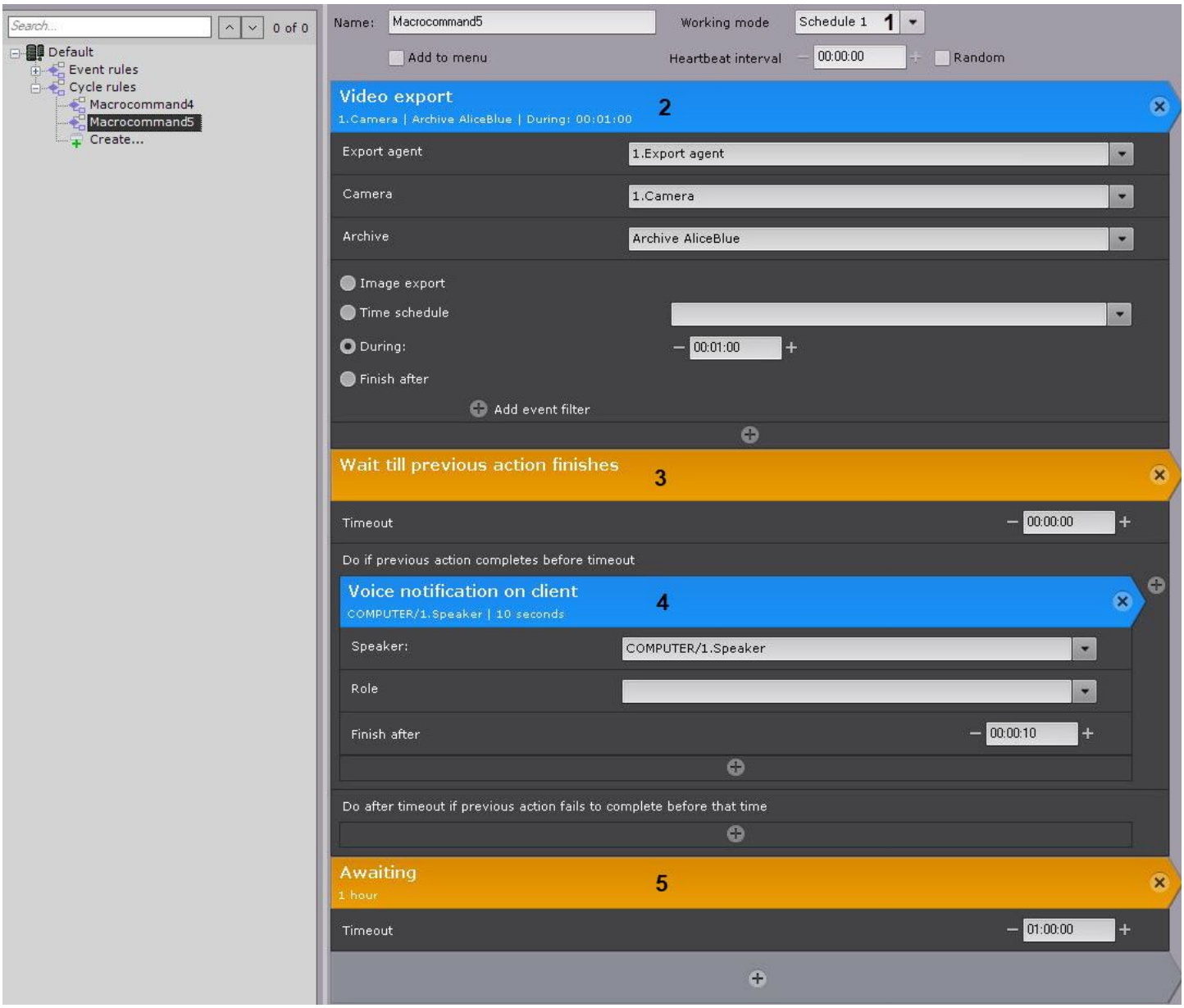
> **Attention!**
>
> If you do not have the **Wait** command in a cyclic macro, the time-out between cycles is 1 second.

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(see page 414)
Wait till previous action finishes(see page 415)

15.6 Configuring user permissions

In *Axxon One*, every user has permissions based on his 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.

Roles and users can be added and configured in **Settings**, on the **Users** tab.

There are two types of users: local (stored in the Server database) and LDAP[152] (see Connecting LDAP users(see page 102)).

To enable LDAP users, you must configure access to LDAP catalogs.

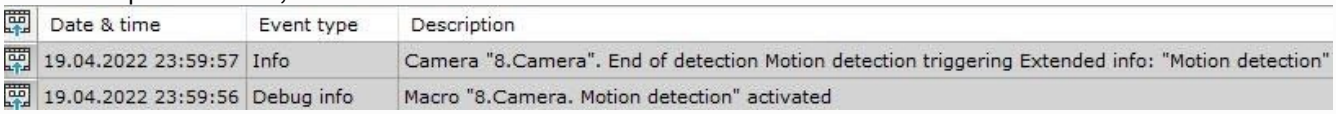
The actions of all system users are recorded in the system log (see The System Log(see page 819)).

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 detection"
19.04.2022 23:59:56	Debug info	Macro "8.Camera. Motion detection" activated

15.6.1 Types of user permissions to hardware, archives and macros

In *Axxon One*, it is possible to set user permissions both for a specific device 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(see page 201)).	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

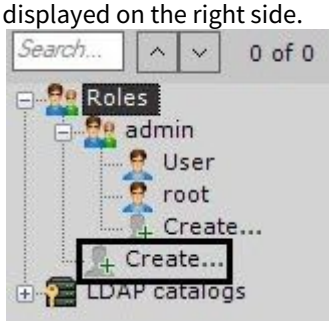
152 https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

15.6.2 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.



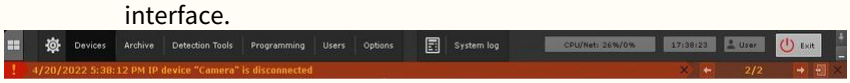
2. Configure the access permissions.

Role		
	Basic	
1	Name	Role
	Map control	
2	Map management	No access
	Access to Functions	
3	Access to confidential comments	Yes
	Access to Search in archive mode	Yes
	Adding camera to layout in monitoring mode	Yes
	Adding/editing presets	Yes
	Alarms processing	Full access
	Allow comments in archive	Create/Protect/Edit and delete
	Allow to delete records	Yes
	Allow unprotected export	Yes
	Export	Yes
	Layouts editing	Yes
	Minimize to taskbar	Yes
	Operating domain	Yes
	Permission to access via WebUI	Yes
	Show captions	Yes
	Show faces	Yes
	System log	Yes
	Unlock camera menu button	Yes
	View masked video	Yes
	Access to Interfaces	
4	Group panels	Yes
	Layouts tab	Yes
	Objects panel and Camera search panel	Yes
	Access to Settings	
5	Archive settings	Yes
	Detection settings	Yes
	Device settings	Yes
	Options settings	Yes
	Programming setup	Yes
	Show error messages	Yes
	User Permission settings	Yes
	Additional	
6	Comment	
	Supervisor confirmation	
7	Supervisor for access to export	
	Supervisor for authorization in client	
	Time schedule management	
8	Time schedule	

Expand the table with access permission settings

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
Access to Functions		Set access permissions to *Axxon One* functions (**3**)
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(see page 721))
	No	
Adding camera to layout in monitoring mode	**Yes**	Add a camera to a layout in live video mode (see Adding cameras to cells(see page 479))
	No	
Adding/editing presets	**Yes**	Add and edit presets for PTZ cameras (see Selecting a preset(see page 679))
	No	
Alarms processing	–	Alarms management (see Video surveillance in alarm management mode(see page 714))
	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(see page 667)) and protected records (see Protecting video footage from FIFO overwriting(see page 228))
	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(see page 704))
	No	

Parameters	Access level	Description
Allow unprotected export	**Yes**	Export frames and video recordings without password protection (see Frame export(see page 808), Standard video recordings export(see page 809)). Set **No** to require setting a password when exporting (see Exporting frames and video recordings(see page 808))
	No	
Export	**Yes**	Export frames and video recordings (see Exporting frames and video recordings(see page 808))
	No	
Layouts editing	**Yes**	Edit layouts (see Editing layouts(see page 473))
	No	
Minimize to taskbar	**Yes**	Minimize the Client to the tray (see Interface of the Axxon One Software Package(see page 56))
	No	
Operating domain	**Yes**	Manage Axxon domain (see Axxon Domain operations(see page 108))
	No	
Permissions to access via WebUI	**Yes**	Access to the Web-Server (see Working with Axxon One through the Web-Client(see page 823))
	No	
Show captions	**Yes**	Display captions (see Viewing titles from POS terminals(see page 670))
	No	
Show faces	**Yes**	Showing faces (see Masking faces(see page 526))
	No	
System log	**Yes**	View the system log (see The System Log(see page 819))
	No	
Unlock camera menu button	**Yes**	Context menu of a video camera (see Viewing Tile Context Menu(see page 630))
	No	
View masked video	**Yes**	View masked video (see Setting up privacy masking in Video Footage(see page 527), Specific settings for People masking detection tool(see page 382))
	No	
Access to Interfaces		Configure the access permissions to the interfaces (**4**)
Group panels	**Yes**	Configure the access permissions to video camera groups in the **Hardware** tab and to the video camera groups in the **Layouts** interface
	No	
Layouts tab	**Yes**	Configure the access permissions to the **Layouts** tab. This parameter applies to both the Client and the Web-Client (see Web-Client GUI(see page 826))
	No	
Objects panel and Camera search panel	**Yes**	Configure the access permissions to the Objects panel (see Objects Panel(see page 648)) and the Camera search panel (see Camera Search Panel(see page 646))
	No	
Access to Settings		

<table>
<tr><th>Parameters</th><th>Access level</th><th>Description</th></tr>
<tr><td rowspan="10">Archive settings</td><td>Yes</td><td rowspan="10">Configure the access permissions to the Settings tabs and to the system error messages (5).
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, all users of the given role will have the rights to change only the access rights to the connected devices.
If the Programming setup is not available for the user role, the user will not be able to use the created macros until the appropriate rights are granted.
Critical error messages in the system, such as "Insufficient network bandwidth", are displayed regardless of the Show error messages setting.</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Detection settings</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Device settings</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Options settings</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Programming settings</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">Show error messages</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td rowspan="2">User Permission settings</td><td>Yes</td></tr>
<tr><td>No</td></tr>
<tr><td colspan="3">Additional</td></tr>
<tr><td>Comment</td><td>–</td><td>Specify additional information about the user, if necessary (6). If no value is specified, users can view all videos</td></tr>
<tr><td colspan="2">Supervisor confirmation</td><td>Set the parameters to apply the four-eye principle (7)</td></tr>
<tr><td>Supervisor for acccess to export</td><td>–</td><td>If the administrator has to confirm the launch of export for users of this role (see Exporting frames and video recordings(see page 808)), select the corresponding role in the list</td></tr>
<tr><td>Supervisor for authorization in client</td><td>–</td><td>If the administrator has to confirm the login of users of this role (see Starting an Axxon One Client(see page 94)), select the corresponding role in the list</td></tr>
<tr><td colspan="3">Time schedule management</td></tr>
<tr><td>Time schedule</td><td>–</td><td>If you need to grant the users in this role permissions only for a certain period of time, select a time schedule (8) from the list. These users will not be able to use their permissions outside of the selected time schedule</td></tr>
<tr><td colspan="3">Video walls management</td></tr>
<tr><td rowspan="2">Server</td><td>Yes</td><td rowspan="2">Configure the rights to manage the connected Clients' monitors by setting permissions for each Server on Axxon domain (9). A user who has management permissions for the monitors of a particular Server can manage monitors of any Client connected to that Server</td></tr>
<tr><td>No</td></tr>
</table>

3. On the **Groups** tab, configure the default permissions (**10**, see Configuring user permissions(see page 450)).

> **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.

Expand the table with default access permissions

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(see page 675))
	Low level	
	Medium level	
	High level	
	Maximum level	

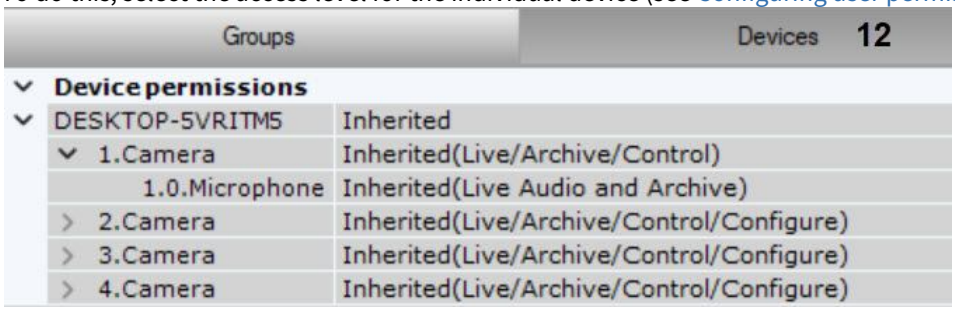
4. On the **Groups** tab, configure the group permissions if there are camera groups (**11**, see Configuring video camera groups(see page 200)).

Expand the table with group access permissions

Device	Access level	Description
Misc		Configure group access permissions to cameras (see Configuring user permissions(see page 450))

Device	Access level	Description
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, **12**).
To do this, select the access level for the individual device (see Configuring user permissions(see page 450)).



Expand the table with object access permissions

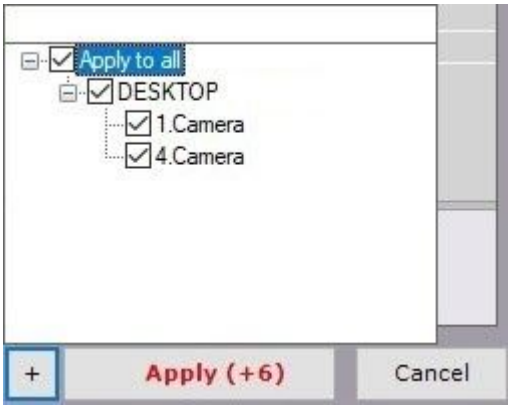
Access level	Device	Access level to device
Inherited	**Camera**	Access levels are inherited from the **Groups** tab **"Default permissions"** or from the group permissions
	Microphone	Access levels are inherited from the **Groups** tab **"Default permissions"**
	PTZ	
Archive only	**Camera**	Archive only
	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

Access level	Device	Access level to device
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.

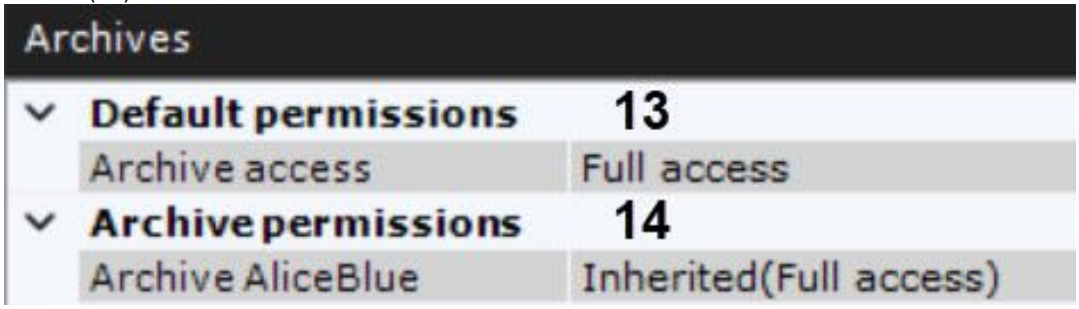
b. Click the + button and select the cameras to which you want to specify the same access level.



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 (**13**) or to a specific archive (**14**).

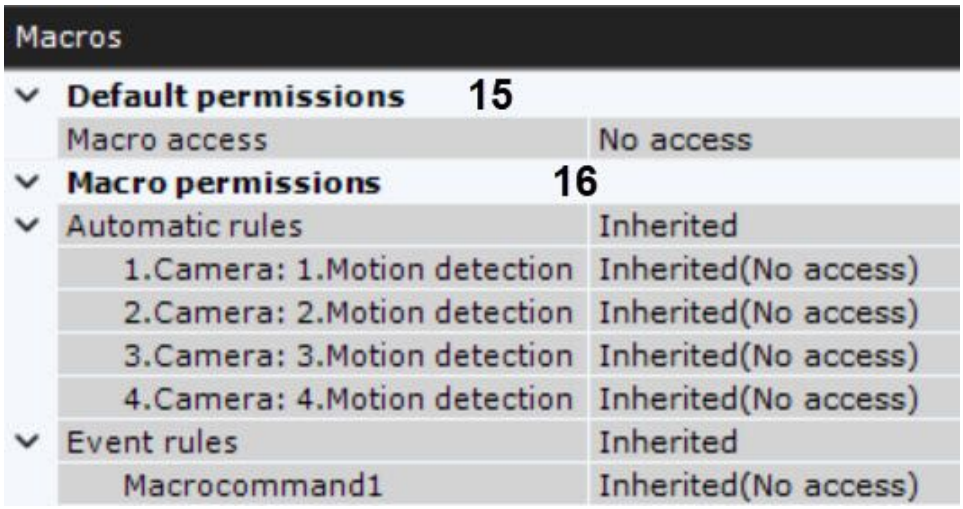


Expand the table with archive access permissions

Device	Access level	Description
Default permissions		Configure the default access permissions to the archive (see Configuring user permissions(see page 450))
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(see page 450))
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 and counters(see page 400)) 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.



Expand the table with macros access permissions

Macro type	Access level	Description
Default permissions		Configure the default permissions to macros (**15**, see Configuring user permissions(see page 450))
Macro access	**No access**	No access to macros
	Full access	Full access to macros
Macro permissions		Configure the access permissions to a specific macro (**16**, see Configuring user permissions(see page 450))
Automatic rules	**Inherited**	Access level is inherited from the **Default permissions** tab
	No access	No access to macros

Macro type	Access level	Description
	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.

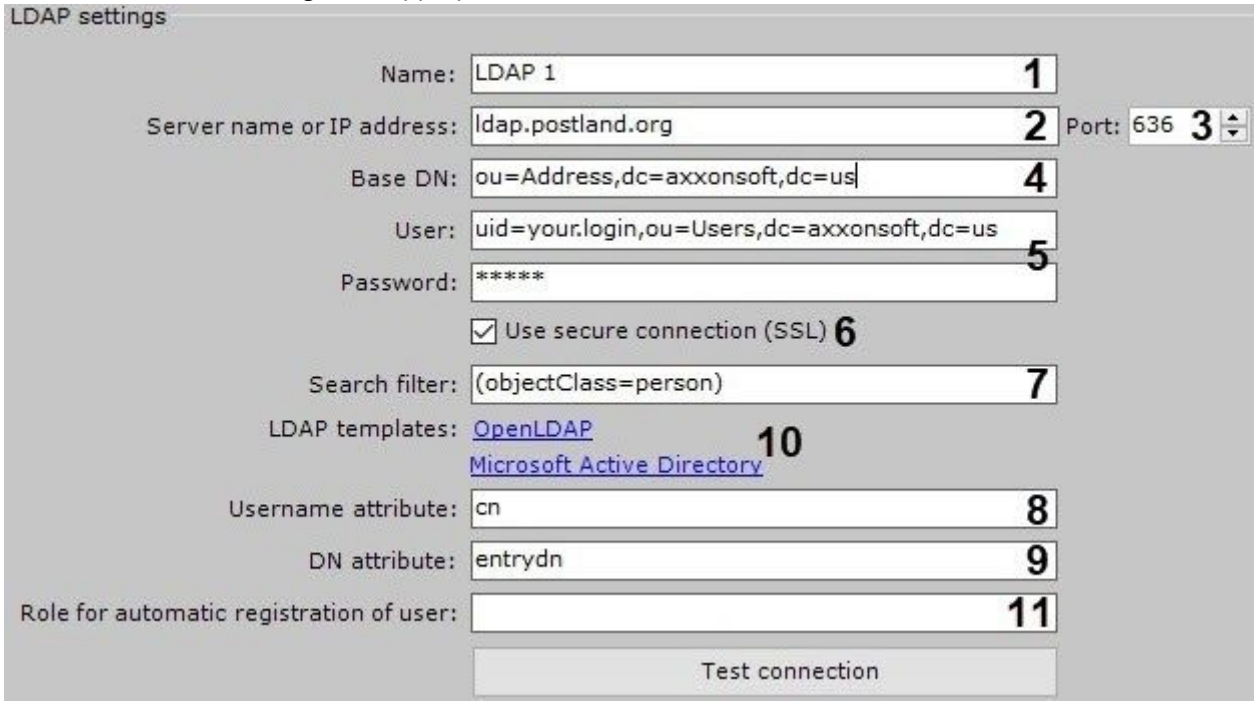
15.6.3 Connecting to an LDAP catalog

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

15.6.4 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.

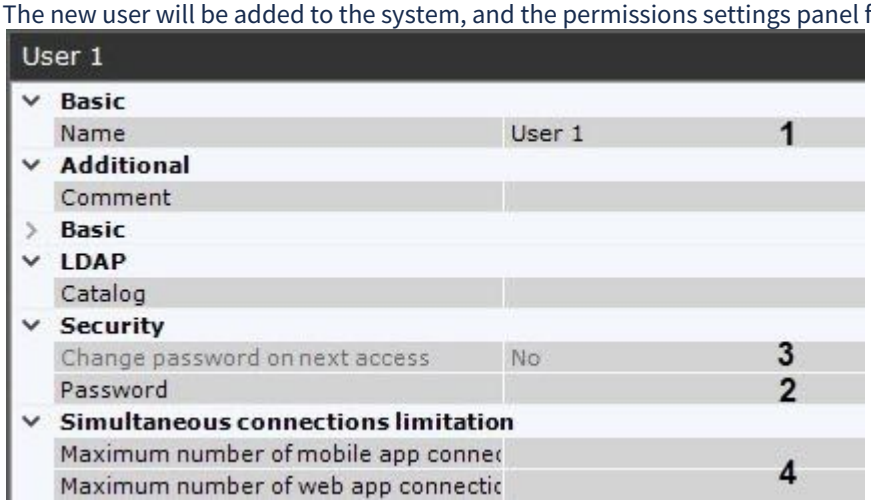
15.6.4.1 Creating local users

15.6.4.1.1 Registering local users

To register a local user, do the following:

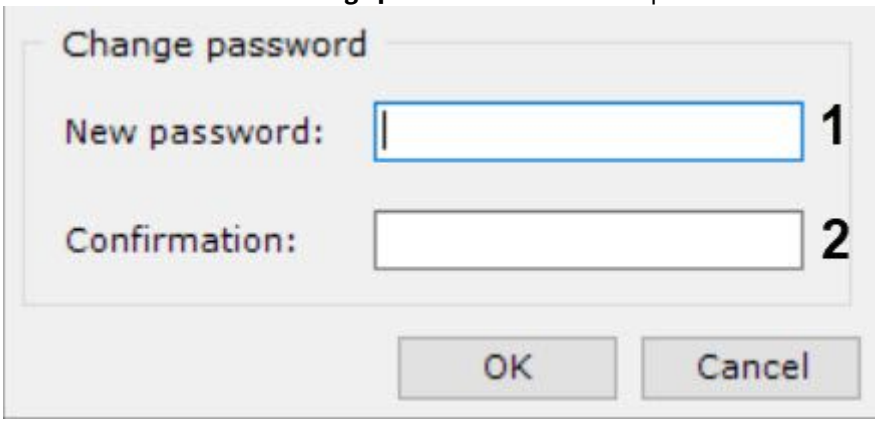
1. Click the **Create** link at the end of the list of a role to which you want to add a user.

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(see page 469)

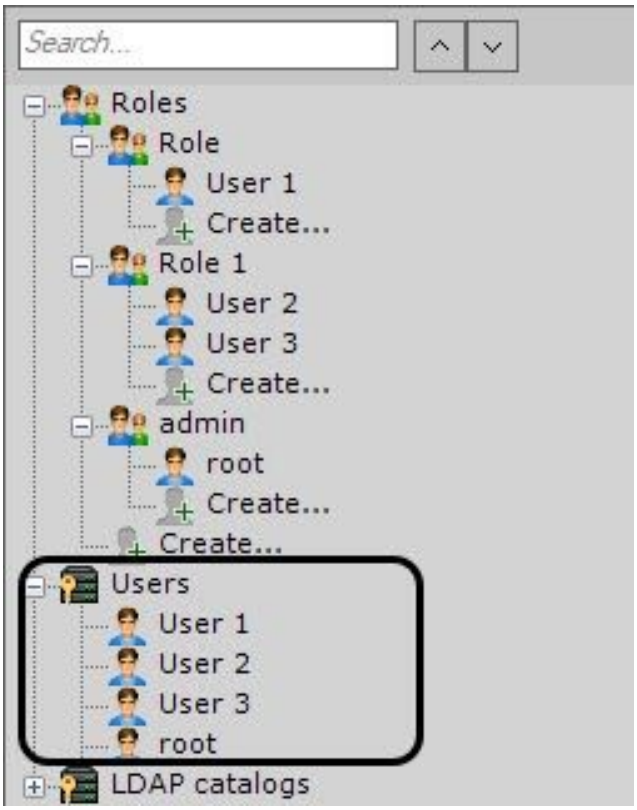
   c. In the **Confirmation** field (**2**), reenter the password.
   d. Click the **OK** button to save the settings.
4. In order for the user to change the password upon the next connection to the Client, set the corresponding parameter (**3**) to **Yes**.
5. If you want to limit the number of connections 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(see page 94)).

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.



15.6.4.1.2 Adding users to a role

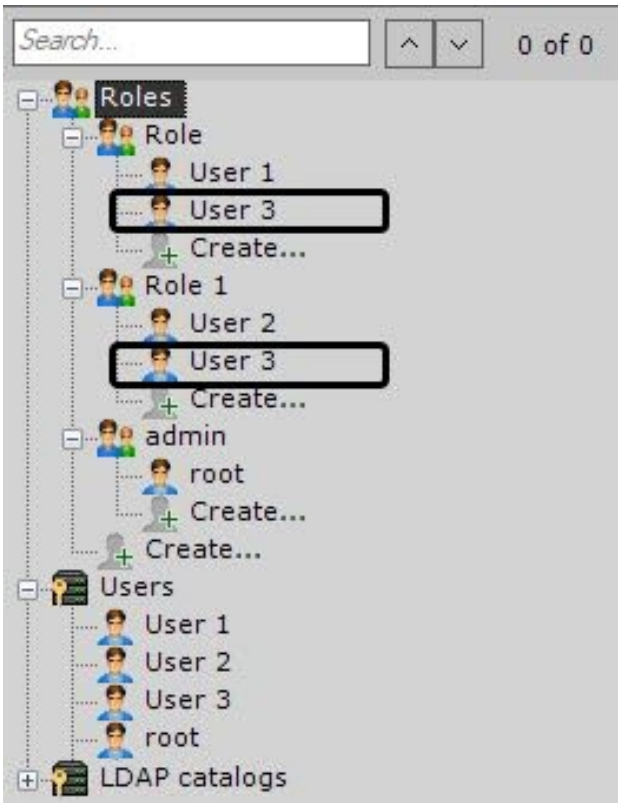
In *Axxon One*, you can add a user to several roles. To do this, do the following:

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[153].
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.

153 https://en.wikipedia.org/wiki/Drag_and_drop



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[154].
3. Click the **Apply** button.

As a result, the user will be moved from one role to another.

Configuring user permissions(see page 450)
Deleting users(see page 469)

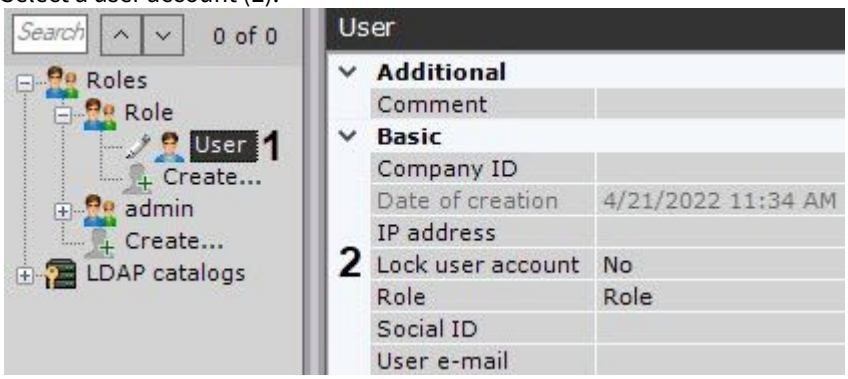
15.6.4.2 Locking a user account

You can lock user accounts to prevent unwanted logins.

To do this:

154 https://en.wikipedia.org/wiki/Drag_and_drop

1. Select a user account (**1**).



2. In the **Lock user account** field, select **Yes** (**2**).
3. Click **Apply**.

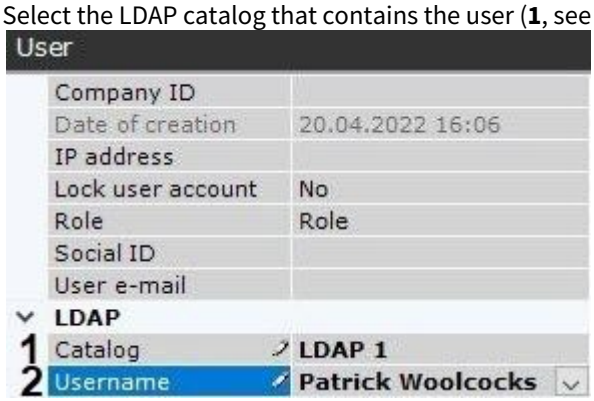
To unlock an account, select **No** in the **Lock user account** field.

15.6.4.3 Creating LDAP connections

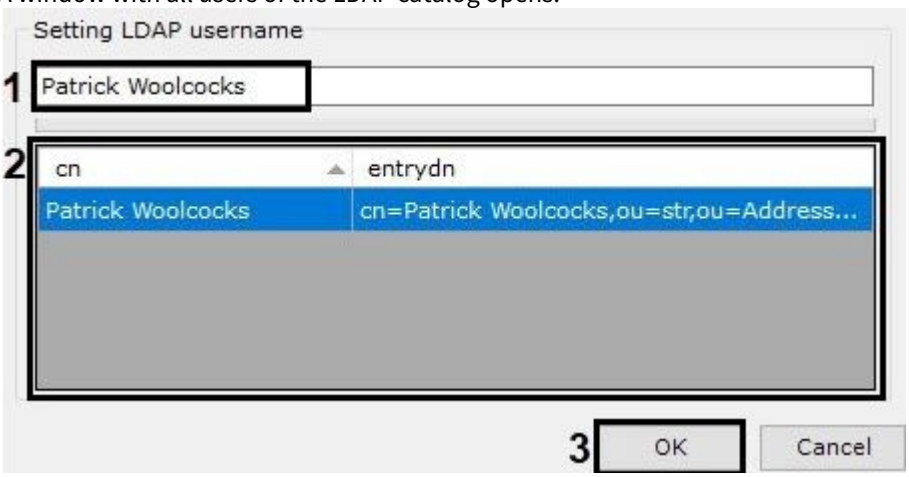
When adding an LDAP user, the user's login is selected from the specified LDAP catalog. No password is required.

To add an LDAP user:

1. Add the user to the system (see Creating local users(see page 464)).
2. Select the LDAP catalog that contains the user (**1**, see Connecting to an LDAP catalog(see page 462)).



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(see page 464)).
6. Click the **Apply** button to save the settings.

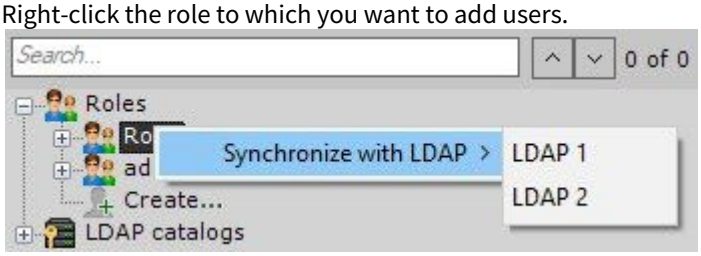
The user has now been added and assigned a role.

When an LDAP user connects, the user's login from Server settings is used with the password from the LDAP catalog.

15.6.4.4 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(see page 462)).

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.

15.6.4.5 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.

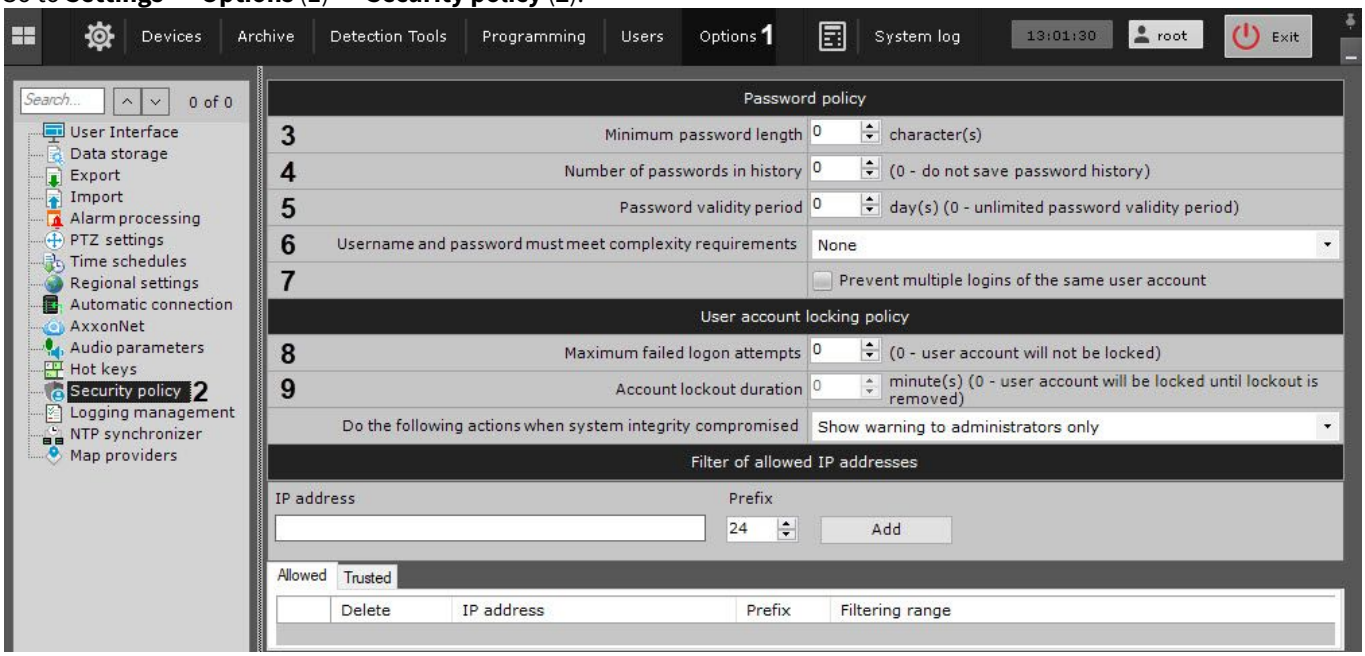
The user has now been deleted from the tree.

> **Attention!**
>
> If you delete a user account on the LDAP server, it will be automatically deleted from *Axxon One* VMS.

15.6.5 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. **0**—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.

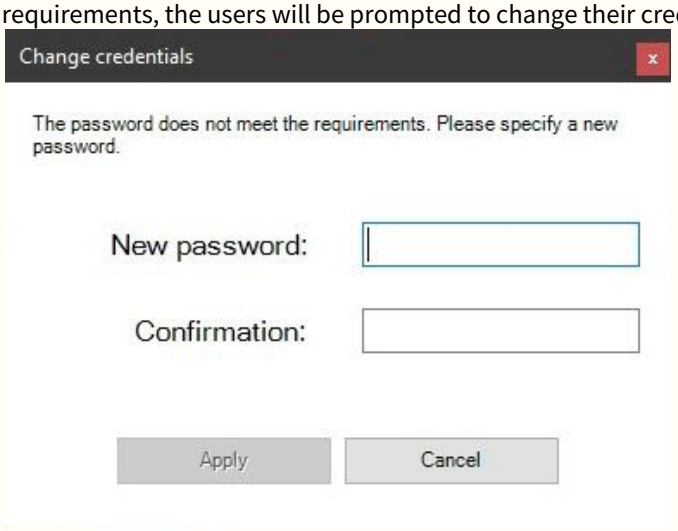
> **Attention!**
>
> When unblocked, the user is offered only one authentication attempt. A successful authentication will reset the failed attempts counter to zero, otherwise the user account will be blocked again.

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(see page 467)).
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 VMS PC integrity check fails(see page 538)
IP address filtering configuration(see page 571)

15.7 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.

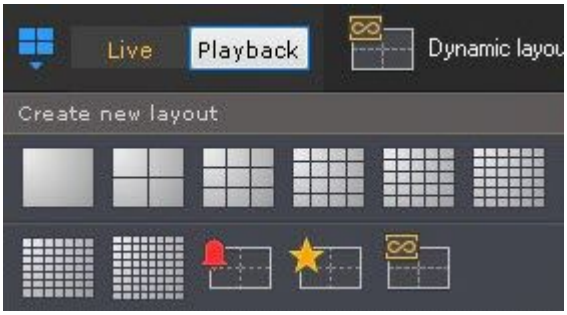
Note

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(see page 450)).

After you configure user's layouts, you may limit user's privileges.

15.7.1 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(see page 474)).

> **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(see page 648), Camera Search Panel(see page 646)).
> 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.

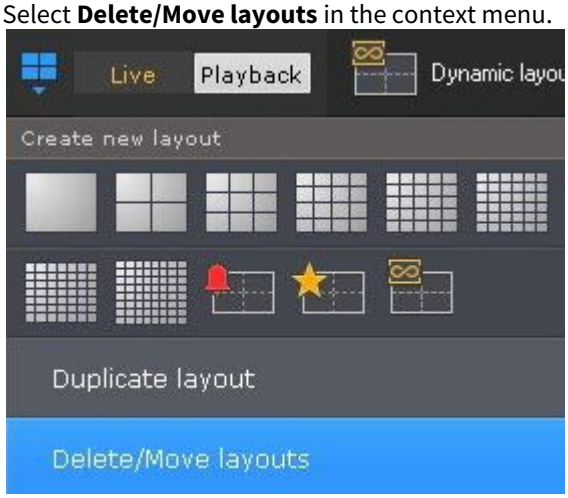
To save the layout, exit layout editing mode and save changes (see Exiting Layout Editing mode(see page 499)).

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.

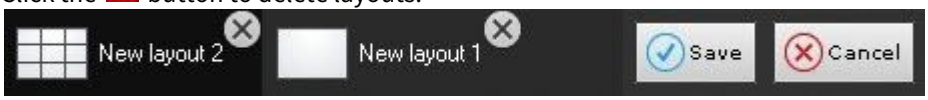
To delete layouts:

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.

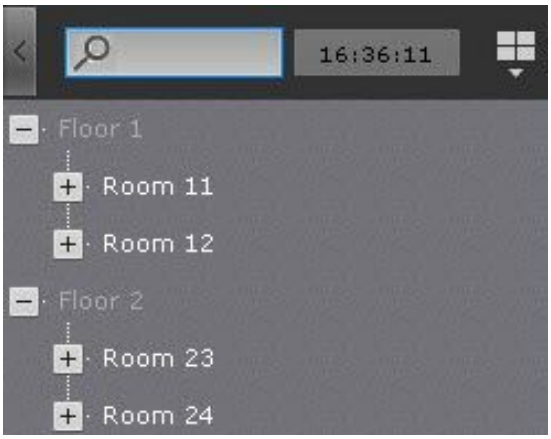
The layouts have now been deleted.

15.7.2 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(see page 648)).



15.7.3 Reorder Layouts

To reorder layouts in the ribbon:

1. Go to Manage Layouts mode (see Creating and deleting layouts(see page 471)).
2. Drag & drop layouts.
3. Click **Save**.

You have now reordered layouts.

15.7.4 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.

15.7.5 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.

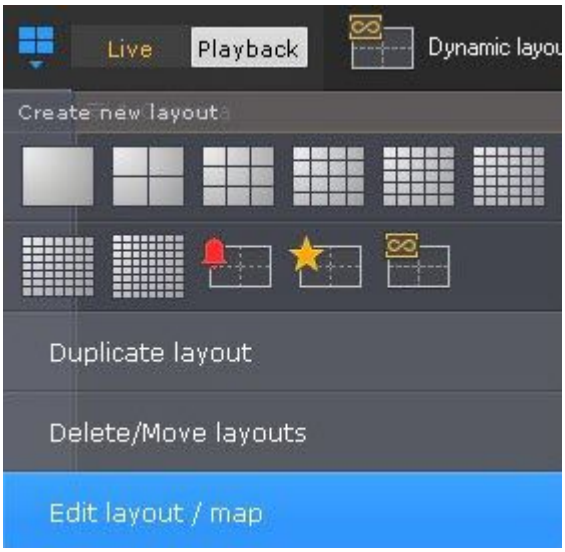
Information boards are available on the layouts panel in the editing mode.

When a camera is added to a cell, a surveillance window appears.

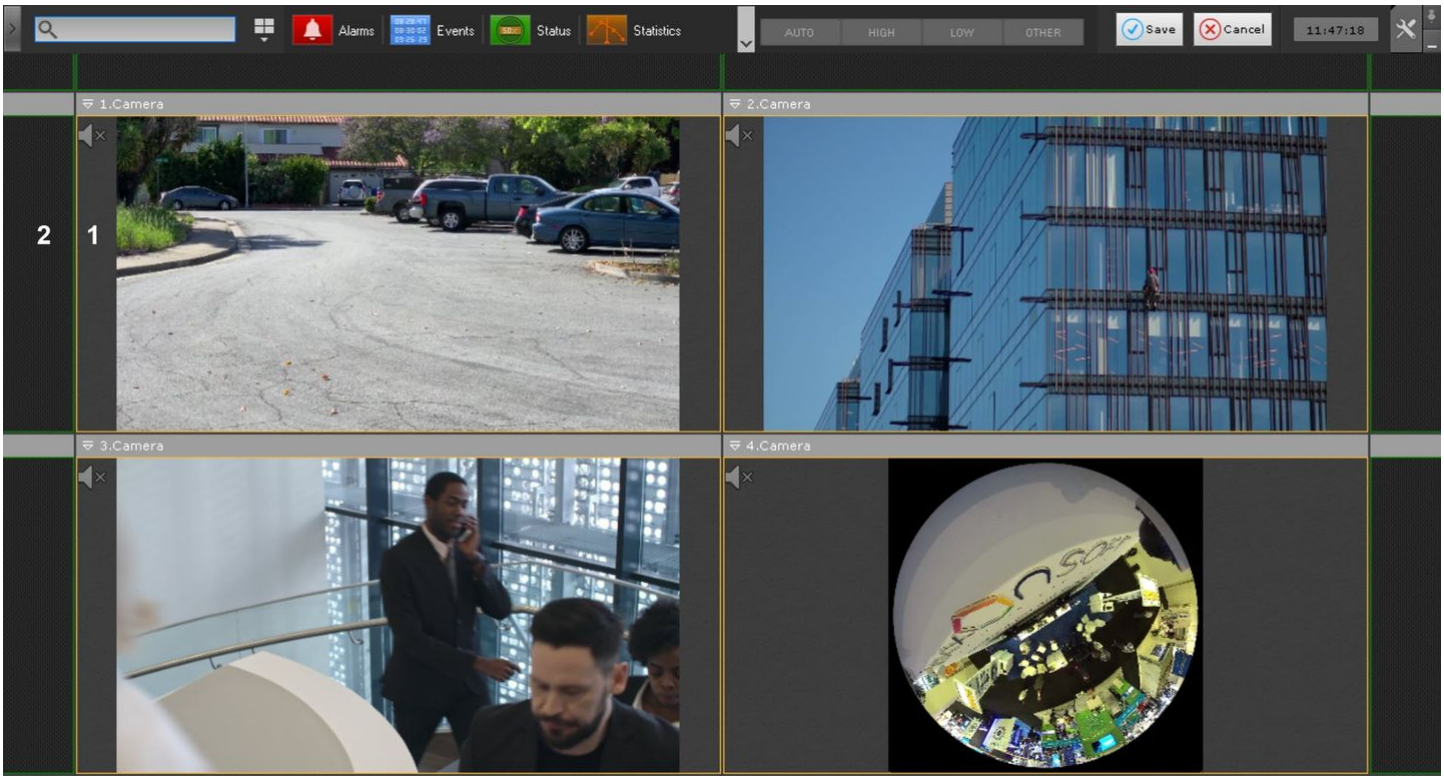
15.7.5.1 Switching to layout editing mode

You can switch to the layout editing mode either automatically when creating a new layout (see Creating and deleting layouts(see page 471)), 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(see page 450)).



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(see page 475)).

15.7.5.2 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(see page 644)).
2. Switch to the Layout Editing mode (see Switching to layout editing mode(see page 474)).

Otherwise, select a layout for editing in the layouts ribbon. You can also use Layout Editing mode to create a new layout (see Creating and deleting layouts(see page 471)) for editing.

15.7.5.3 Configuring layout cells

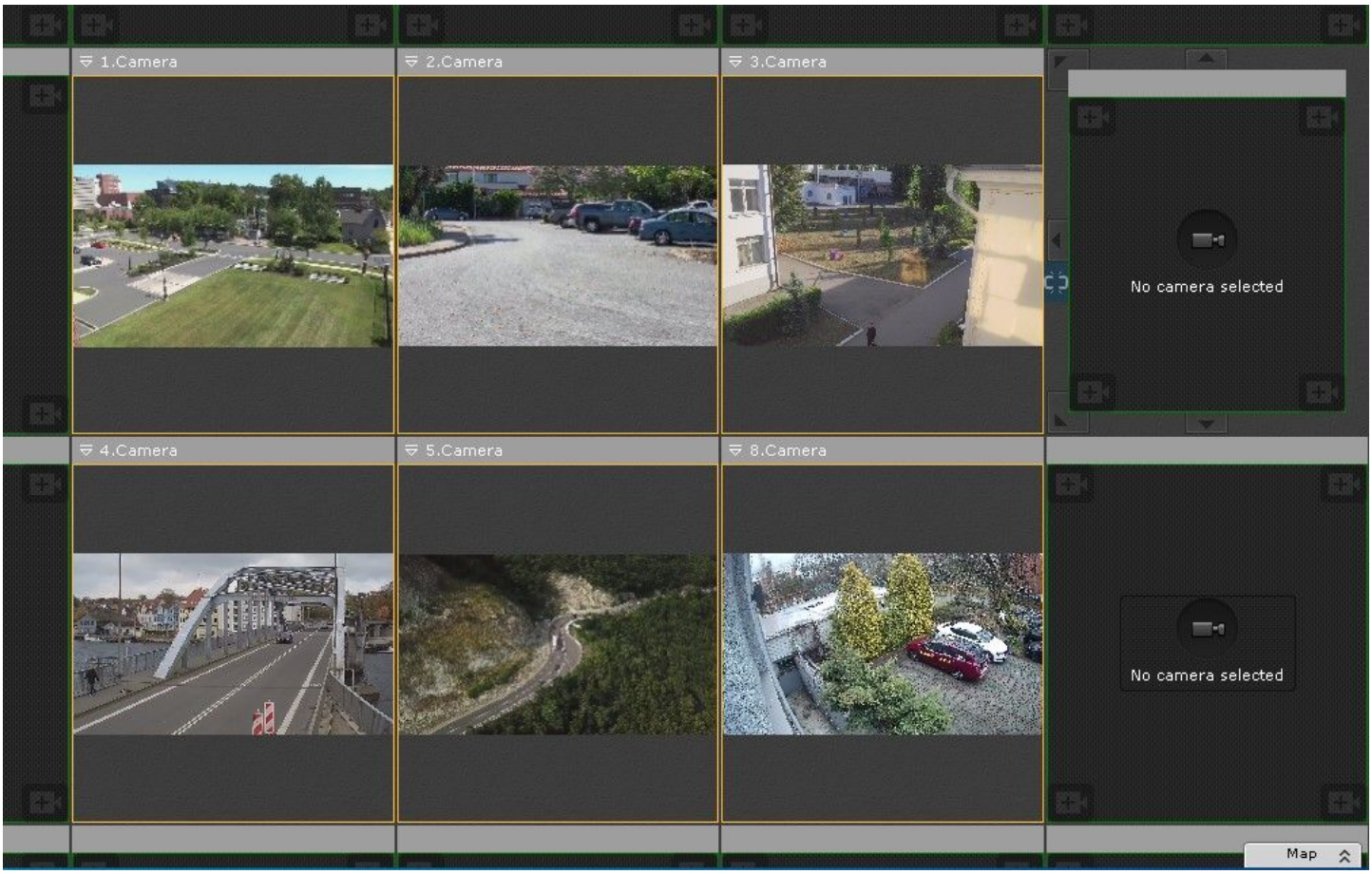
15.7.5.3.1 Adding new cells to a layout

Switching to layout editing mode(see page 474)

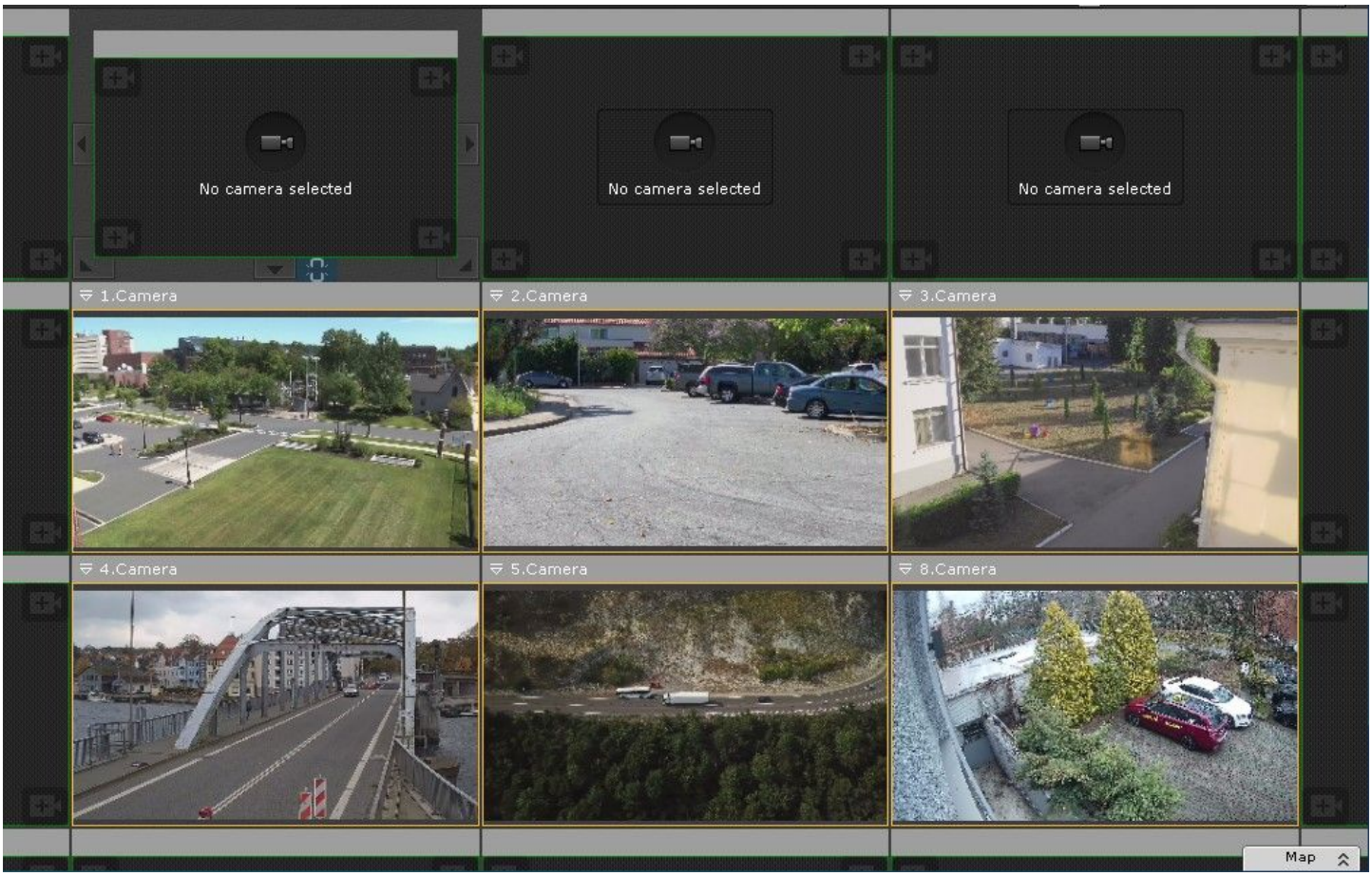
You can add new cells to a layout in one of three ways:

1. Drag a non-empty cell onto a grid square fragment (see Moving cells(see page 479)).
2. Left-click a grid square fragment and resize it (see Resizing cells(see page 478)).
3. Left-click a grid square fragment and select a video camera or information board in it (see Adding cameras to cells(see page 479)).

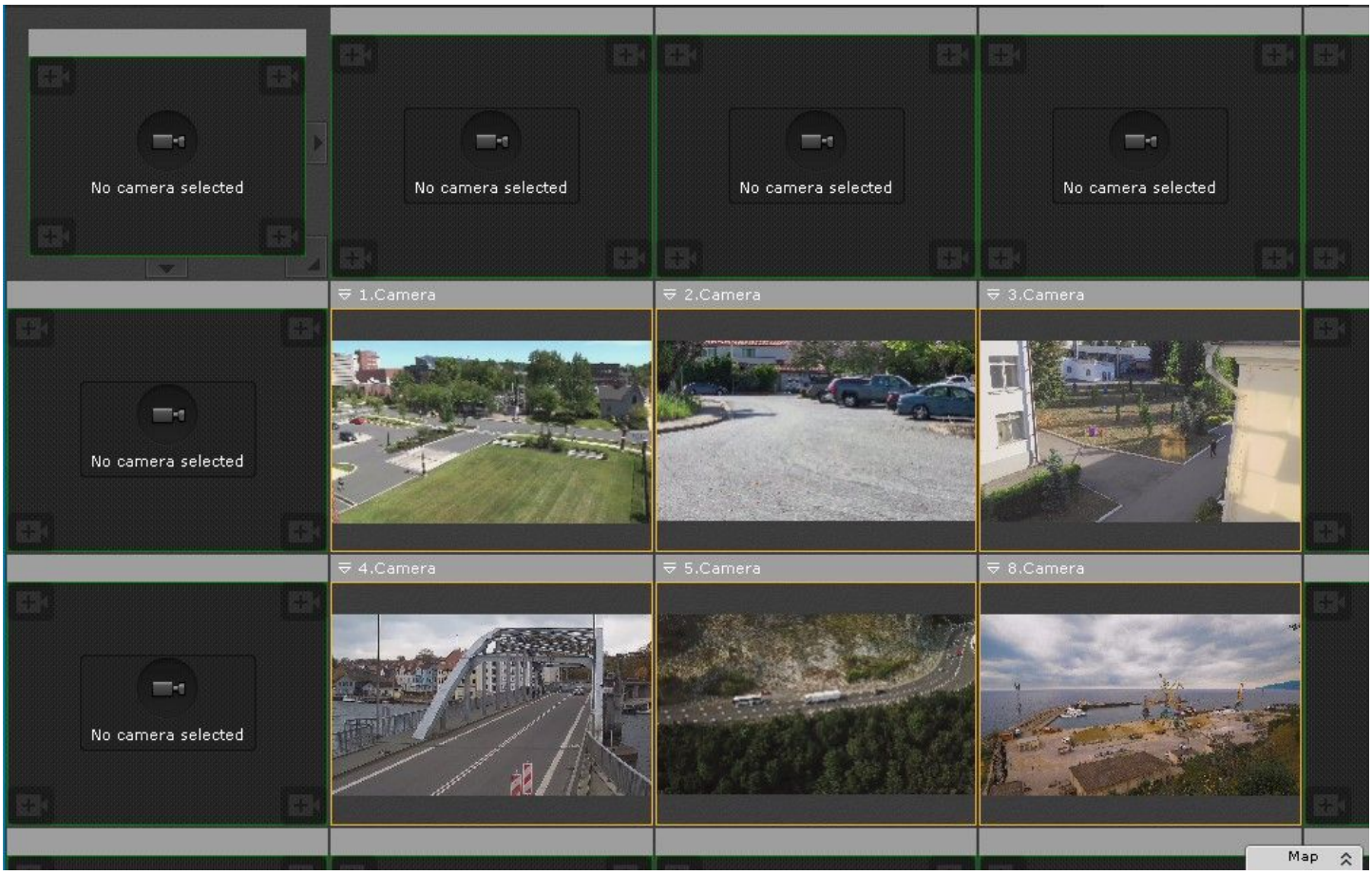
Cells are added in rows. For example, when editing a six-square (3*2) layout, a column of two grid squares is added when a fragment is chosen on the left or right side of the screen.



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.



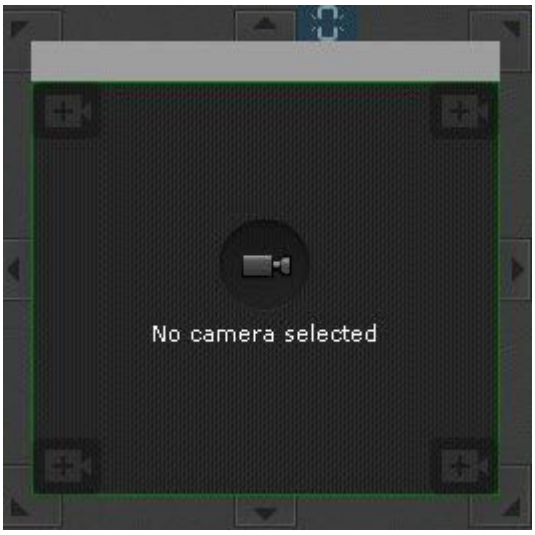
15.7.5.3.2 Resizing cells

Switching to layout editing mode(see page 474)

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.

15.7.5.3.3 Moving cells

Switching to layout editing mode(see page 474)

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(see page 475)).

15.7.5.3.4 Adding cameras to cells

Switching to layout editing mode(see page 474)

There are two ways to add a video camera to a cell:

1. Using the **Objects Panel**.
2. Using the **Camera Search Panel**.

A video camera can be added to an empty cell or to a cell containing an information panel or another video camera.

Note

Cameras from any Axxon domain can be added to the layout.

Note

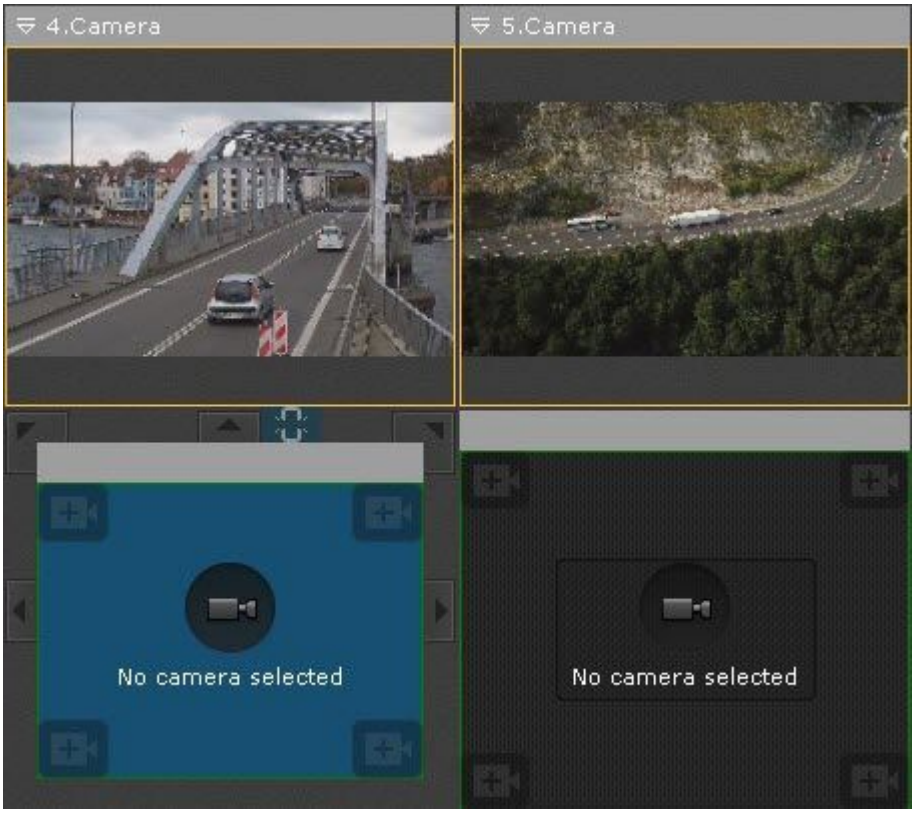
The same video camera can be added to several cells of the same layout.

Adding a video camera using the Objects Panel

To add a video camera using the **Objects Panel**, perform the following steps:

1. Switch the cell to the active mode (with a mouse click).
2. Click a video camera in the **Objects Panel** (see Objects Panel(see page 648)).

You can drag&drop cameras to a cell too. The empty cell with the cursor in it, is highlighted when you drag the camera.



To add multiple cameras to a layout, do the following:

1. In the objects pane, shift-click several cameras to select.
2. Left-click on any selected camera.
3. Drag the icon onto the layout.
4. Release the mouse button.

You can use the **Object Panel** for adding all cameras within a group/Axxon domain to the layout. To do it, follow the steps below:

1. Left click on the group/Axxon domain in the panel.
2. While keeping the mouse button pressed, move the cursor to the layout.
3. Release the mouse button.

Adding a video camera using the Camera Search Panel

To add a video camera to a cell, perform the following steps:

1. Switch the cell to the active mode with a mouse click and select a video camera from the list in the **Camera Search Panel** (see Camera Search Panel(see page 646)).
2. Select a video camera from the list in the **Camera Search Panel** with the mouse pointer and, holding down the mouse button, move the pointer into a cell. Then release the button.

15.7.5.3.5 Adding information boards to cells

Switching to layout editing mode(see page 474)

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.

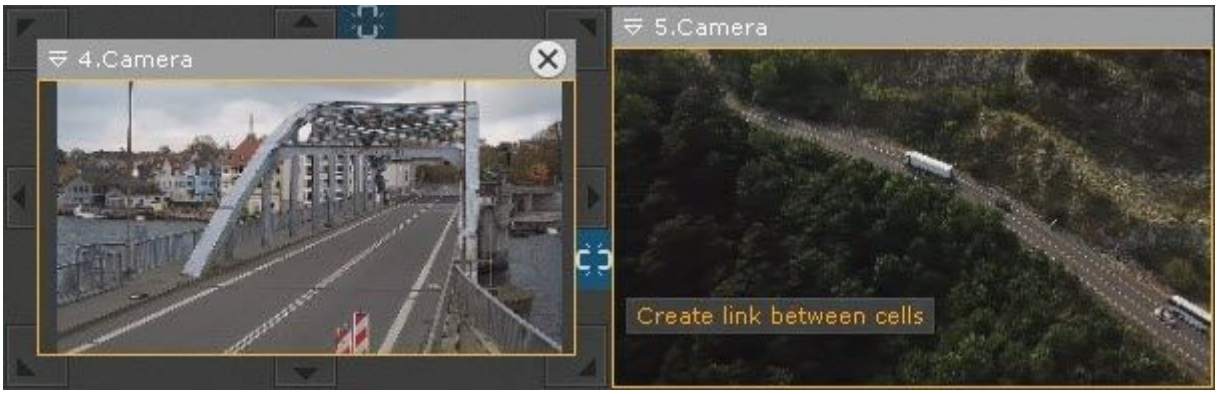
Note

After you add an information board to the cell, you should configure it (see Configuring information boards(see page 489)).

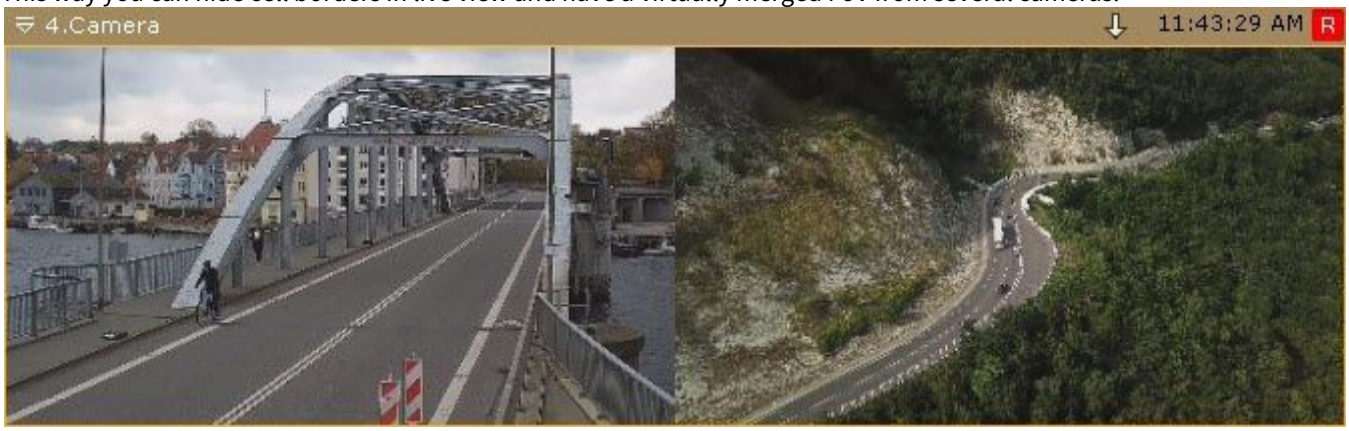
15.7.5.3.6 Linking cells

Switching to layout editing mode(see page 474)

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(see page 774)).
3. Also, you can link 2 information panels or empty cells to panels (see Configuring Alarmed cameras layout(see page 502)).

All linked cells have a different scaling logic (see Scaling the surveillance window(see page 654)).

15.7.5.3.7 Merging videos from adjacent cameras (FrameMerge)

Switching to layout editing mode(see page 474)

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.

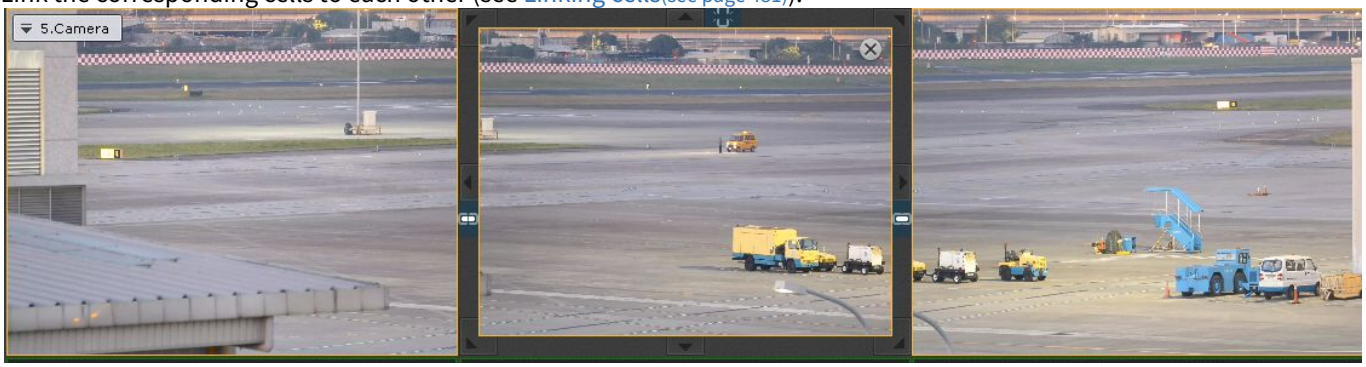
For best results in merging, ensure the following:

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.

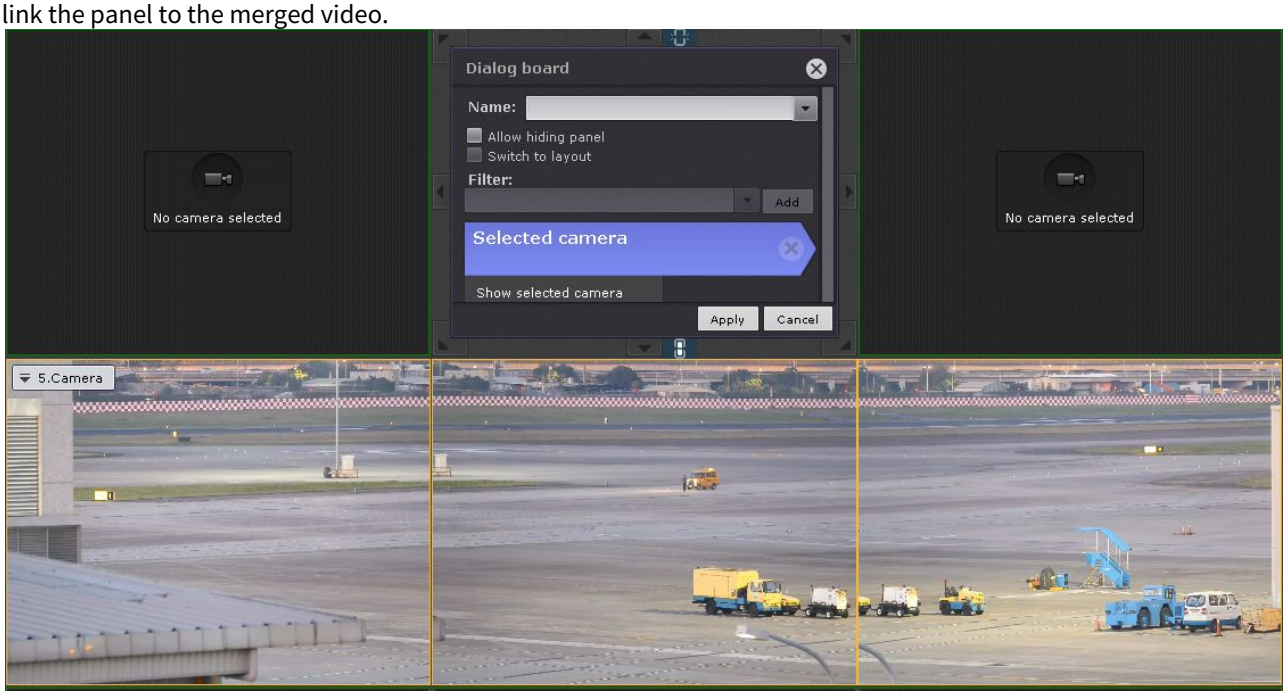
To configure video merging, do the following:

1. Place the cameras horizontally within the layout.
2. Link the corresponding cells to each other (see Linking cells(see page 481)).



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(see page 495));
   b. configure the panel to display the selected camera;

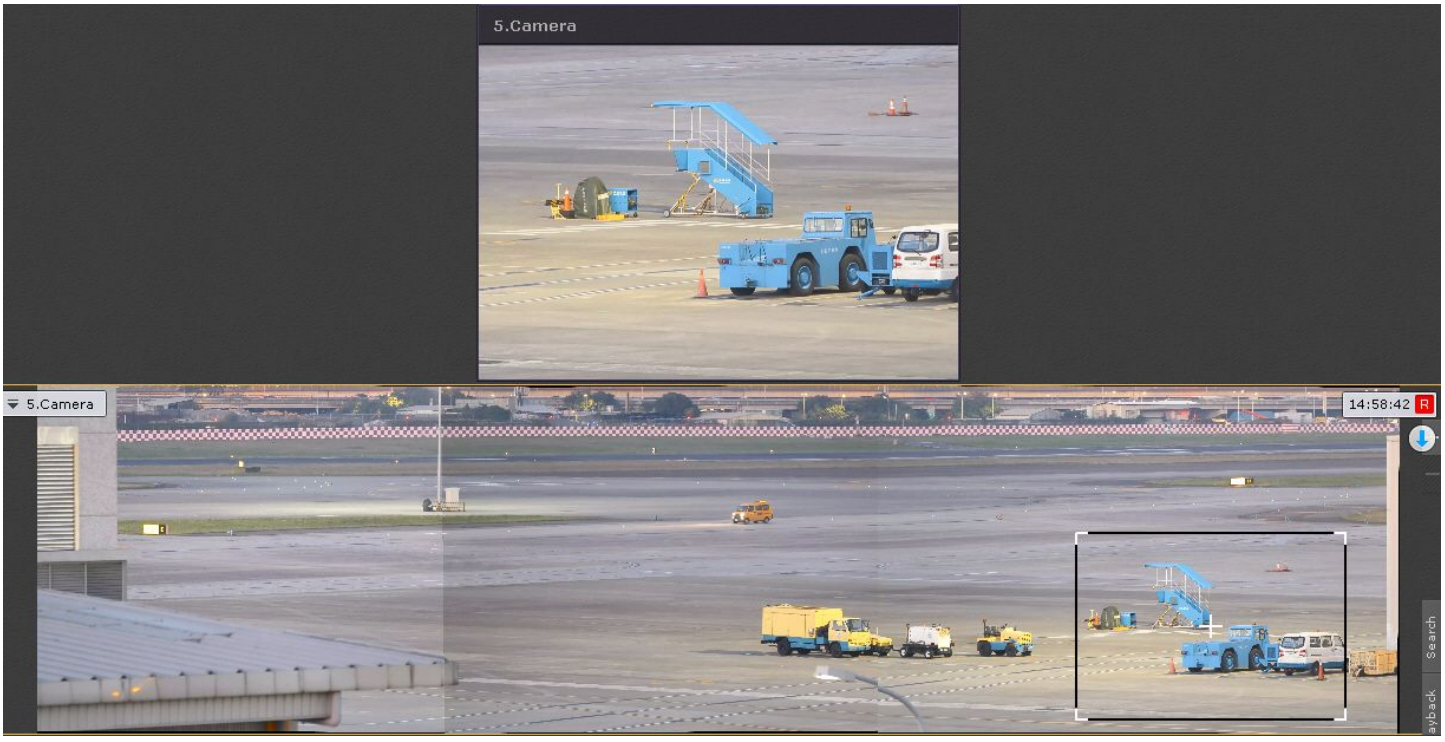
c. link the panel to the merged video.



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(see page 684)), 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.

15.7.5.3.8 Clearing cells

Switching to layout editing mode(see page 474)

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.

15.7.5.4 Configuring viewing tiles

15.7.5.4.1 Selecting default functions for viewing tiles

Switching to layout editing mode(see page 474)

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(see page 690), Tracking objects(see page 663), Autozoom(see page 691), Video image processing(see page 657), Selecting viewing mode for videos from a fisheye camera(see page 761)) and save changes before exiting the mode.

15.7.5.4.2 Selecting the default video stream for all cameras on the layout

Switching to layout editing mode(see page 474)

You can select the defaut video stream (see The Camera object(see page 122)) for all video cameras on the layout on the top panel:

- **Auto**—use GreenStream technology. A low-quality video stream is used by default. When you select a surveillance window, the video stream is switched to a high-quality video stream. When you select another camera, the video stream is switched back to a low-quality.
- **High**—use a high-quality video stream.
- **Low**—use a low-quality video stream.
- **Other**—use a specific video stream of a video camera.

15.7.5.4.3 Selecting the default video mode for a camera

Switching to layout editing mode(see page 474)

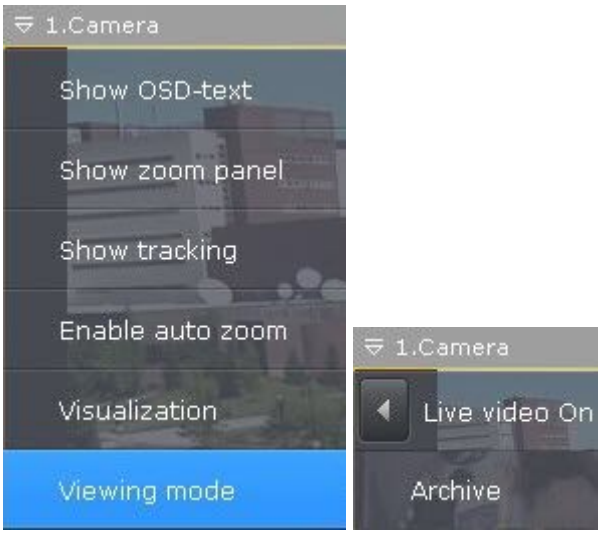
By default, when you switch to a layout, all video cameras are in Real-time/Live viewing mode.

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.

15.7.5.4.4 Moving input and output icons in a viewing tile

Switching to layout editing mode(see page 474)

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.

15.7.5.4.5 Configuring default zoom levels (the Fit screen function)

Switching to layout editing mode(see page 474)

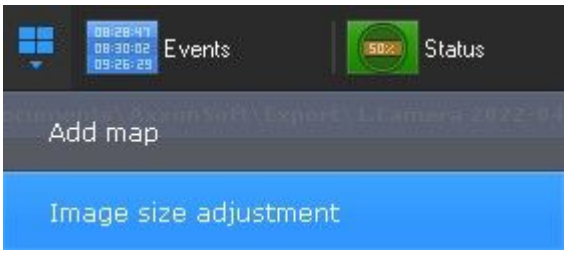
The Fit screen function allows displaying a viewing tile by default so that it occupies all of the available space on the screen (full screen). The default zoom level for full screen display is calculated automatically as a minimum zoom value thal allows filling the available screen space with the viewing tile contents.

To enable the Fit screen function for a specific video tile, display the digital zoom controller (see Digitally Zooming Video Images(see page 655)), click the button on it, and save changes when exiting editing mode.

Note

To disable the Fit screen function, click the button again.

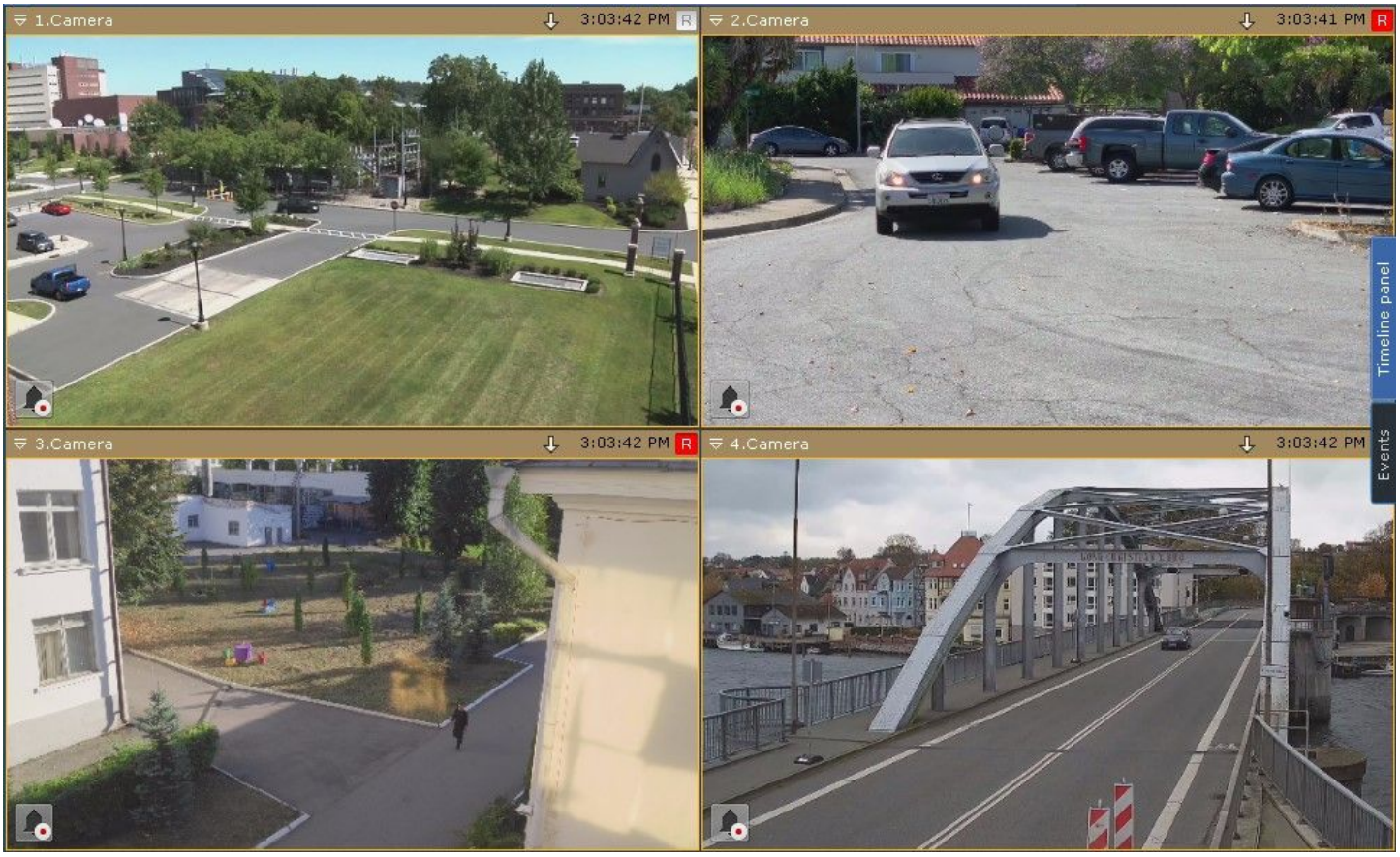
To enable the Fit screen function for all video tiles on the layout open the context menu and select **Image size adjustment**.



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.



15.7.5.4.6 Configuring pan/tilt angle for video cameras with Immervision lenses in 180o Panorama display format

Switching to layout editing mode(see page 474)

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(see page 763)).

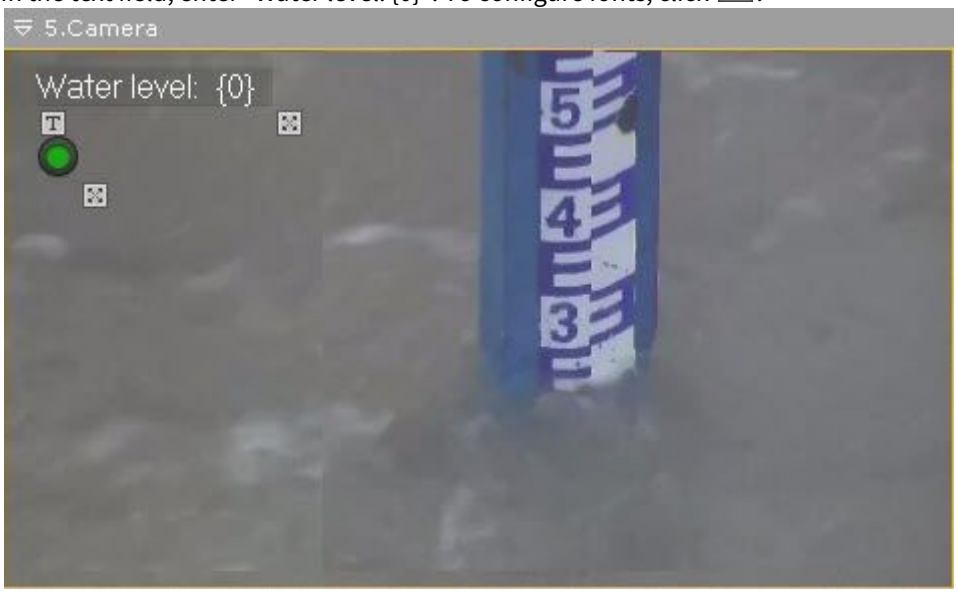
15.7.5.4.7 Configuring display of water level detection

Switching to layout editing mode(see page 474)

If you have created a water level detector for a camera (see Configuring Water level detection(see page 390)), you can see the water level sensor in the camera window.

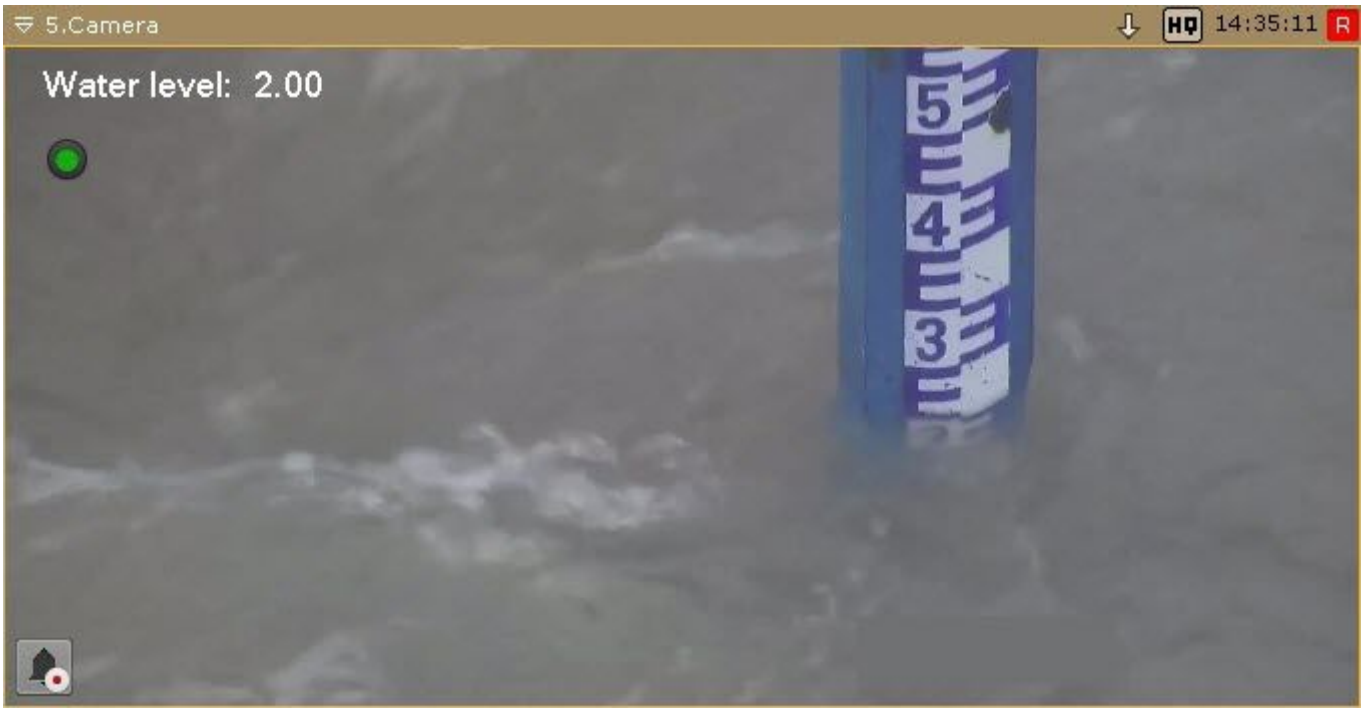
You can also display numerical value of current water levels for the detector. To do it, follow the steps below:

1. In the text field, enter "Water level: {0}". To configure fonts, click T.



2. Use buttons to scale up/down the text and the sensor icon.
3. You can move the sensor just as any other object (see Moving input and output icons in a viewing tile(see page 485)).

When the layout is saved, you see the information displayed in the camera window.



15.7.5.4.8 Adding links to other cameras to the Camera Window

Switching to layout editing mode(see page 474)

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(see page 670)).

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(see page 648)), 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[155]).

When the layout is saved, you see the newly created link in the Camera Window.

15.7.5.5 Configuring information boards

15.7.5.5.1 Configuring information board templates

> Switching to layout editing mode(see page 474)

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.

155 https://docs.axxonsoft.com/confluence/display/one1en/Moving+input+and+output+icons+in+a+viewing+tile

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.

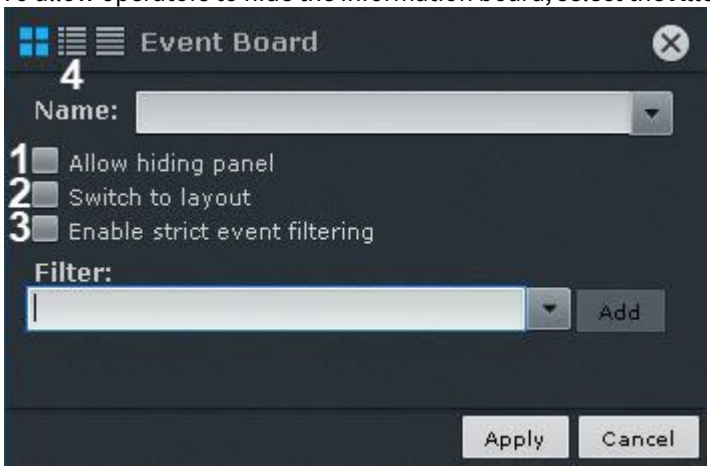
15.7.5.5.2 Configuring an Event Board

Switching to layout editing mode(see page 474)

Event Boards display some or all system events.

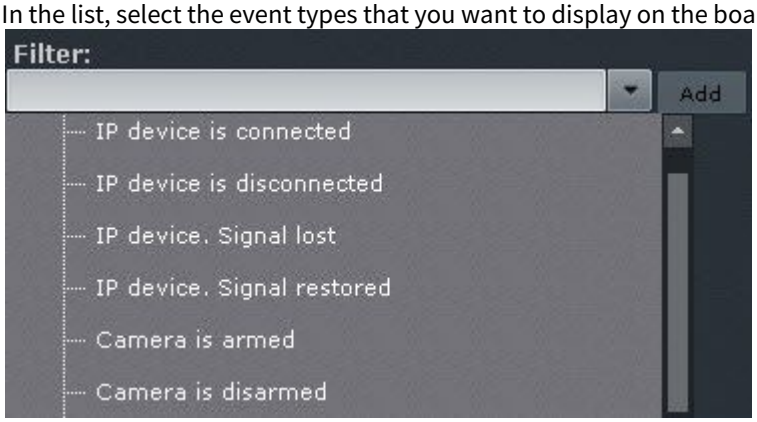
To configure an **Event Board**:

1. Add an information board to the layout (see Adding information boards to cells(see page 481)).
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. To automatically open the layout with this information board when an event matching the filter occurs, select the **Switch to layout** check box (**2**) (see paragraph 5).
   If other layouts contain information boards with the same parameters, the layout with the smallest number of cells is opened. If there are multiple layouts with identical numbers of cells, the layout that comes first in the alphabet is chosen.
   If a layout containing this information board is open when an event is received, no switch to another layout is performed.
5. 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 (**3**).

6. 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"**.

7. Select the default view for information on the **Event Board** (see Options for displaying information on Events Boards(see page 772)): the first frame of the event and time, first frame and text, or text only (**4**).
8. Click the **Apply** button to save changes.

Configuration of the **Event Board** is complete.

15.7.5.5.3 Configuring a Health Board

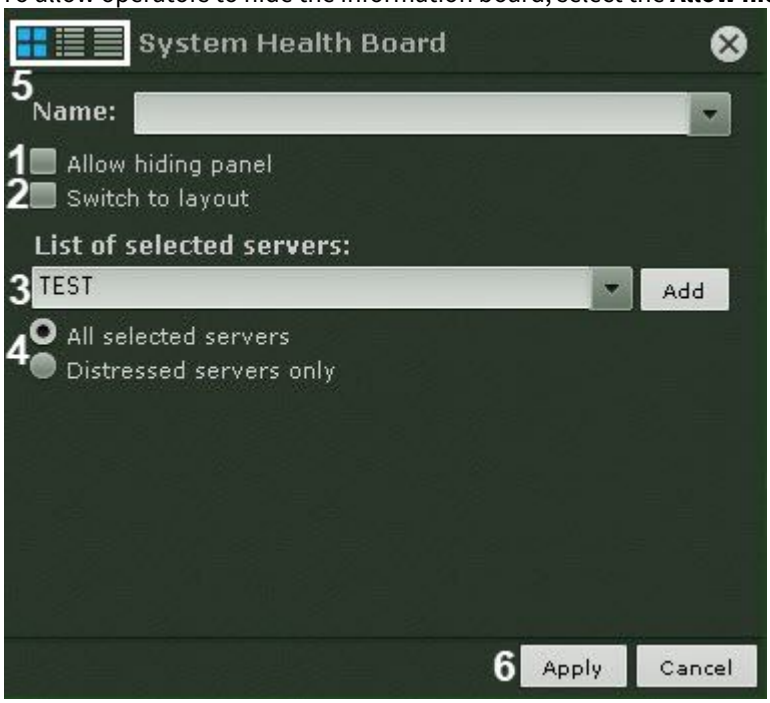
Switching to layout editing mode(see page 474)

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(see page 481)).
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. To automatically open the layout with this information board when the status of a monitored server or camera changes, select the **Switch to layout** check box (**2**) (see paragraphs 5 and 6).
   If other layouts contain information boards with the same parameters, the layout with the smallest number of cells is opened. If there are multiple layouts with identical numbers of cells, the layout that comes first in the alphabet is chosen.
   If a layout containing this information board is opened when an event is received, no switch to another layout is performed.
5. 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**) (**4**) and click the **Add** button.

   > **Note**
   >
   > To remove the selected server, click the button.

6. To display the status of only distressed servers out of those selected, select **Distressed servers only** (**4**).
   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(see page 774).

7. Select the default view for display of information on the Health Board (see Working with System Health Boards(see page 774)): diagram, diagram with text, or table (**5**).
8. Click the **Apply** button to save changes (**6**).

Configuration of the Health Board is complete.

15.7.5.5.4 Configuring a Statistics Board

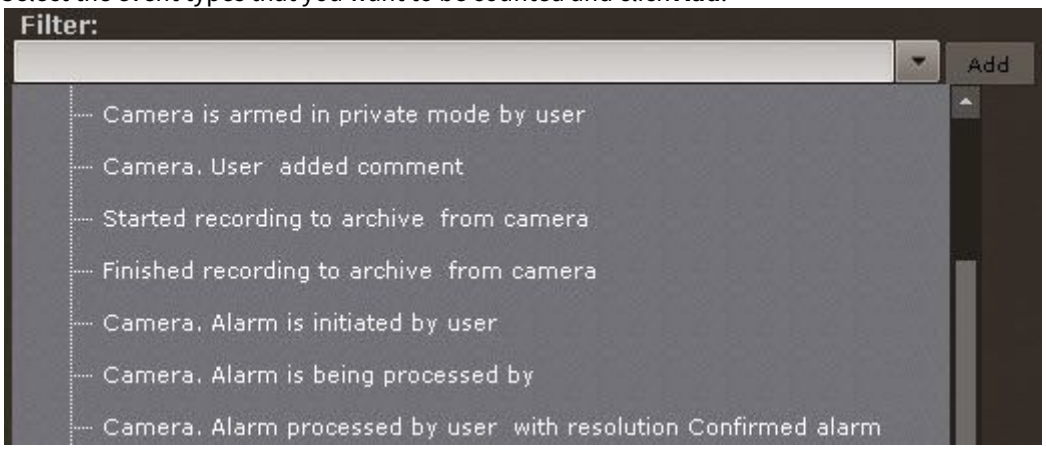
Switching to layout editing mode(see page 474)

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(see page 481)).
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.

15.7.5.5.5 Configuring a Web Board

Switching to layout editing mode(see page 474)

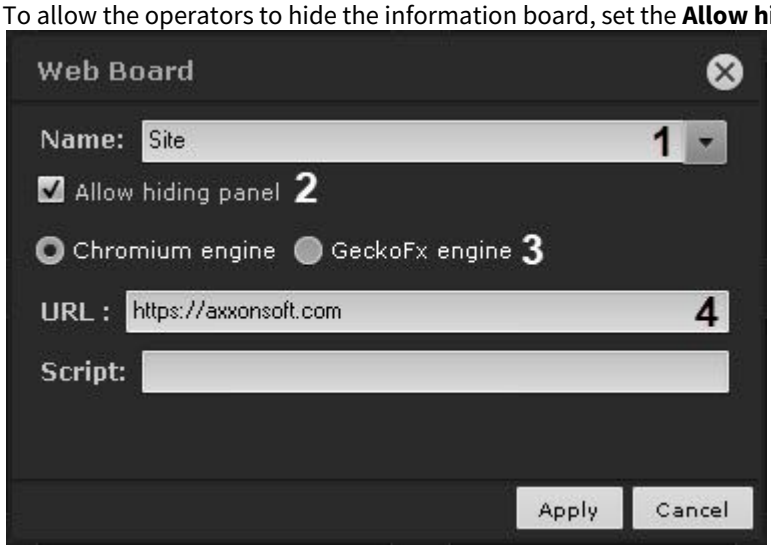
The **Web Board** allows you to view a specific web page on the layout.

> **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(see page 481)).
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**).

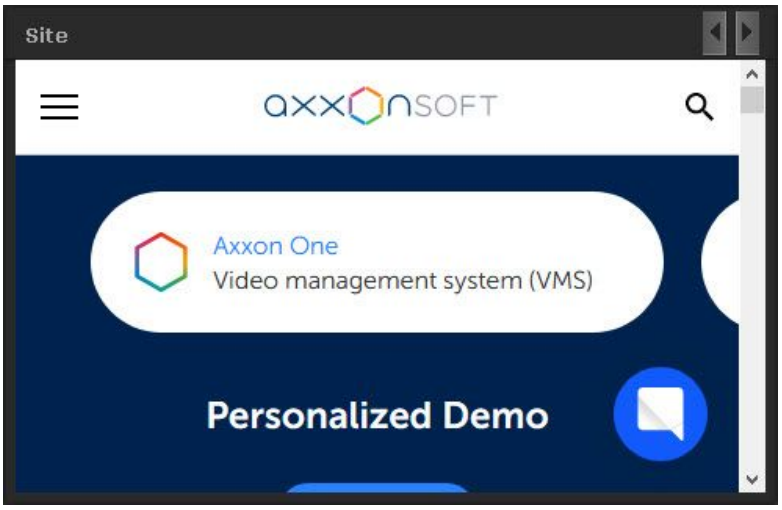


5. Select the web page output: Chromium or Gecko (**3**).
6. Enter the address in the **URL** field (**4**).

> **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**.



15.7.5.5.6 Configuring a Dialog Board

Switching to layout editing mode(see page 474)

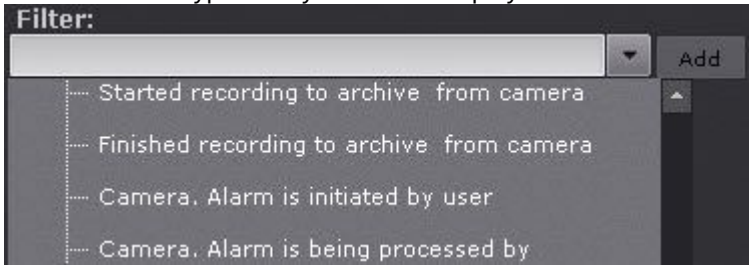
Dialog board allows users to view info about alerts/detection events and quickly start macros to respond.

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(see page 481)).
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 **Switch to layout** check box (**2**) (see paragraph 5) to automatically open the layout with this information board when an event matching the filter occurs.
If other layouts contain information boards with the same parameters, the layout with the smallest number of cells is opened. If there are multiple layouts with identical numbers of cells, the layout that comes first in the alphabet is chosen.
If a layout containing this information board is opened when an event is received, no switch to another layout is performed.
5. Select the event types that you want to display on the board and click **Add**.


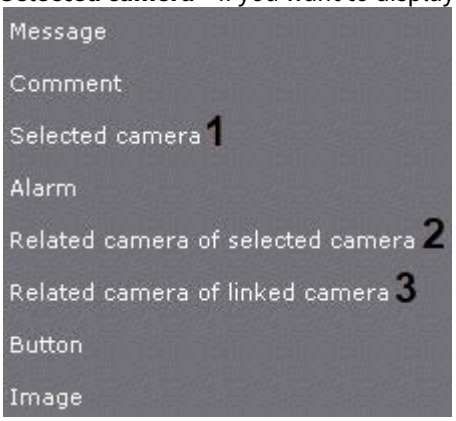
To add events of the same type from different devices, enter the name of the event in the **Filter** field. This will list only the events of the chosen type. To list all events, clear the filter field.

> **Note**
>
> To remove an added event type, click the button.

> **Note**
>
> If the board has video, the event filter is not required.

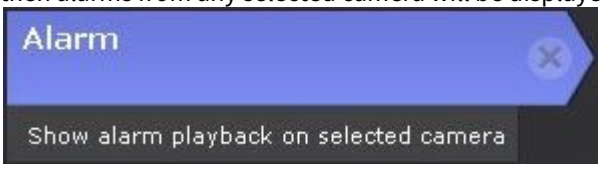
If no event type is selected, all system events are displayed on the information board.

6. 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**).



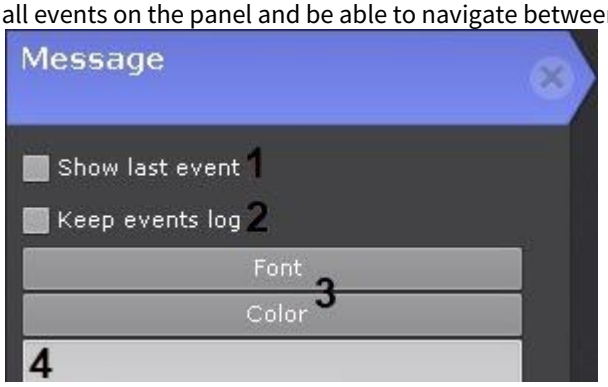
      ii. **Related camera of selected camera** – if you want to display video from the related (alternative, see The Camera object(see page 122)) camera of the selected camera (**2**).
      iii. **Related camera of linked camera** – if you want to display video from the related (alternative, see The Camera object(see page 122)) 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 (see item e below). It is color-coded as follows: green – **False alarm**, yellow – **Non-critical alarm**, red – **Critical alarm**.

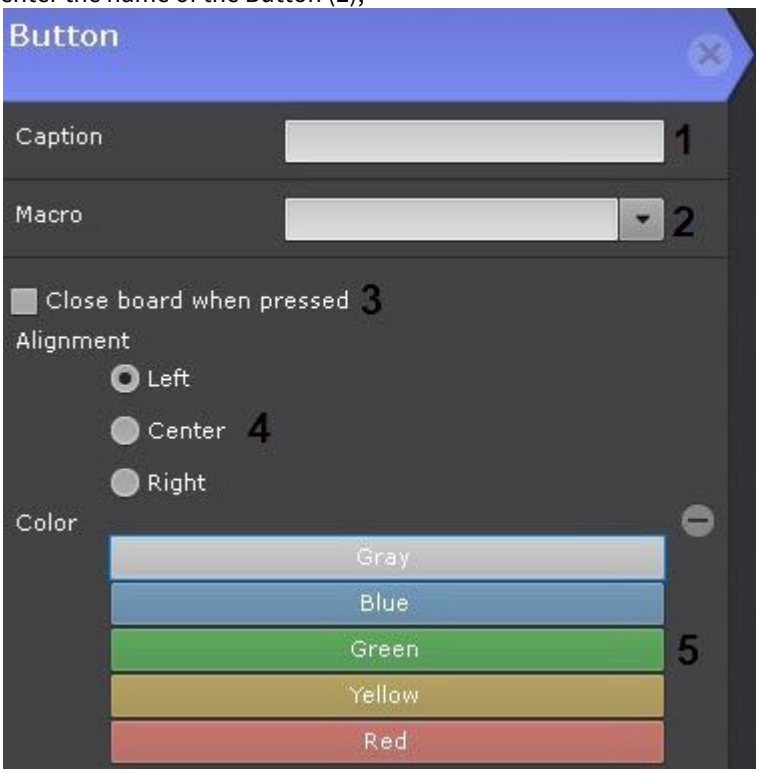
d. If necessary, add a message that will be displayed on the panel in case of event (**4**). You can select the font and color (**3**) of the message. If it is necessary to display the event text, set the **Show last event** checkbox (**1**). To keep all events on the panel and be able to navigate between 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**).

7. Click **Apply** to save the changes

Configuration of the Dialog board is complete.

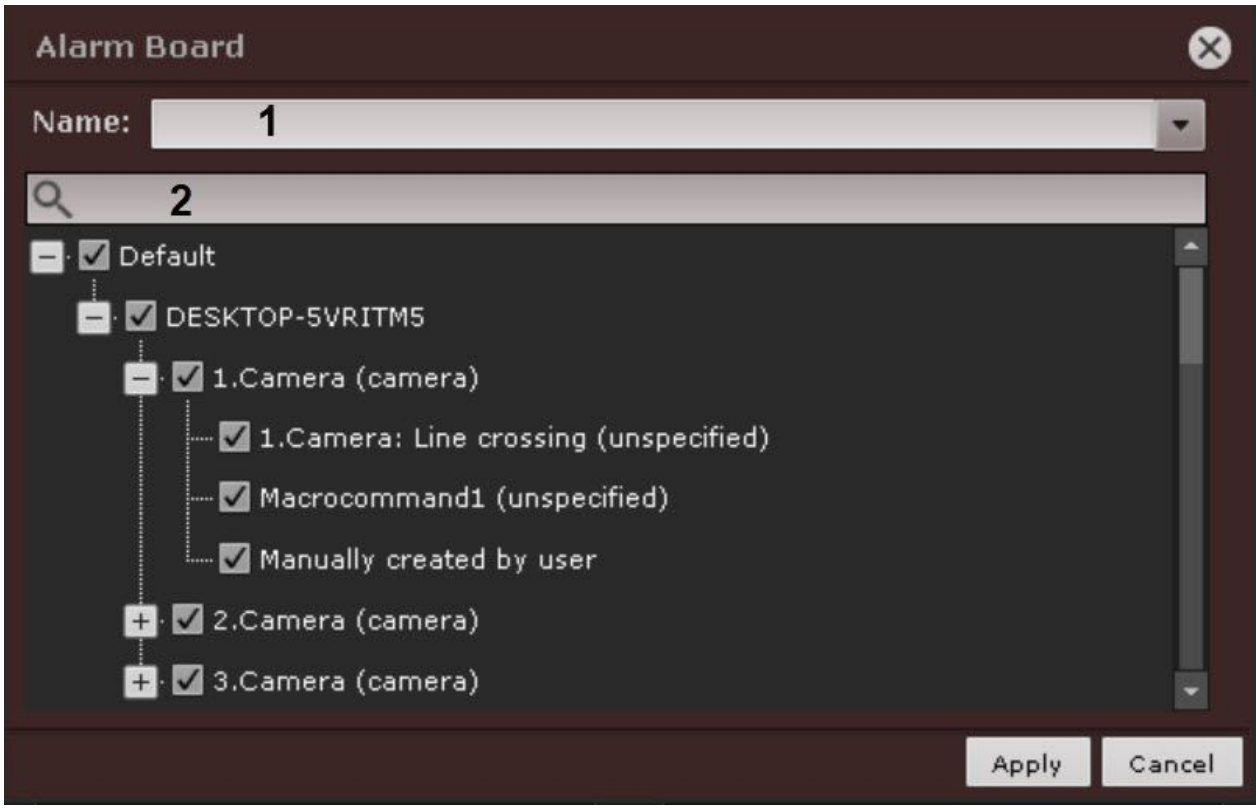
15.7.5.5.7 Configuring an Alarm Board

Switching to layout editing mode(see page 474)

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(see page 481)).
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.

15.7.5.6 Configuring Alarms Panel on a layout

You can configure the size of Alarms Panel (see Alert panel(see page 646)) 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(see page 646)).
3. Switch to the Layout Editing mode (see Switching to layout editing mode(see page 474)).
4. Exit the Layout Editing mode and save changes (see Exiting Layout Editing mode(see page 499)).

The Alarms Panel will always open as you have specified it for this layout.

15.7.5.7 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**.

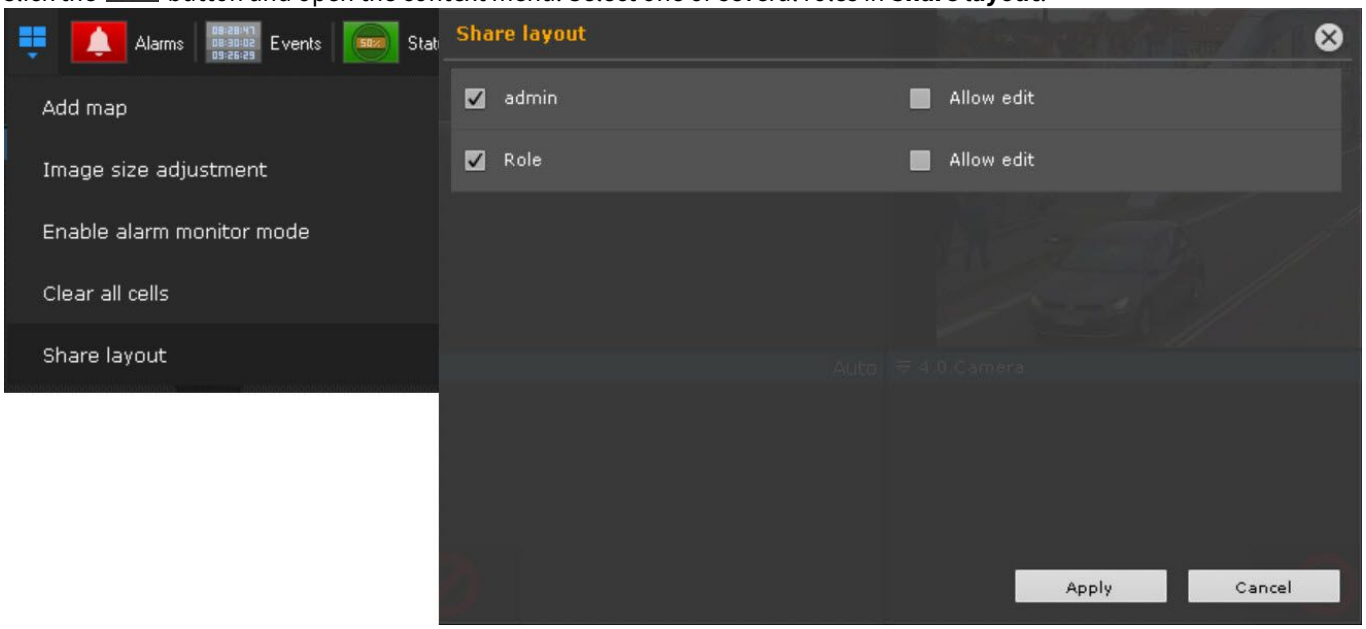
15.7.6 Share Layouts

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(see page 475)) and go to Layout Editing mode (see Switching to layout editing mode(see page 474)).
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(see page 646).

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(see page 499)).

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(see page 644)).
2. Delete it from their list (see Creating and deleting layouts(see page 471)).

> **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(see page 473)). If you copy the layout, you are the owner of your copy. You can edit it.

Shared layouts are sealed with the following sign:

15.7.7 Configuring special layouts

15.7.7.1 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:

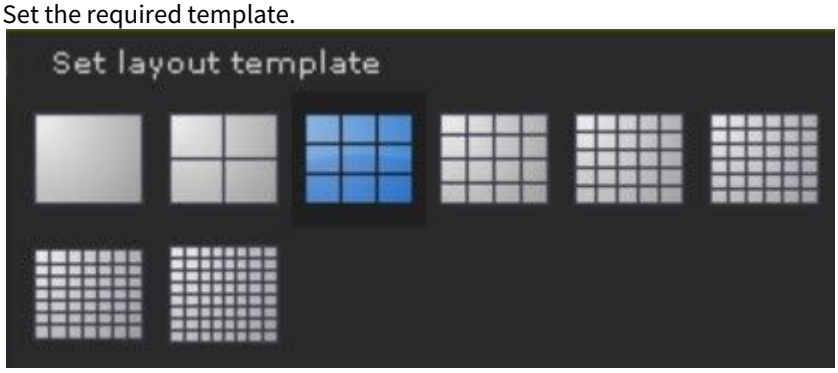
1. Click the button to open the **Layouts** context menu.
2. Select the required layout.

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.

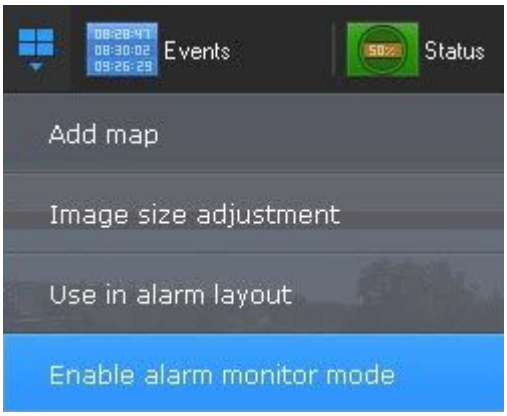
The number of cameras on the **Marked cameras** layout and the **Alarmed cameras** layout can be limited by the layout template—1, 4, 9, 16, 25, 36, 49, 64. To set the layout template, do the following:

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

.

15.7.7.2 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:

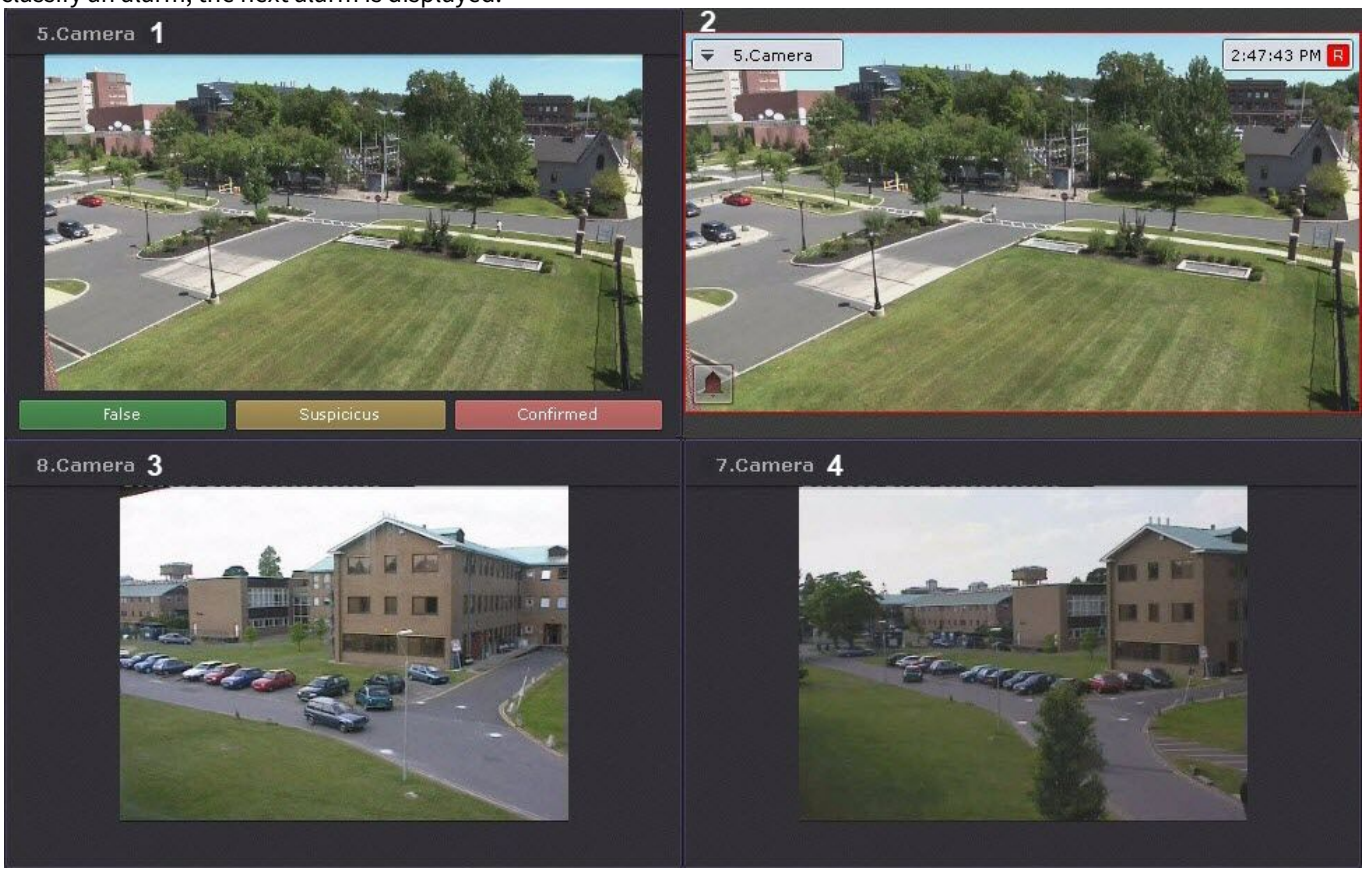
1. Select the layout (see Selecting a layout for editing(see page 475)).
2. Open the context menu and select: **Use in alarm layout**.

3. Save changes (see Exiting Layout Editing mode(see page 499)).

> **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.

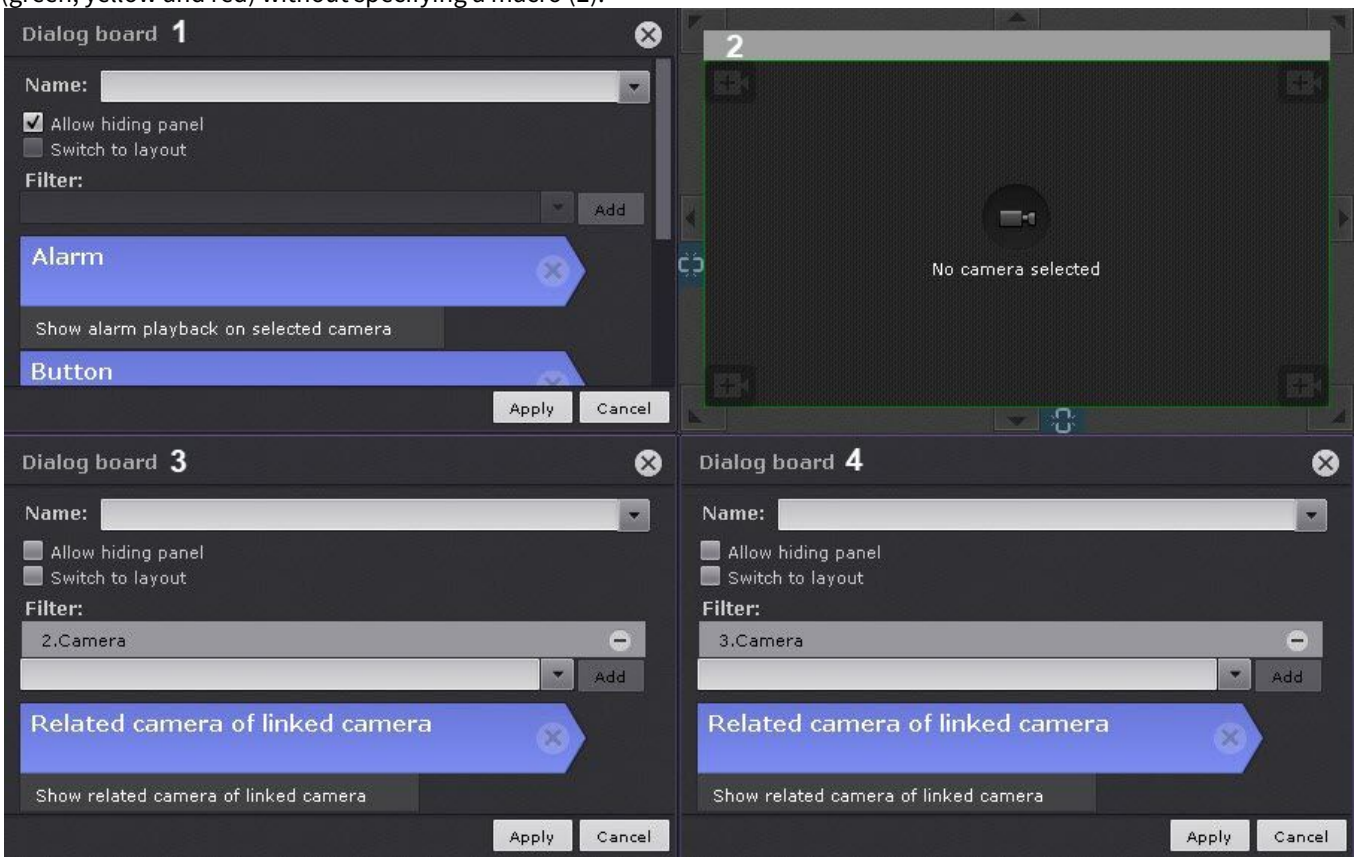


2. An alerted camera in Live Video mode (**2**).
3. 2 additional cameras (**3**, **4**) in Live Video mode (for example, the 2 nearest ones to the alarmed one).

Do the following:

1. Switch to the Layout Editing mode (see Switching to layout editing mode(see page 474)).

2. In the first cell, add a Dialog board (see Configuring a Dialog Board(see page 495)) 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(see page 481)).
6. Save the layout.
7. For each camera, select 2 stand-by cameras (for example, those closest to it, see The Camera object(see page 122)).

> **Note**
>
> In cell **4**, the first stand-by camera will be displayed, in cell **3** – the second.

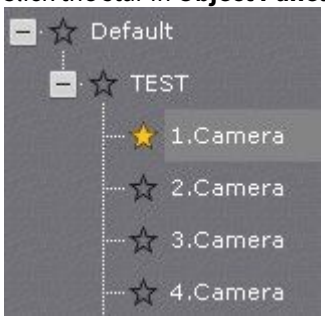
15.7.7.3 Configuring Marked cameras layout

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(see page 646));

- Click the star in **Object Panel** (see Objects Panel(see page 648));



Attention!

You can add tags to cameras on any video wall (see Managing monitors on a local Client(see page 790)).

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(see page 473) to create a copy of the current special layout.

15.7.8 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(see page 554)).

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(see page 471)).
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.

15.7.9 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(see page 471)).
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**.

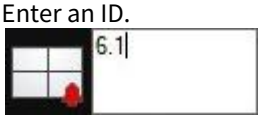
15.7.10 Setting a layout ID

You can set an ID for a layout. This may appear useful for calling layouts with hotkeys (see Notes regarding hot key actions(see page 579)).

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

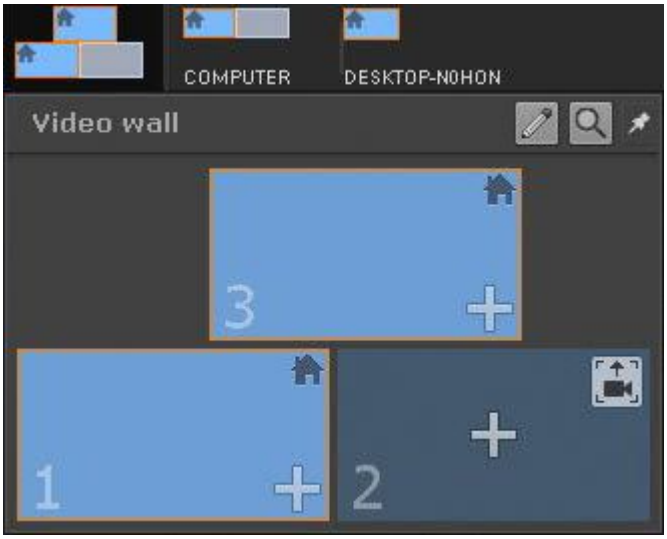
When you hover the mouse cursor over a layout, the name and ID (if specified) of the layout are displayed separately.

15.8 Configuring Videowall

A Videowall is a set of display monitors physically and logically connected to act as a single screen.

A Videowall may include any monitor connected to any Client within the Axxon-domain.

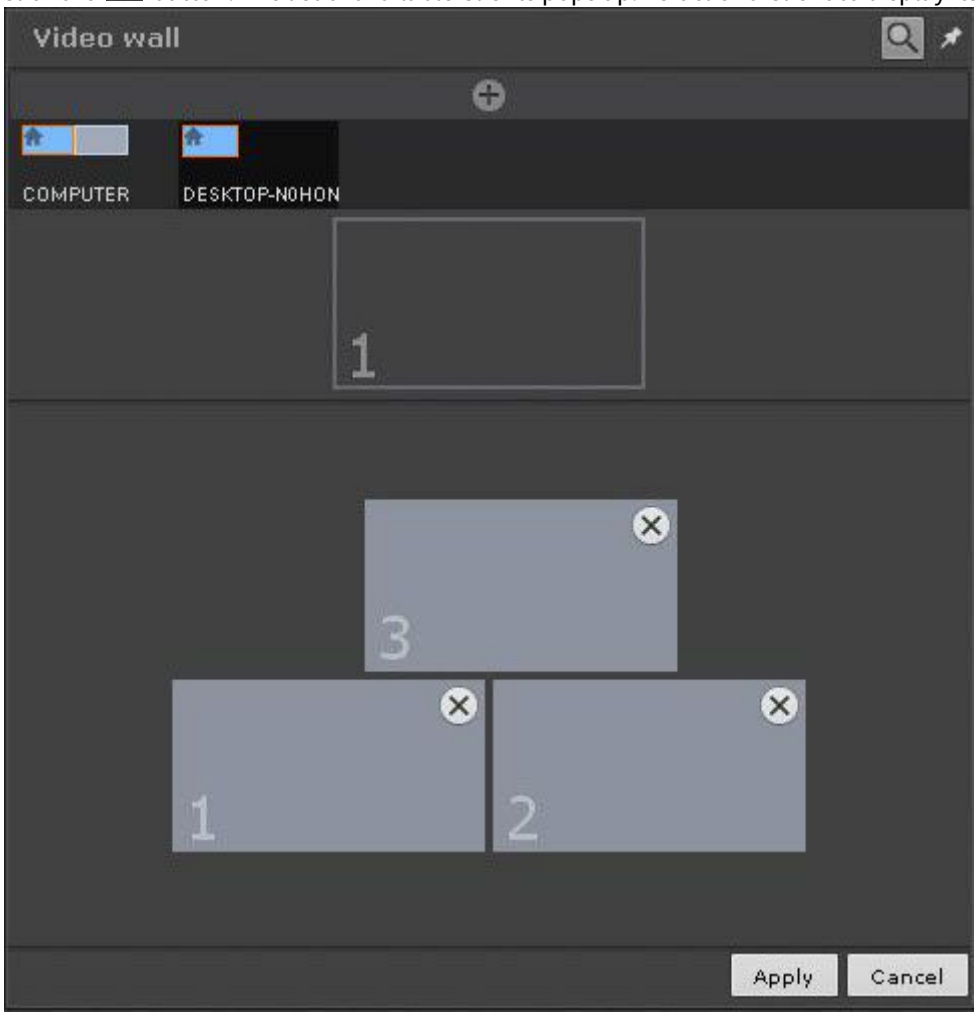
You can set up a Videowall via a dedicated panel (see Videowall Panel(see page 643)).



To set up a Videowall, do the following:

1. Click the button.

2. Click the button. The list of available Clients pops up. Left click a Client to display its active monitors.



3. Drag and drop monitor icons according to their monitors' physical locations on the Videowall.

> **Note**
>
> An ID number is assigned to each monitor added to a Videowall. To display the ID number of a monitor, click .

4. Click **Apply**.

Now, the Videowall is configured.

> **Note**

You can manage Videowall's monitors the same way as Client monitors (see Managing monitors on a local Client(see page 790), Managing monitors on remote Clients within the Axxon-domain(see page 792)).

15.9 Configuring the interactive map

Configuration of the interactive map is performed in layout editing mode (see the sections Interactive Map(see page 645), Switching to layout editing mode(see page 474)).

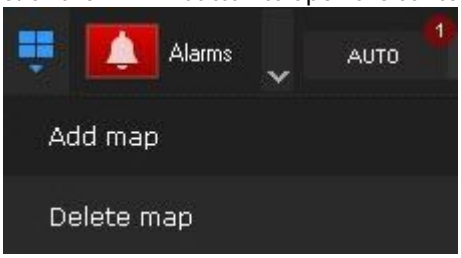
Note

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(see page 450)).

15.9.1 Adding a new map

Vector maps in Axxon One(see page 545)

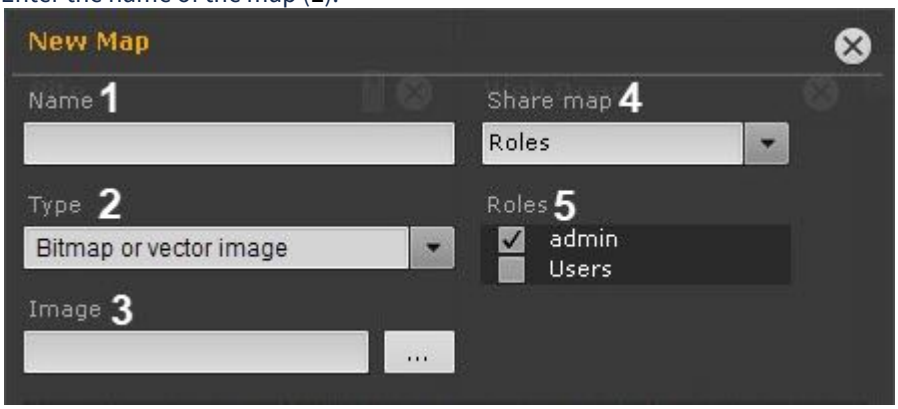
To add a new map, do the following:

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**).



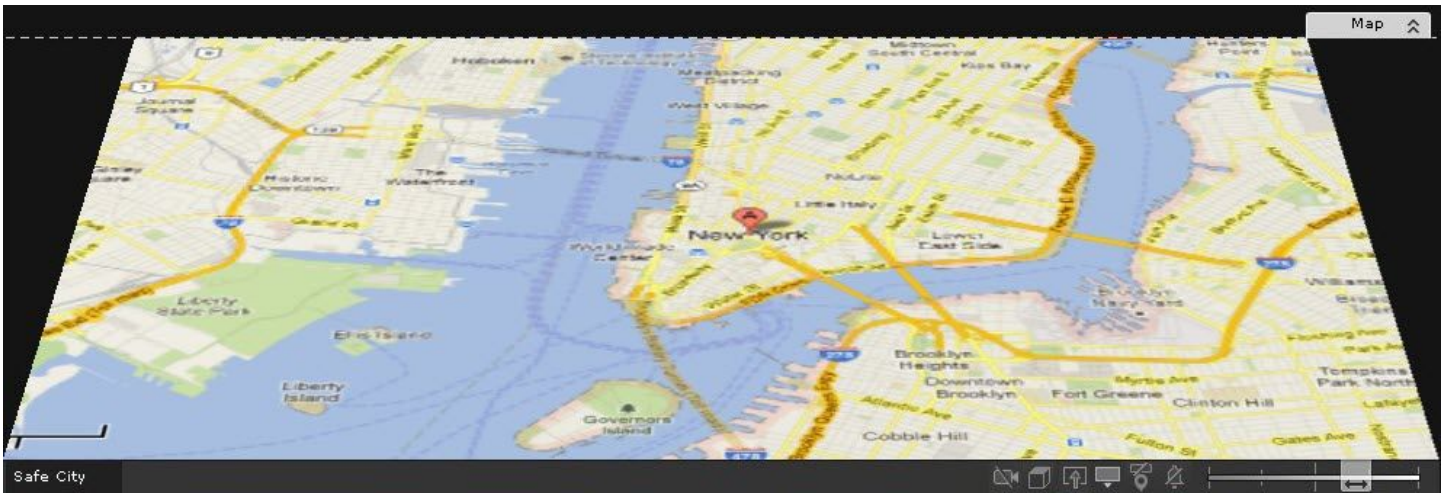
3. Select what will be used as a map (**2**, see Vector maps in Axxon One(see page 545)):
   a. **Raster or vector image**.
   b. **Google:**
      i. **Google Map;**
      ii. **Google Hybrid;**
      iii. **Google Satellite.**
   c. **OpenStreetMap.**
4. If you select the **Raster or vector image** 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. Raster image: 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.



15.9.2 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.

15.9.2.1 Adding video cameras and changing size of their icons on the map

You can add video cameras to the map by dragging a video camera icon from the Camera Search Panel (see Camera Search Panel(see page 646)) or the Object Panel (see Objects Panel(see page 648)) to the map.

> **Attention!**
>
> When you add a video camera with the specified coordinates to the geomap (see The Camera object(see page 122)), the video camera icon is automatically positioned according to the coordinates.
> 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(see page 517)).

To add a video camera to the map, you can also left-click a video camera icon on the Camera Search Panel or on the Object Panel and, holding it down, drag the mouse cursor to the map.

If you use this method to move a group of cameras to the map, all cameras in the group will be added.

To change the size of the camera icons, use the **Change icon size** slider in the lower right corner of the screen in the layout editing mode.

15.9.2.2 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(see page 648)).

2. Drag and drop the inputs/outputs to the map.

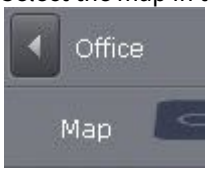
15.9.2.3 Adding switches to another map

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.

1. Select **Add transition to map**.

2. Select the map in the system to which the new switch will point.



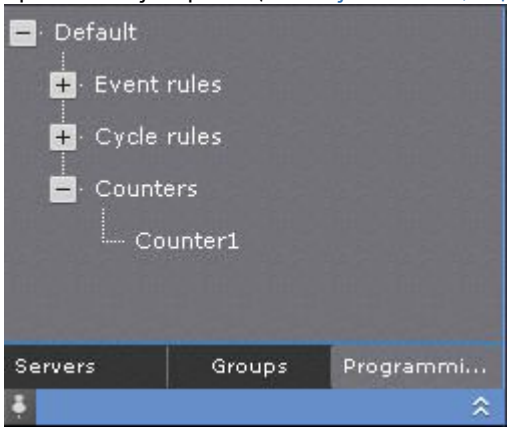
Addition of the switch is now complete.

Then drag the switch icon to the necessary place on the map.

15.9.2.4 Adding counters

To add counters (see General information about the counters(see page 401)) to the map, do as follows:

1. Open the Object panel (see Objects Panel(see page 648)) and go to the **Programming** tab.



2. Drag and drop the counter to the map.

3. To set up a counter on the map, do as follows:

   a. Configure the counter coverage area on the map. You can do so by dragging the anchor points of the area . To add a new point, click . To delete it, right − click on the point.

   > **Note**
   >
   > To remove the counter from the map, click the point .

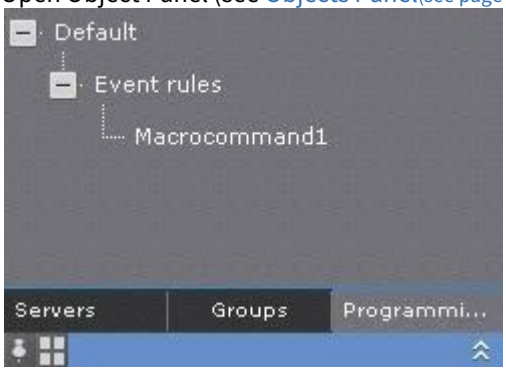
   b. Select the color of the counter.

> **Note**
>
> To hide/display the color settings, use and buttons.

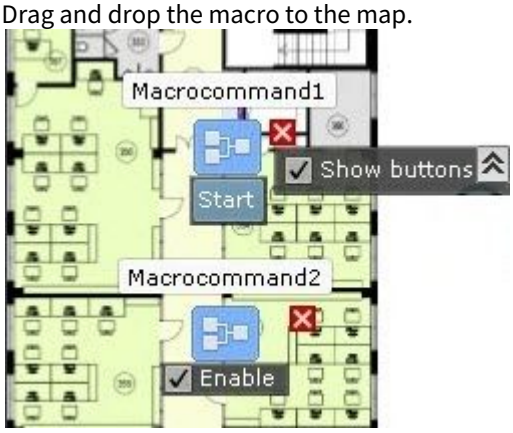
15.9.2.5 Adding macros

To add macros (see General information about the macros(see page 400)) to the map, do as follows:

1. Open Object Panel (see Objects Panel(see page 648)) 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 .

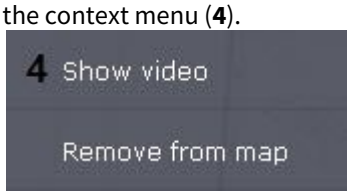
15.9.3 Configuring cameras on the map

15.9.3.1 Configuring a camera in standard map viewing mode

After you add a camera to the map (see Adding video cameras and changing size of their icons on the map(see page 512)), perform the following actions:

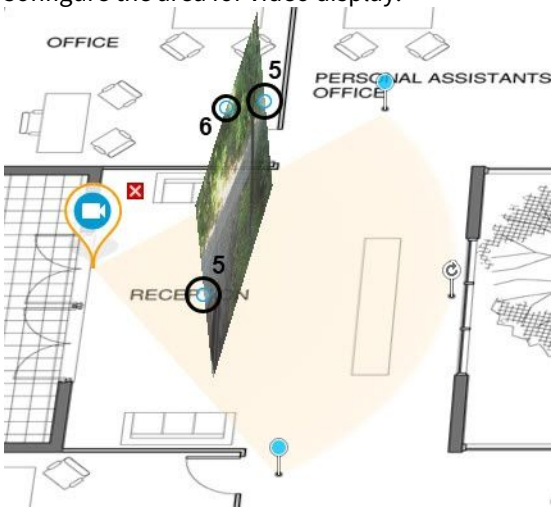
1. Drag the video camera's icon to the place on the map that represents the camera's actual location at the site (**1**).

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 fish-eye cameras(see page 127)), 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 fish-eye cameras(see page 127)).
> 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(see page 801)).

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.

15.9.3.2 Configuring cameras with an embedded GPS tracker

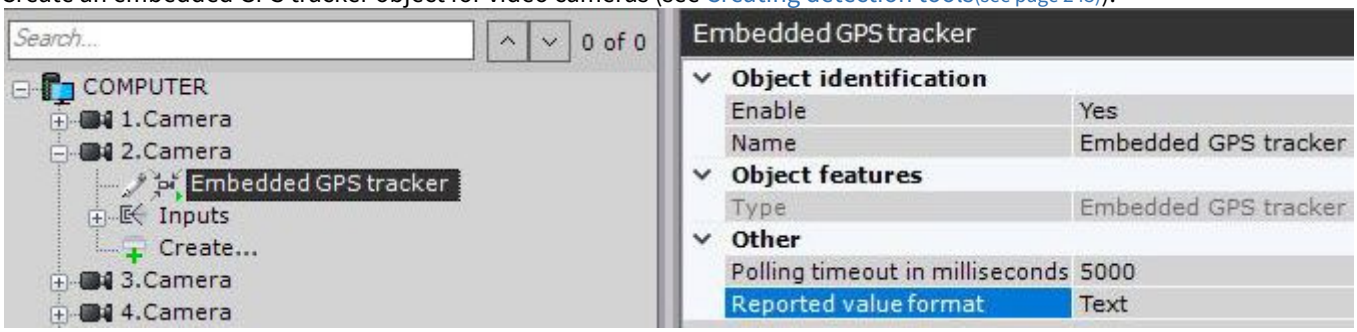
Some devices contain an embedded GPS tracker that transmits the current coordinates of the device to *Axxon One* VMS.

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 Creating detection tools(see page 243)).



2. Create a geomap (see Adding a new map(see page 510)).
3. Add video cameras to the geomap (see Adding video cameras and changing size of their icons on the map(see page 512)).

15.9.3.3 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(see page 802)).

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:

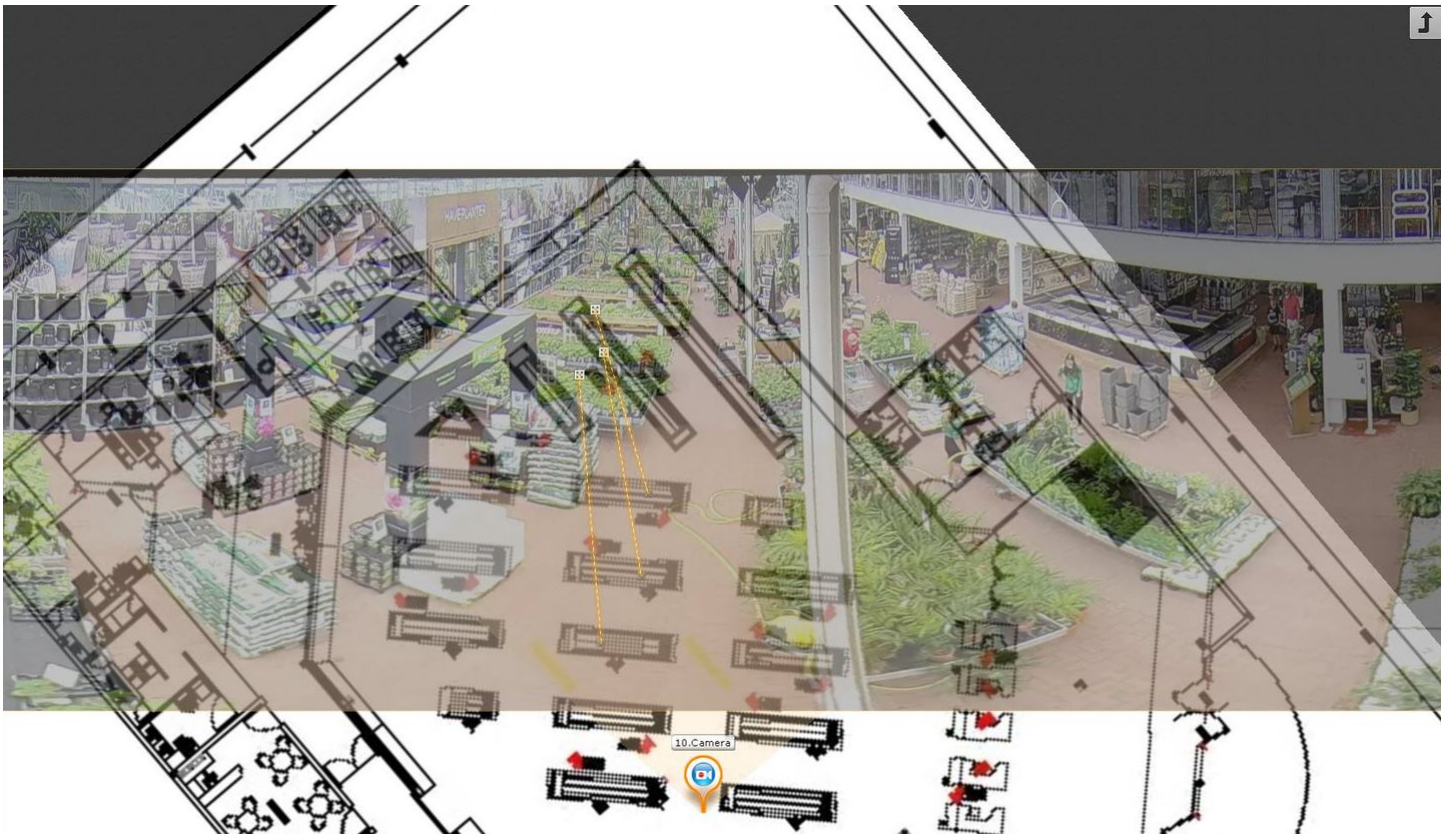
1. Click an object in the video. A point is added.

> **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.

15.9.4 Attaching a map to a layout

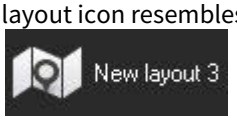
You can attach a map to a layout. This means that when you switch to the layout, the attached map opens automatically.

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(see page 471) and Selecting a layout for editing(see page 475)).
2. Go to map editing mode (see the section Opening and closing the map(see page 796))
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(see page 801) and Adding a new map(see page 510)).
4. Save changes and exit layout editing mode (see Exiting Layout Editing mode(see page 499)).

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.

15.9.5 Configuring the floors

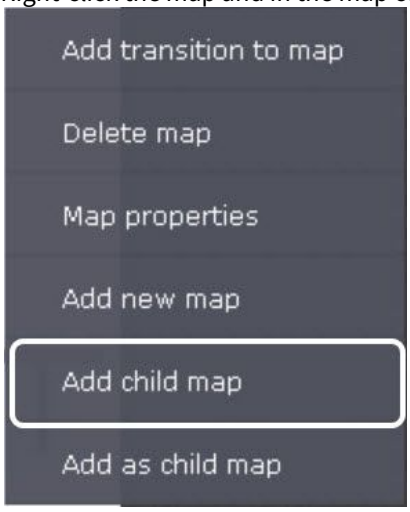
15.9.5.1 Creating a new floor

You can create a new floor in two ways: by adding child map or by adding a map as a child.

15.9.5.1.1 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(see page 510)).

2. Enter the name of the floor (**1**).

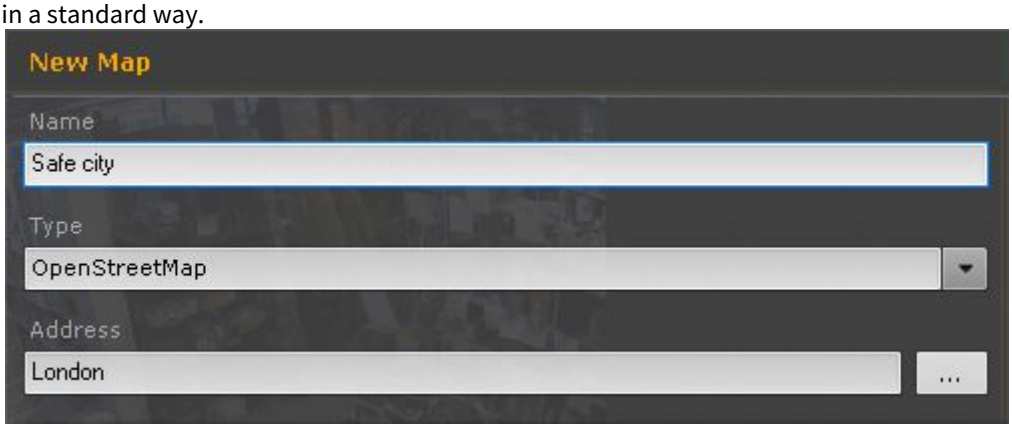
3. Select the item that will be used as a floor map: an image or geodata from the OpenStreetMap provider (**2**).

> **Note**
>
> *Axxon One* uses the geodata provided by the OpenStreetMap through the Mapbox service. The connection to the service is described on the Adding a new map(see page 510) page.

4. Clicks the ... button and select the image (**3**), which will be used as a graphic plan of the protected area (if the **Raster 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.

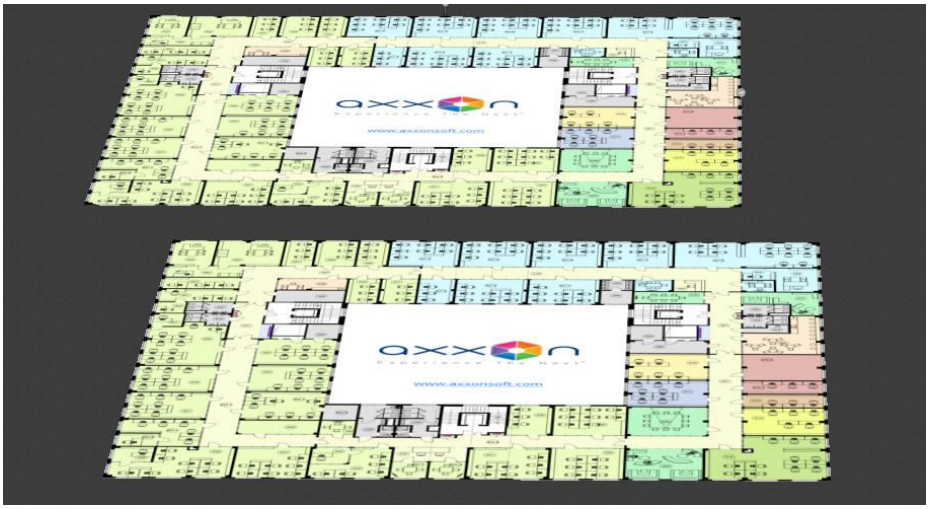
   > **Note**
   >
   > The maximum image size is 4 million pixels (the number of pixels in the resolution 2000x2000). The floor will not be created if the selected image is larger than the allowed size.

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 on browsing the OpenStreetMap, see the provider's website[156]) 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.



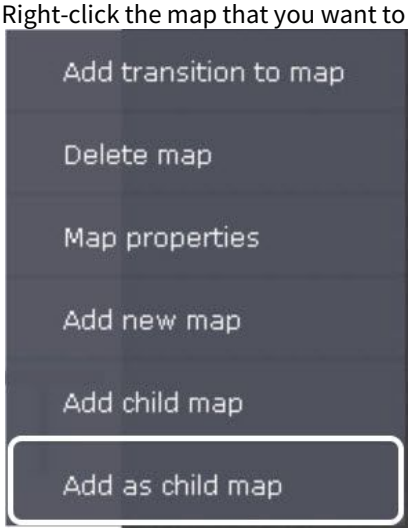
15.9.5.1.2 Adding as child map

You can add a map as a child map only to an existing map (see Adding a new map(see page 510)).

To add a map as a child map, do the following:

156 https://wiki.openstreetmap.org/wiki/Browsing

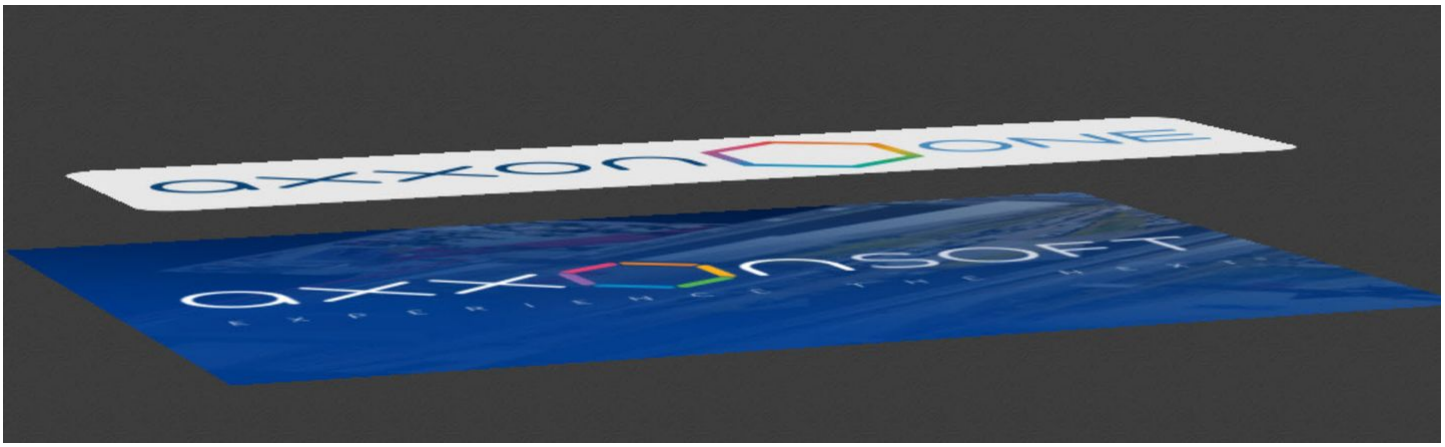
1. Right-click the map that you want to add as a child and in the map context menu, select the **Add as child map** item.



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.

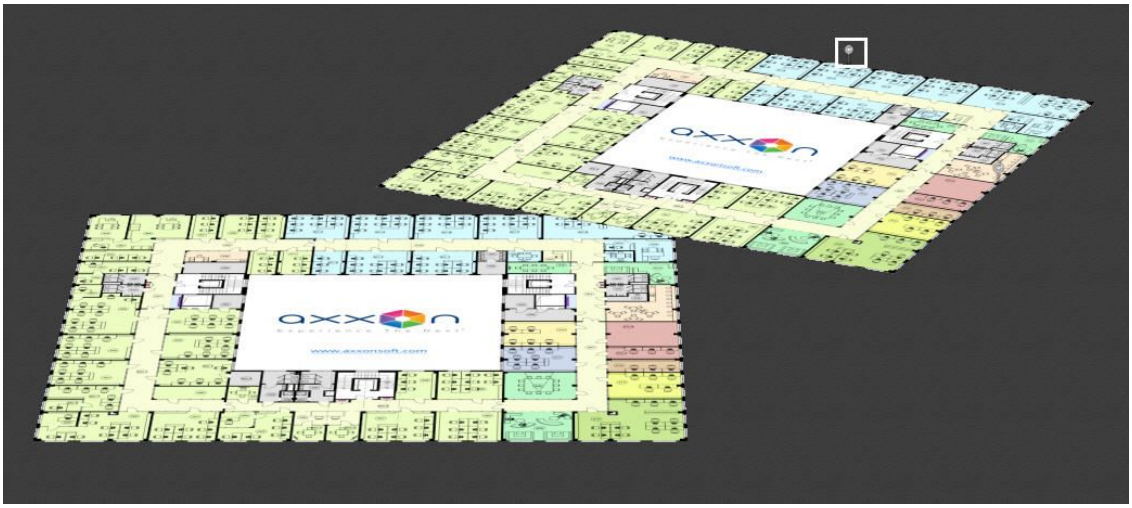


15.9.5.2 Configuring floor location on the map

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.



15.9.5.3 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(see page 512).
2. Configuring the display of added video cameras — see Configuring cameras on the map(see page 515).
3. Removing objects from a floor — see Removing objects from the map(see page 523).

4. Changing the type and display — see Changing map type and display(see page 524).
5. Changing the name of the floor — see Renaming the map(see page 524).

15.9.5.4 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:

15.9.6 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.

15.9.7 Setting keywords for geo map search

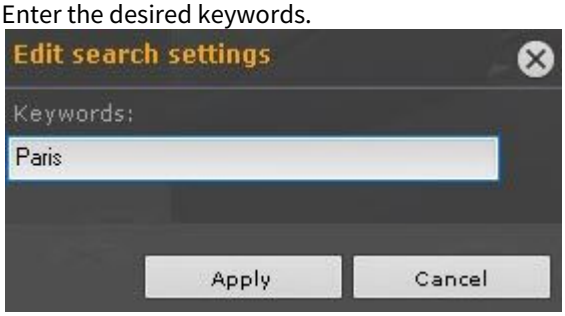
The keywords are needed to locate a site or a street on OpenStreetMap.

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(see page 510)).

To set new keywords, you need to:

1. Click in the lower panel.
2. Enter the desired keywords.



3. Click **Apply**.

15.9.8 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(see page 510)).

15.9.9 Renaming the map

To rename the map, in the lower-left corner of the screen, left-click a tab and specify a new name.

15.9.10 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.

15.9.11 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**.

15.10 System preferences

15.10.1 Server settings

15.10.1.1 Configuring Forensic Search MomentQuest in Archive

On the page:

- Turning on the video stream metadata recording(see page 525)
- Configuring user permissions for Forensic Search in archive(see page 526)

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)(see page 526)).
2. There are video stream recordings from the desired video camera in the archive (see Configuring recording to an archive(see page 224)).
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 Scene Analytics detection tools(see page 254), Face detection tools(see page 278)) or received from a video camera (see Embedded Detection Tools(see page 393)).
4. The user has the appropriate permissions.

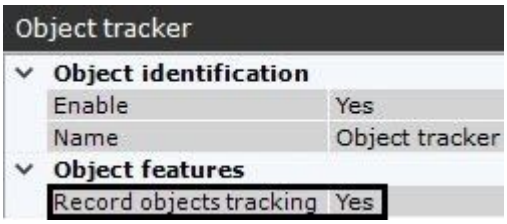
This section contains information on how to configure the *Axxon One* software package to satisfy these conditions.

15.10.1.1.1 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(see page 277)).

> **Note**
>
> Information on configuring storage of metadata is provided in the section titled Configuring storage of the archive, system log, and metadata(see page 539).

15.10.1.1.2 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(see page 450)).

15.10.1.1.3 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(see page 256)).

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.

15.10.1.2 Setting up privacy masking

15.10.1.2.1 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.

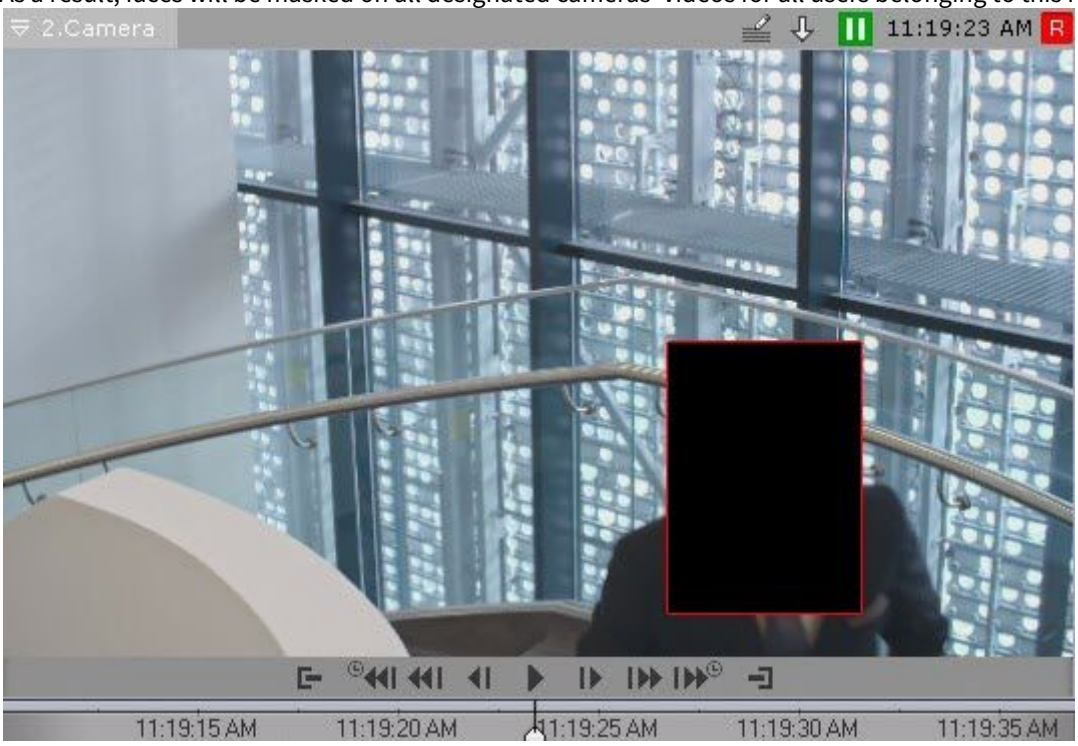
Attention!

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 Functions of face detection tools(see page 279)).
2. Set **No** for the **Show faces** parameter in the Role Settings panel (see Creating and configuring roles(see page 452)).

As a result, faces will be masked on all designated cameras' videos for all users belonging to this role.



15.10.1.2.2 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!

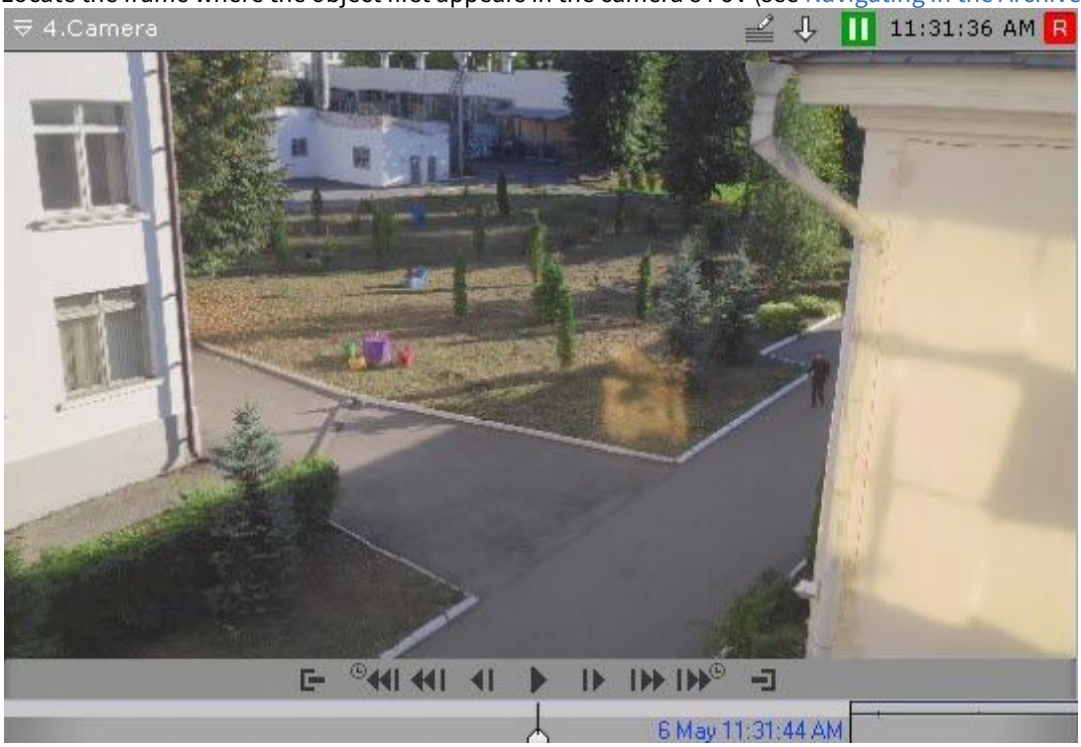
Privacy masks are displayed in the standalone Client software only. You cannot use masks with both web and mobile Clients.

To do this, set **No** for the **View masked video** option in Role Settings (see Creating and configuring roles(see page 452)). The objects will be masked for all users belonging to this role.

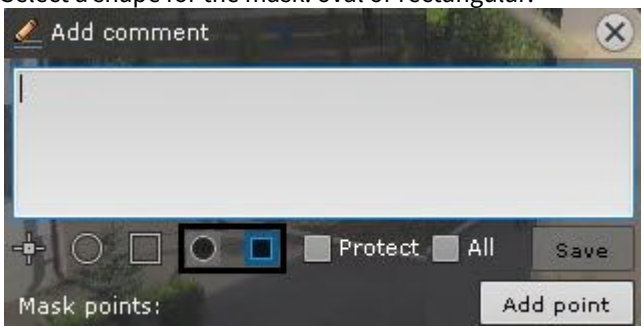
To mask an object from Video Footage viewing, do the following:

1. Proceed to Archive Mode and find the object to be masked (see Switching to Archive Mode(see page 695)).

2. Locate the frame where the object first appears in the camera's FoV (see Navigating in the Archive(see page 705)).

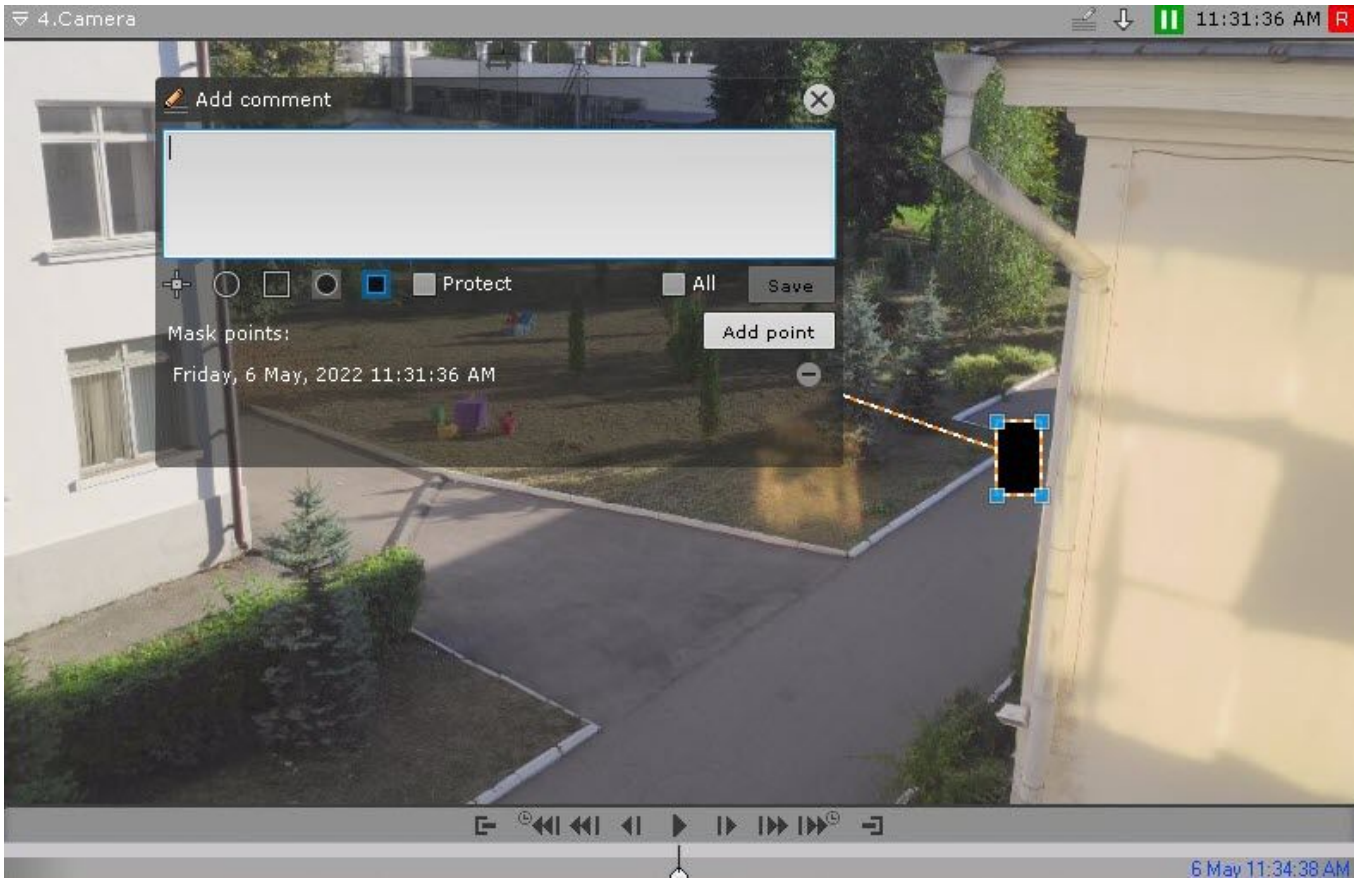


3. Click the button.
4. Select a shape for the mask: oval or rectangular.

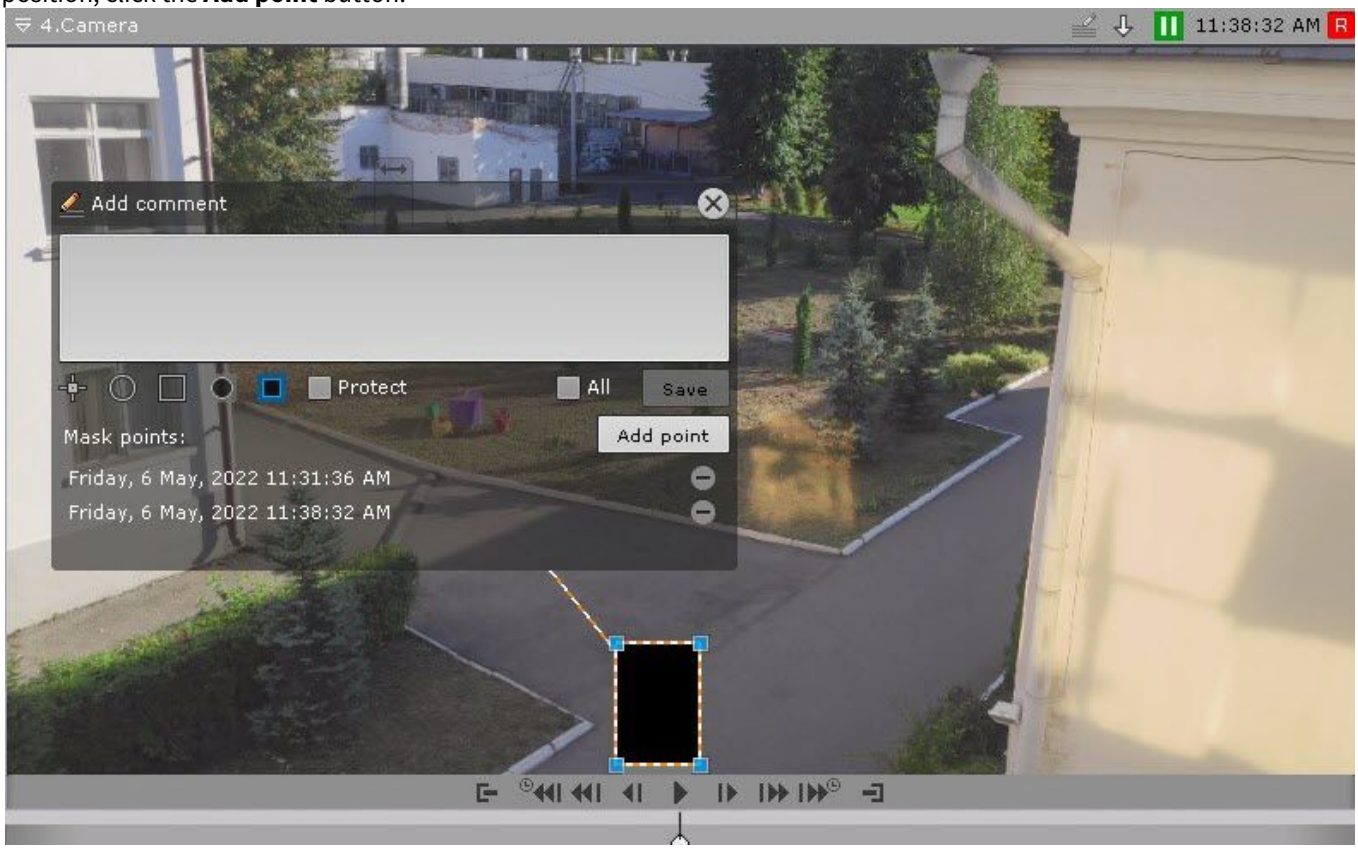


5. Apply the mask over the object.

> **Note**
>
> The procedure of setting up a mask is similar to adding a comment (see Adding a comment(see page 668)).

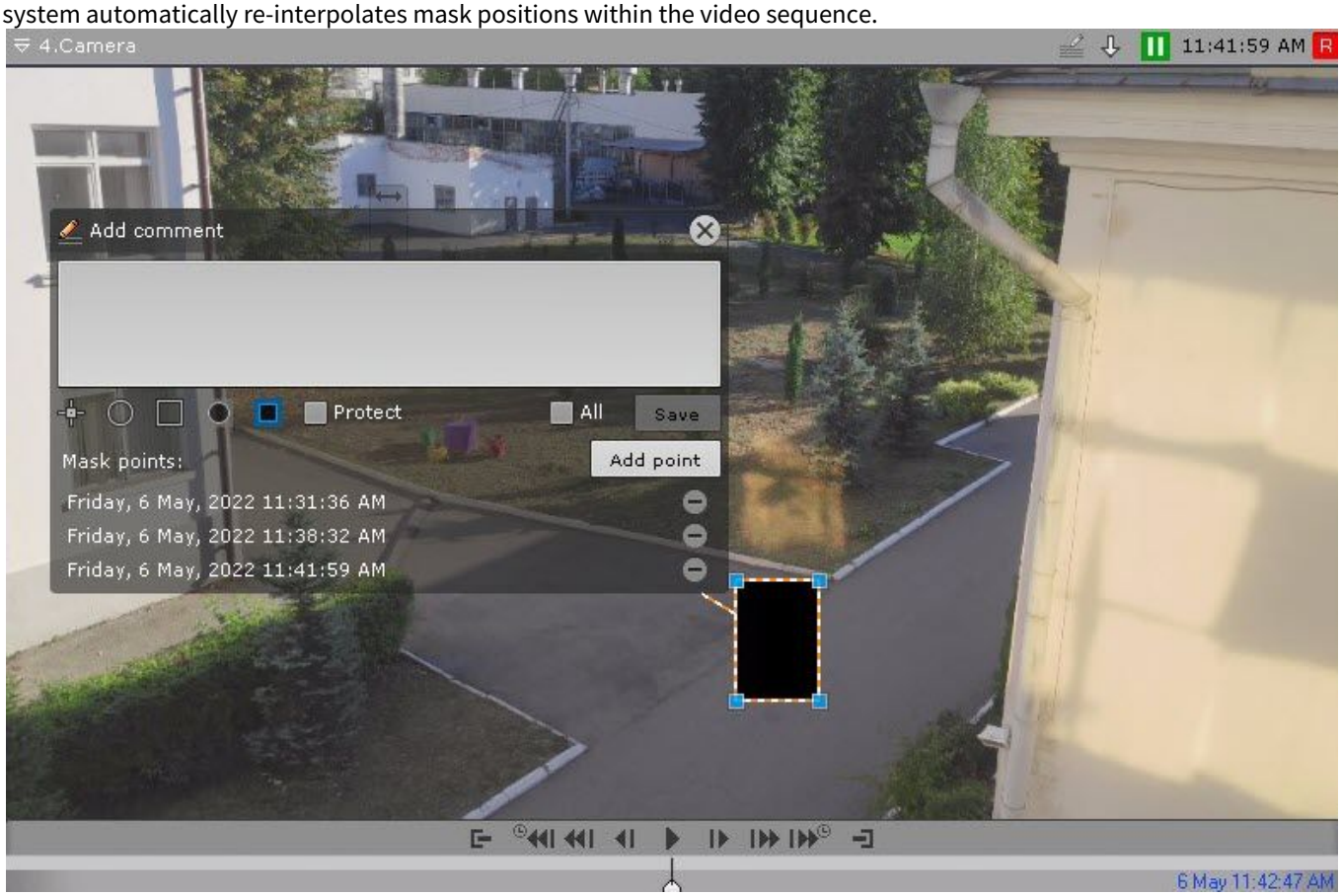


6. Locate the last frame before the object disappears from the camera's FoV and place the mask over it. To save mask position, click the **Add point** button.



7. The system automatically interpolates the mask position on intermediate frames, assuming the object's motion is uniform and rectilinear.

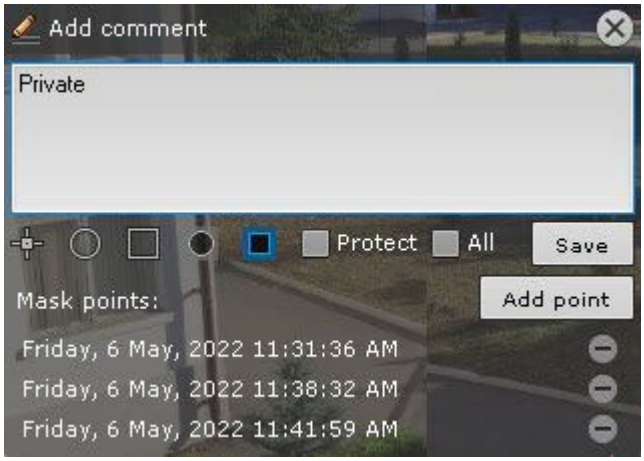
8. Check the video. If necessary, you can specify additional mask positions on intermediate frames for better masking. The system automatically re-interpolates mask positions within the video sequence.



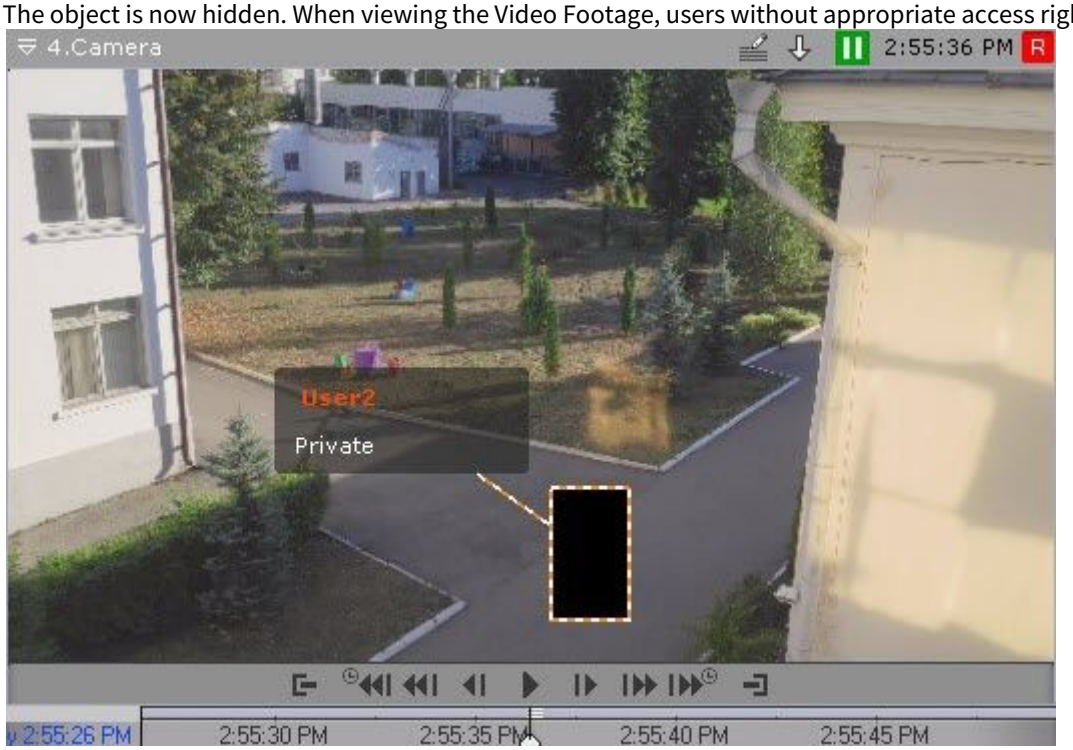
> **Note**
>
> To remove a mask position, click the button.

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(see page 452)).



The object is now hidden. When viewing the Video Footage, users without appropriate access rights will see the object masked.



15.10.1.3 Analyzing video from external systems (Offline Analytics)

You can run *Axxon One* analytics on any video file from either external or internal storage.

To do this, you need to import(see page 531) the video file and index(see page 533) it.

After that, you will have the following options available:

1. Forensic Search for Fragments (MomentQuest)(see page 730).
2. Face search(see page 744).
3. LPR search(see page 741).
4. Searching comments(see page 729).

> **Note**
>
> You can search only by text comments entered after the video is imported (see Operator comments(see page 667)).

5. Compressed playback of archives (TimeCompressor)(see page 699).
6. Search by events(see page 727).

Select a mirror archive (see Selecting an Archive(see page 697)) to run video analytics on and **Offline Analytics** for metadata source (see Forensic Search for Fragments (MomentQuest(see page 730)).

15.10.1.3.1 Importing video to Axxon One

To import external video data, do as follows:

1. Create an archive. It must be equal to or larger than the total size of all files in it (see Creating archives(see page 209)).
2. Run IP Device Discovery Wizard (see Adding and removing IP devices(see page 112)):
   a. In the form for manually adding an IP device, select **AxxonSoft** in the **Vendor** drop-down list (**1**).

   b. Select **ExternalArchive** from the models list (**2**).

c. Select the archive file to which video recordings will be added (**3**).

d. Click the button.

> **Attention!**
>
> When you add a camera:
>
> i. Continuous replication from the on-board storage to the selected archive file (see Configuring data replication(see page 226)).
>
> ii. The **Scene Analytics** object will be created (see Creating detection tools(see page 243)) and metadata enabled (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)).

3. Configure **Object Tracking** (see Setting general parameters of Tracker-based Scene Analytics detection tools(see page 260)). If you want to find persons and car numbers in video footage, then create and configure the appropriate detection tools (see Configuring License plate recognition (VT)(see page 314), Configuring Face detection(see page 280)).

> **Attention!**
>
> Do not remove the Object Tracker from your system. Otherwise you cannot import videos into your system.

4. If necessary, change the mode of data replication (see Configuring data replication(see page 226)). If you select **On Demand** mode you can start the analysis of the video image manually (see Indexing video from external sources(see page 533)).

> **Attention!**
>
> Replication is performed only to the end of the archive. It is not possible to overwrite existing data in the archive (see Configuring data replication(see page 226)).
> If you ignore this rule, the videos will not be indexed.
> It's preferable to import all the videos from a folder at once, otherwise you have to manually remove metadata and records from the Archive before the next replication (see Indexing video from external sources(see page 533)).

5. In the **Folder** field, specify the storage location of the video footage that will be used as External Archive.

> **Attention!**
>
> The following compression algorithms are supported: MJPEG, MPEG-2, MPEG-4, MxPEG, H.264, H.265, Hik264 (x86 only) as well as uncompressed ('raw") video.
> A "raw" format is a stream of consecutive frames without time stamps.

6. Imported folders with video footage or video files must be ISO 8601 timestamped: YYYYMMDDTHHMMSS.

a. If the timestamp is in the folder name, all the videos starting from the specified date and time will be imported without exception. The video recordings are ordered according to the file name as follows:

> **Note**
>
> For example, if the **20220506T100000_camera1** folder contains 3 files (1.avi, 2.avi, 3.avi), they will come into the archive as follows:
> 1.avi: [6 May 2022, 10:00:00; 6 May 2022, 10:00:00 + the duration of 1.avi].
> 2.avi: [6 May 2022, 10:00:00 + the duration of 1.avi; 6 May 2022, 10:00:00 + the duration of 1.avi and 2.avi].
> 3.avi: [6 May 2022, 10:00:00 + the duration of 1.avi and 2.avi; 6 May 2022, 10:00:00 + the duration of 1.avi and 2.avi and 3.avi].

b. If the folder name does not have the timestamp, all the video files will be imported in accordance with their timestamps. If the file name is incorrect, the starting point of the recording on the timeline will correspond to the modification date of the file.

> **Attention!**
>
> *Axxon One* operation may be incorrect if video recordings in the folder overlap. No error messages are displayed in this case.
> The date in the folder name or file name (or their creation dates) may not precede the metadata storage period as defined in the system (see Configuring storage of the system log and metadata(see page 539)).

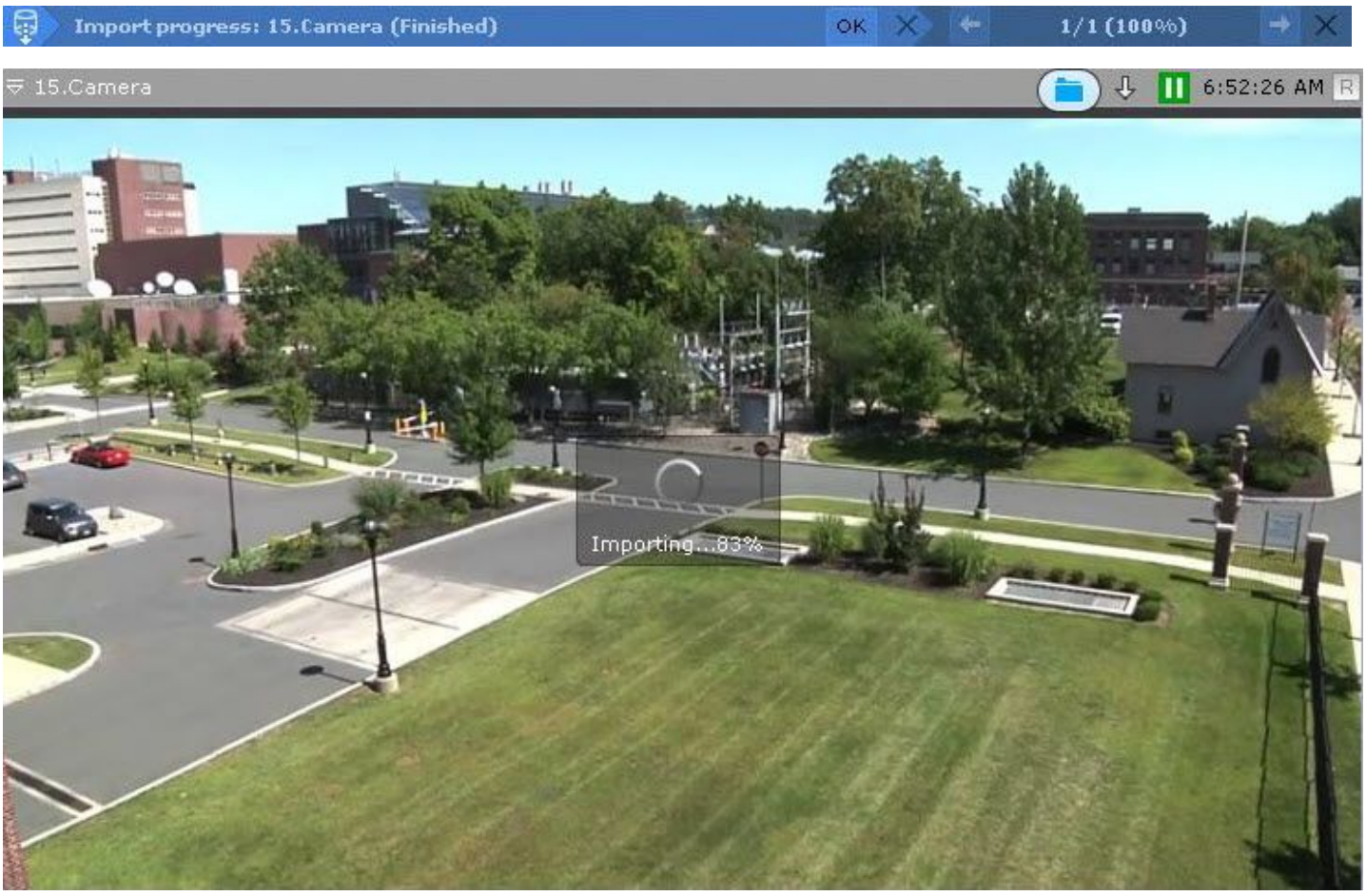
If you add a **Z** character to the end of the timestamp, the time zones for the videos will be GMT+0, otherwise – the time zone of the Server.
For example, 20220228T125130Z.avi. In the Archive mode, this video recording will fit into the timeline from 28 February 2022, 12:51:30 GMT+0 to February 28, 2022, 12:51:30 + recording time GMT+0.

7. Click the **Apply** button.

15.10.1.3.2 Indexing video from external sources

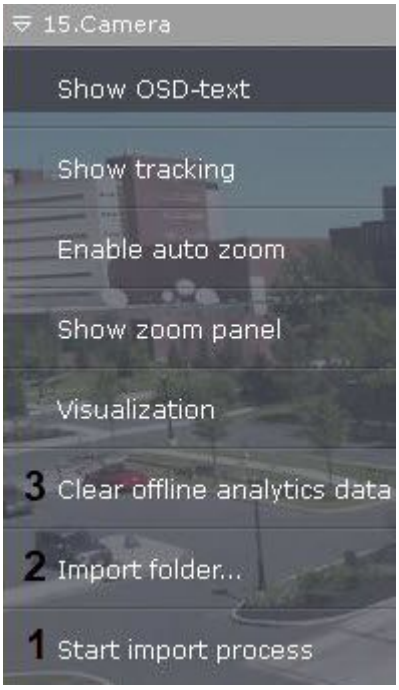
By default, indexing starts automatically after specifying video files (see Importing video to Axxon One(see page 531)).

This may take a while and increase the CPU usage. Similar to the export process, the status of the indexing process is displayed at the top of the screen (see Viewing export progress(see page 817)) and in the viewing tile.



> **Attention!**
>
> You should not view the replicated archive during indexing.
> Also, do not run multiple simultaneous indexing procedures.

If you set the **On demand** replication period (see Configuring data replication(see page 226)), then to start the indexing procedure select **Start import process** (**1**) from the context menu of the viewing tile.



If you want to index the video from another folder, click **Import folder...** (**2**), or click in the viewing tile.

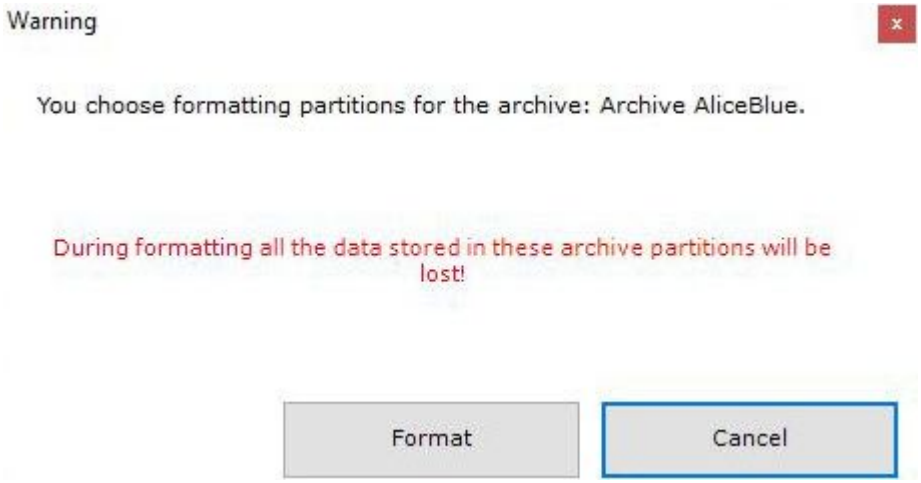
Attention!

If you change the folder, all files in Mirror Archive and metadata will be lost.

Attention!

You can select only the folder specified in the settings and its sub-folders.

To remove metadata and video from an archive, select **Clear offline analytics data** (**3**) and confirm file formatting.

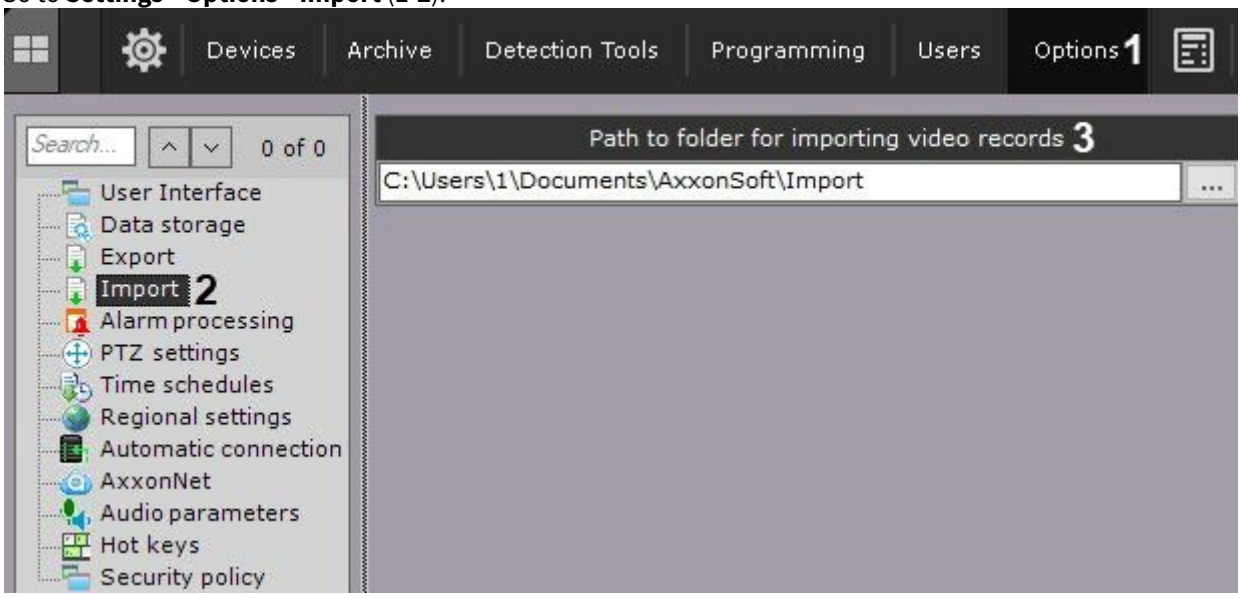


15.10.1.3.3 How to set a folder to import videos from

If you need videos from a different folder on Server to be indexed in addition to already processed footage, you can select only the folder specified in the settings, and its sub-folders (see Indexing video from external sources(see page 533)).

To specify the folder, do the following:

1. Go to **Settings**->**Options**->**Import** (**1**-**2**).



2. Specify the path to the folder (**3**).
3. Click the **Apply** button.

15.10.1.4 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(see page 535)).
2. Using the NVDEC chip on NVIDIA graphics cards (see Hardware-based decoding with NVIDIA NVDEC chips(see page 537)).

In addition, decoding with both Intel QSV and NVDEC is possible (see Simultaneous decoding with Intel Quick Sync Video and NVIDIA NVDEC chips(see page 538)).

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.

15.10.1.4.1 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(see page 699) 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[157].

   > **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[158]).
3. The graphics driver supports Intel Quick Sync Video. We recommend using the latest version of the Intel HD Graphics Driver[159].

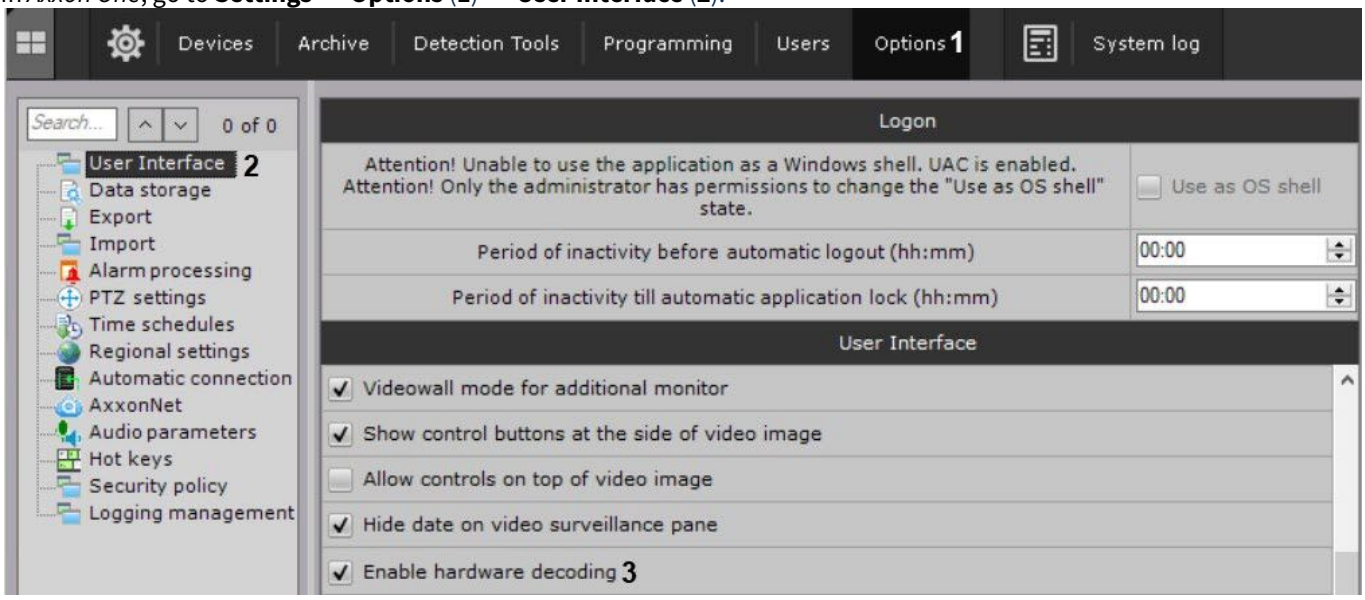
   > **Note**
   >
   > You can also update the driver automatically using the Intel Driver Update Utility[160].

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**).

157 http://ark.intel.com/
158 https://en.wikipedia.org/wiki/Flexible_Display_Interface
159 https://downloadcenter.intel.com/search?keyword=Intel%C2%AE+HD+Graphics+Driver
160 http://www.intel.com/content/www/us/en/support/detect.html?iid=dc_iduu

5. Click the **Apply** button.

Intel Quick Sync Video in *Axxon One* is enabled.

15.10.1.4.2 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(see page 699) 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[161].

Note

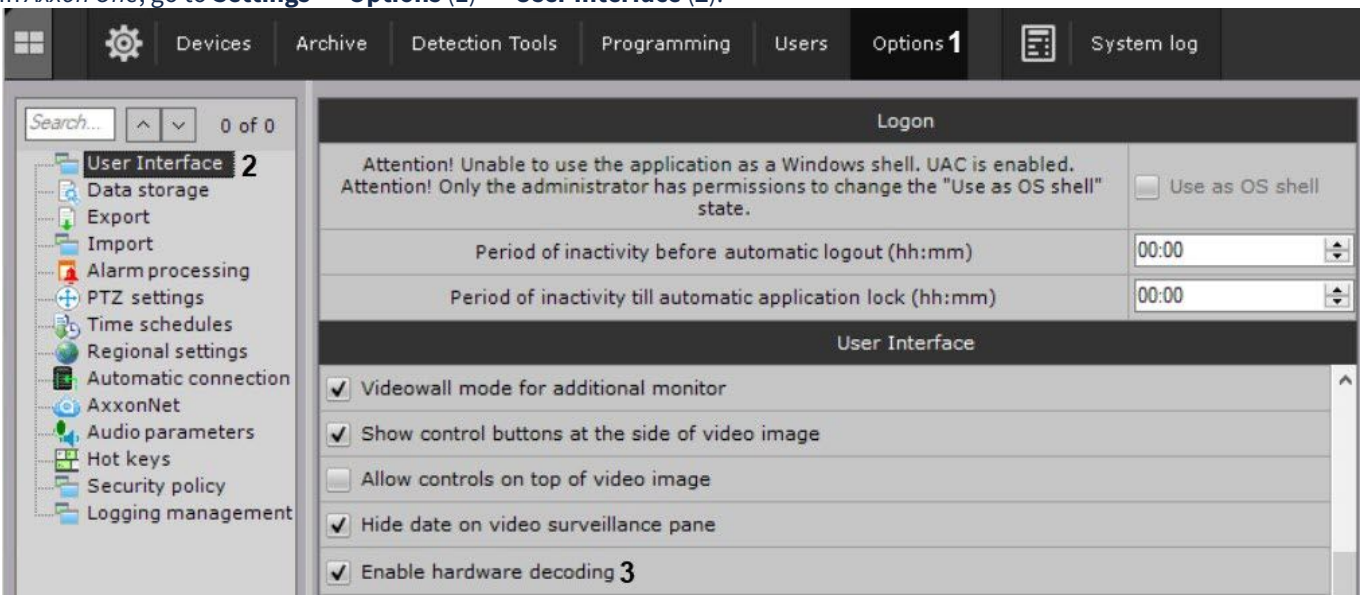
When decoding with NVIDIA NVDEC chips on portable computers due to the specifics of the devices interaction, the resources of the built-in graphics card will also be used.

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.

161 https://developer.nvidia.com/video-encode-decode-gpu-support-matrix

Decoding with NVDEC chips is enabled.

15.10.1.4.3 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(see page 535)) and with NVIDIA NVDEC chips (see Hardware-based decoding with NVIDIA NVDEC chips(see page 537)).

15.10.1.5 Configuring automatic response when Axxon One VMS PC integrity check fails

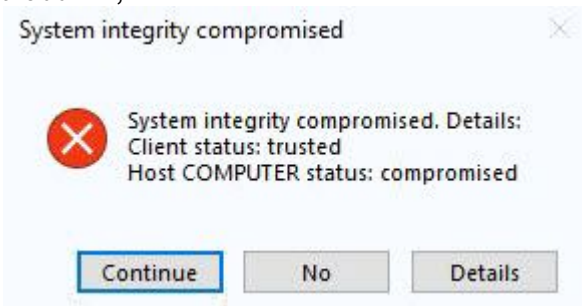
When you start Servers and Clients, *Axxon One* automatically checks the digital signature for all executable files (exe, dll, so).

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(see page 819)).

Otherwise, you can set the system to automatically perform one of the pre-configured actions. To select a response, do as follows:

1. Select **Settings** → **Options** → **Security policy** (**1**-**2**).

2. From the **Do the following actions when system integrity compromised** (**3**) choose the necessary response:
   a. **Show warning to administrators only –** if selected, when the Client starts, an alert will be displayed for users of the **admin**;



> **Note**
>
> To resume launching the Client, click **Continue**; to quit, click **No**. To open a text file containing the list of compromised files, click **Details**.

   b. **Show warning to all users** – in this case, all users will be alerted;
   c. **Block all users without administrator rights** – allows only users in the **admin** role to access the Server. For all non-administrators who were in the system at the time of the check, the Client will shut down and a notification will be displayed;

d. **Stop non-vital services** – shuts down all system objects that are subject to licensing (video cameras, detection tools, etc.). Upon launching the Client, each user will see a notification message.

3. Click **Apply**.

15.10.1.6 Configuring storage of the system log and metadata

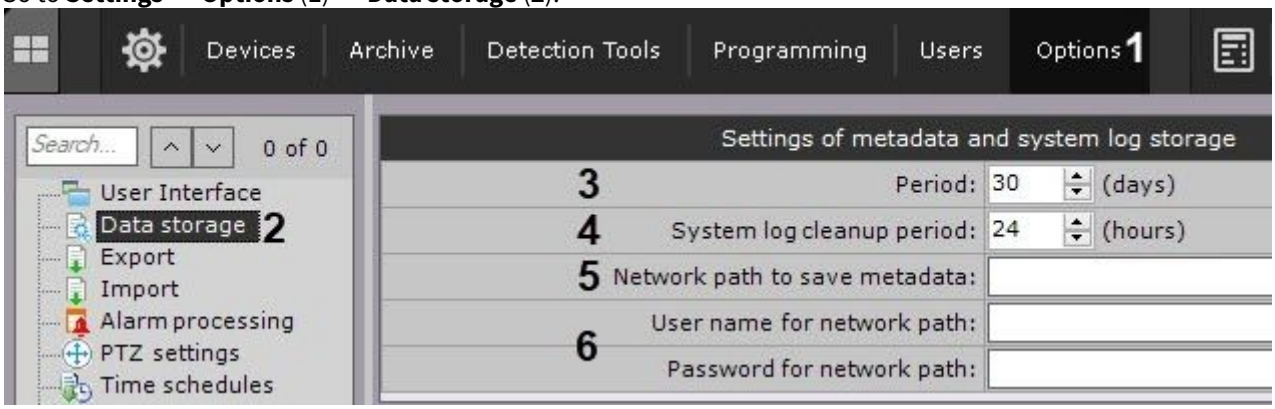
The system log is a log containing system information on events, including system error entries.

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(see page 450)).

By default, metadata files are stored in Server's metadata database: C:\AxxonOneData\vmda_db\VMDA_DB.0\vmda_schema; if necessary, you can place them 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 **Period** field, enter the amount of days to store the system log in the Server's database and to store metadata in the database (**3**). The maximum time is 1000 days.

> **Attention!**
>
> If you enter **zero** value:
> a. System Log events will be stored 0 days.
> b. Metadata retention time becomes unlimited.
>
> If you have less than 15 GB of free disk space, the metadata DB is overwritten – new data records over the oldest data records (see General information about the self-diagnostics service(see page 619)).

3. In the appropriate 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 step 2.

> **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)(see page 730)).
>
> If the camera is not recording when DB is cleaned up, then its recordings are preserved irrespective of their timestamp.

4. The metadata database can be stored on NAS if necessary (by default, it is located locally as set during Installation(see page 62)). Do the following:
   a. Enter a path to the network destination for metadata database (**5**).
   b. Enter the user name and password (**6**). 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

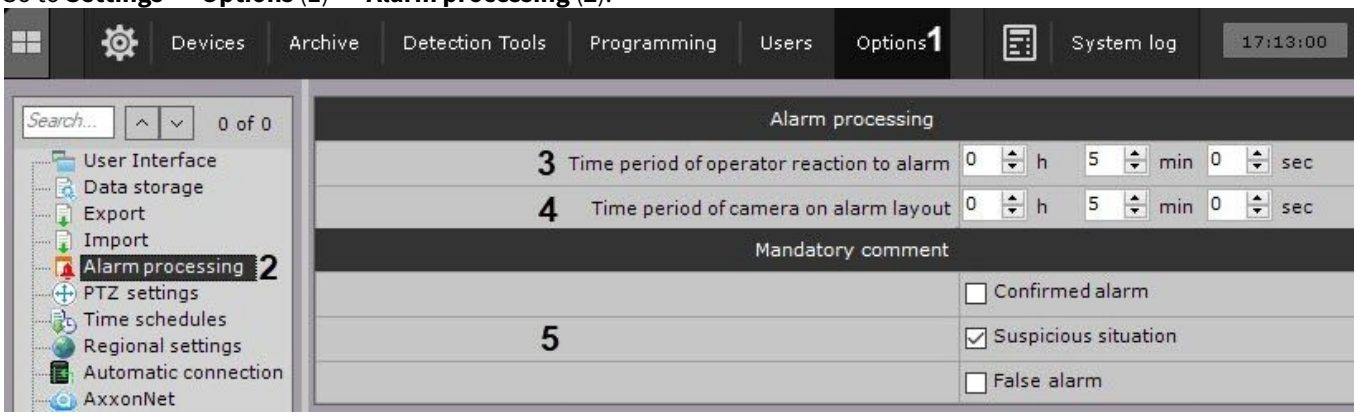
5. Click the **Apply** button.

Configuration of the system log is now complete.

15.10.1.7 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.

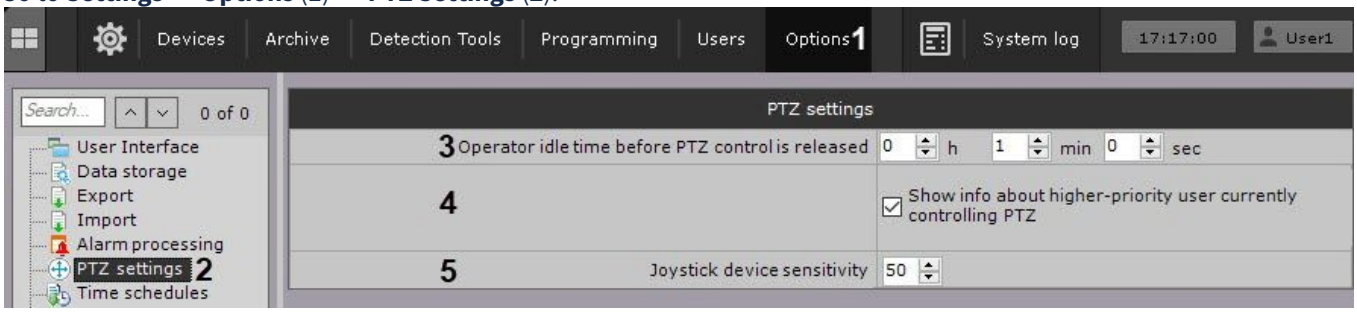
3. Set the maximum time for an alarm to stay on a special layout (**4**, see Working with Special layouts(see page 788)). After the specified time has elapsed, the alarm will be removed from the layout and its place will be taken by the next one, which has not yet been displayed on the layout.
4. Select 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.

15.10.1.8 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(see page 581)). 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(see page 675)
Creating and configuring roles(see page 452)

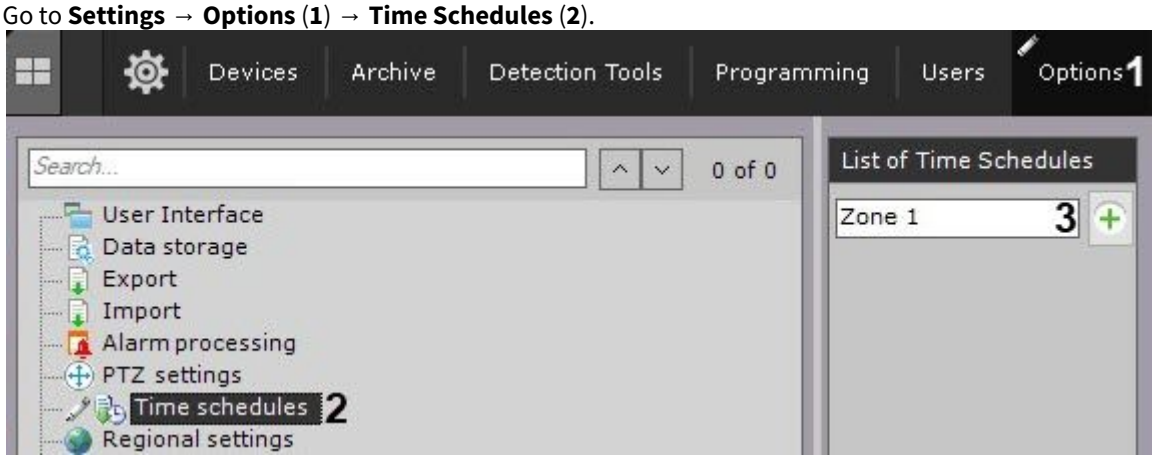
15.10.1.9 Configuring schedules

A schedule consists of all the time intervals for which video streams from video cameras will be recorded to archive.

15.10.1.9.1 Creating schedules

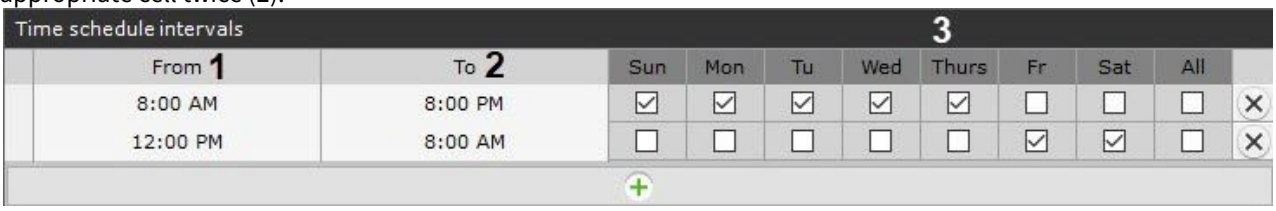
To create a schedule, complete the following steps:

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**).

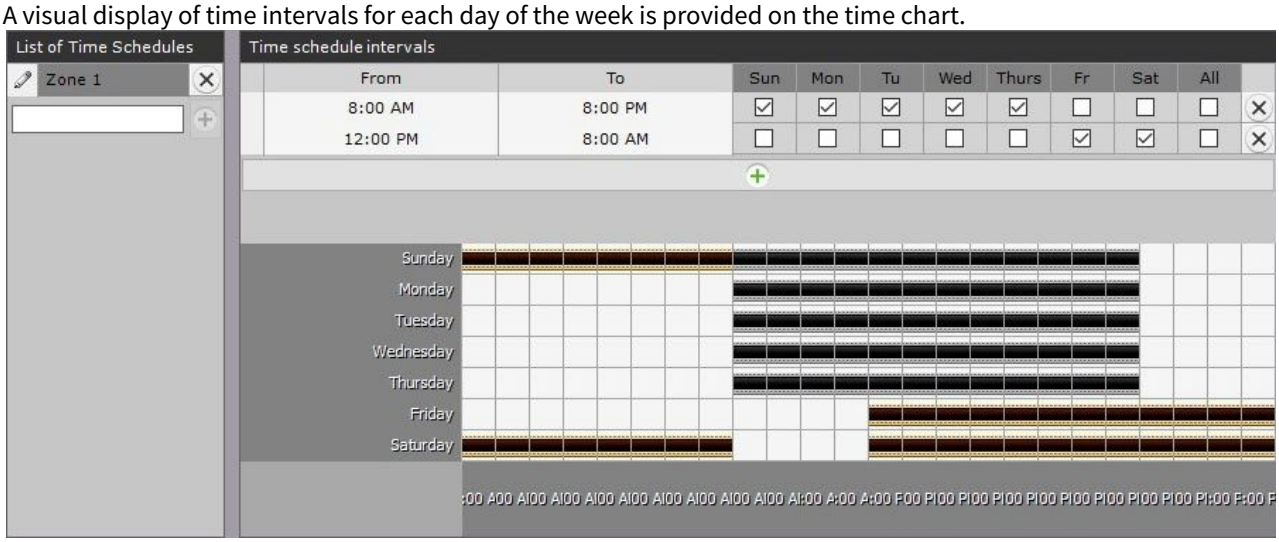


Button	Action
	Shift the interval start back by 1 hour
	Shift the interval start back by 5 minutes
	Shift the interval start ahead by 5 minutes
	Shift the interval start ahead by 1 hour

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.

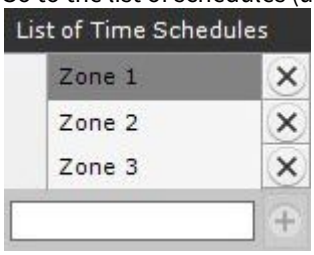
Creation of a schedule is now complete.

Configuring recording to an archive(see page 224)
Create Macros(see page 403)

15.10.1.9.2 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.

15.10.1.10 Configuring the Server ports

On this page:

- Changing the gRPC API port(see page 543)
- Changing the port range of the Server(see page 543)

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(see page 57)).

15.10.1.10.1 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 10. Creating system variable(see page 951)).

15.10.1.10.2 Changing the port range of the Server

To change the port range for a Server, use the Network settings utility (see Network settings utility(see page 899)).

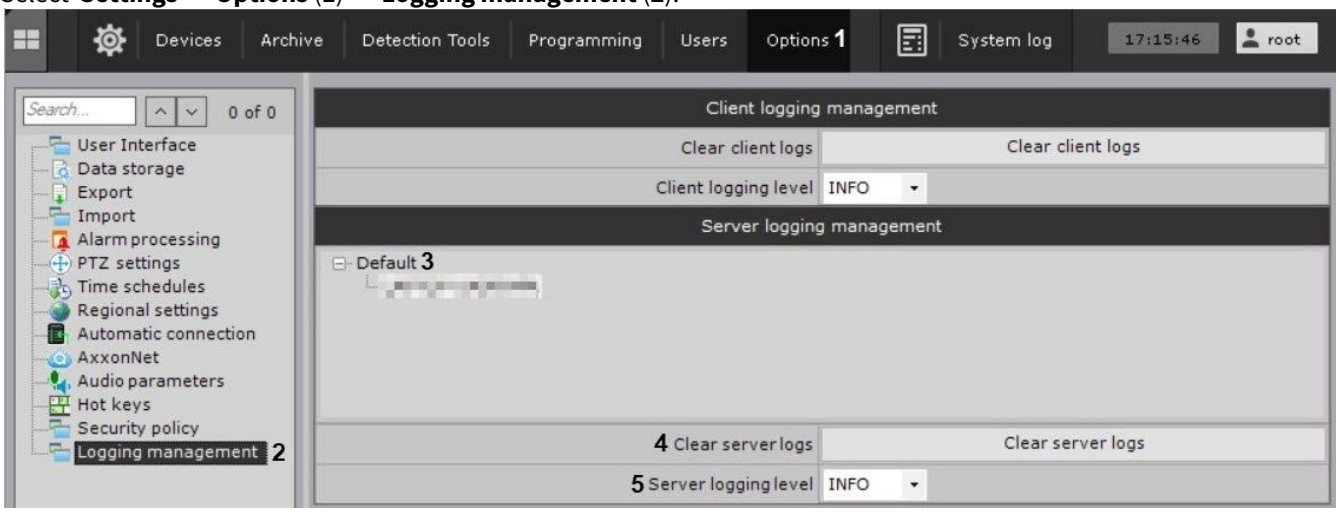
15.10.1.11 Configuring Server logging

By default, the Server logging level is set in a special utility

You can change the logging level of the Server and restart it for changes to take effect. The next time the Server is started, the logging level will correspond to the new settings in the logging management utility (see Log Management Utility(see page 870)).

To change the Server logging level, do as follows:

1. Select **Settings** → **Options** (**1**) → **Logging management** (**2**).



2. Select the Axxon-domain Server where you want to change the logging level (**3**).
3. Select the desired logging level (**5**). Levels are described in more detail here Configuring Logging levels(see page 872).
4. Click **Apply**.

You can also delete all Server logs. Please follow the steps below:

1. Click **Clear server logs** (**4**).
2. Click **Apply**.

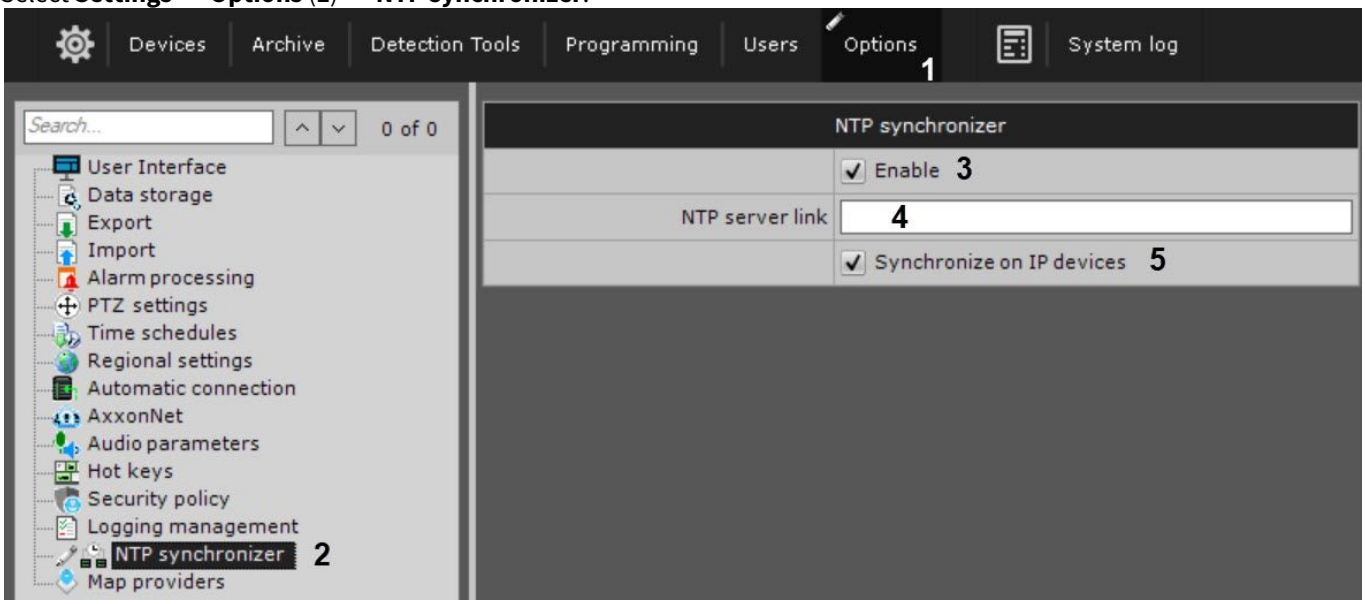
15.10.1.12 Configuring NTP synchronization

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.

15.10.1.13 Vector maps in Axxon One

On the page:

- Raster or vector image(see page 546)
- Google(see page 546)
- OpenStreetMap(see page 550)

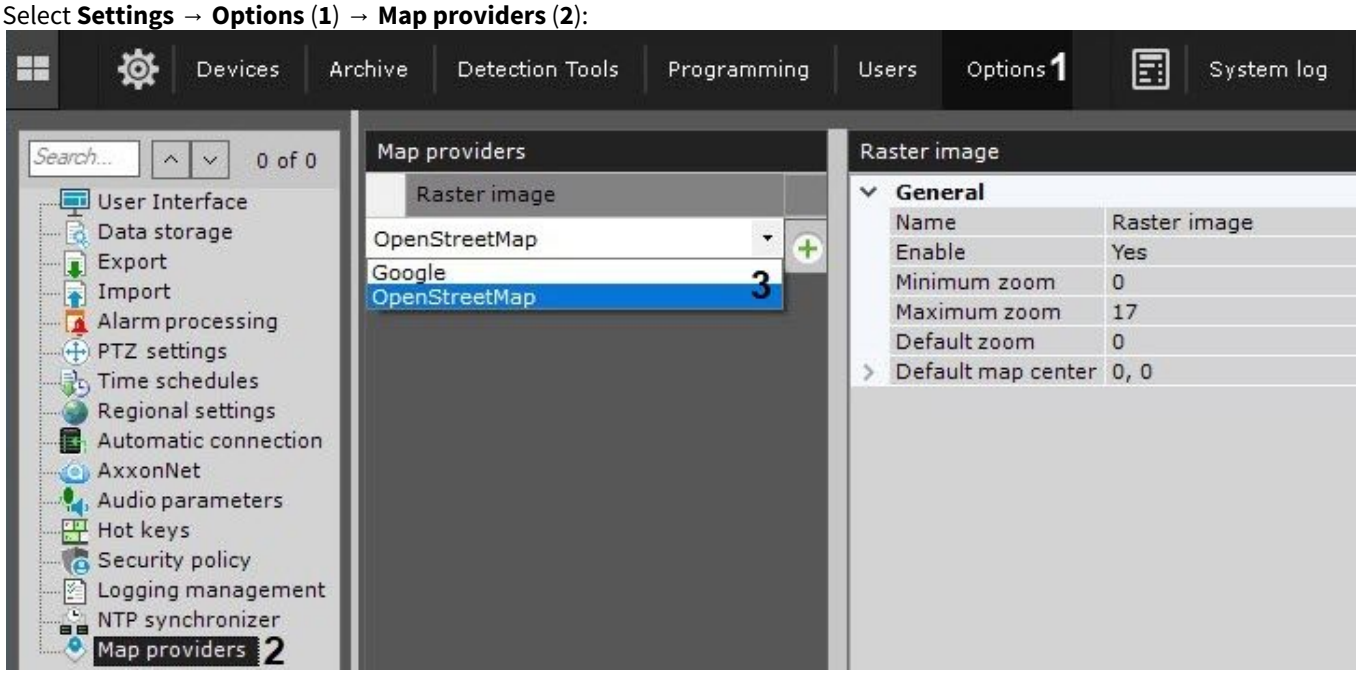
You can use vector maps in *Axxon One*: Raster image, Google Maps, and OpenStreetMap.

> **Attention!**
>
> If you upgrade to *Axxon One* 2.0 from earlier versions, you must add vector maps to *Axxon One* again. The previous settings of vector maps will be saved in the system.

Adding vector maps

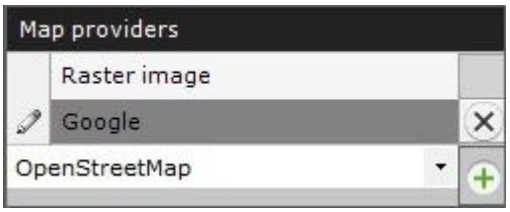
To add vector maps as an interactive map to *Axxon One*, do the following:

1. Select **Settings** → **Options** (**1**) → **Map providers** (**2**):



2. In the **Map providers** table, click the button. From the list, select the necessary map provider (**3**) 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.



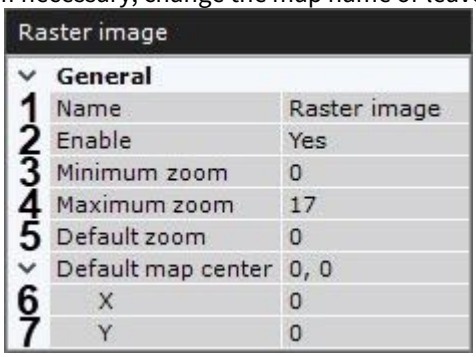
To cancel adding a vector map or to delete a map, click the button.

15.10.1.13.1 Raster or vector image

Raster 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 raster or vector image in *Axxon One*, do the following:

1. If necessary, change the map name or leave the default name (**1**).



2. Enable **Raster or vector image** (**2**) by selecting the **Yes** value from the **Enable** list.
3. Set the minimum and maximum zoom of the map (**3**, **4**). The values must be in the range [0; 19].
4. Set the scale of the map that will be displayed by default (**5**). The value must be in the range [0; 19].
5. Set the coordinates of the map center that will be displayed by default:
   a. **X**—latitude (**6**);
   b. **Y**—longitude (**7**).
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(see page 99), Starting an Axxon One Client(see page 94)).
8. Configure the map display (see Adding a new map(see page 510)).

Configuring the display of the Raster or vector image map in *Axxon One* is complete.

15.10.1.13.2 Google

You can use Google Maps in *Axxon One*. To use Google Maps 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://mapsplatform.google.com/pricing/.
   c. Configure Google Maps using Maps Static API[162] and Maps JavaScript API[163].

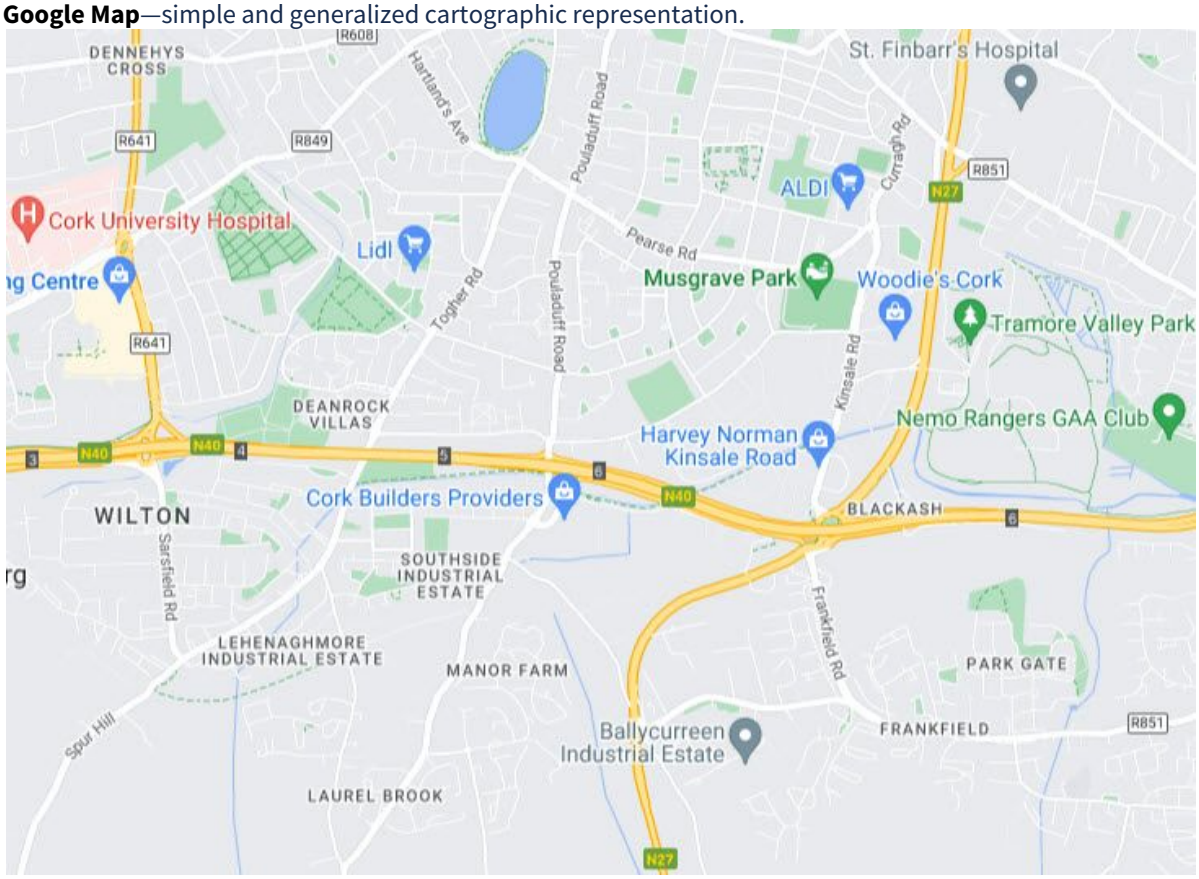
162 https://developers.google.com/maps/documentation/maps-static
163 https://developers.google.com/maps/documentation/javascript

2. Configure Google maps display in *Axxon One:*
   a. If necessary, change the provider name or leave the default name (**1**).

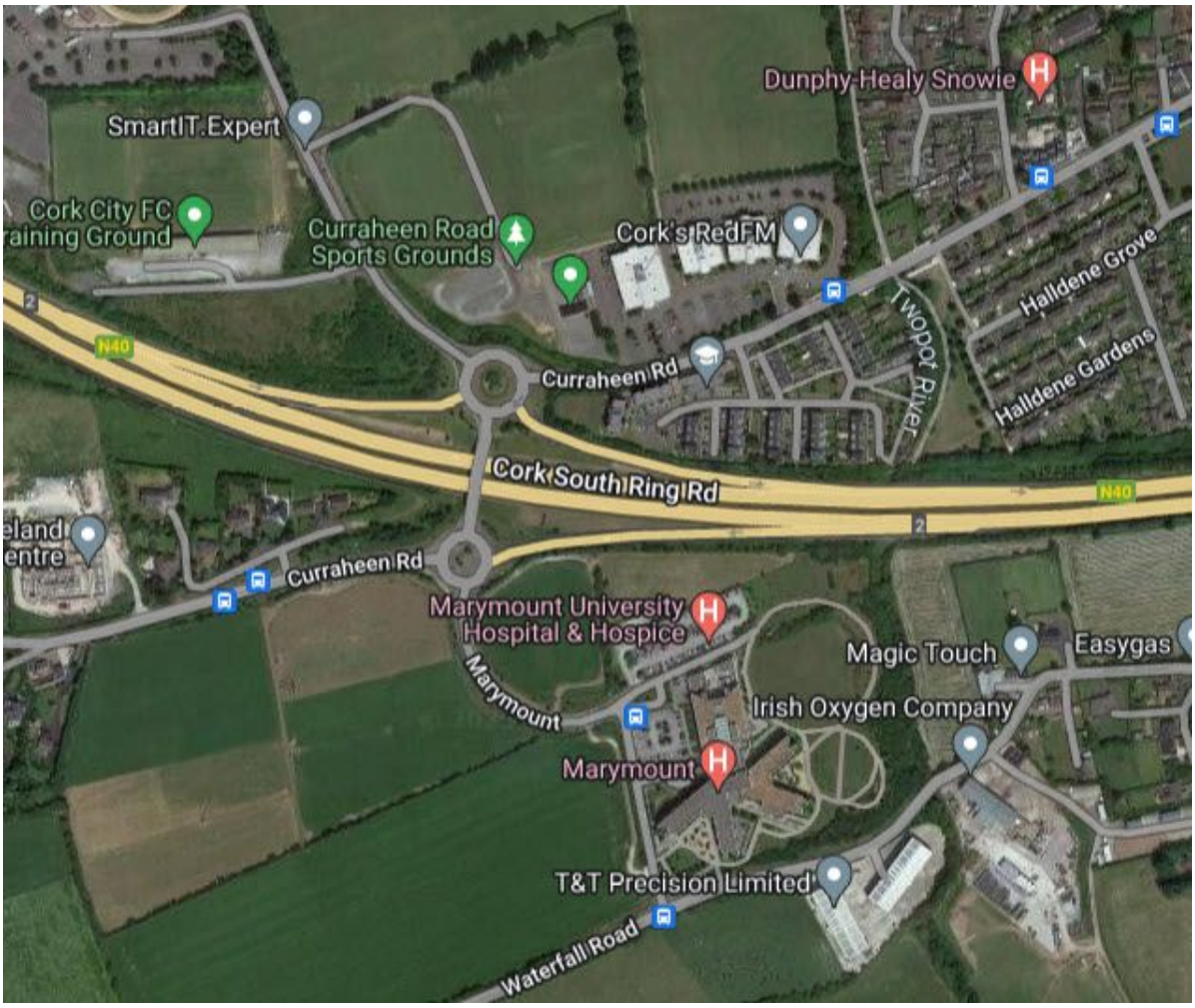
Google		
	General	
1	Name	Google
2	Api key	
	Google Map	
3	Name	Google Map
4	Enable	Yes
5	Minimum zoom	3
6	Maximum zoom	19
7	Default zoom	9
	Default map center	0, 0
8	X	0
9	Y	0
	Google Hybrid	
	Name	Google Hybrid
	Enable	No
	Minimum zoom	3
	Maximum zoom	17
	Default zoom	9
	Default map center	0, 0
	Google Satellite	
	Name	Google Satellite
	Enable	No
	Minimum zoom	3
	Maximum zoom	17
	Default zoom	9
	Default map center	0, 0

   b. Enter the **ApiKey** (**2**).
   c. Select the type of the map display:

i. **Google Map**—simple and generalized cartographic representation.



ii. **Google Hybrid**—satellite cartographic representation combined with a simple and generalized cartographic representation.


Dunphy Healy Snowie
SmartIT.Expert
Cork City FC
aining Ground
Curraheen Road
Sports Grounds
Cork's RedFM
Halldene Grove
Halldene Gardens
Twopot River
N40
Curraheen Rd
Cork South Ring Rd
N40
2
eland
entre
Curraheen Rd
Marymount University
Hospital & Hospice
Magic Touch
Easygas
Marymount
Irish Oxygen Company
Marymount
T&T Precision Limited
Waterfall Road

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(see page 510)).

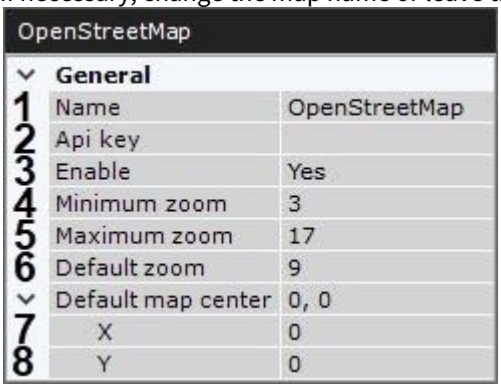
d. Configure the settings of the selected type of the map display:
   i. If necessary, change the map name or leave the default name (**3**).
   ii. Enable **Google Map**/**Google Hybrid**/**Google Satellite** (**4**) by selecting the **Yes** value from the **Enable** list.
   iii. Set the minimum and maximum zoom of the map (**5**, **6**). The values must be in the range [0; 19].
   iv. Set the scale of the map that will be displayed by default (**7**). The value must be in the range [0; 19].
   v. Set the coordinates of the map center that will be displayed by default:
      1. **X**—latitude (**8**);
      2. **Y**—longitude (**9**).
e. Click the Apply button. To cancel the changes, click the Cancel button.
f. Restart the *Axxon One* Client (see Shutting down an Axxon One Client(see page 99), Starting an Axxon One Client(see page 94)).
g. Configure the map display (see Adding a new map(see page 510)).

Configuring the display of Google maps in *Axxon One* is complete.

15.10.1.13.3 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 Static Tiles 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 or leave the default name (**1**).



   b. Enter the **ApiKey** (**2**).
   c. Enable **OpenStreetMap** (**3**) by selecting the **Yes** value from the **Enable** list.
   d. Set the minimum and maximum zoom of the map (**4**, **5**). The values must be in the range [0; 19].
   e. Set the scale of the map that will be displayed by default (**6**). The value must be in the range [0; 19].
   f. Set the coordinates of the map center that will be displayed by default:
      i. **X**—latitude (**7**);
      ii. **Y**—longitude (**8**).
   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(see page 99), Starting an Axxon One Client(see page 94)).
4. Configure the map display (see Adding a new map(see page 510)).

Configuring the display of OpenStreetMap in *Axxon One* is complete.

15.10.2 Client settings

15.10.2.1 Configuring the user interface

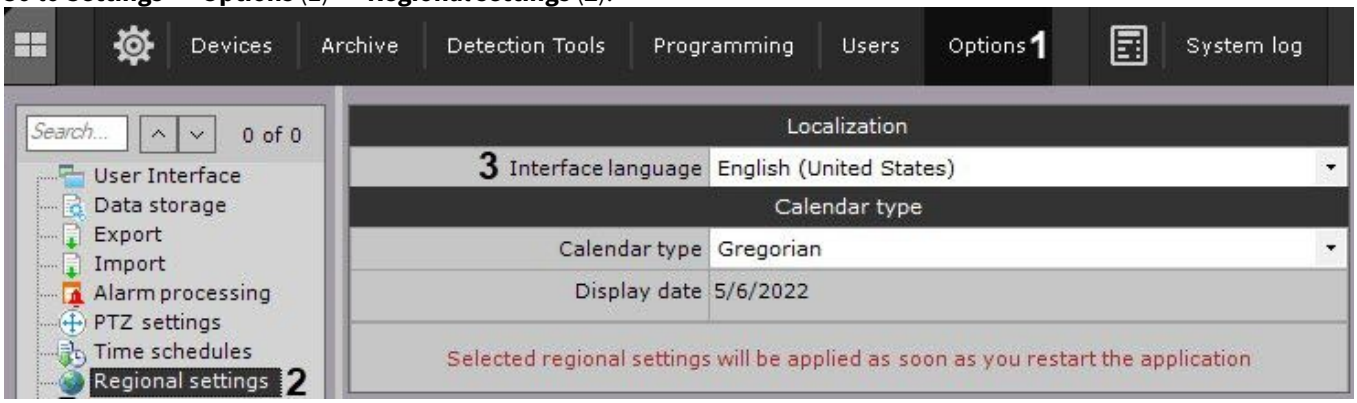
15.10.2.1.1 Selecting the interface language

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(see page 99), Starting an Axxon One Client(see page 94)).

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(see page 100), Starting a Server(see page 94)).

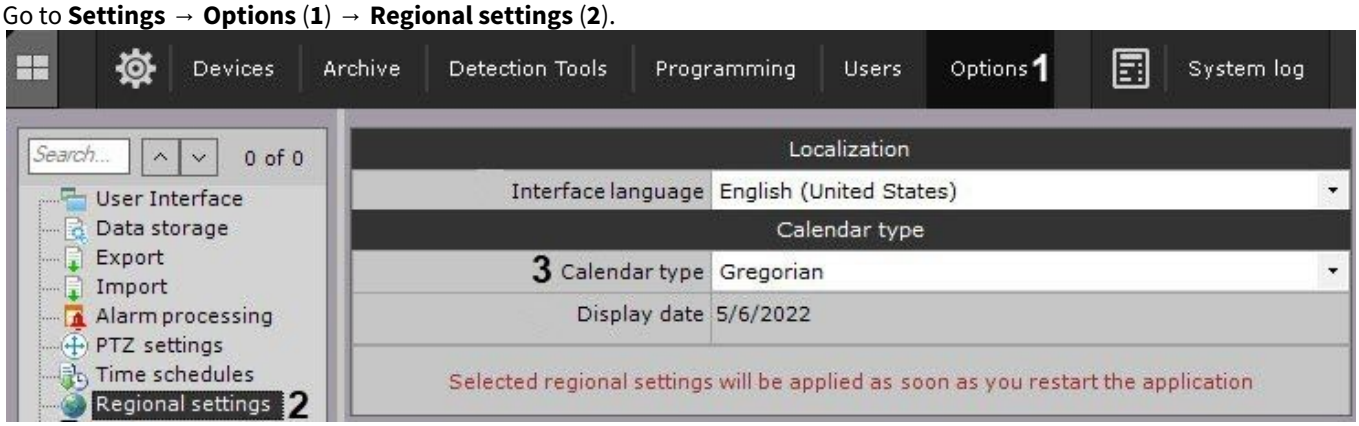
The language of the events in the system log is changed.

15.10.2.1.2 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(see page 99), Starting an Axxon One Client(see page 94)).

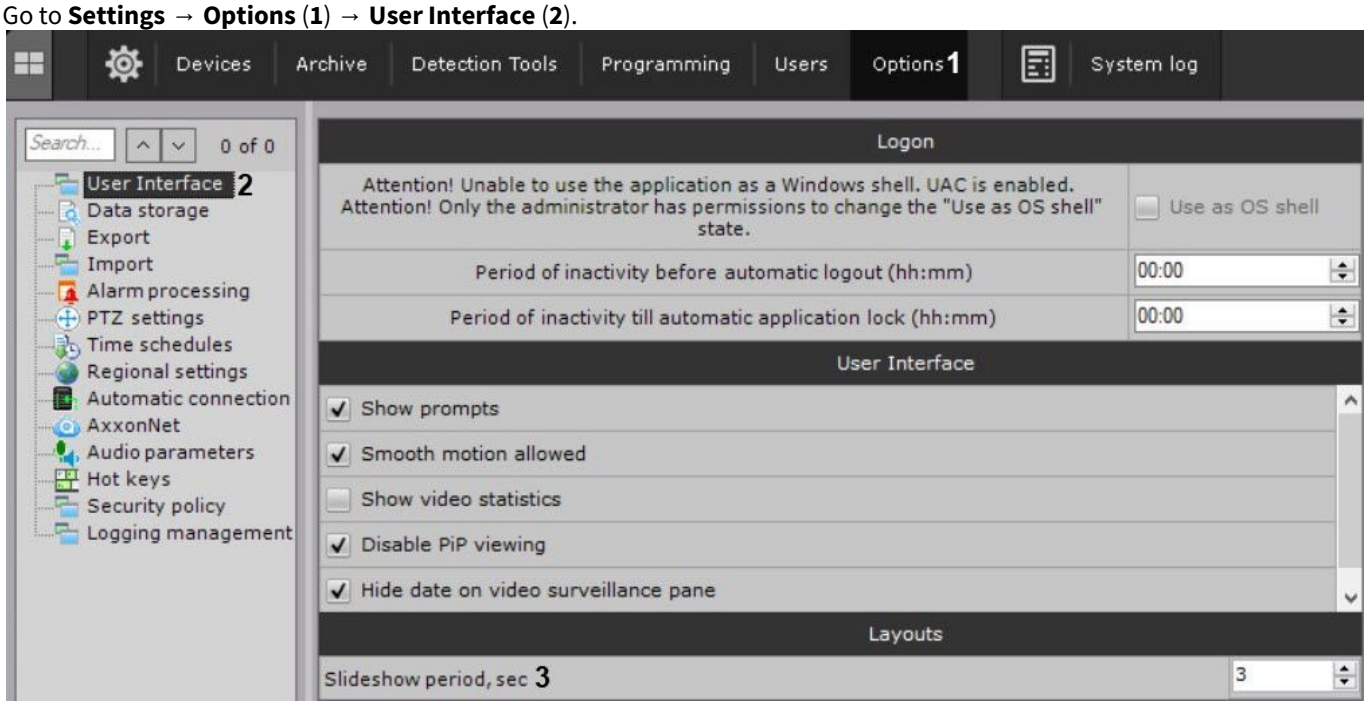
When *Axxon One* is restarted, the selected calendar type will be applied.

15.10.2.1.3 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.

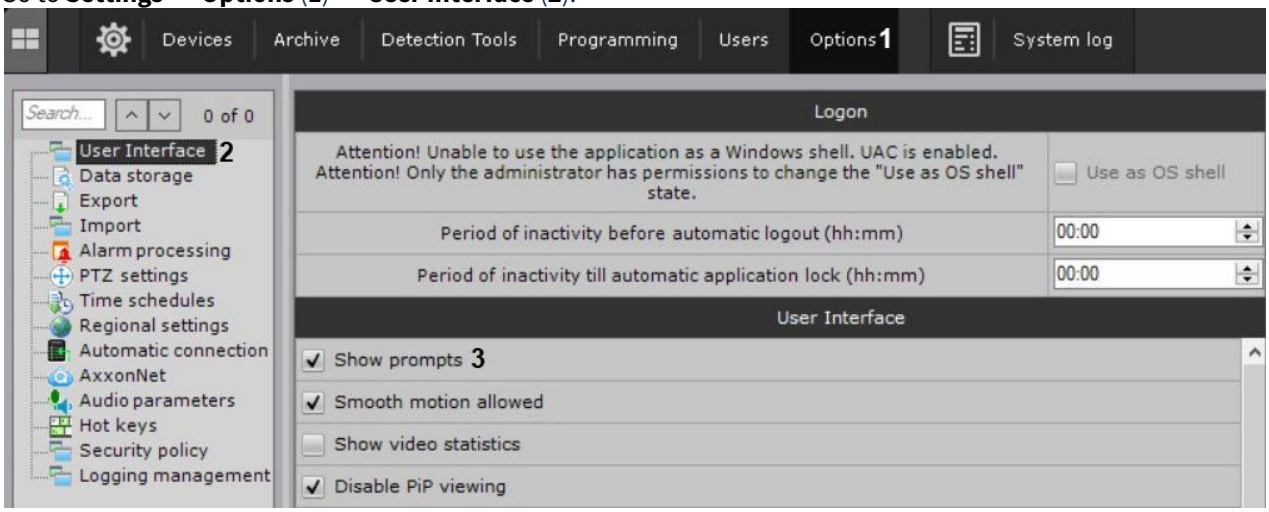
> **Note**
>
> Only the users with the **Layout editing** permission can switch the modes (see Creating and configuring roles(see page 452)).

15.10.2.1.4 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.

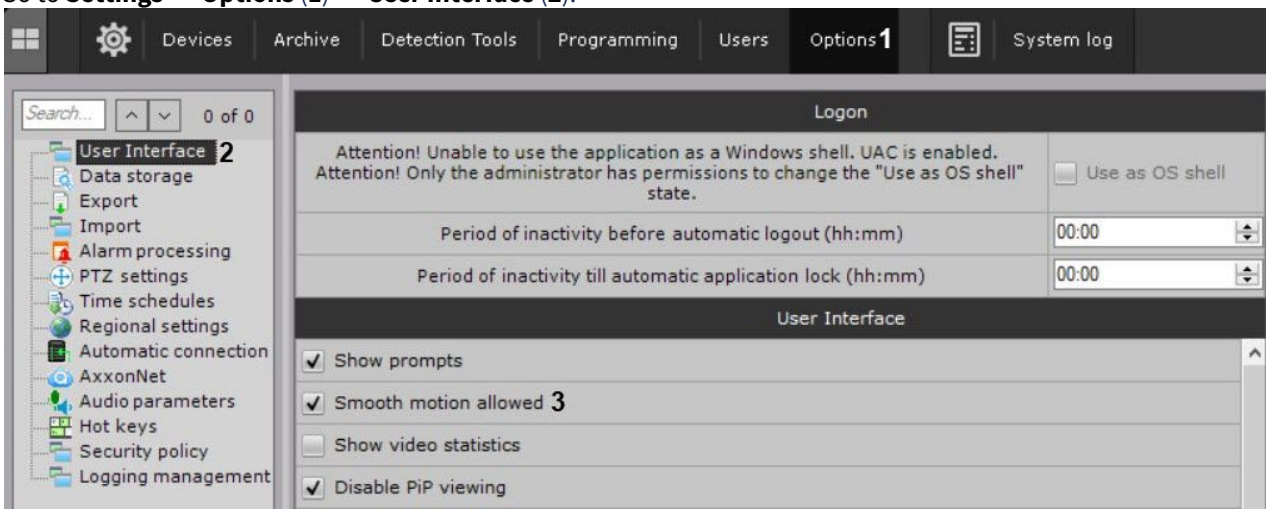
Prompts are now disabled. You can re-enabled prompts by setting the **Show prompts** checkbox.

15.10.2.1.5 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.

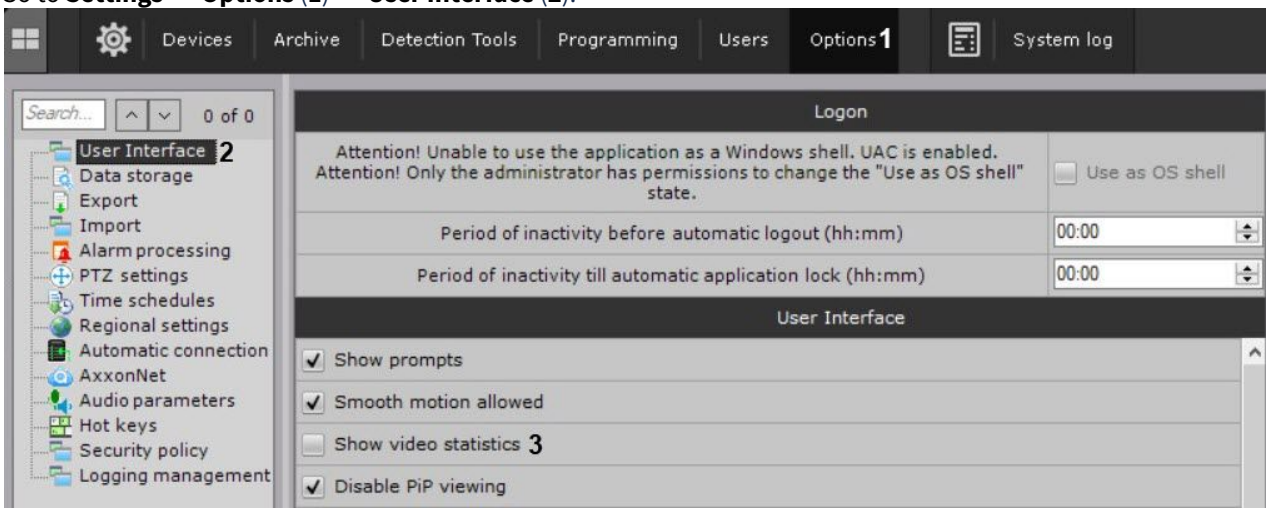
15.10.2.1.6 Configuring display of video statistics

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.

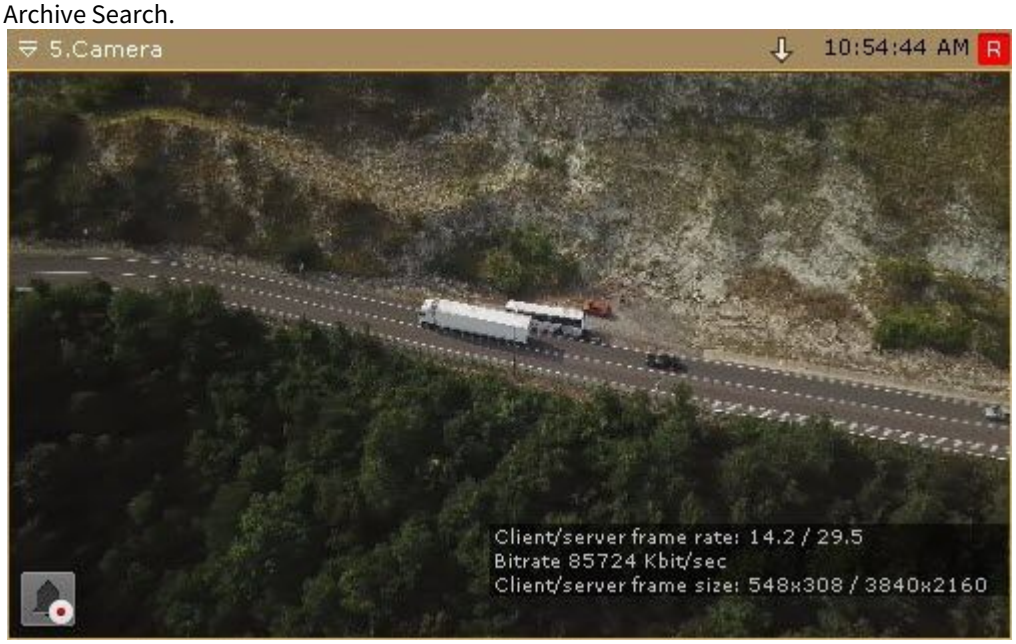
To display video statistics, do the following:

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.

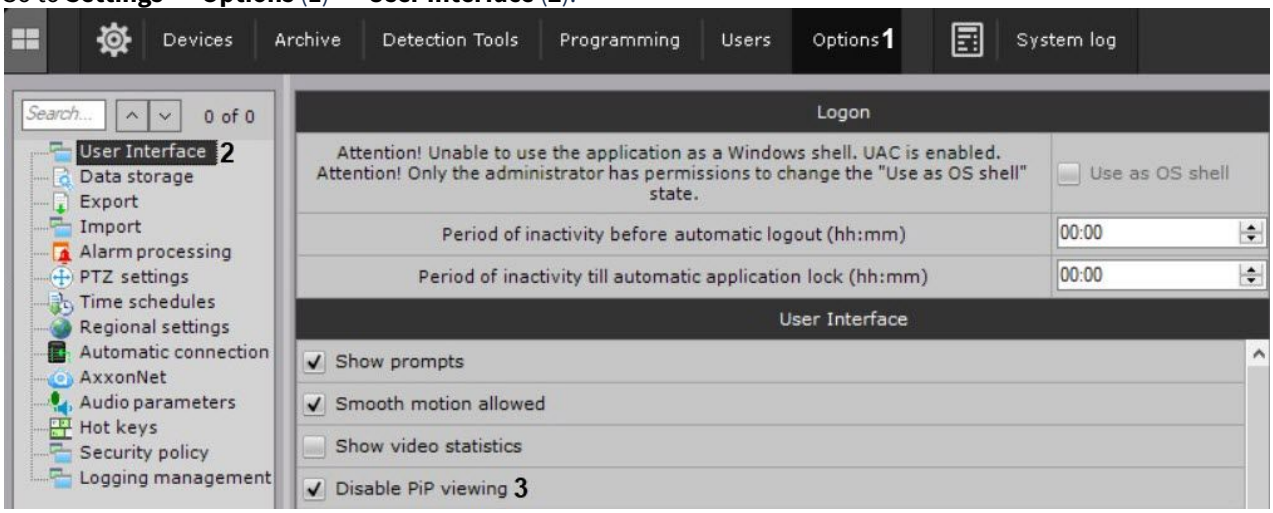


15.10.2.1.7 Configuring preview of alarm events

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.

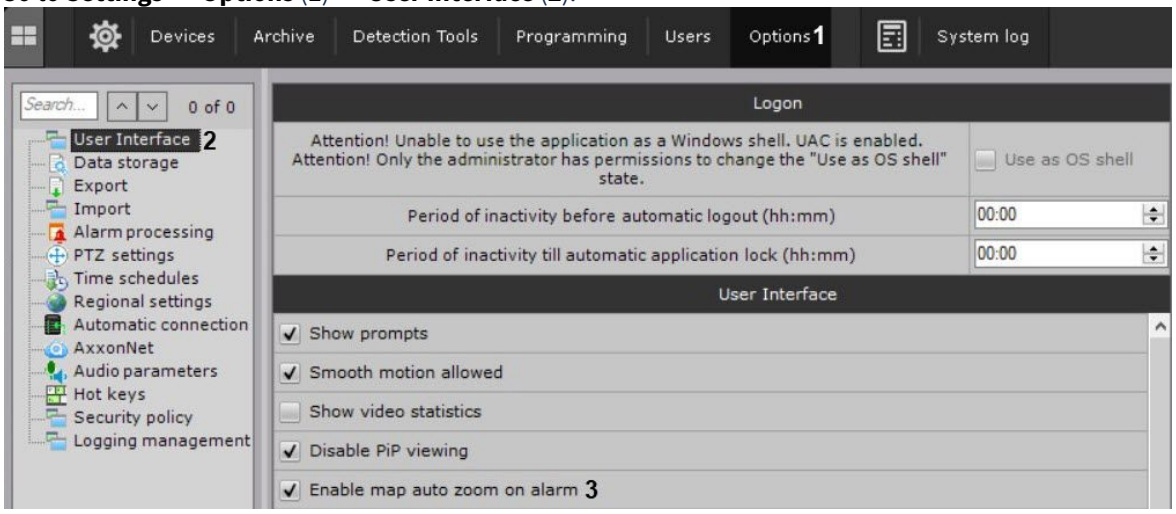
Preview of alarm events is disabled.

15.10.2.1.8 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.

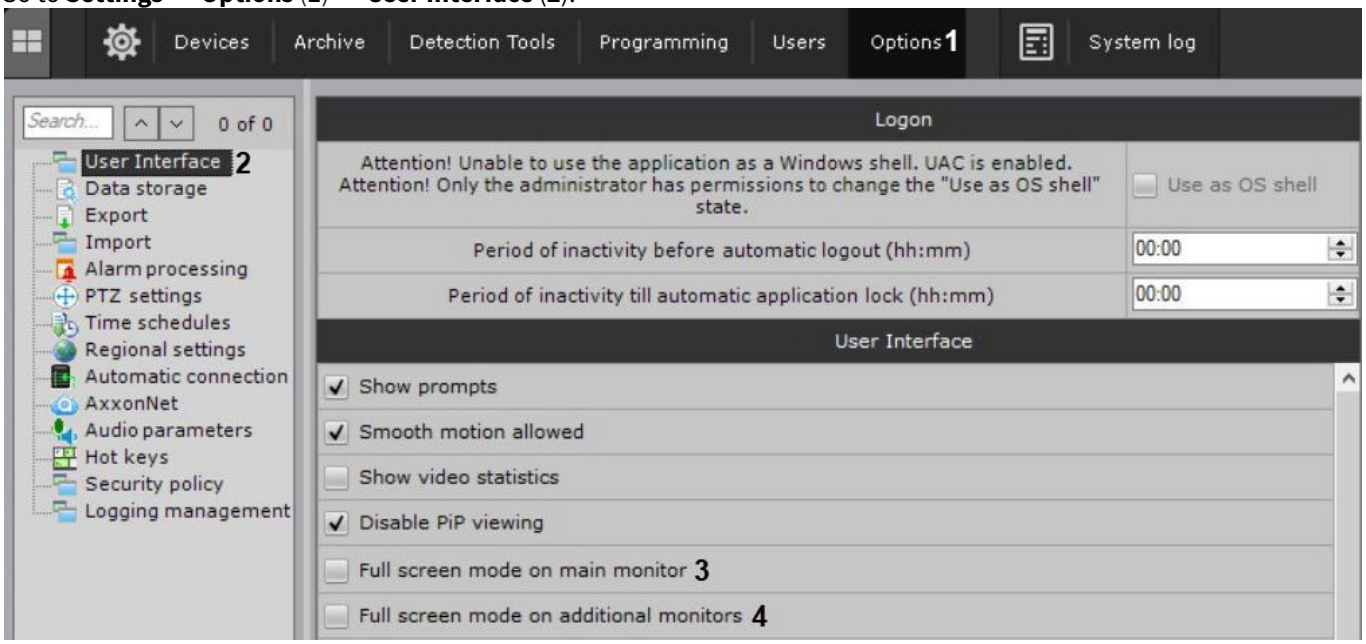
15.10.2.1.9 Configuring the Client screen mode (full screen or window)

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(see page 99), Starting an Axxon One Client(see page 94)).

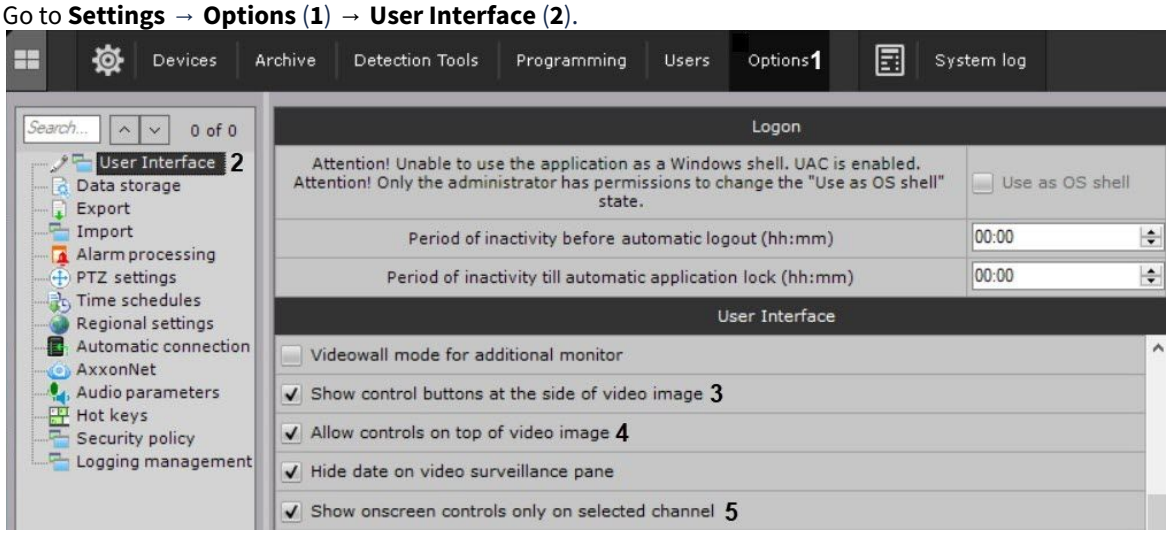
The window mode is configured. The *Axxon One* Client will be displayed in window mode on new start.

15.10.2.1.10 Configuring the display of the surveillance window

Surveillance window(see page 628)

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(see page 654)) and the immersive mode button (see Immersive mode(see page 802)).

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(see page 644)).

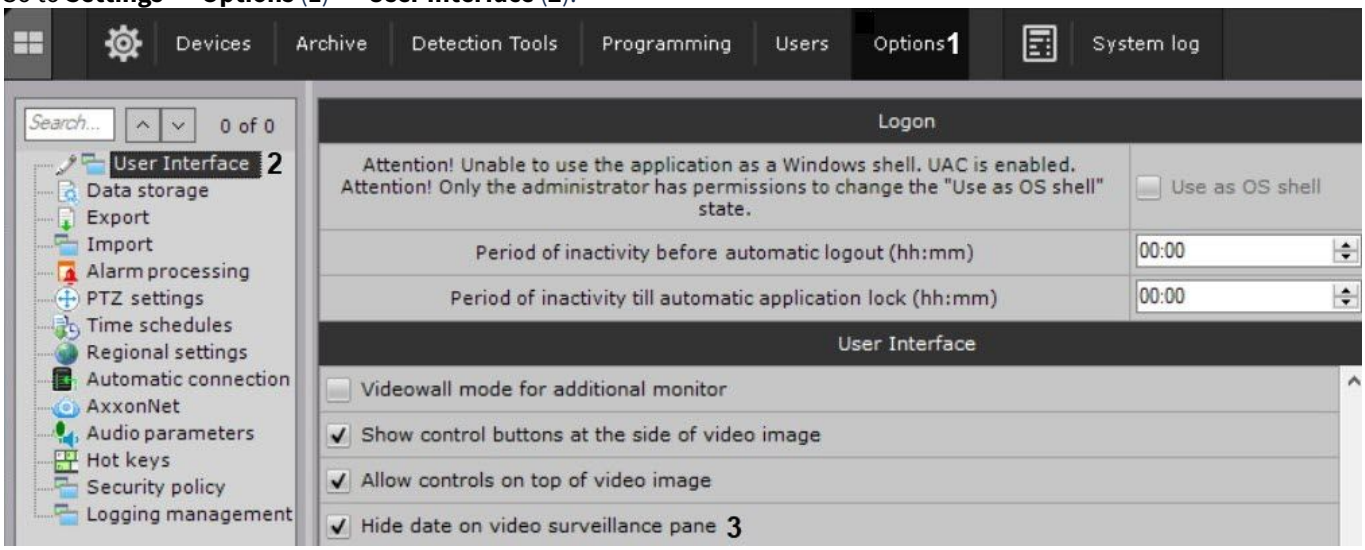
Configuring the display of the surveillance window is complete.

15.10.2.1.11 Configuring time display

By default, the time indicator (see Time Display(see page 631)) 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(see page 786)).

The time indicator is configured. The date will be displayed to the left of the time.

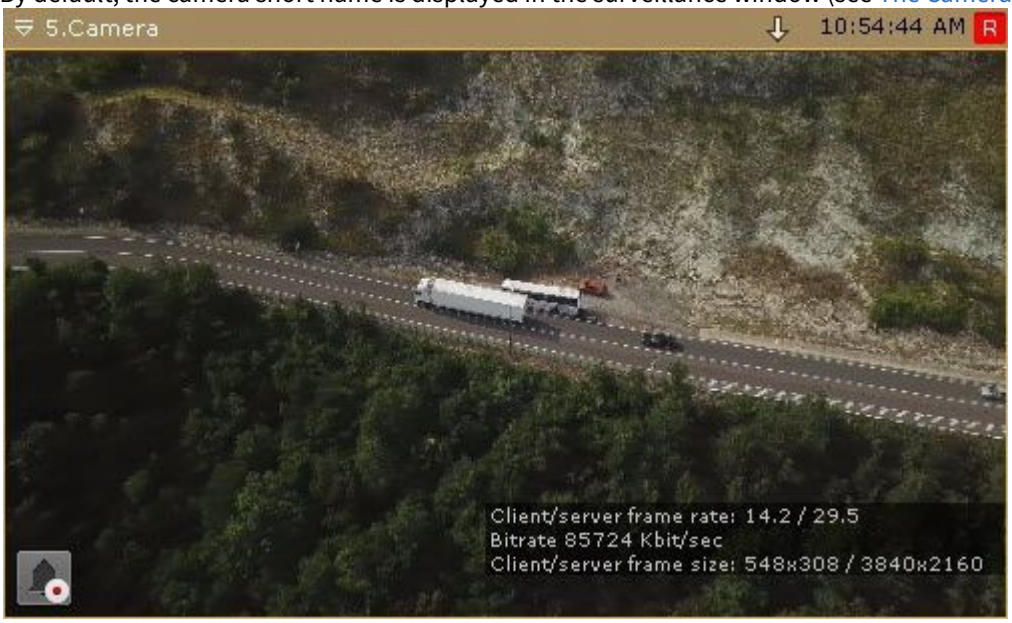
You can also hide the time indicator in the surveillance window. To do it, do the following:

1. Go to the role settings (see Creating and configuring roles(see page 452)).
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.

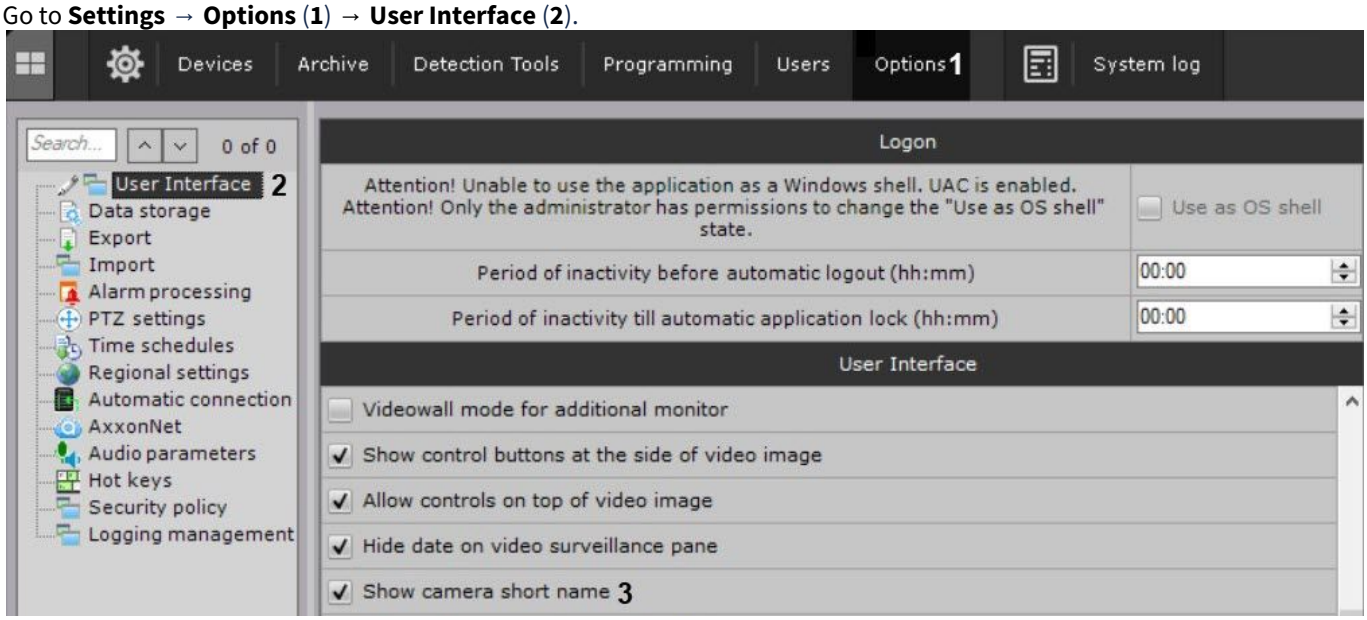
15.10.2.1.12 Configuring the display of the camera short name

By default, the camera short name is displayed in the surveillance window (see The Camera object(see page 122)).



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(see page 786)).

The camera short name display is disabled.

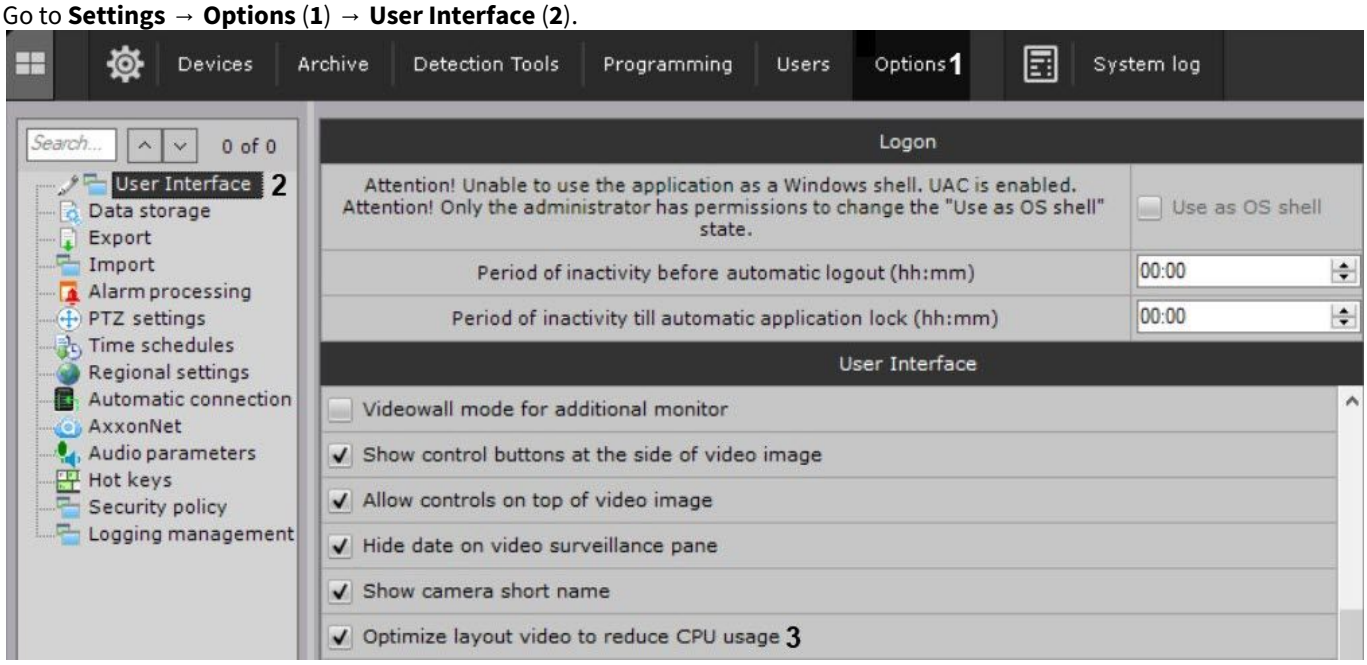
15.10.2.1.13 Optimizing video image on the layout

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**).

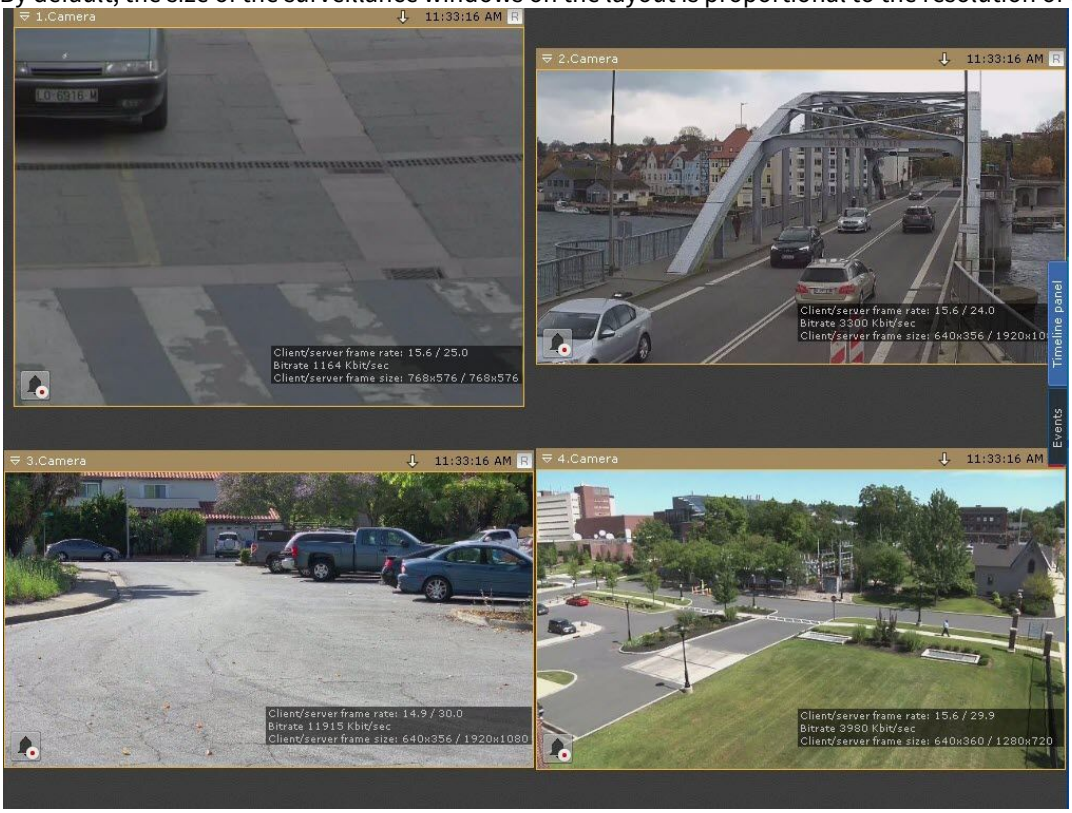


2. Clear the **Optimize layout video to reduce CPU usage** checkbox (**3**).
3. Click the **Apply** button.

Video image optimization is disabled.

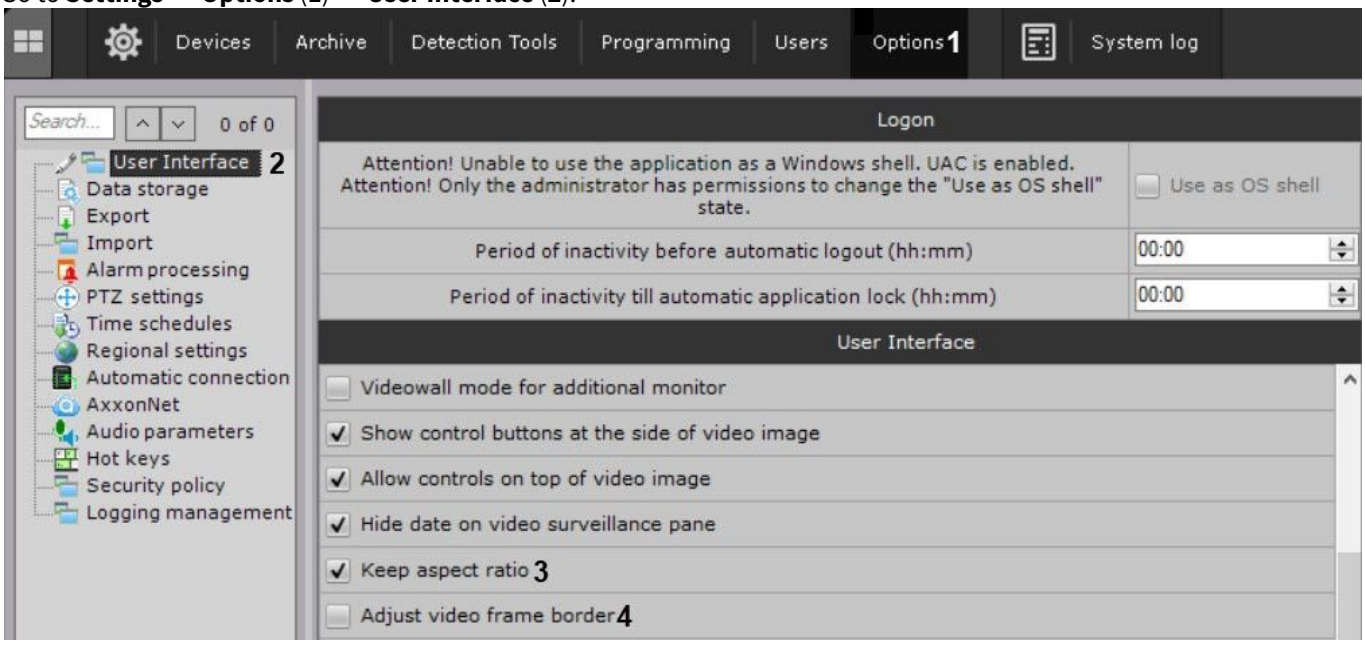
15.10.2.1.14 Configuring video display on the layout

By default, the size of the surveillance windows on the layout is proportional to the resolution of the video image.



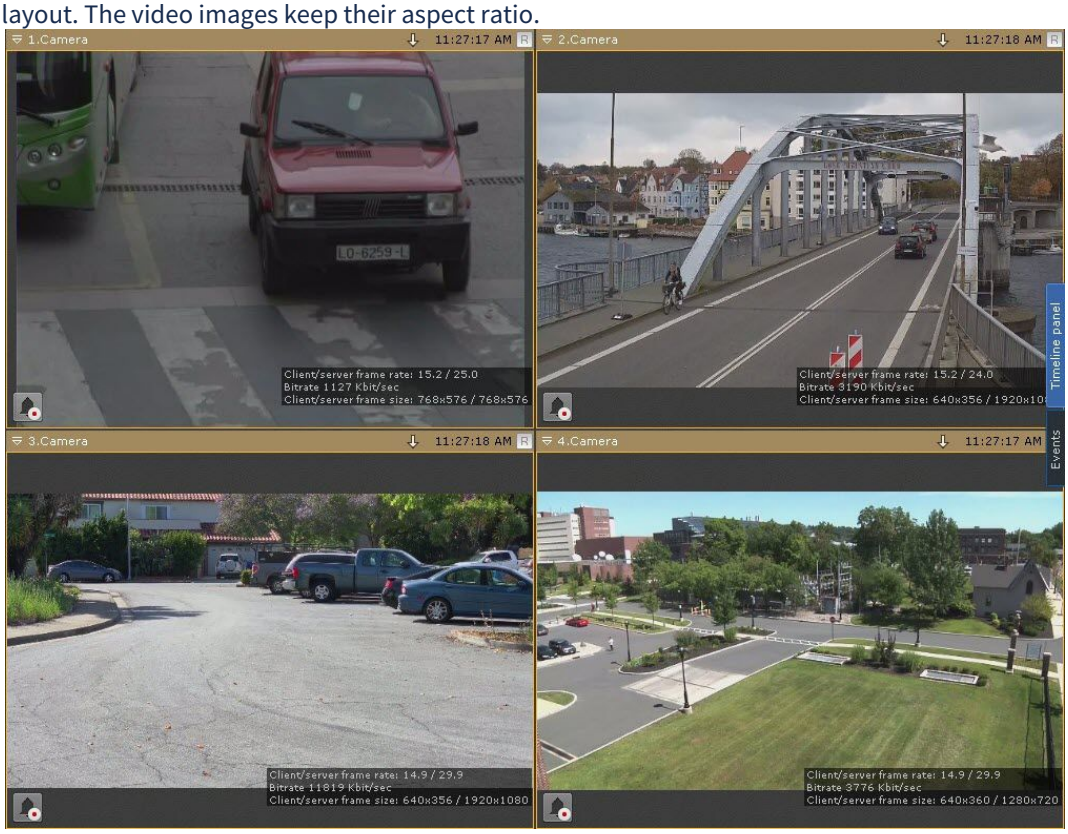
For the surveillance windows to be of a fixed size and occupy the entire area of the layout, do the following:

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(see page 786)).

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(see page 786)).

Configuring the surveillance windows is complete. The video image is expanded to the entire surveillance window.

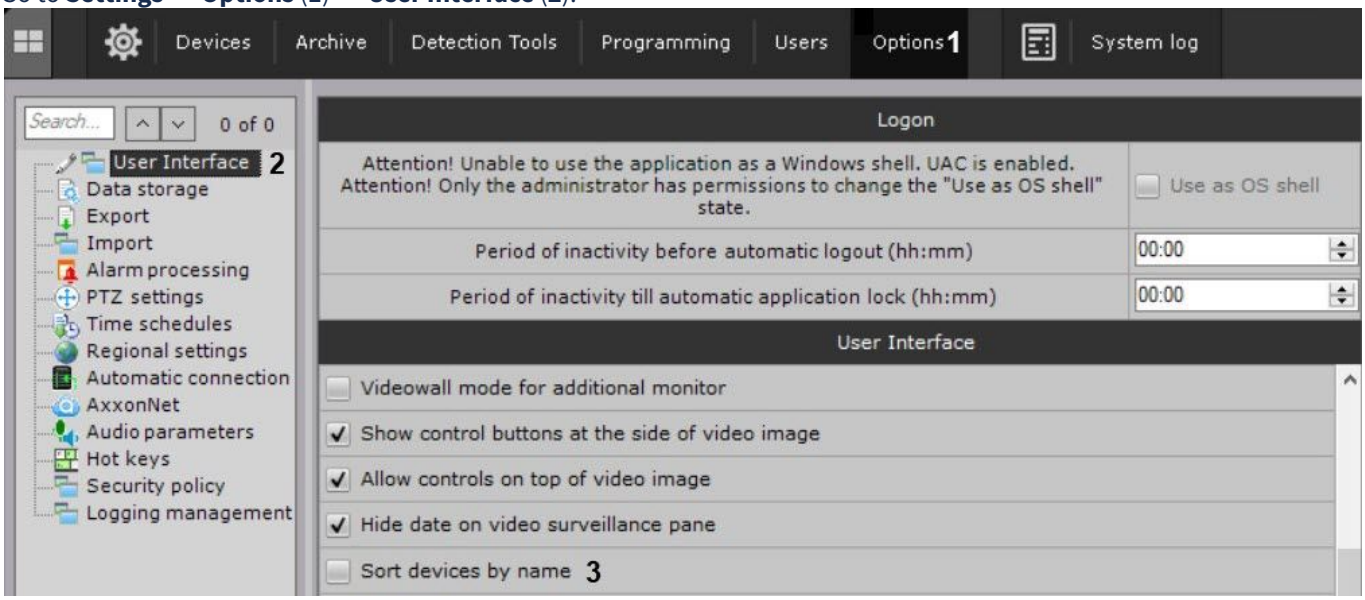
Configuring layouts(see page 471)
Configuring viewing tiles(see page 484)

15.10.2.1.15 Configuring camera sorting on Objects Panel

By default, the cameras on the Objects Panel (see Objects Panel(see page 648)) are sorted by the short name (see The Camera object(see page 122)).

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.

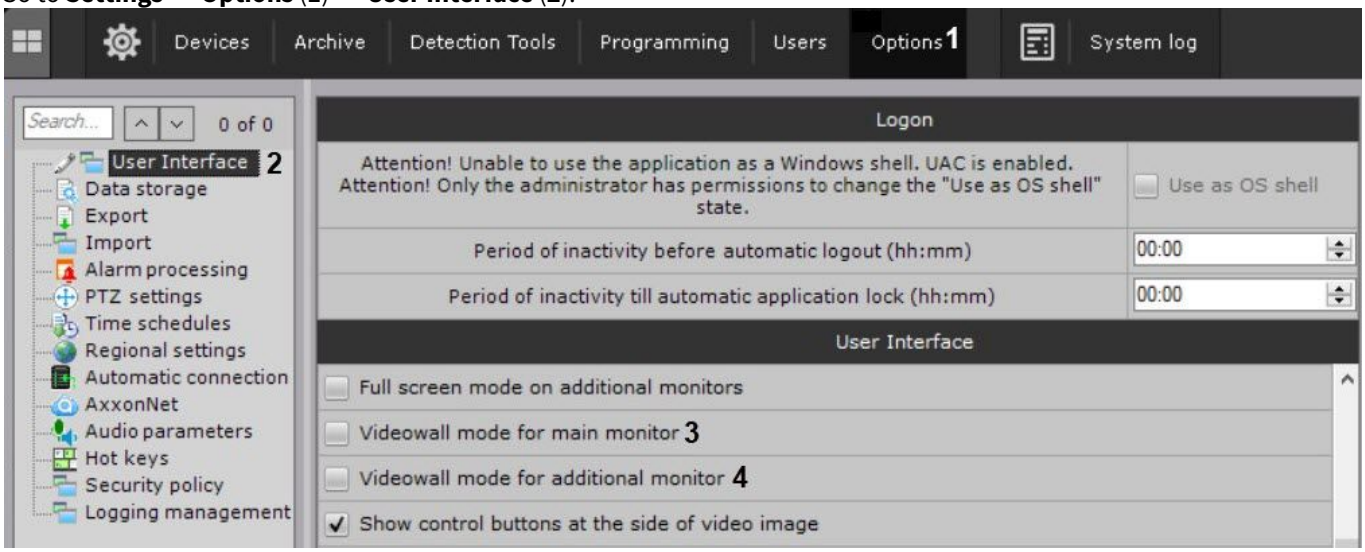
Sorting the cameras by the name on the Objects Panel is enabled.

15.10.2.1.16 Configuring the videowall mode

Configuring Videowall(see page 508)

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(see page 99), Starting an Axxon One Client(see page 94)).

The videowall mode is configured.

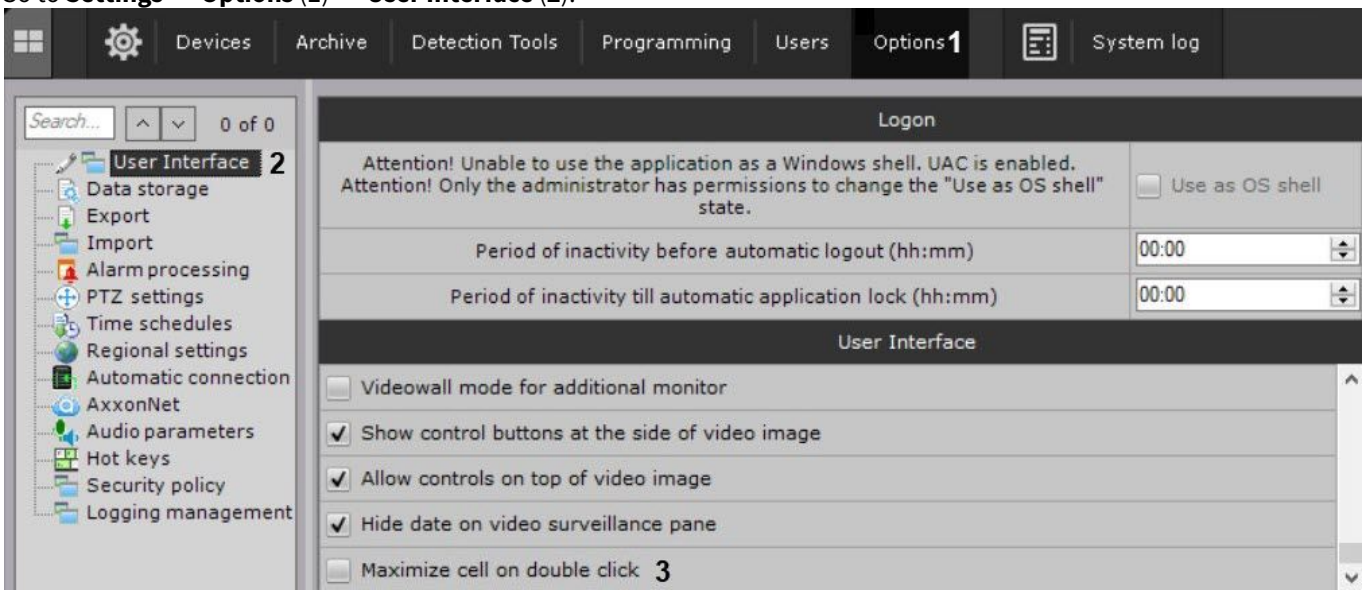
At a new start of the *Axxon One* Client:

1. On the main monitor, the panel pin button won't be active (see Interface of the Axxon One Software Package(see page 56)). The Archive navigation panel and the Event Board (see The Archive Navigation Panel(see page 636)), the Layouts panel (see The Layouts panel(see page 644)), messages about system errors that occurred (see Control in Live Video mode(see page 818)), the Alert panel (see Alert panel(see page 646)) won't be displayed.
2. The additional monitor won't display the Objects panel (see Objects Panel(see page 648)), the Archive navigation panel and the Event Board (see The Archive Navigation Panel(see page 636)), the Alert panel (see Alert panel(see page 646)).
3. The map (see Working with the interactive map(see page 795)) will be available on the main monitor and on the additional monitor.

15.10.2.1.17 Configuring cell maximization on double click

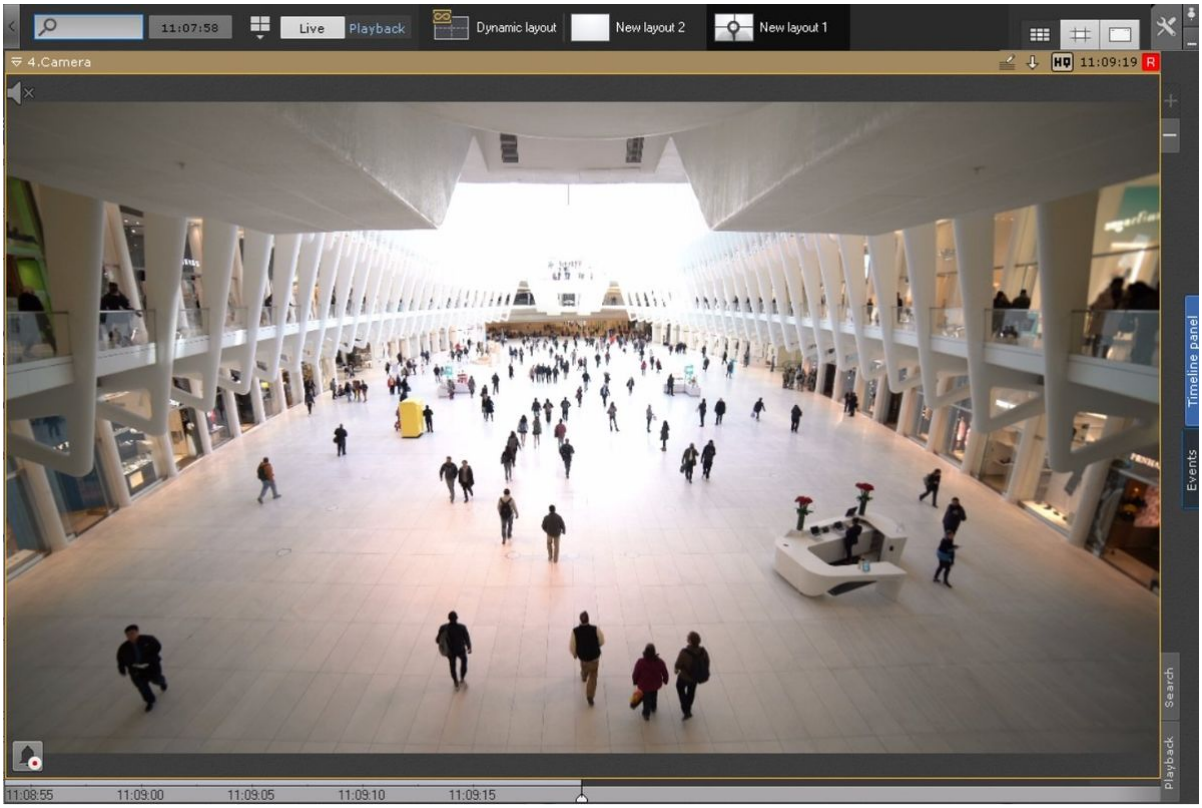
To maximize the cell on double click, do the following:

1. Go to **Settings** → **Options** (**1**) → **User Interface** (**2**).

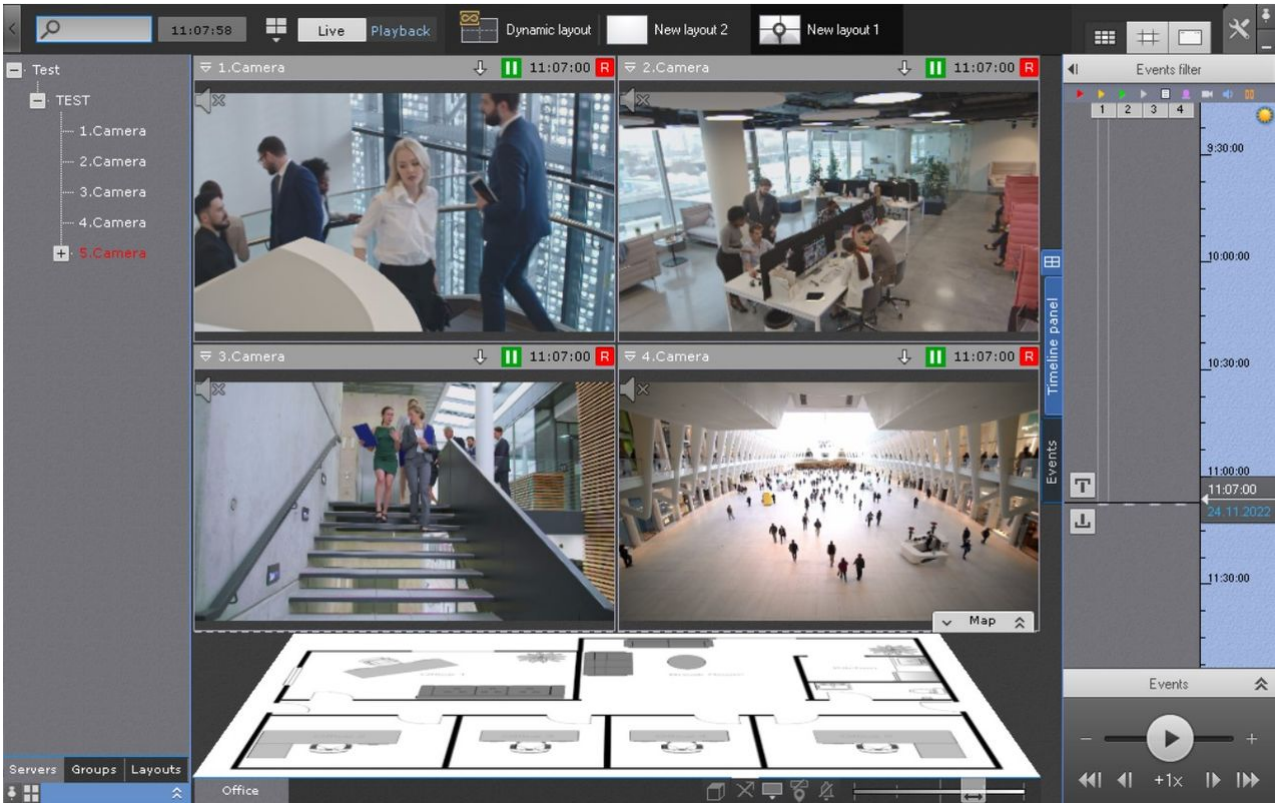


2. Set the **Maximize cell on double click** checkbox (**3**).
3. Click the **Apply** button.

Configuring the cell maximization on double click is complete. When you double click the surveillance window, the side panels and the map won't be displayed on the main and on the additional monitor. The side panel buttons will always be displayed.



You can exit the full-screen mode in the same way. The side panels and the map will be displayed again.



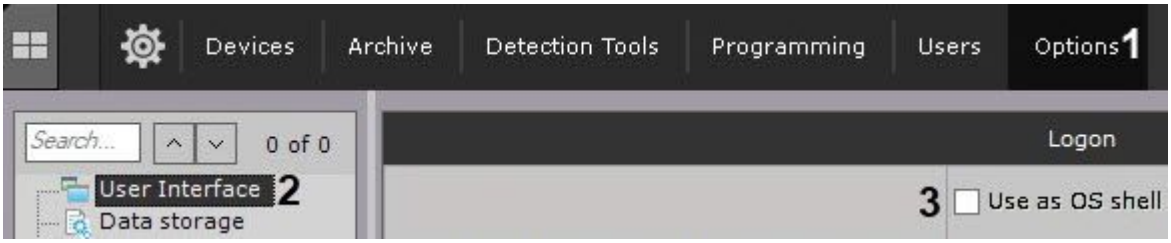
15.10.2.2 Configuring how Axxon One starts

15.10.2.2.1 Configuring Axxon One 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 OS 8, 8.1 and 10 you also need to make changes to the registry[164] and reboot your PC.

164 http://winaero.com/blog/how-to-turn-off-and-disable-uac-in-windows-10/

15.10.2.2.2 Configuring Cross-System Client and autologon

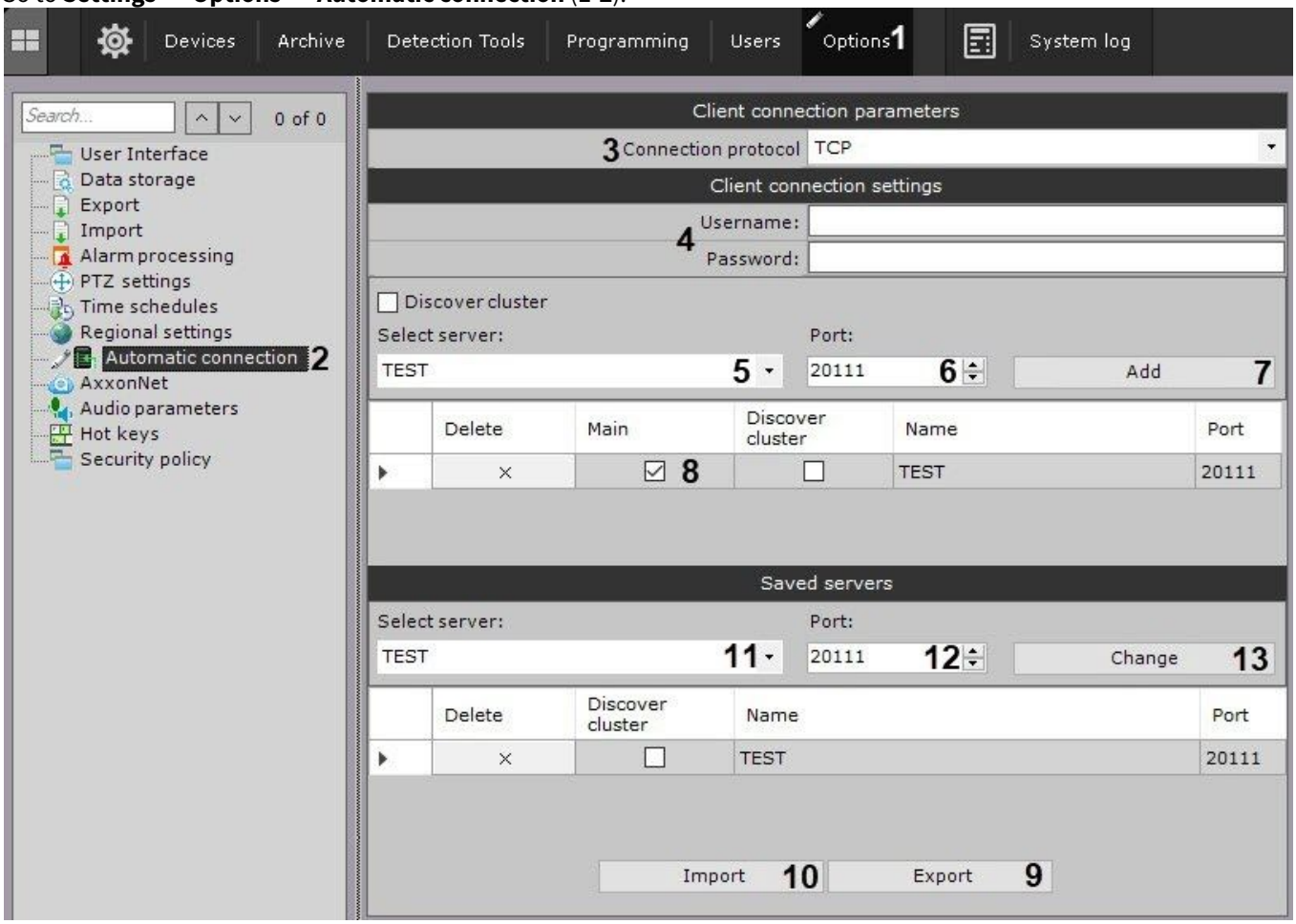
It is possible for the Client to automatically connect to Servers on different Axxon domains – Cross-System Client(see page 101).

For this to take place, the following conditions must be true:

- Professional or Universe license has been activated on each Server to which the Client is connected;
- connection to all Servers made via with the same user name/password combination on each Axxon domain;
- Server names and IP addresses are unique.

Configuration of automatic connection to Servers on different Axxon domains is performed as follows:

1. Go to **Settings** → **Options** → **Automatic connection** (**1**-**2**).



2. Configuring the protocol used by Clients to connect to the Server allows prioritizing reliability or speed of data transmission (**3**).The connection protocol is set individually for each Server in an Axxon-domain. All Clients connected to the Server will receive video streams over the selected protocol.
   Descriptions and recommendations for selecting a protocol are given in the table.

Protocol	Description
TCP	This protocol is more reliable but bandwidth-intensive. Recommended for Servers with small numbers of cameras.
UDP unicast	UDP is typically faster but less reliable for data transmission. Unicast involves data transmission to a single recipient. This protocol is best for Servers with many cameras connected to a single Client.
UDP multicast	Multicast refers to data transmission to a group of recipients. This protocol is designed for Servers with many cameras connected to multiple Clients. **Important!** This protocol has to be supported by all network components, in particular, switches.

3. Type the user name and password needed for logging in to each Axxon domain (**4**).

4. Indicate the Servers to connect to. For each Server, perform the following steps:
   a. select the Server in the list (**5**);
   b. indicate the port for connecting to the Server (**6**).

   > **Note**
   >
   > If the **Port** field is left blank, the standard port (20111) will be used for connecting.

   c. Click the **Add** button (**7**).

   > **Note**
   >
   > It is possible to connect to only one Server on an Axxon domain. So when a Server is added to the list, all other Servers on the Axxon domain become unavailable for selection.

   > **Note**
   >
   > To remove a Server from the list, click the ✕ button.

5. After all Servers have been added to the list, select the main Axxon domain.
   When connecting, the Client will use the parameters (maps, layouts, user rights) of the main Axxon domain.
   To select a main Axxon domain, select the check box in the relevant column of a Server that is on the Axxon domain (**8**).
6. Click the **Apply** button.

Click **Export** (**9**) to save the automatic Server connection and Preferred Servers (see Selecting Preferred Servers(see page 571)) configuration to the JSON file.

To load the preset configuration to other Clients, do the following:

1. Click **Import** (**10**).
2. Click **Apply**.

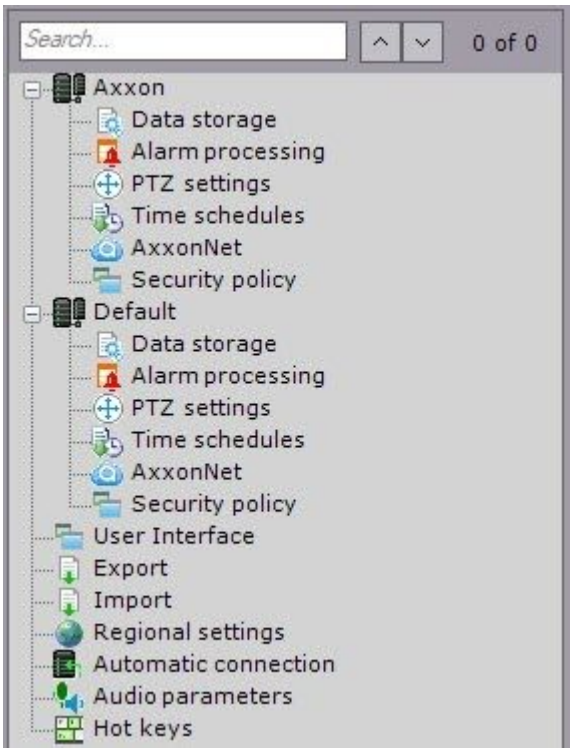
To change a port on an added Server, do the following:

1. Select this Server again from the list (**11**).
2. Enter a new port (**12**).
3. Click **Change** (**13**).

Autoconnection to Servers on different Axxon domains is now complete.

The next time *Axxon Next* is started, connection to the selected Servers with the specified user credentials will occur automatically.

If the Client is connected to several Servers, the Server settings are reproduced for each Server (see Server settings(see page 525)).

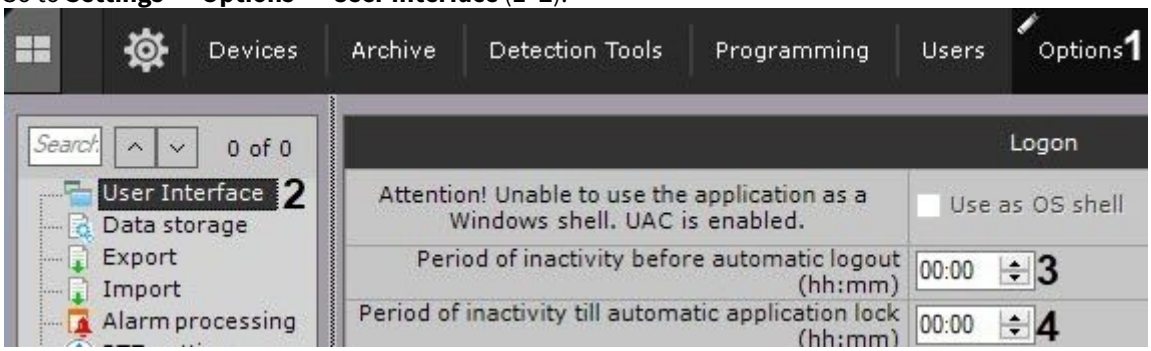


15.10.2.2.3 Configuring automatic exiting and locking of the Client

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(see page 578), Appendix 6. Hotkeys in Axxon One(see page 912)).

4. Click the **Apply** button.

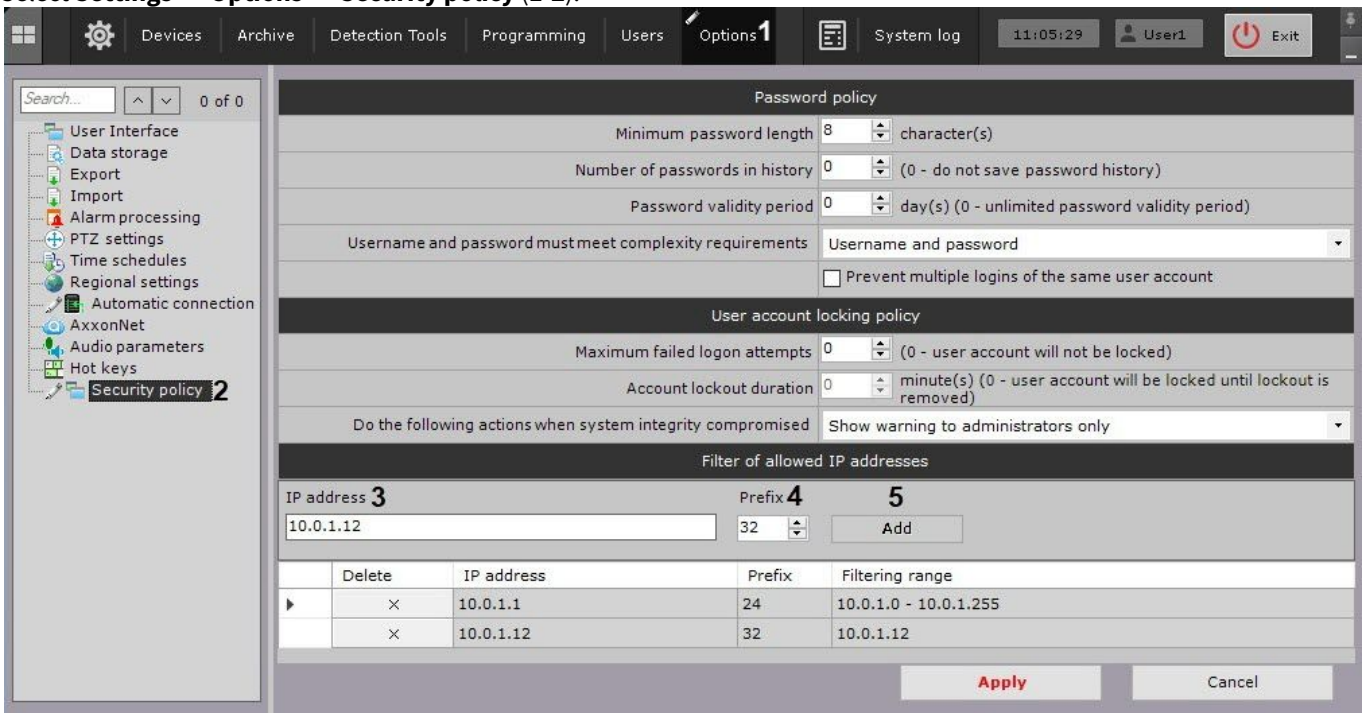
Configuration of automatic quit of the Client is now complete.

15.10.2.2.4 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[165] (**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**.

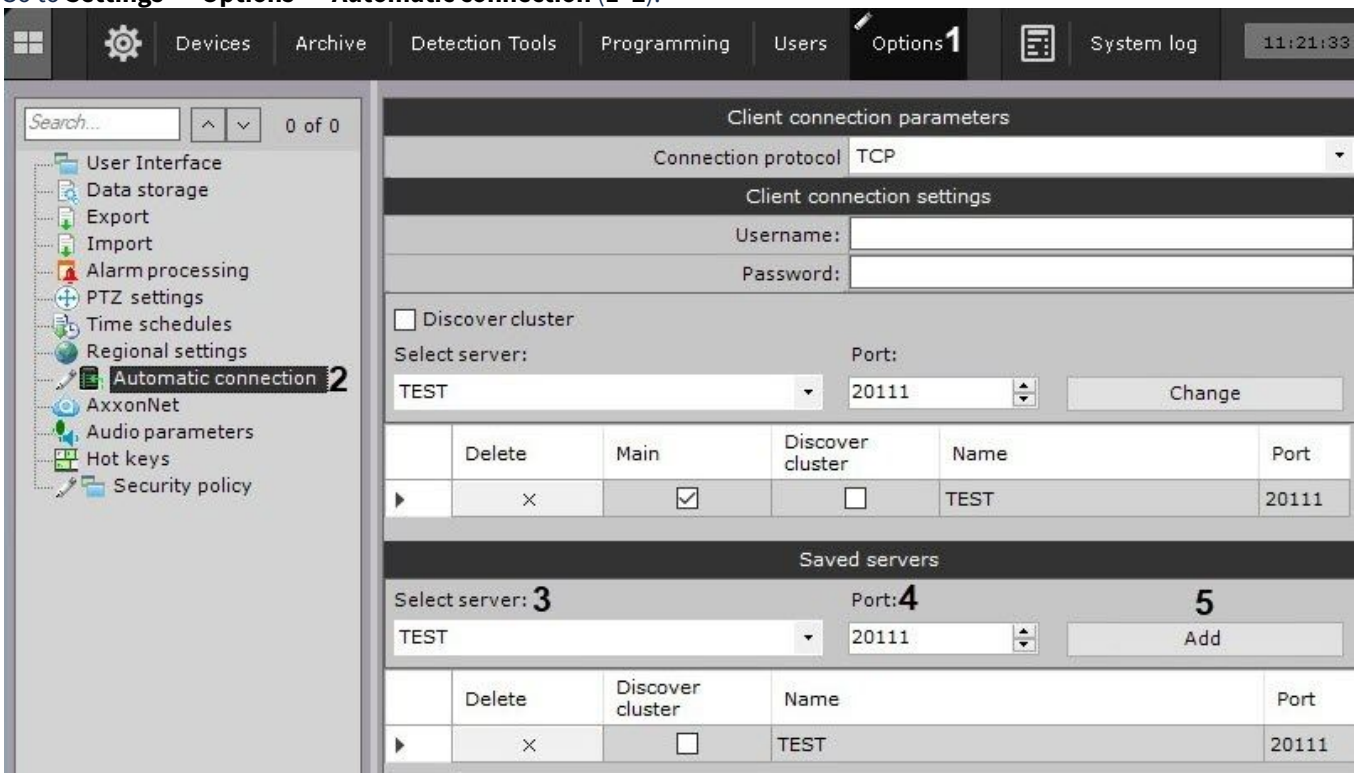
15.10.2.2.5 Selecting Preferred Servers

You can set Preferred Servers, which will be displayed at the top of the list when you launch Client (see Starting an Axxon One Client(see page 94)).

To do it, follow the steps below:

165 https://en.wikipedia.org/wiki/Subnetwork

1. Go to **Settings** → **Options** → **Automatic connection** (**1**–**2**).



2. In the **Saved servers** group, select the Server from the list (**3**).
3. Change the default port if needed (**4**).
4. Click **Add** (**5**).
5. Repeat the steps for all target Servers.
6. Click **Apply**.

> **Note**
>
> You can save the Preferred Servers list to a JSON file and load it to another Client (see Configuring Cross-System Client and autologon(see page 568)).

15.10.2.3 Configuring export

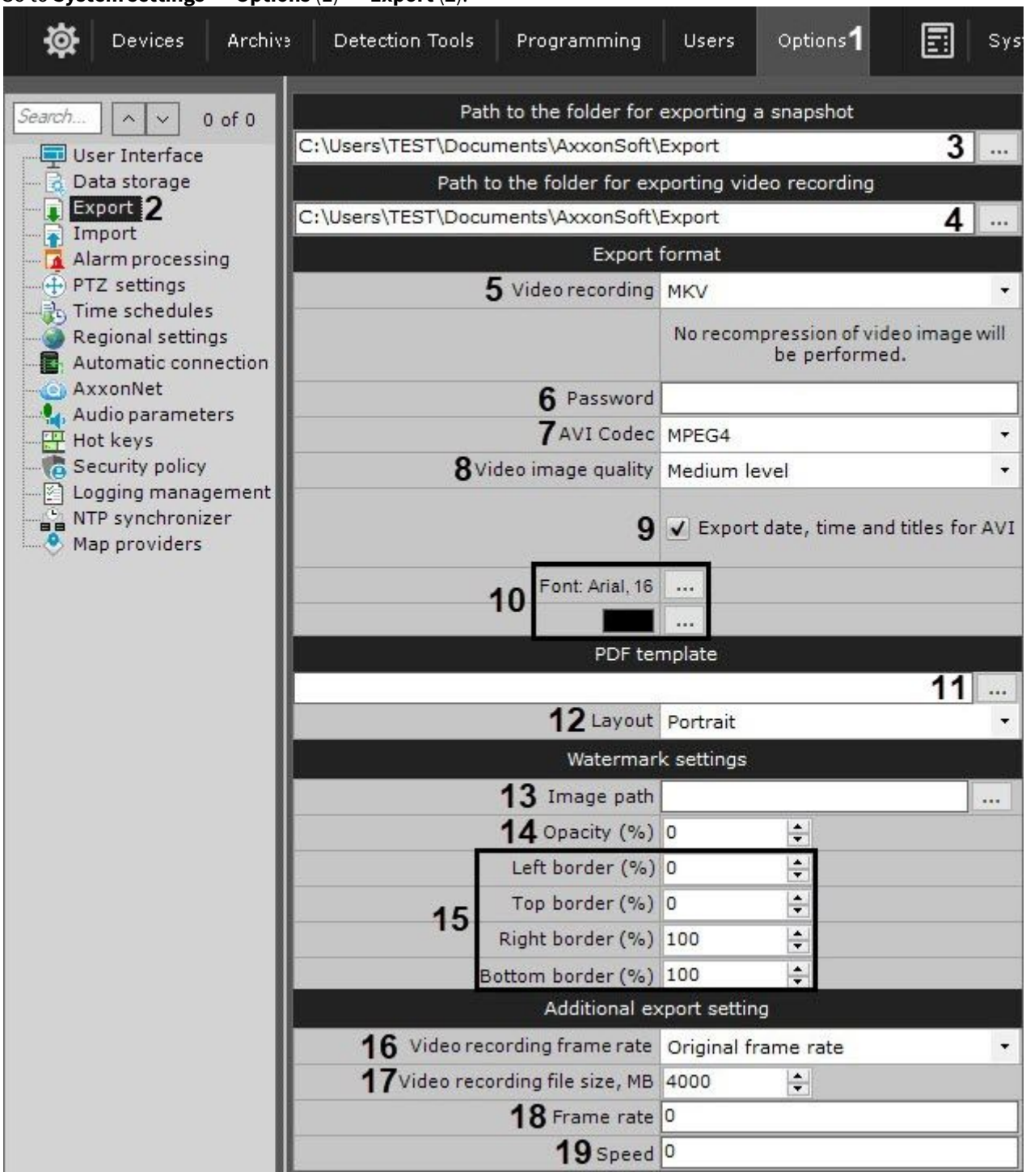
15.10.2.3.1 Configuring export options

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 ID;
- {1}—camera name;
- {2}—date;
- {3}—time;
- {4}—recording duration (for video export only).

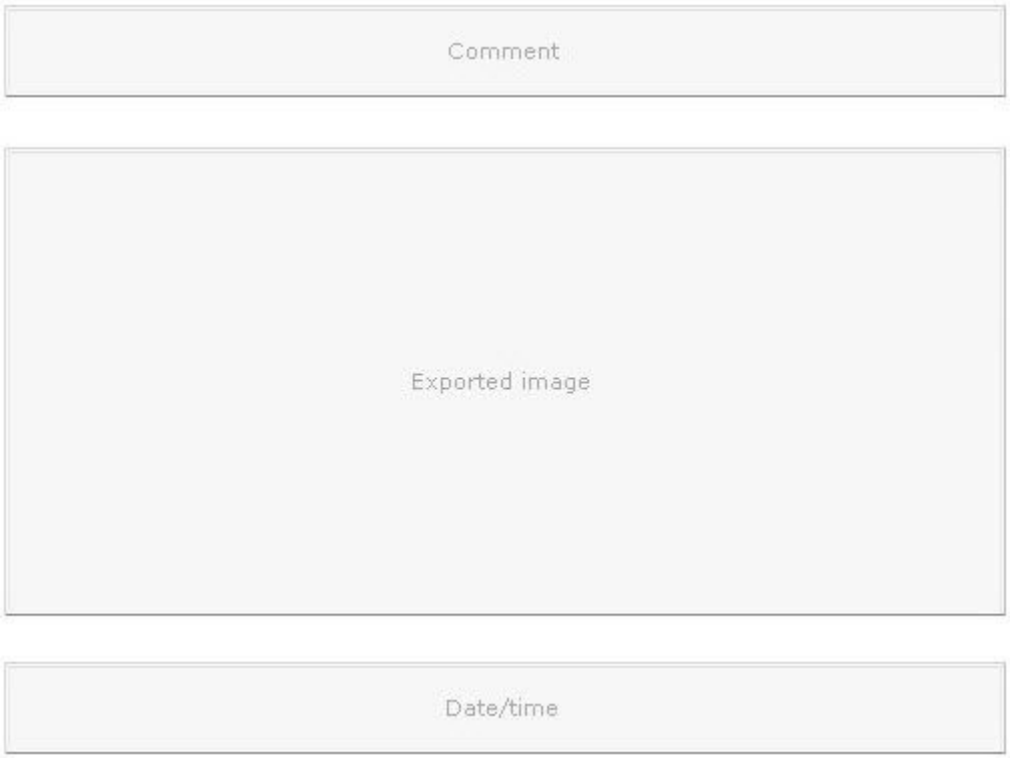
3. Select the default formats for export of video and snapshots (**5**). You can select any available format during export. Snapshots can be exported in two formats: JPG and PDF. Videos can be exported into the following four formats: MP4, MKV, EXE and AVI.

   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**).
   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[166].

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,

166 https://support.microsoft.com/en-US/windows

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.

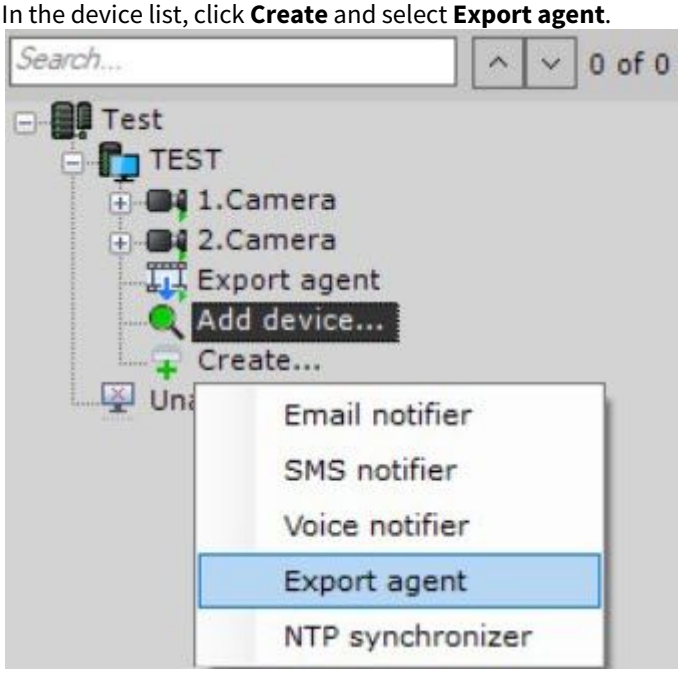
15.10.2.3.2 Configuring Export agent

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 and counters(see page 400)).

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(see page 572).
6. Click the **Apply** button.

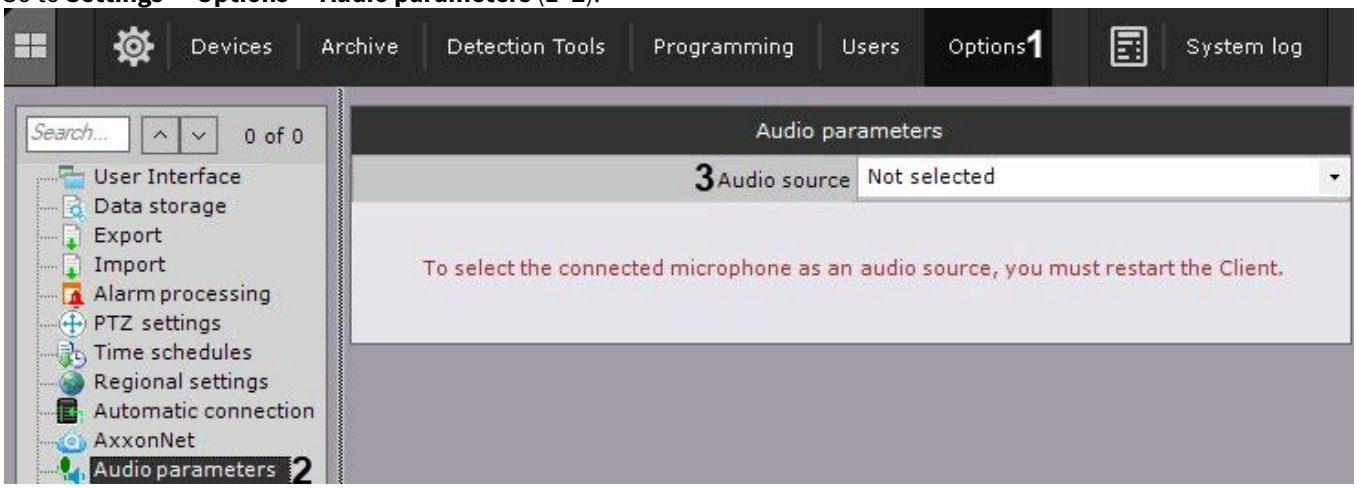
Creating and configuring the Export agent is now complete.

15.10.2.4 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.

15.10.2.5 Configuring hot keys

15.10.2.5.1 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:

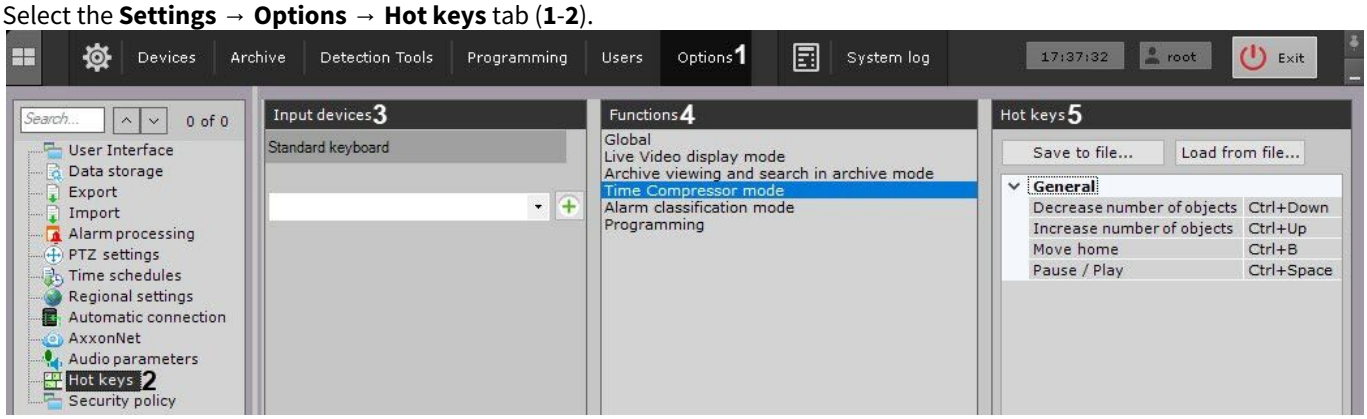
- the same shortcut can be used for different actions in different modes;
- a shortcut in any particular mode can be associated with only one action;
- shortcuts set in Global mode cannot be redefined in other modes;
- hot keys are available only when the Client is active;
- on standard keyboards, alphanumeric 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(see page 912) to this guide.

15.10.2.5.2 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(see page 578)).
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.

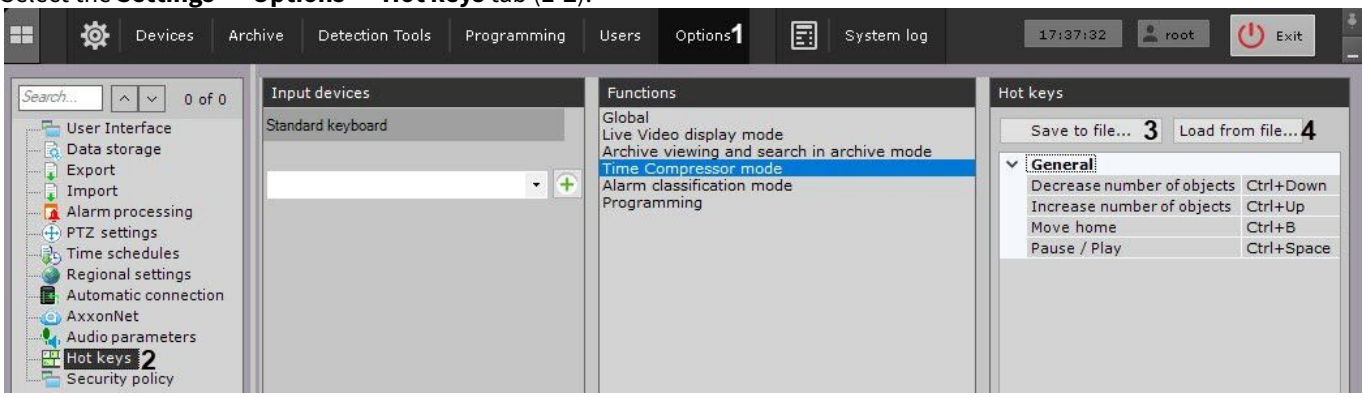
Assignment of hot keys is now complete.

15.10.2.5.3 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:

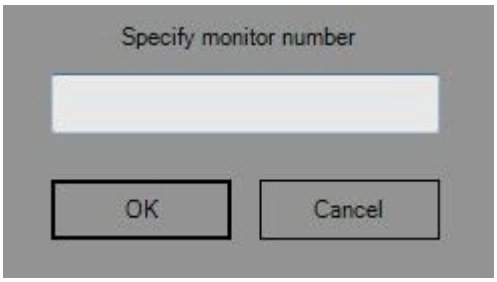
1. Select the **Settings** → **Options** → **Hot keys** tab (**1**-**2**).
2. Click the **Load from file...** button (**4**).
3. Select a file that contains a hot key configuration. Click the **Open** button.
   The hot key combinations are imported into the Client, so long as a valid file is selected.
4. Click the **Apply** button.

Import of hot keys is now complete.

15.10.2.5.4 Notes regarding hot key actions

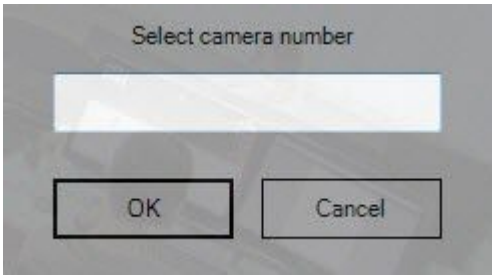
To select an active monitor in a multi-monitor configuration (see Managing monitors on a local Client(see page 790)), click **Select Monitor by number** (Global mode).

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.

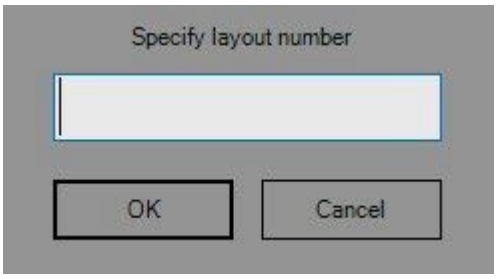
When a key or key combination assigned to the **Camera selection in current layout** action (Global mode) is pressed, the go to camera by ID window opens.



Enter the destination camera's user- friendly ID (see The Camera object(see page 122)), then click **OK**.

If the current layout contains a camera with the specified ID, the relevant viewing tile becomes active. If the current layout does not contain a camera with the specified ID, 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(see page 507)).

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(see page 705)).

15.10.2.5.5 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!

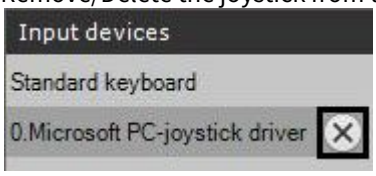
Do not set values outside the range and edit other parameters in the file.

   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.

15.10.2.6 Configuring video capturing on operator monitor

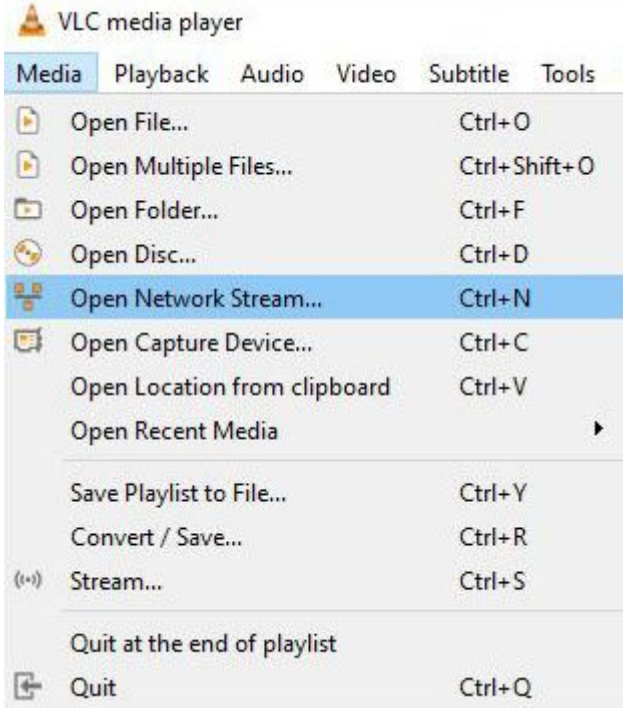
Video recording from the computer monitor is used to control the operator's actions. You can broadcast video from the computer monitor to *Axxon One* via the common protocols using the third-party software, for example:

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.

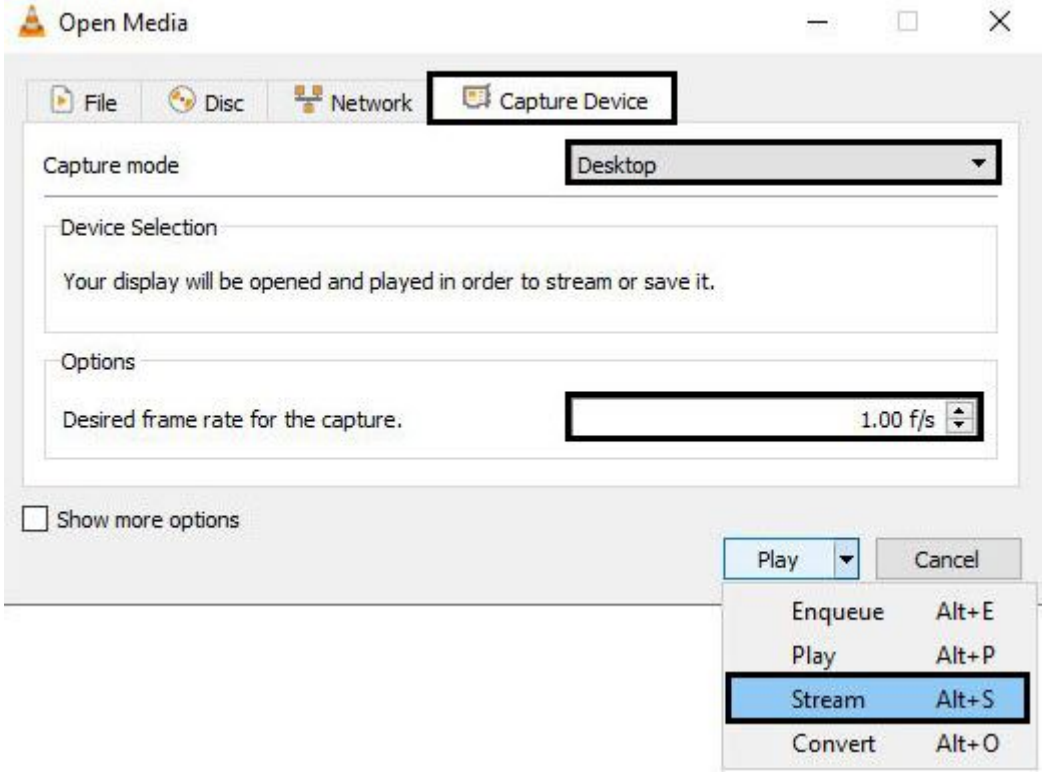
This section describes how to configure VLC Media Player to broadcast video from the computer monitor to *Axxon One* via the RTSP protocol. Configuring *Axxon One* to receive and record such a video stream is performed in a standard way as described in Configuring an RTSP Server(see page 120) and Configuring recording to an archive(see page 224).

Configuring VLC Media Player to broadcast video from the computer monitor to *Axxon One* via the RTSP protocol is performed in the following way:

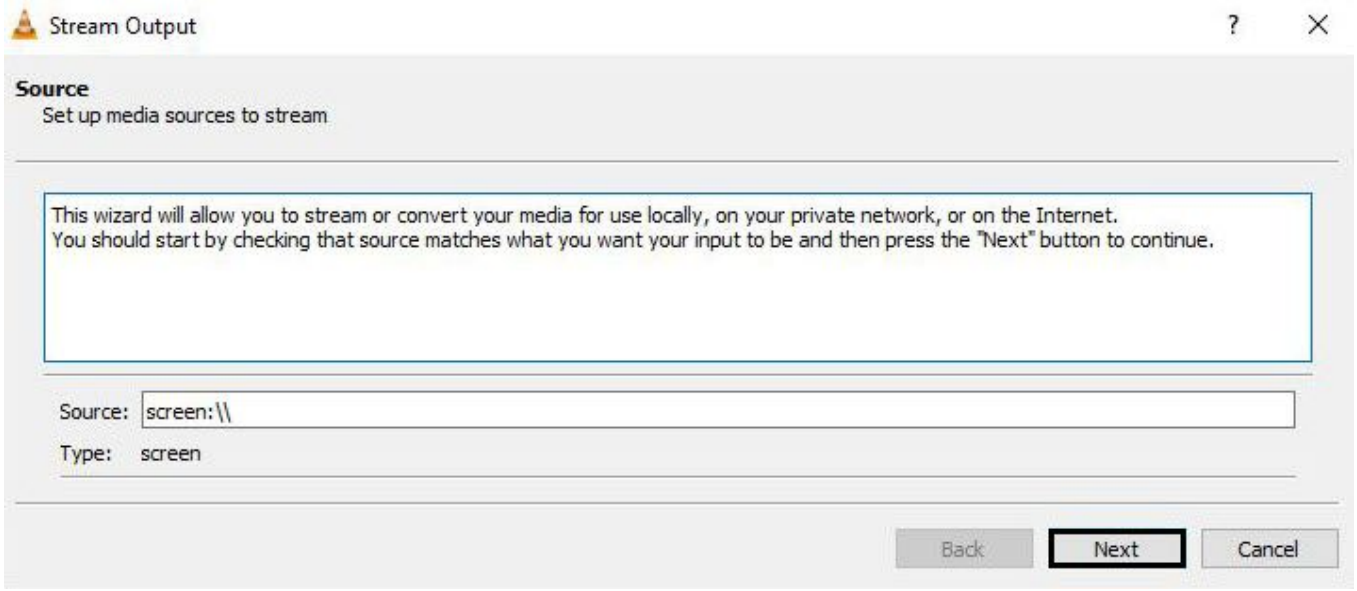
1. Run VLC Media Player.
2. Select the **Open Network Stream...** item in the **Media** menu.



3. In the appeared window go to the **Capture Device** tab.

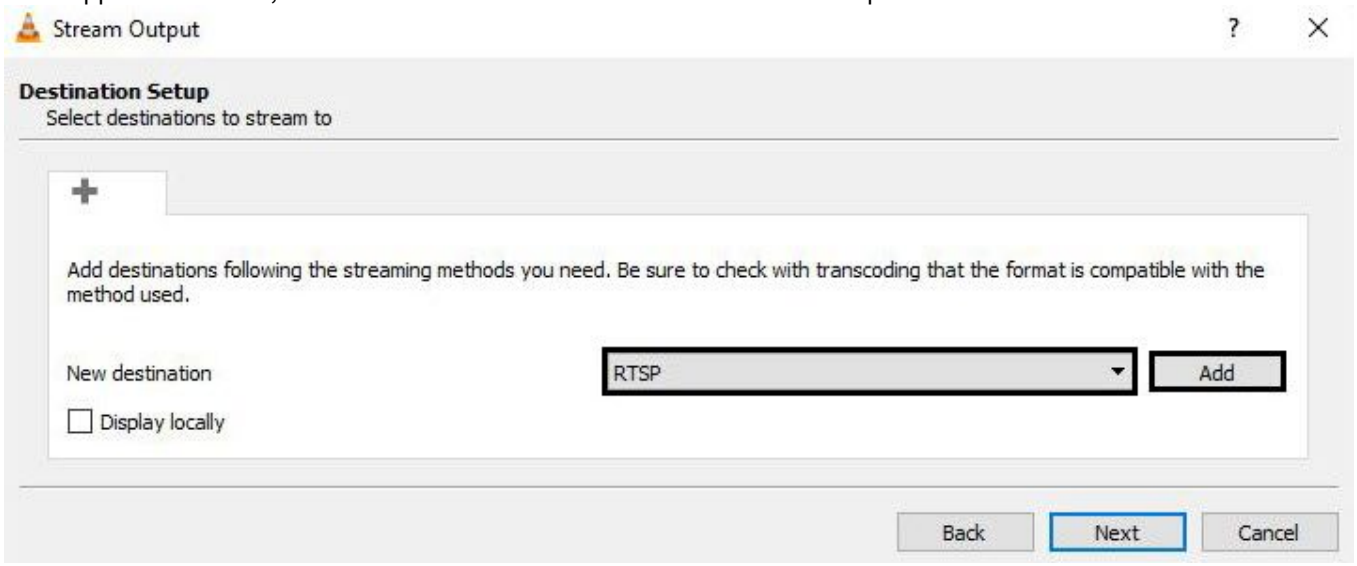


4. From the **Capture mode** drop-down list, select the **Desktop** value.
5. Set the required frame rate value for the capture in the corresponding field.
6. In the **Play** drop-down list, select the **Stream** value. As a result, the **Stream Output** window will appear.

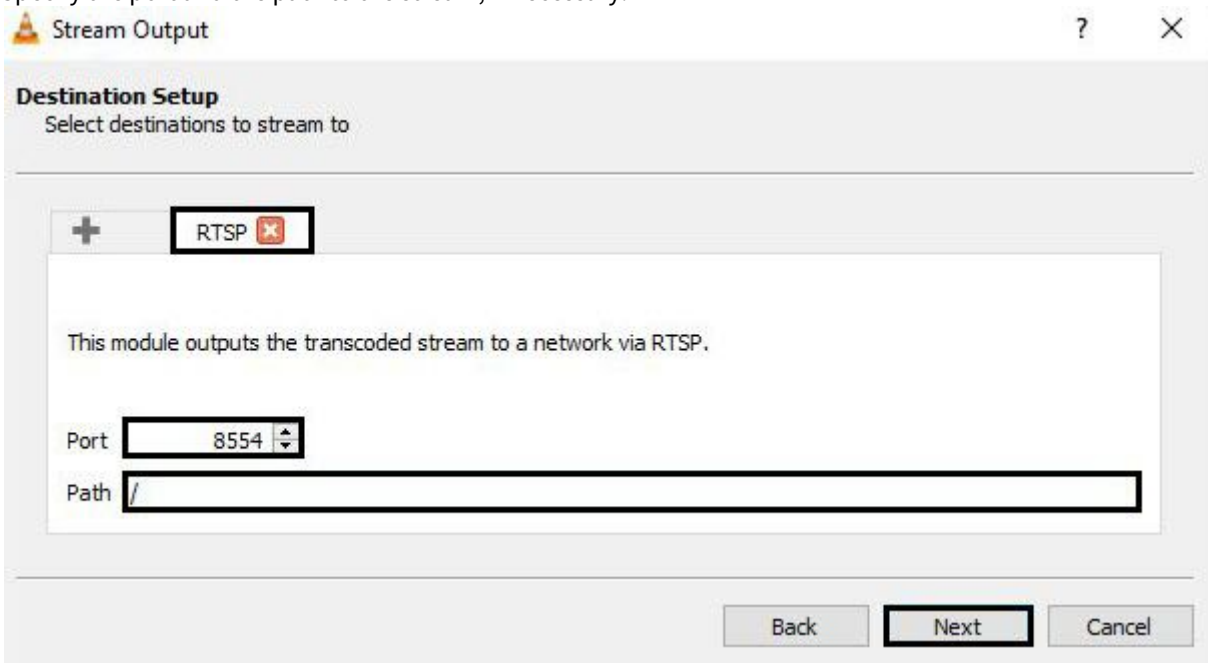


7. Click the **Next** button.

8. In the appeared window, select the **RTSP** value from the **New destination** drop-down list and click the **Add** button.

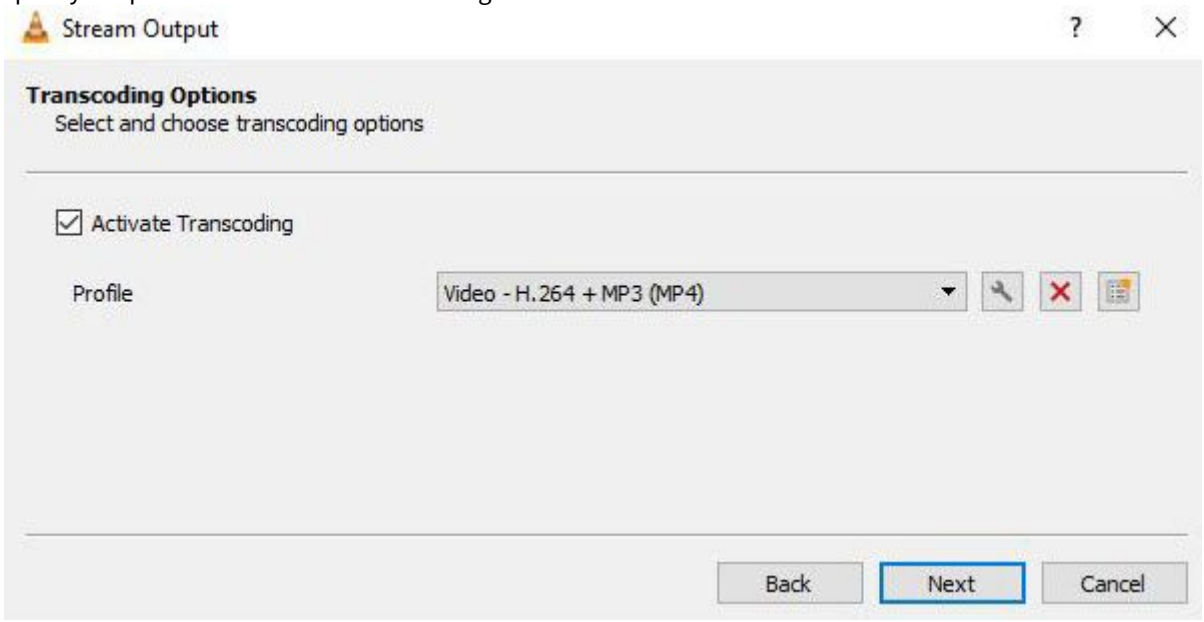


9. Go to the **RTSP** tab.
10. Specify the port and the path to the stream, if necessary.

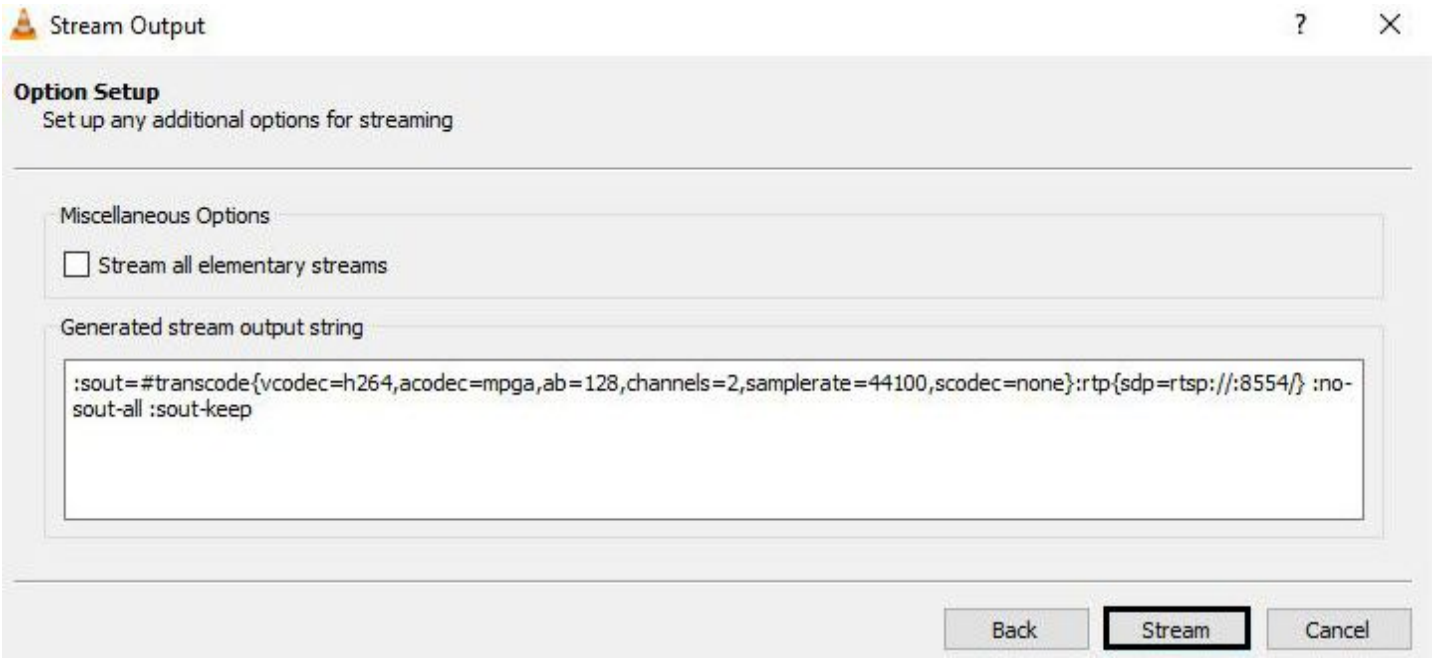


11. Click the **Next** button.

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(see page 131) and Configuring recording to an archive(see page 224)).

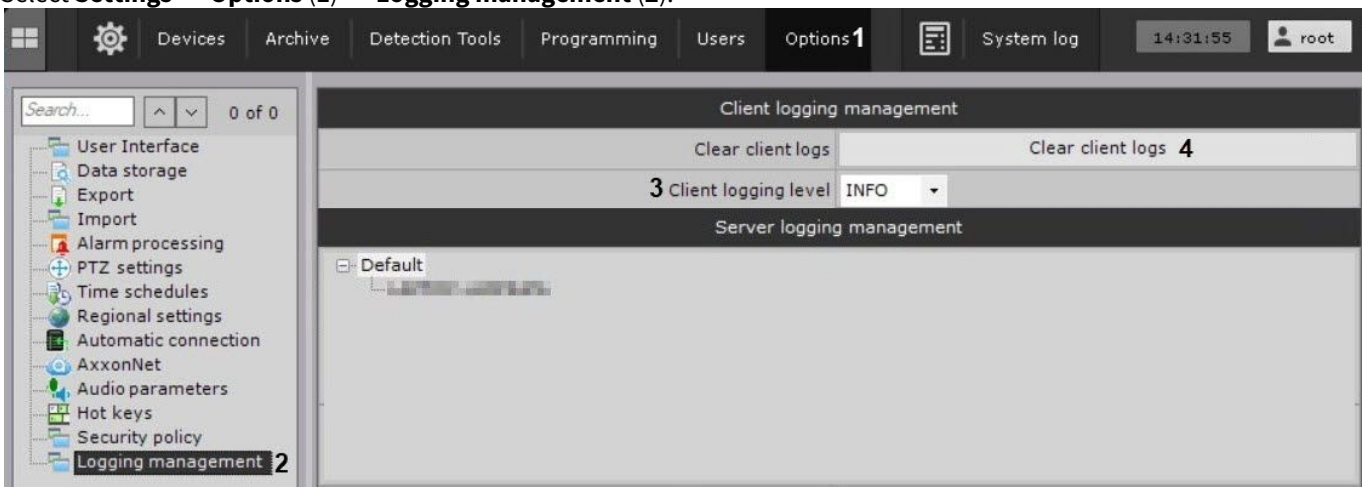
Configuring VLC Media Player to broadcast video from the computer monitor to *Axxon One* via the RTSP protocol is completed.

15.10.2.7 Configuring Client logging

By default, the Client logging level is set in a special utility (see Log Management Utility(see page 870)). You can change the logging level of the Client before you exit it.

To change the logging level of the Client, do the following:

1. Select **Settings** → **Options** (**1**) → **Logging management** (**2**).



2. Select the required logging level (**3**). Levels are described on the Configuring Logging levels(see page 872) page.
3. Click the **Apply** button.

Client logging level is changed. The next time the Client is started, the logging level will correspond to the new settings in the logging management utility.

You can also delete all Client logs. To do this, do the following:

1. Click the **Clear client logs** button (**4**).
2. Click the **Apply** button.

15.11 Configuring Failover VMS

15.11.1 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:

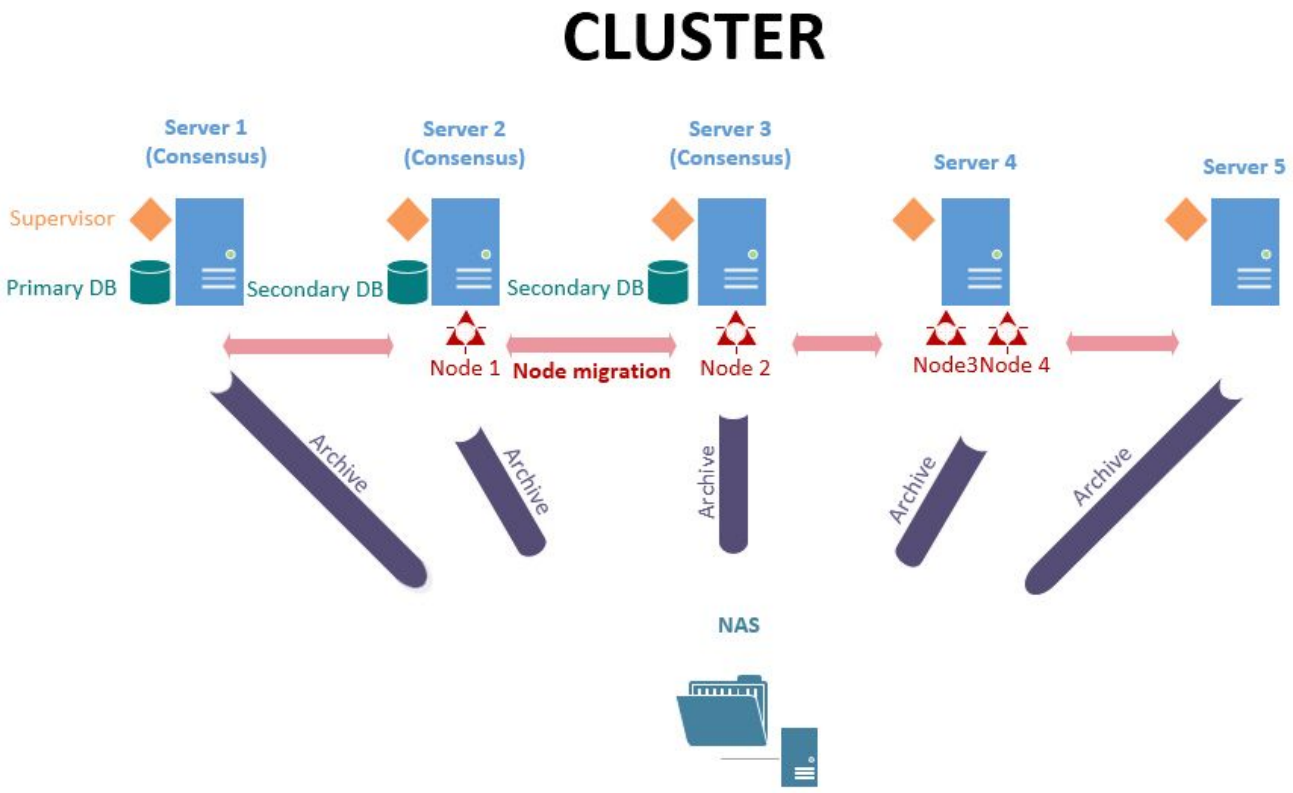
- **Server**—a computer with **Failover Server and Client** configuration of *Axxon One* installed;
- **Node**—an instance of the Server services. A Server can have multiple nodes running;

- **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:



Note

You can install *Axxon One* Server in the Failover mode in Linux OS (see Installing from repository(see page 918), Manual installation(see page 919)).

15.11.2 Ports used by the failover system

Each failover system server uses the following ports:

- 4000 (Supervisor Web-Interface(see page 589), only TCP),
- 4646 (Nomad[167] HTTP API, only TCP),
- 4647 (Nomad[168] RPC, only TCP),
- 4648 (Nomad[169] LAN/WAN Serf (Gossip), TCP and UDP),
- 8300 (Consul[170] Server RPC, only TCP),
- 8301 (Consul[171] LAN Serf (Gossip), TCP and UDP),

167 https://www.nomadproject.io/docs/install/production/requirements#ports-used
168 https://www.nomadproject.io/docs/install/production/requirements#ports-used
169 https://www.nomadproject.io/docs/install/production/requirements#ports-used
170 https://www.consul.io/docs/install/ports#required-ports
171 https://www.consul.io/docs/install/ports#required-ports

- 8302 (Consul[172] WAN Serf (Gossip), TCP and UDP),
- 8500 (Consul[173] HTTP API, only TCP),
- 8600 (Consul[174] DNS, TCP and UDP).

Moreover, each node of the cluster has its pre-defined unique port range (see Installation(see page 62)).
For best results, use port numbers from 20111 to 32000.

15.11.3 Supervisor Web-Interface

You can configure a failover system in the Supervisor Web-Interface at http://localhost:4000[175].

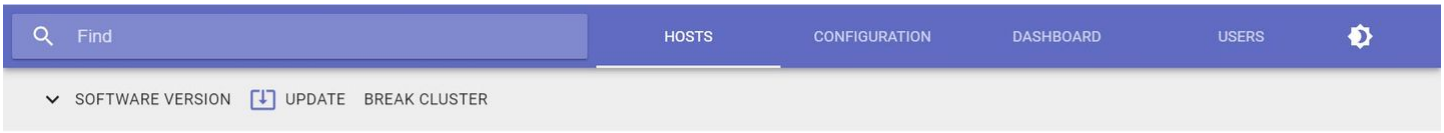
Note

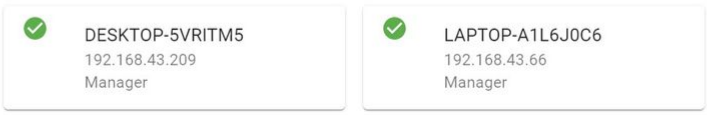
After installation, a shortcut is added to your desktop.

On Linux OS, no additional shortcuts are created after installation. To access the Supervisor Web-Interface, go to http://localhost:4000[176].

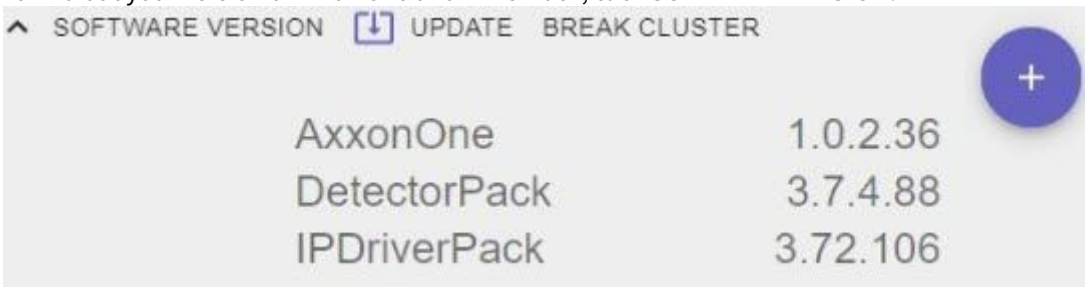
The Supervisor Web-Interface has four tabs:

1. **HOSTS**—Creating a cluster(see page 590).
2. **CONFIGURATION**—Failover Database(see page 594), Configure a Failover System Cluster(see page 595).
3. **DASHBOARD**—Cluster Monitoring(see page 612).
4. **USERS**—Set up access to a supervisor(see page 609).





To find out your version of *Axxon One* and *DriverPack*, click **SOFTWARE VERSION**.



172 https://www.consul.io/docs/install/ports#required-ports
173 https://www.consul.io/docs/install/ports#required-ports
174 https://www.consul.io/docs/install/ports#required-ports
175 http://127.0.0.1:4000.
176 http://127.0.0.1:4000.

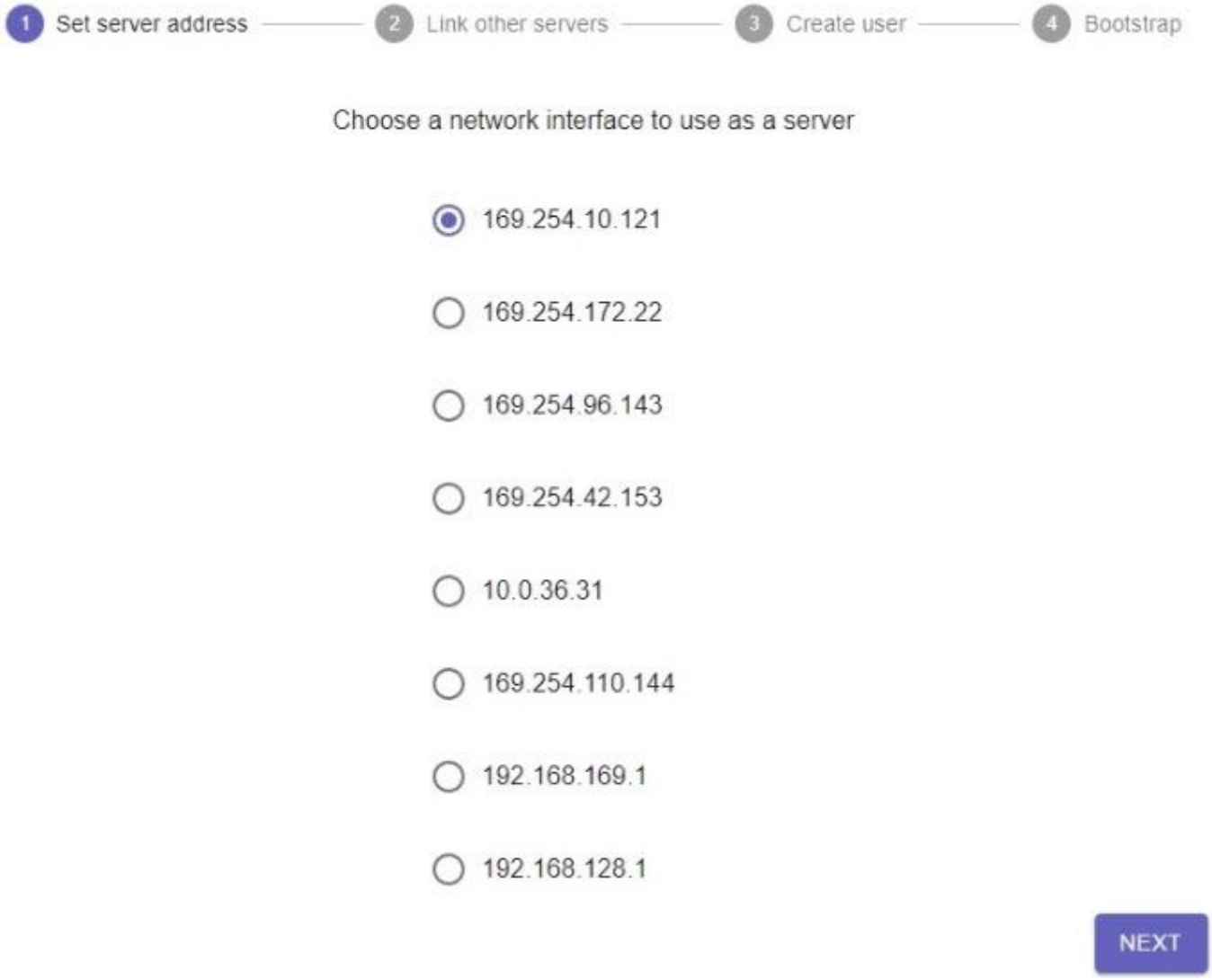
To search hosts and servers, enter their names in the search bar in the **HOSTS** or **DASHBOARD** tabs in the top left part of the interface.

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.

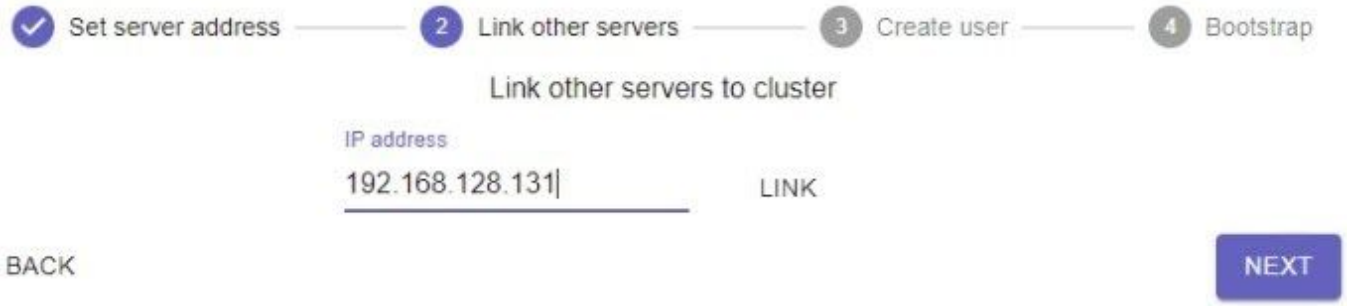
15.11.4 Creating a cluster

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**.



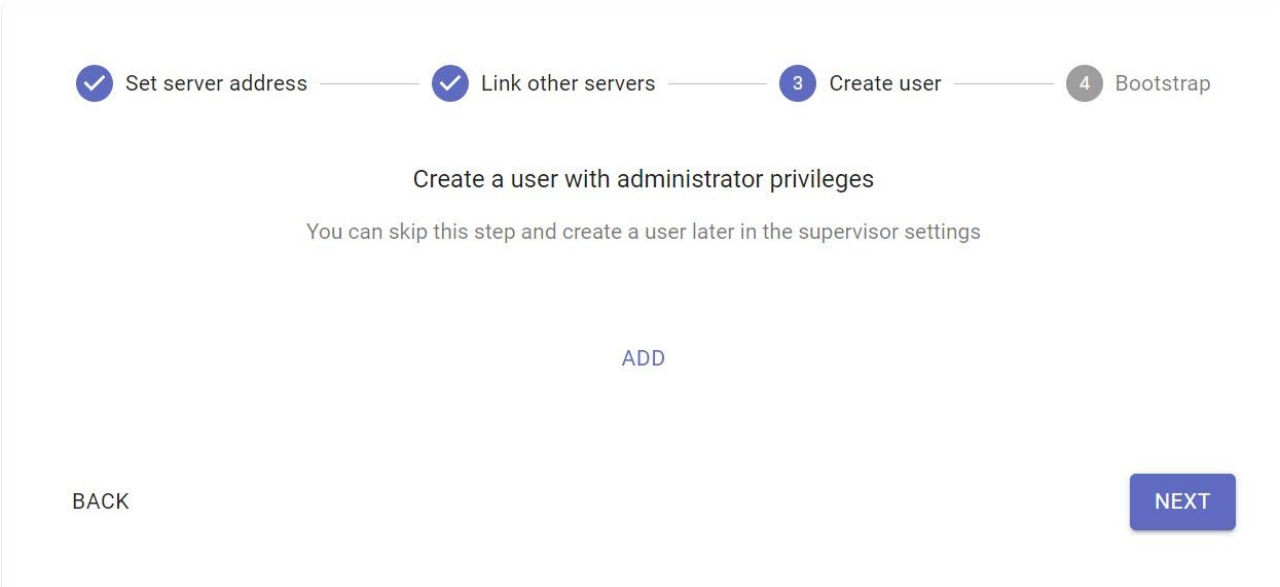
2. Add the required Servers to the cluster. To do this, enter the IP address and click **LINK**.



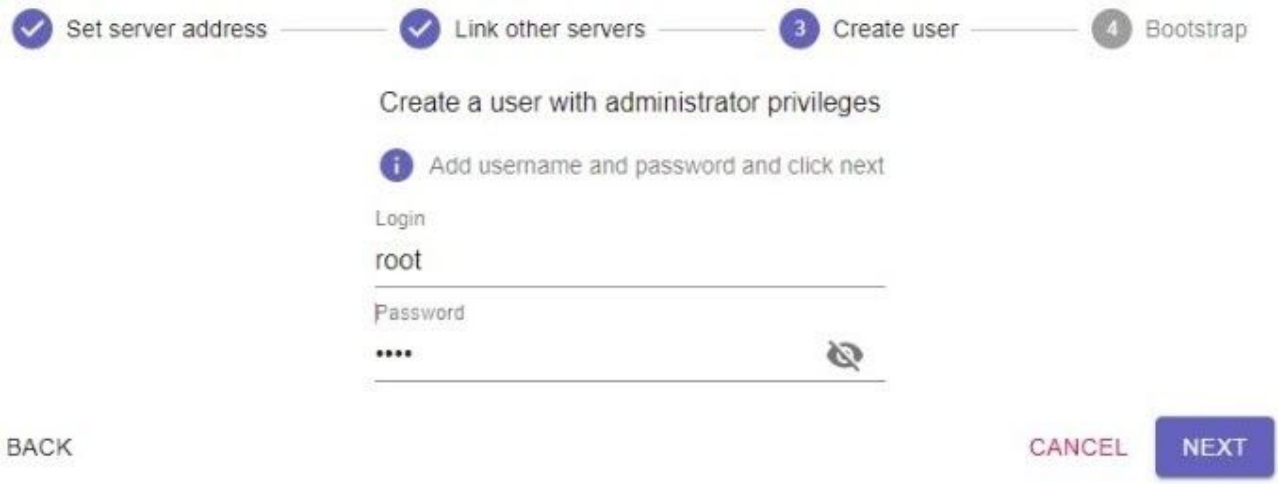
> **Attention!**
>
> All cluster Servers must be available to each other.
> It is necessary to use Servers with the same architecture (x64), OS type and PostgreSQL version.

> **Attention!**
>
> 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 odd, not less than three and not more than five.
> If only two Servers are added, they can be configured as **1+1**—master + backup Server (see 1+1 cluster configuration(see page 604)).

3. If required, you can add a user with administrator rights (see Set up access to a supervisor(see page 609)). After the cluster is created, only this user will have access to the supervisor. Do the following:
   a. Click the **ADD** button.



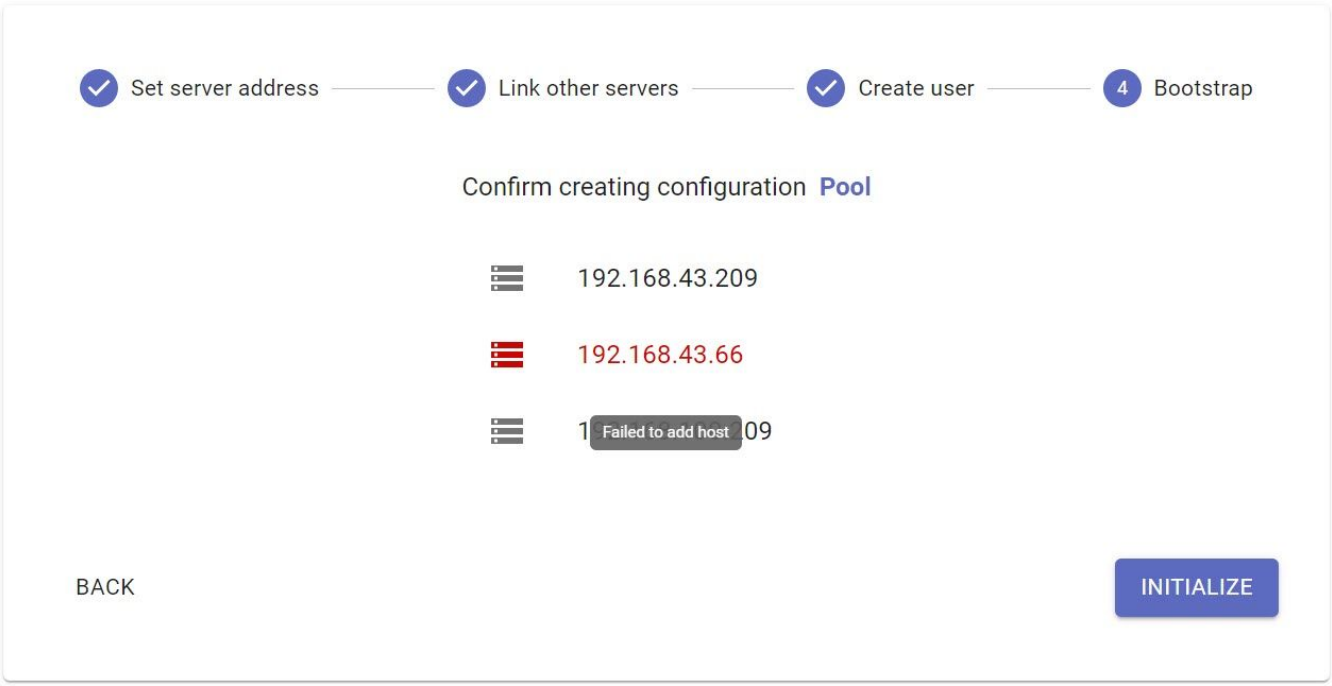
   b. Enter access credentials and click the **NEXT** button.



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.

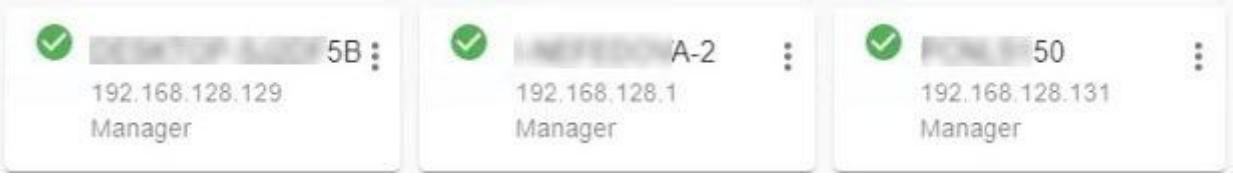


In this case you need to go back to the step of adding the Servers and add the available Servers.

To add other Servers to the cluster, do the following:

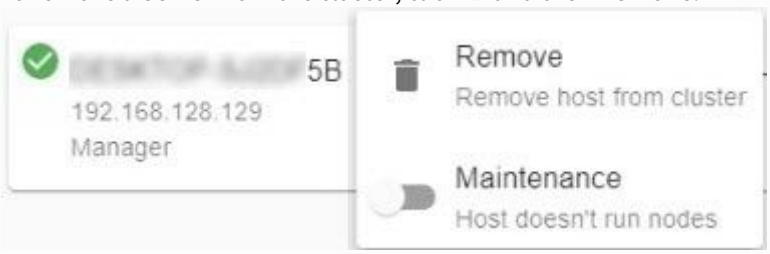
1. On the **HOSTS** tab, click .
2. Enter the IP address of the Server.

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.

15.11.5 Failover Database

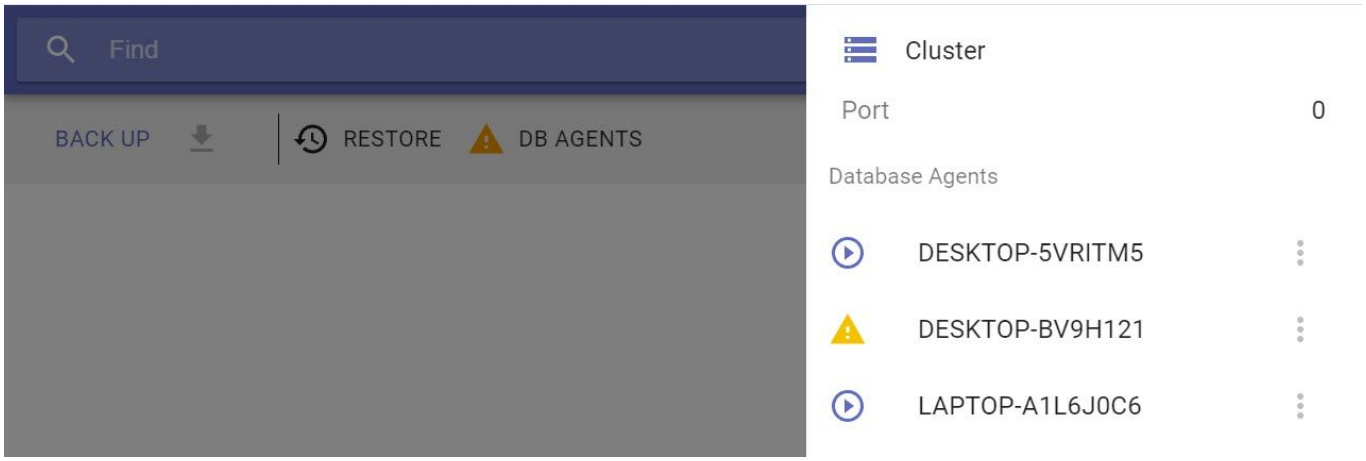
By default, the database is created automatically when the cluster is initialized, and its agents are launched on the master Servers.

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**.

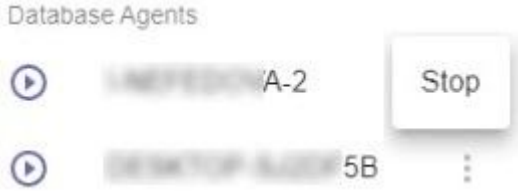


3. The **Port** field specifies the value of the port that the database agents use. If the value is 0, the database agents use dynamic ports.
4. The icon next to the Server indicates the current status of the agent.

Icon	Status
	Launch expected
	Launched
	Stopped

Icon	Status
⚠	Unavailable

5. Click ⋮ to stop or launch the agent, and select the required action.



15.11.6 Configure a Failover System Cluster

A failover system can be configured in two ways:

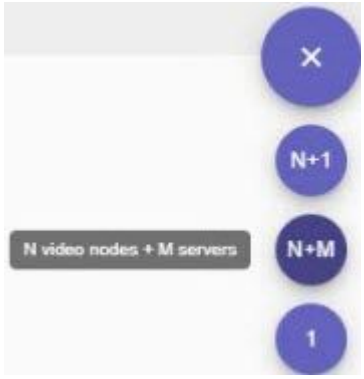
1. Basic configuration. There are no pre-assigned backup Servers in this configuration. The supervisor independently decides where to host a particular node. Only network archives can be used in this configuration.
2. Configuration with the specified backup Server. In this configuration, a backup server 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.

15.11.6.1 Setting up basic configuration

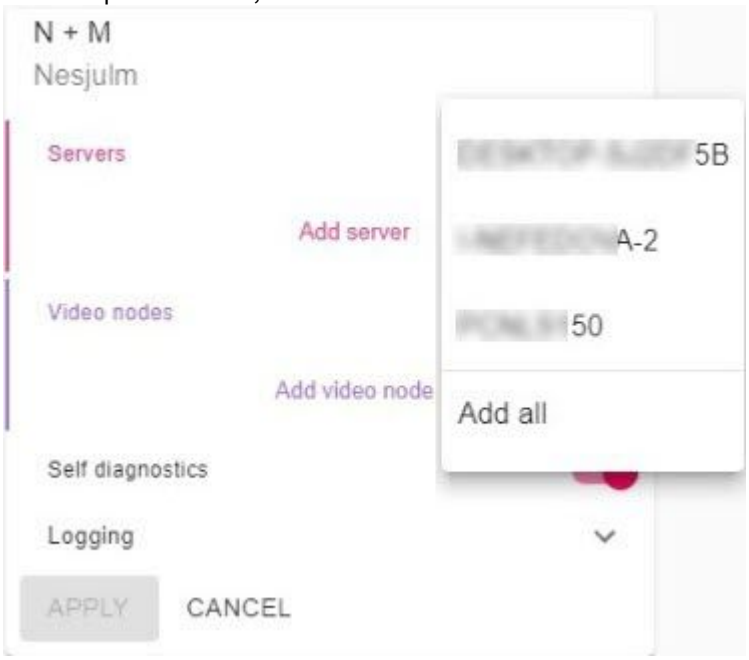
To set up a basic configuration of a Failover system, do the following:

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 .

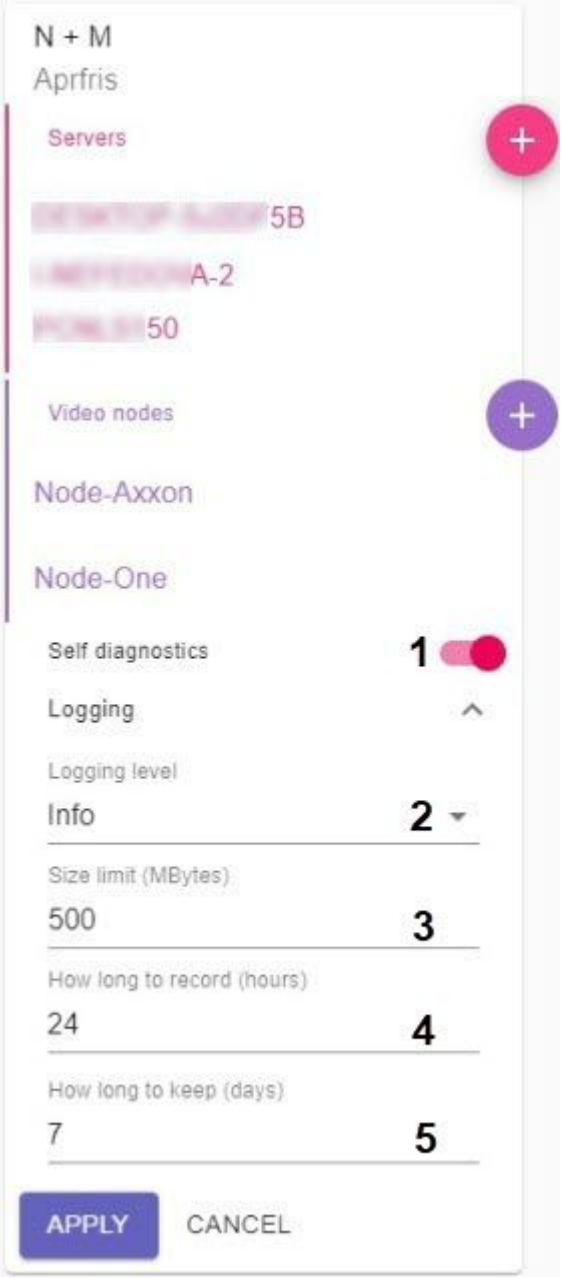
b. Enter the node name and click the **PROCEED** button.

> **Attention!**
>
> A node name may contain Latin and numerical characters, and the "-" symbol.

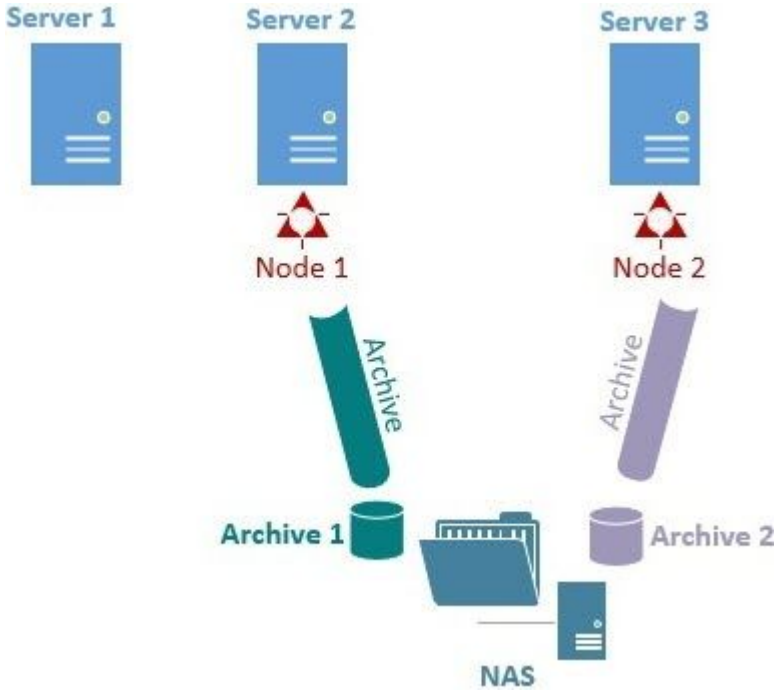
c. Create the required number of nodes.

> **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.

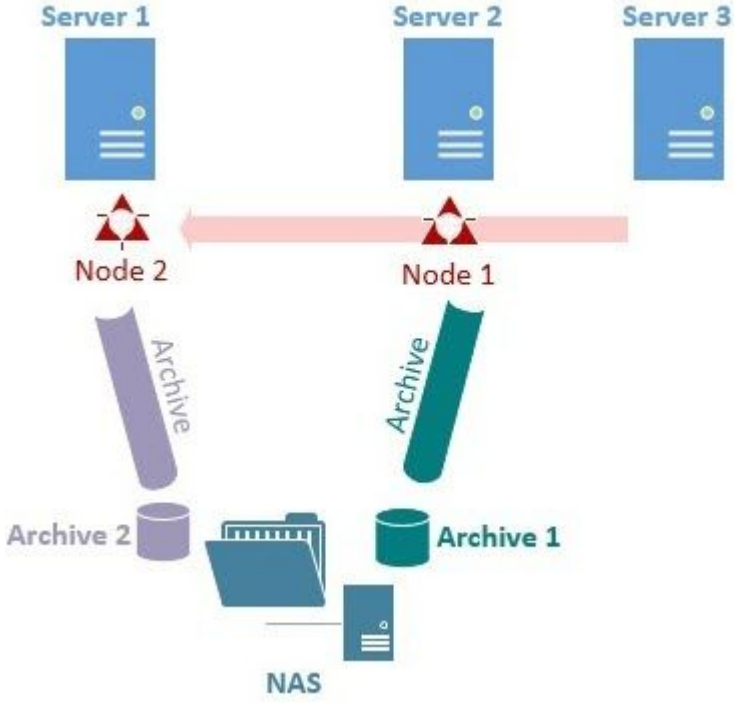
5. By default, the self-diagnostics service is running on all nodes (see Self-diagnostics service(see page 619)). To stop it, deactivate the **Self diagnostics** parameter (**1**).



6. Click the **Logging** button to set the logging options:
   a. Select Logging level (**2**, see Configuring Logging levels(see page 872)).
   b. Set the settings for the archive of logs (**3**-**5**, see Configuring a Log archive(see page 871)).
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(see page 613)).
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(see page 211)).



If the node is moved to a different server, it will continue to write to the specified archive.

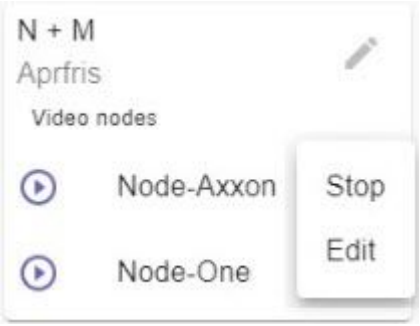


The basic configuration of the Failover system is now complete.

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.



15.11.6.2 Setting up a configuration with the backup Server

A configuration with the backup Server can include two or more Servers.

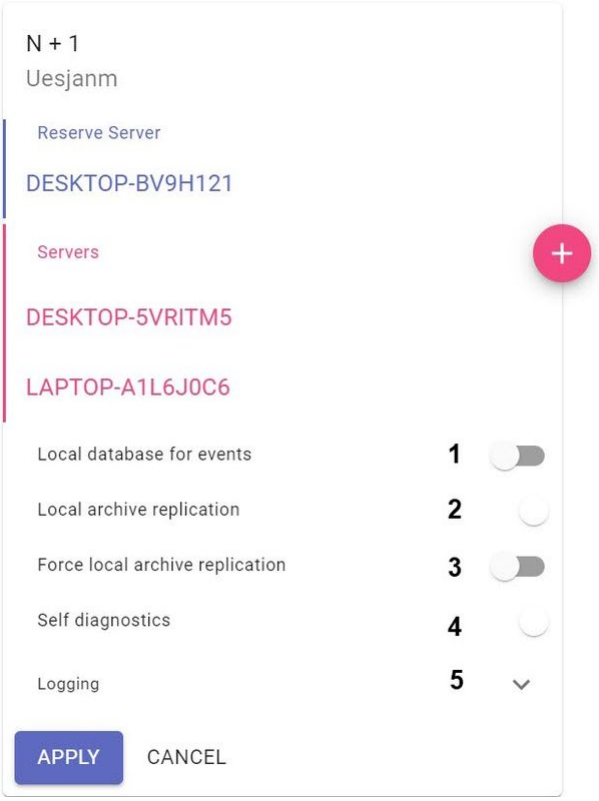
To set up the configuration, do the following:

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**).

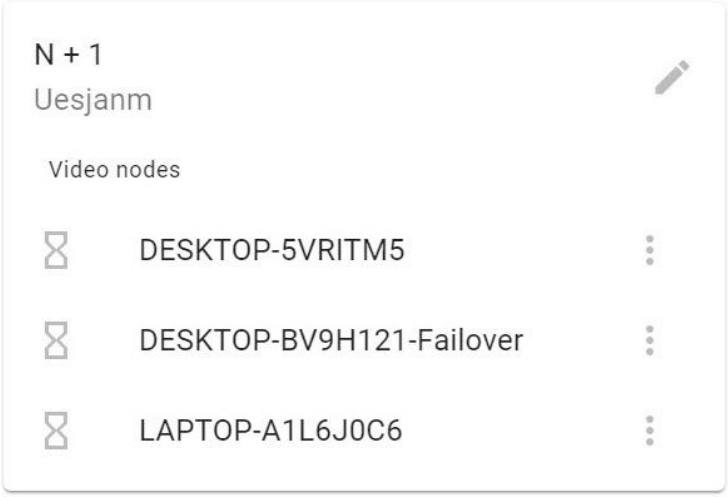


5. If you want to replicate the local archive when the master node is on the backup Server, activate the corresponding switch (**2**).

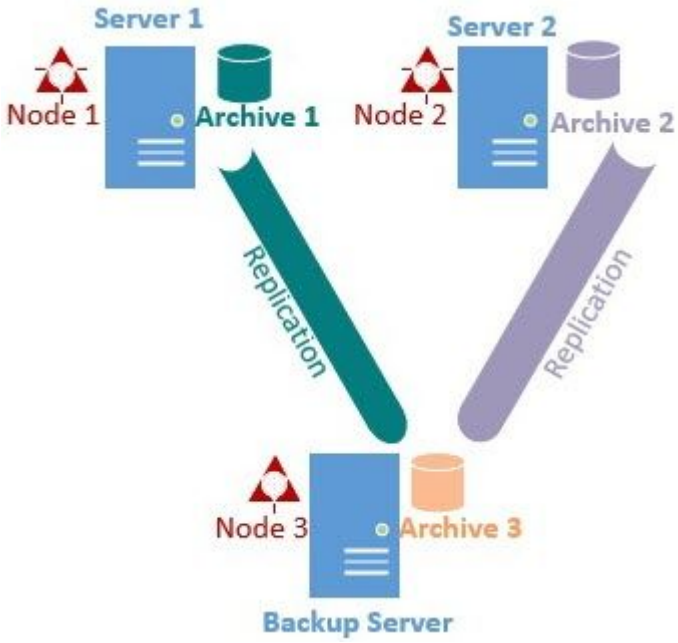
> **Attention!**
>
> The local archive must be created on the master node (see Creating a local archive(see page 209)).

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(see page 619)). 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 Logging levels(see page 872)).
   b. Set the log archive parameters (see Configuring a Log archive(see page 871)).
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(see page 613)).
11. Configure the archives operation:
    a. On the backup node, create an archive for replication (see Creating archives(see page 209)).
    b. On the master nodes, configure the replication from the master Servers' archives to the backup node's archive (see Configuring data replication(see page 226)). 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.

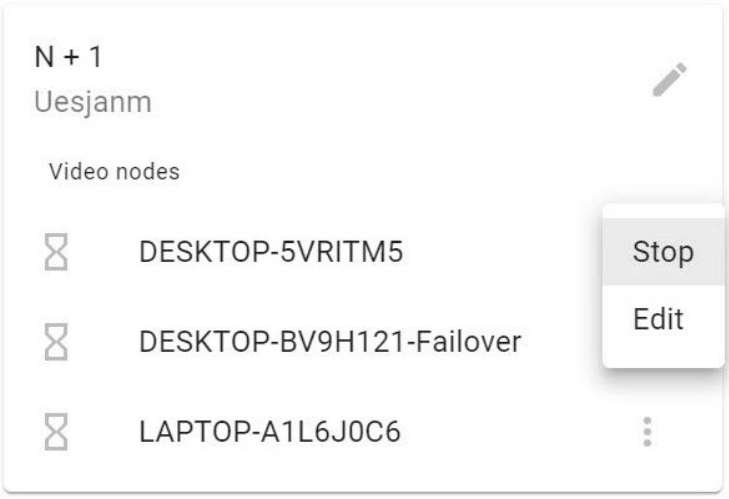
When a master node is migrated to the Failover Server, a temporary archive will be automatically created in the C:/temp_arch folder of the backup Server as a 10 GB file. In *Axxon One*, the temporary archive will be marked as **Archive in failover server**.

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.



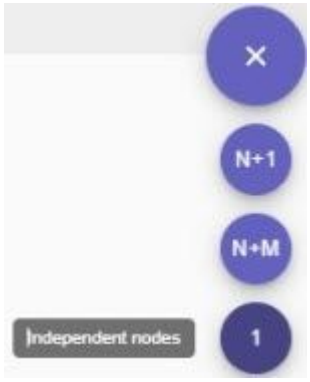
15.11.6.3 Creating and configuring independent nodes

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.

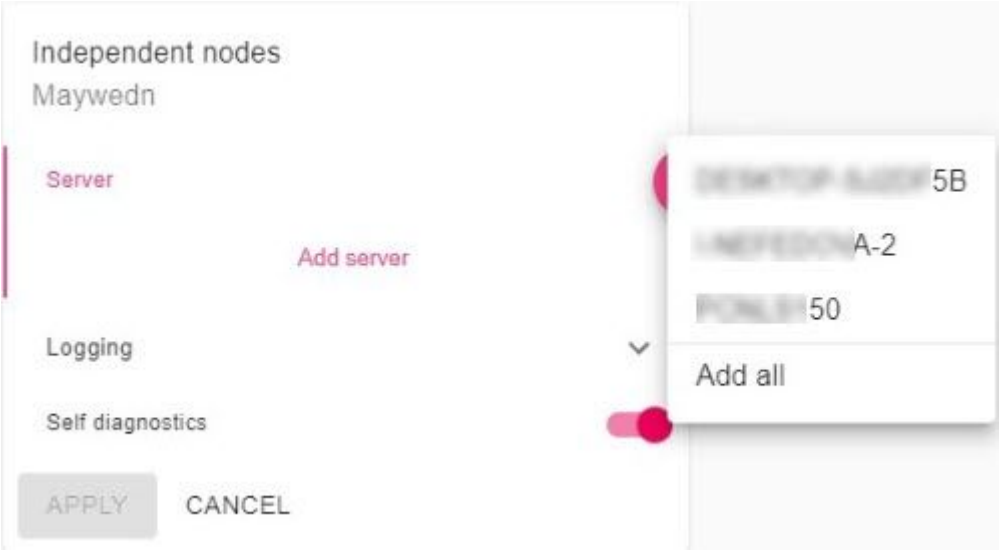
To create an independent node, do as follows:

1. Go to the **CONFIGURATION** tab.
2. Point the cursor at and click **1**.

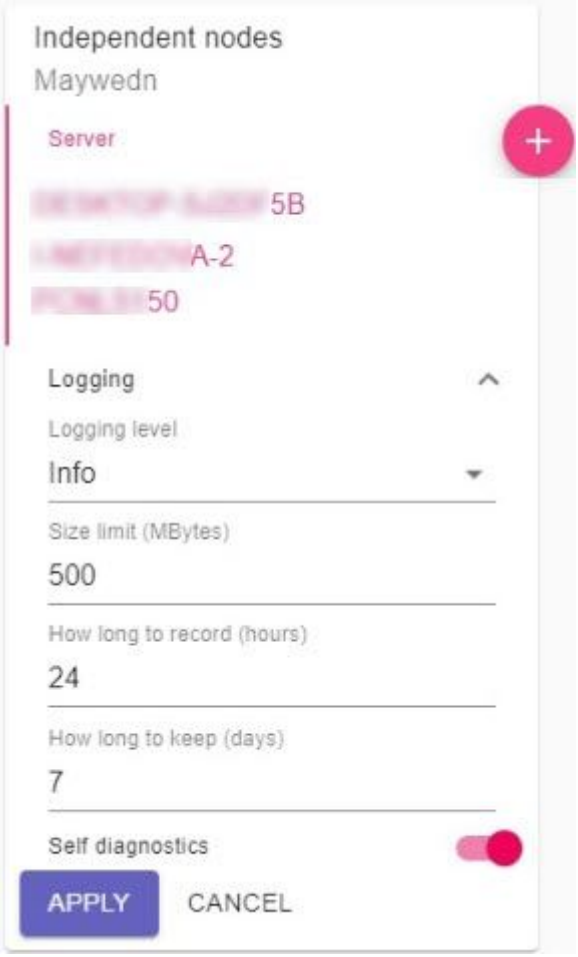


3. Click and select Servers where independent nodes should be launched.

> **Attention!**
>
> You can create only one independent node on each Server.

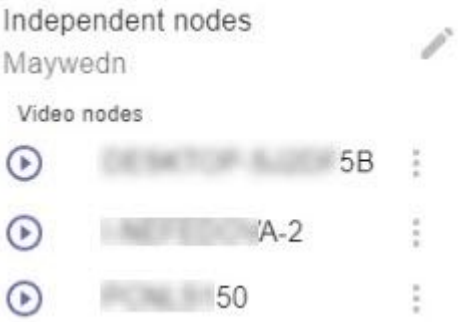


4. By default, the self-diagnostics service is running (see Self-diagnostics service(see page 619)). To stop it, de-activate the **Self diagnostics** parameter.
5. Click the **Logging** button to set the logging options.



6. Click the **APPLY** button.

The nodes are now created; they should start automatically.



15.11.6.4 1+1 cluster configuration

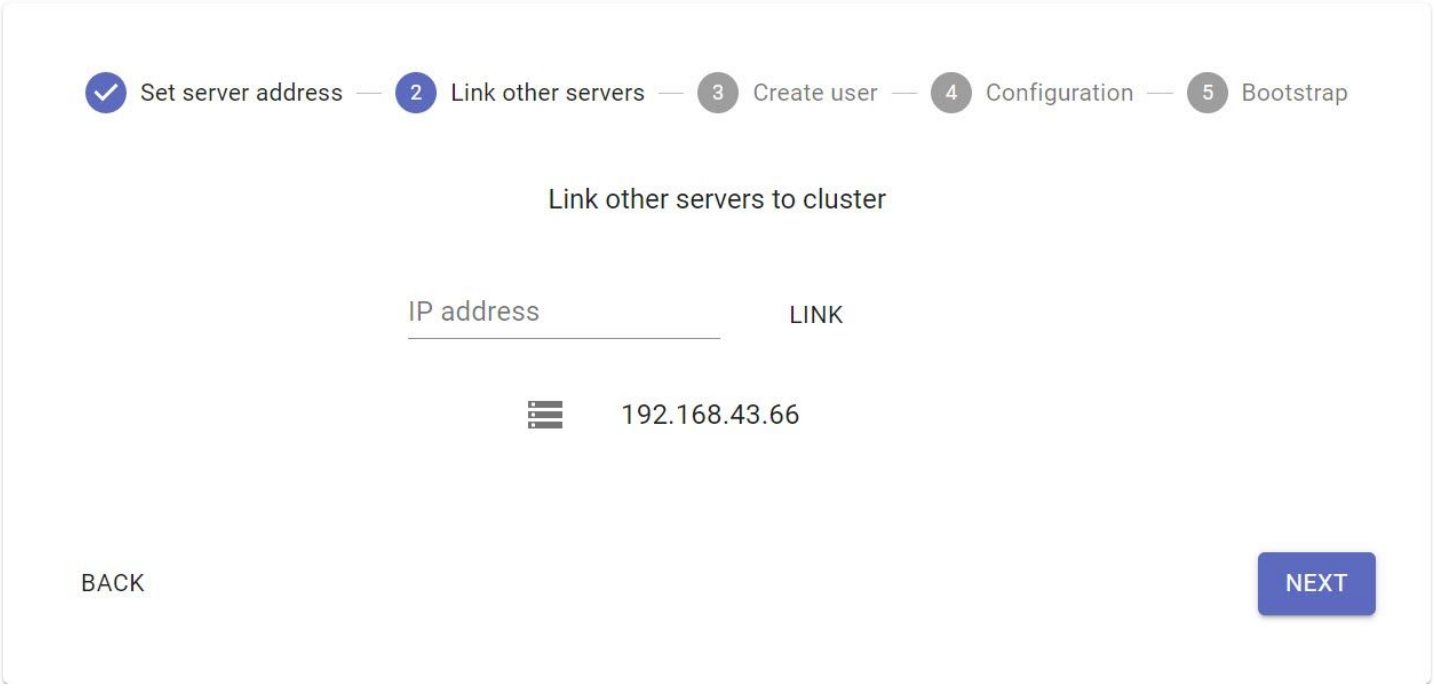
On this page:

- Setting up 1+1 configuration(see page 604)
- Converting to 1+1 configuration(see page 605)
- Editing the configuration(see page 606)
- Setting up archive replication(see page 607)
- How replication will run(see page 608)

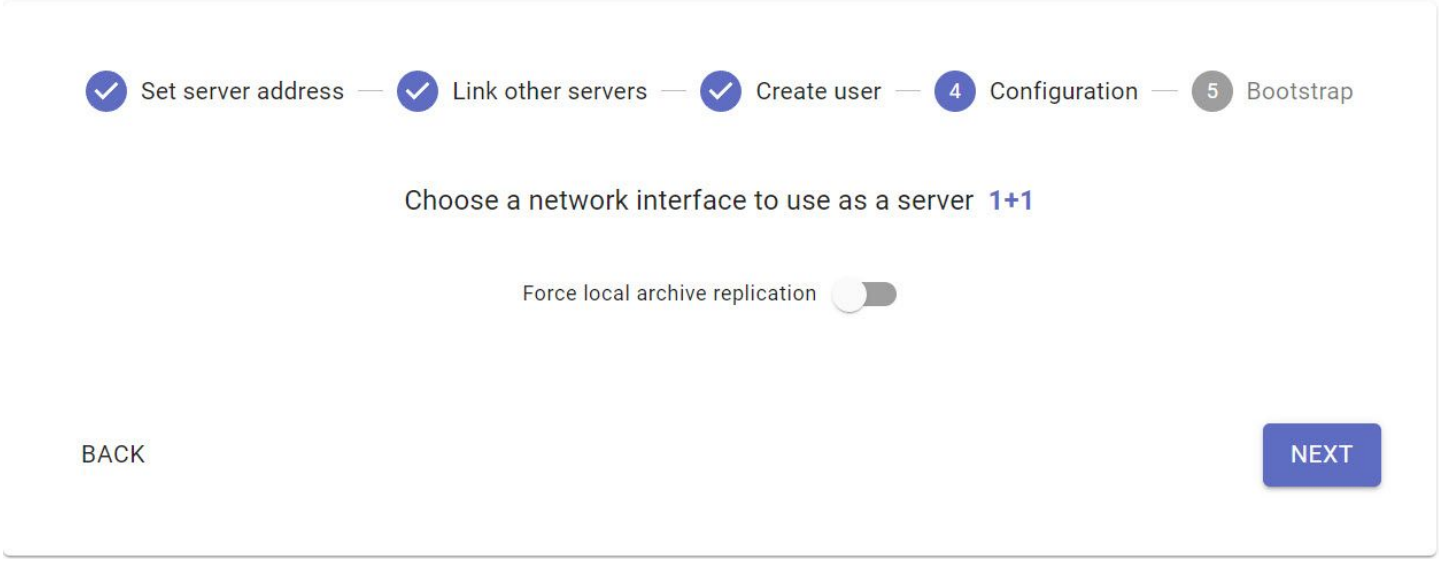
Only two Servers can be added into 1+1 configuration.

15.11.6.4.1 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**.



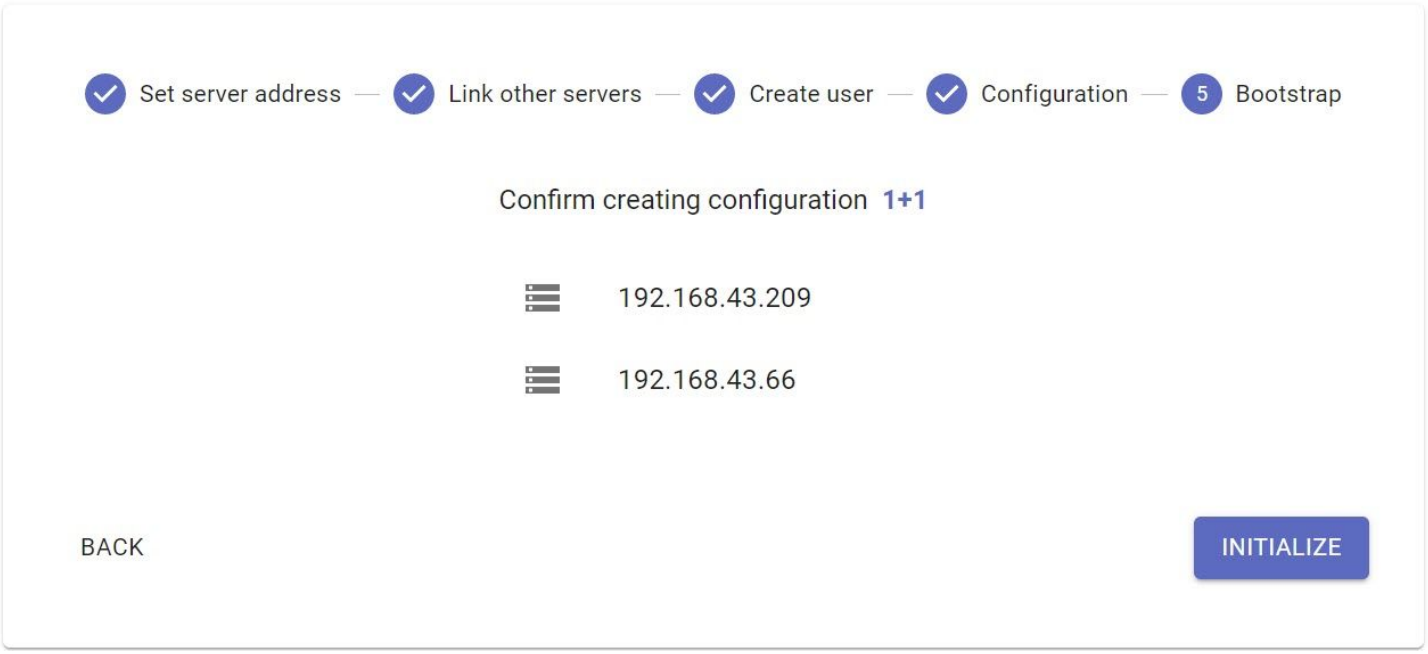
Next, activate the **Force local archive replication** parameter if you want the replication to the backup archive to be continuous regardless of the location of the master node.



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.



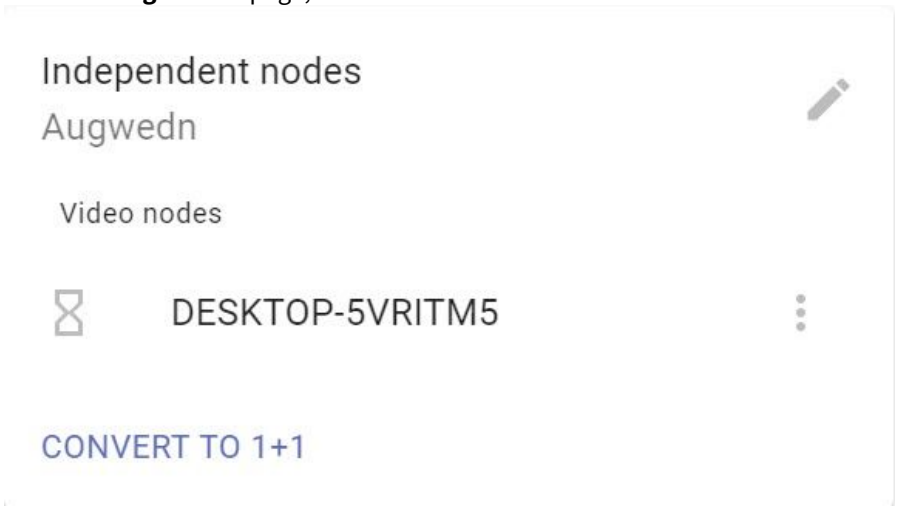
In this case, the master node will be located on the Server from which the cluster was initialized.

15.11.6.4.2 Converting to 1+1 configuration

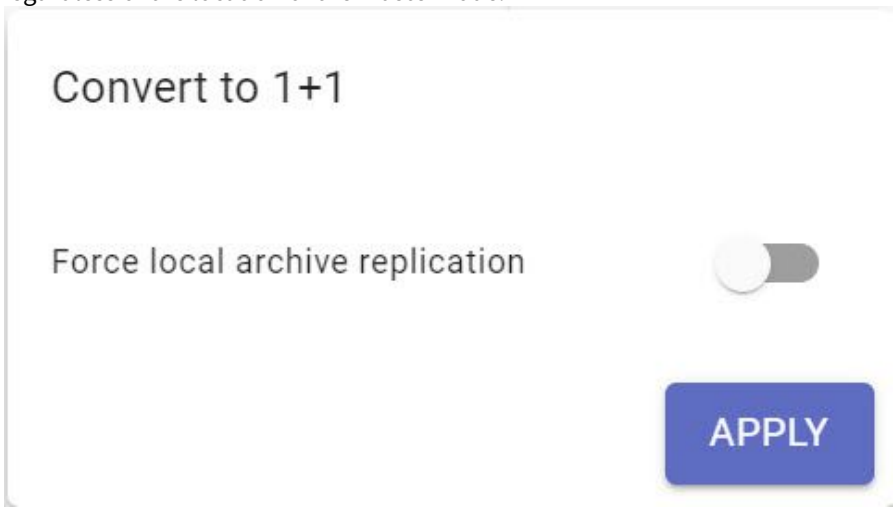
If a cluster was initialized on one Server, do the following:

1. Add a second Server to the configuration (see Creating a cluster(see page 590)).

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.

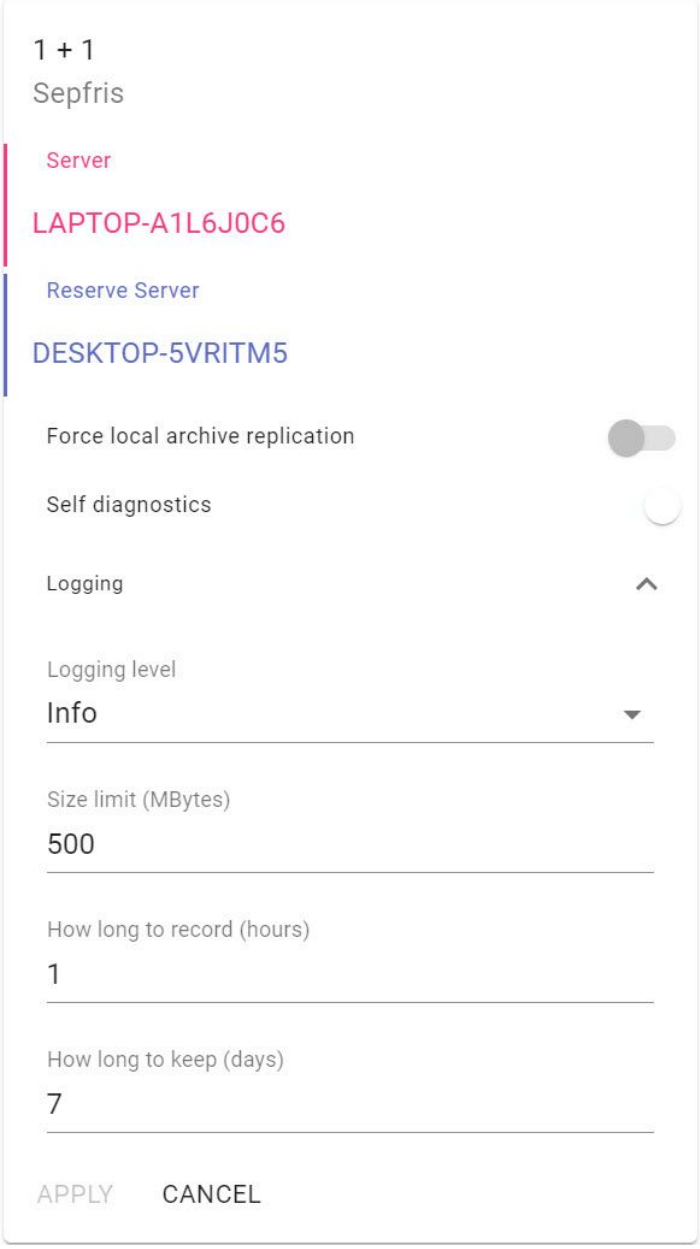


4. Click the **APPLY** button to convert to 1+1 configuration.

15.11.6.4.3 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(see page 619));



- change the logging level (see Configuring Logging levels(see page 872));
- change the log archive parameters (see Configuring a Log archive(see page 871)).

15.11.6.4.4 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 Axxon-domain(see page 109)).
2. Create a local archive on the master node (see Creating archive[177]).
3. Add video cameras on the master node (see Adding and removing IP devices(see page 112)).
4. Set up video camera recording to the local archive (see Configuring recording to an archive(see page 224)).
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(see page 226)). The replication period should be set to **Always**.

177 https://docs.axxonsoft.com/confluence/display/one20en/Creating+archive

Attention!

Archive replication is available only with the *Axxon One* Enterprise license (see Axxon One license types(see page 86)).

15.11.6.4.5 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(see page 697)).

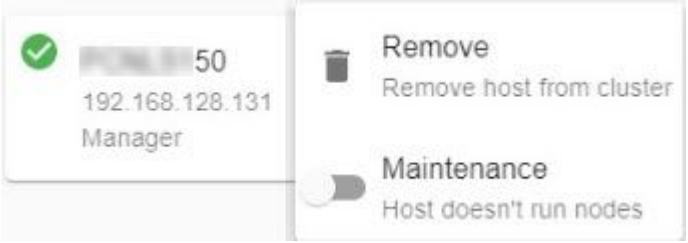
Attention!

- 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.

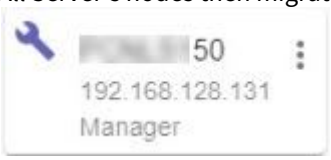
15.11.6.5 Suspending a Server within a cluster

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.

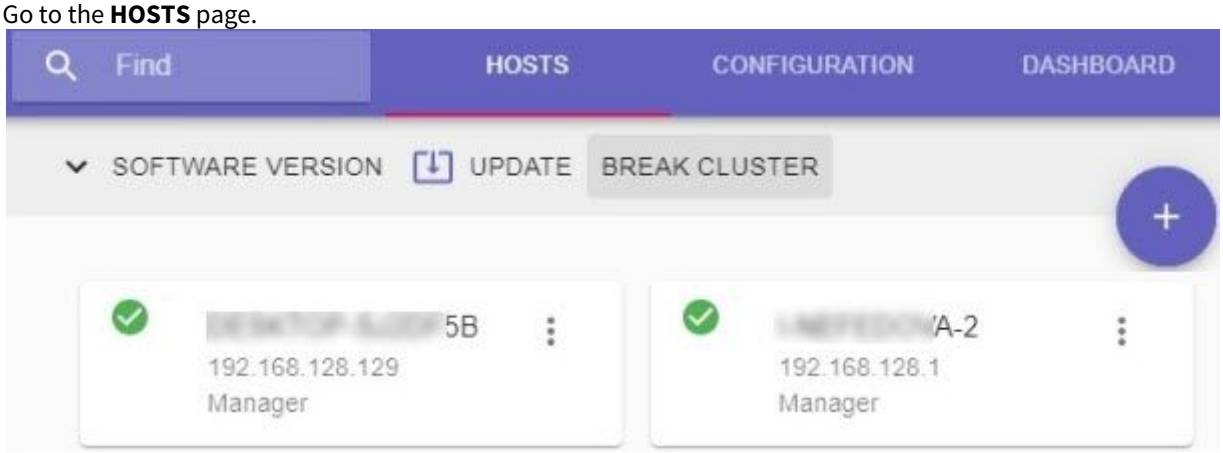


To resume the Server's operation within the cluster, toggle the Service switch to its initial position.

15.11.6.6 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.

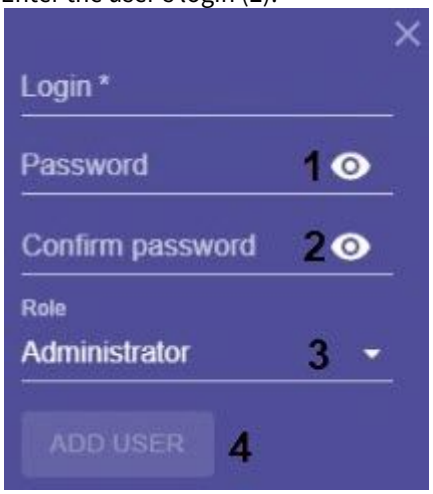
15.11.7 Set up access to a supervisor

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(see page 590)).

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**).



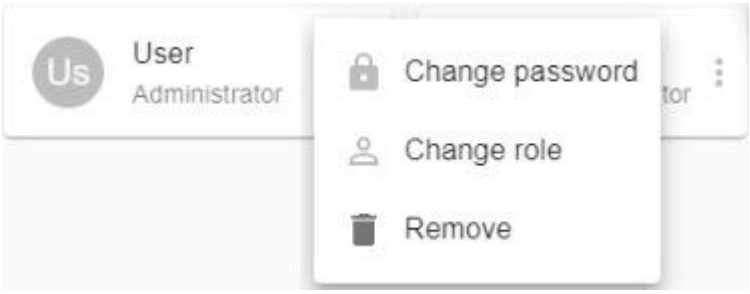
3. Enter the user's password (**2**).
4. Select the role to which the user will be added (**3**).

> **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.

15.11.8 Configuration backup and restore for failover VMS

You can back up your cluster, DBs, 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 completed.

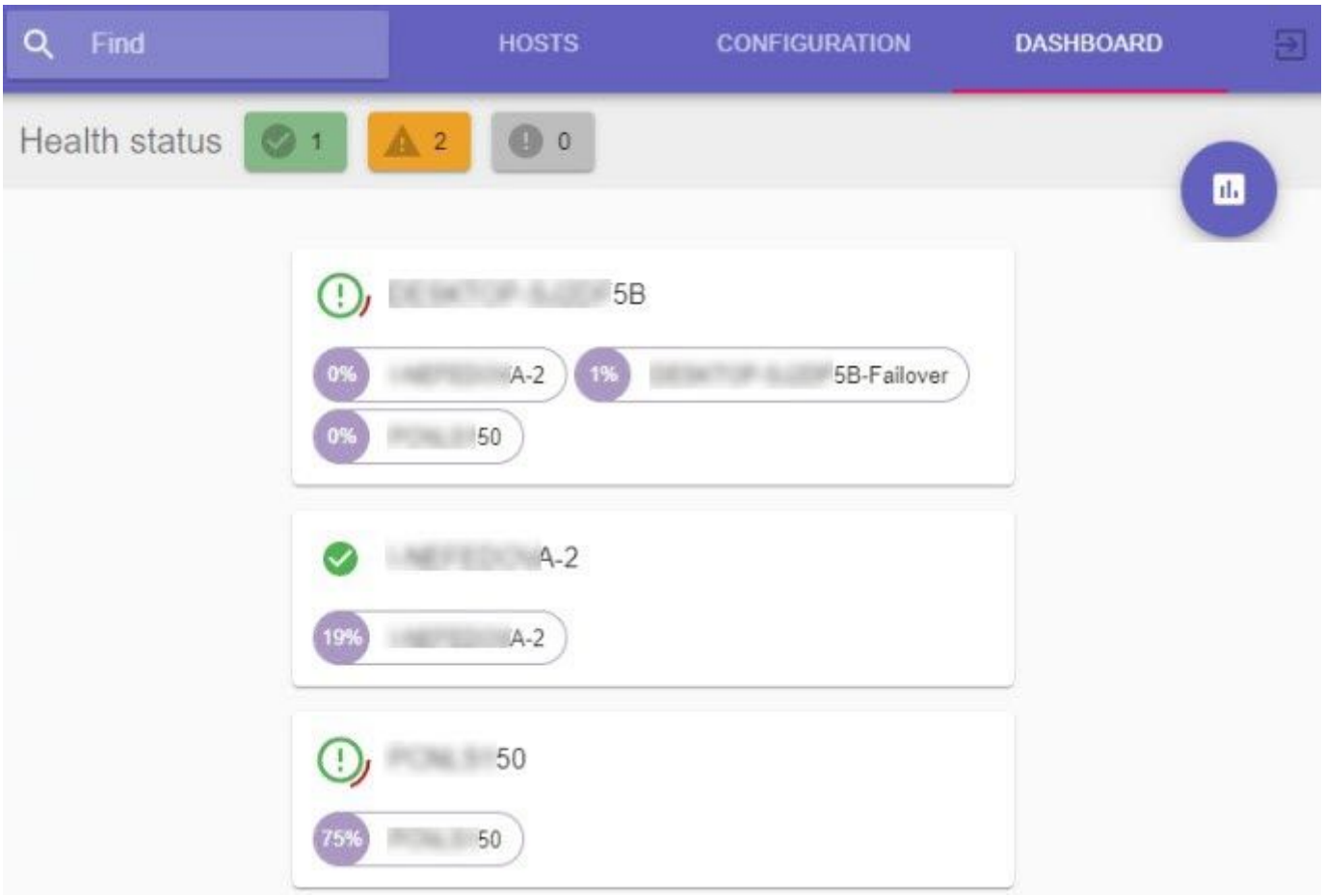
To transfer the configuration from a common security server to a failover system:

1. Create a copy of the configuration on the server (see Configuration backup(see page 885)).
2. Connect to the configuration backup and restore utility on the node (see Connecting to a Node and Configuring of an Axxon domain(see page 613)).

3. Restore the saved configuration (see Configuration restore(see page 889)).

15.11.9 Cluster Monitoring

You can monitor clusters in the **DASHBOARD** tab.



The following information is available:

1. The status of all cluster servers. All cluster servers 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 did not pass some checks. The red stripe around the icon reflects the percentage of failed checks.

2. The percentage of allocated CPU resources is calculated for all running nodes. For example, for a node consuming 9300 standard units out of total of 12400, the percentage is: (9300/12400)*100%=75%.

> **Attention!**
>
> This parameter does not reflect the actual Server CPU load; the amount of the node related load can be either higher or lower than the displayed value.

To open the CPU server load diagram, click **Show Resource**.

You can filter servers by status using the **Health status** panel.

Status	Description
	Servers that passed all checks.
	Servers that did not pass some of the checks.
	Servers that failed all checks.

The icon indicates the number of cluster servers in this status.

15.11.10 Connecting to a Node and Configuring of an Axxon domain

When the cluster is configured, connect the client to the node. Do the following:

1. Start the Client (see Starting an Axxon One Client(see page 94)).

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(see page 108)).

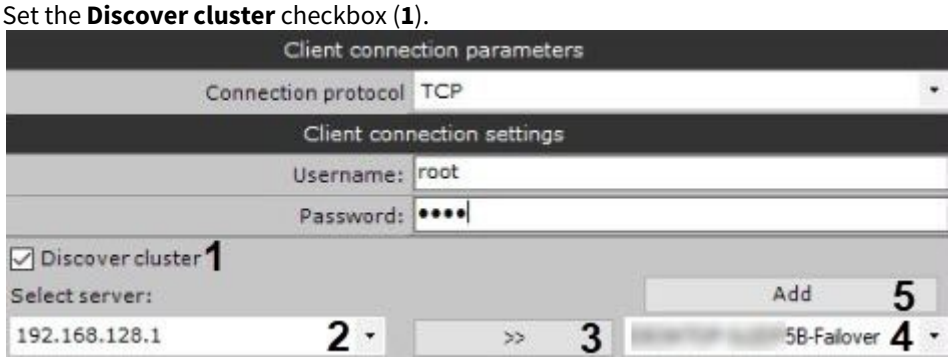
You can then merge nodes into a unified logical structure following standard procedures of Axxon domain configuration (see Configuring Axxon domains(see page 107)).

> **Attention!**
>
> An Axxon domain cannot include nodes from different clusters.

15.11.11 Configuring automatic connections to nodes

The automatic connection to a failover node is configured by connecting to a single Server of the failover system cluster. To add a node to AutoStart, do as follows:

1. Set the **Discover cluster** checkbox (**1**).

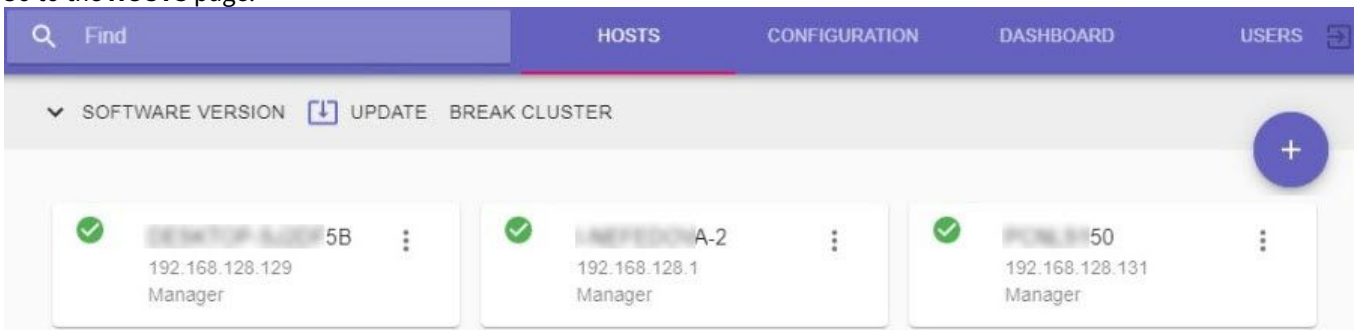


2. Enter the IP address of any cluster Server (**2**) and click the button (**3**).
3. Select from the list the node you want to add to AutoStart (**4**).
4. Click the **Add** button (**5**).

15.11.12 Updating Servers within a cluster

To update all Servers within a cluster, do the following:

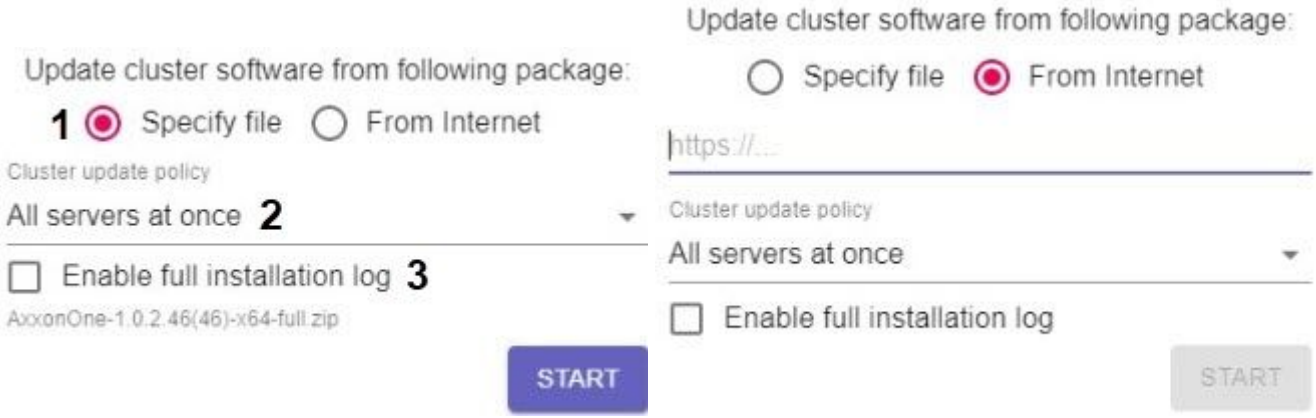
1. Back up the configuration (see Configuration backup and restore for failover VMS(see page 610)).
2. Go to the **HOSTS** page.



3. Click **UPDATE**.

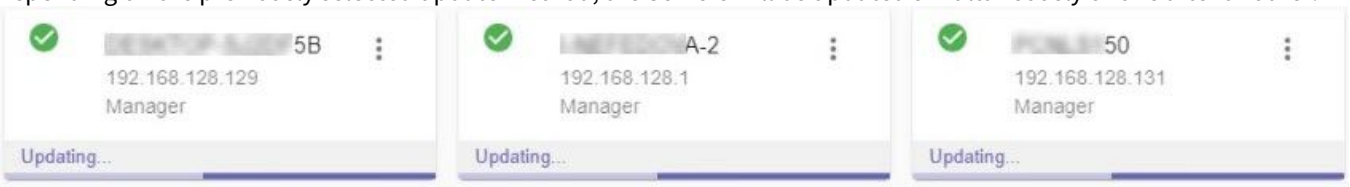
> **Attention!**
>
> You can bulk update the entire cluster only if all of its servers are accessible.

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.

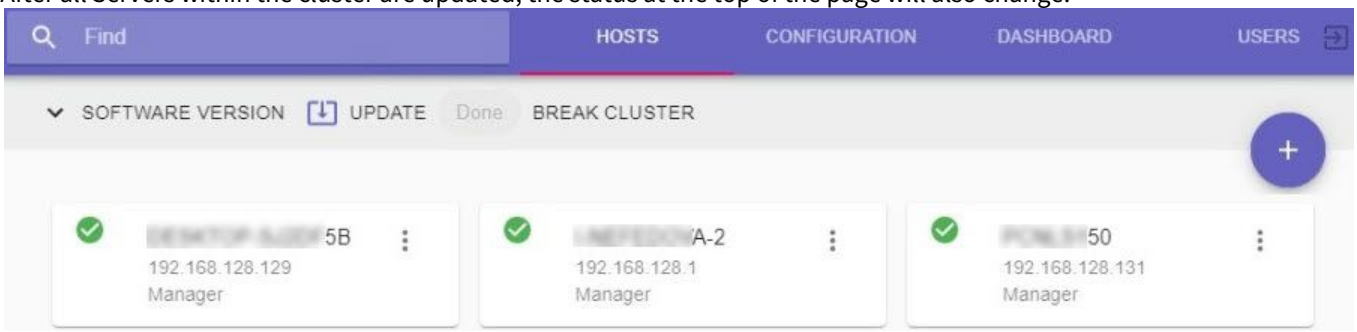
8. After the installation package is downloaded, *Axxon One* will be updated in quiet mode on all Servers within the cluster. Depending on the previously selected update method, the Servers will be updated simultaneously or one after another.



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.



15.11.13 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>
   ```

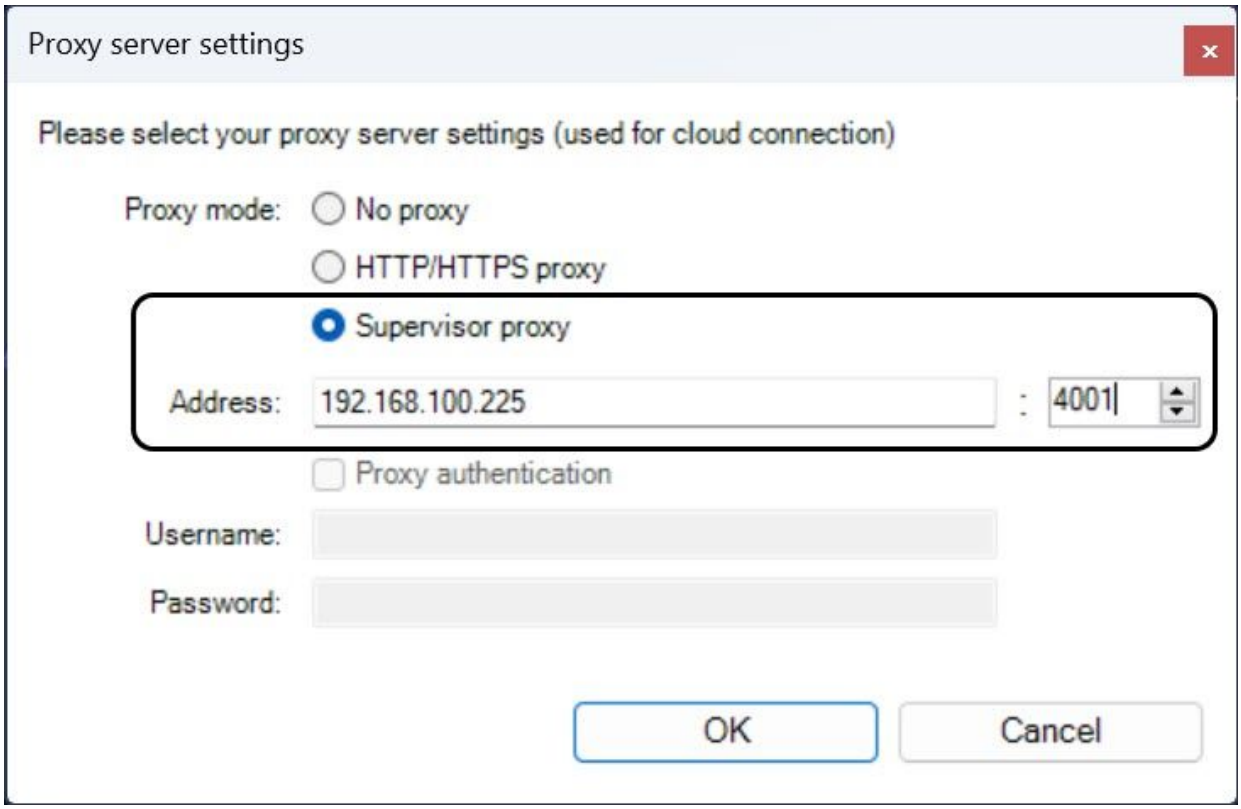
To activate the stale mode, change the value of the parameter to 200 in the file.

> **Note**
>
> Effective work in the stale mode is performed in the clusters with a large number of added Servers.

15.11.14 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(see page 590)).
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(see page 57)).
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 an Axxon One Client(see page 94)).



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.

15.11.15 Changing logging levels for the Consul and Nomad processes in a failover system

On the page:

- Changing the logging level for Consul(see page 618)
- Changing the logging level for Nomad(see page 618)

By default, the logging level for the Consul and Nomad processes is set as Info (see Configuring Logging levels(see page 872)). If you want to log debugging events, you must change the logging level for the Consul and Nomad processes to Debug.

15.11.15.1 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
     ```

15.11.15.2 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.

15.12 Self-diagnostics service

15.12.1 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(see page 620)).

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:

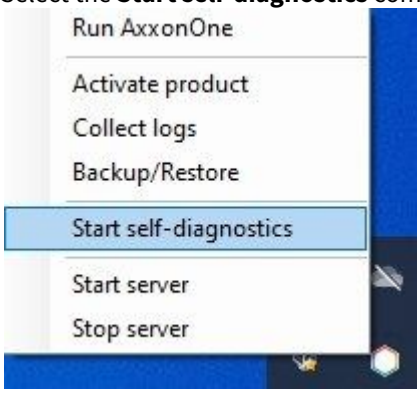
- If less than 20 GB of free memory remains on the system disk, all server logs, including the archived logs, are deleted from the system disk.
- If less than 15 GB of free memory remains on the system disk, the cleanup mechanism of the PostgreSQL event database deletes all events older than one week.

15.12.2 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:

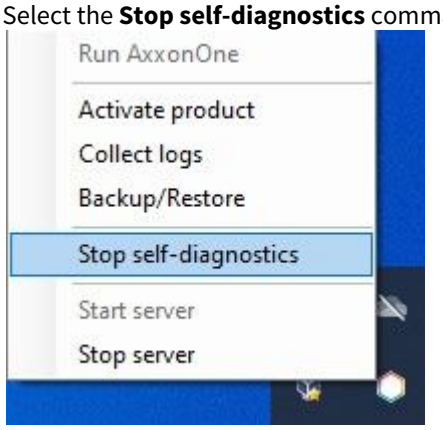
1. Select the **Start self-diagnostics** command in the Axxon One Tray Tool (see page 860)utility.



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(see page 860) utility.



2. Stop the NGP_Self_Diagnostics.

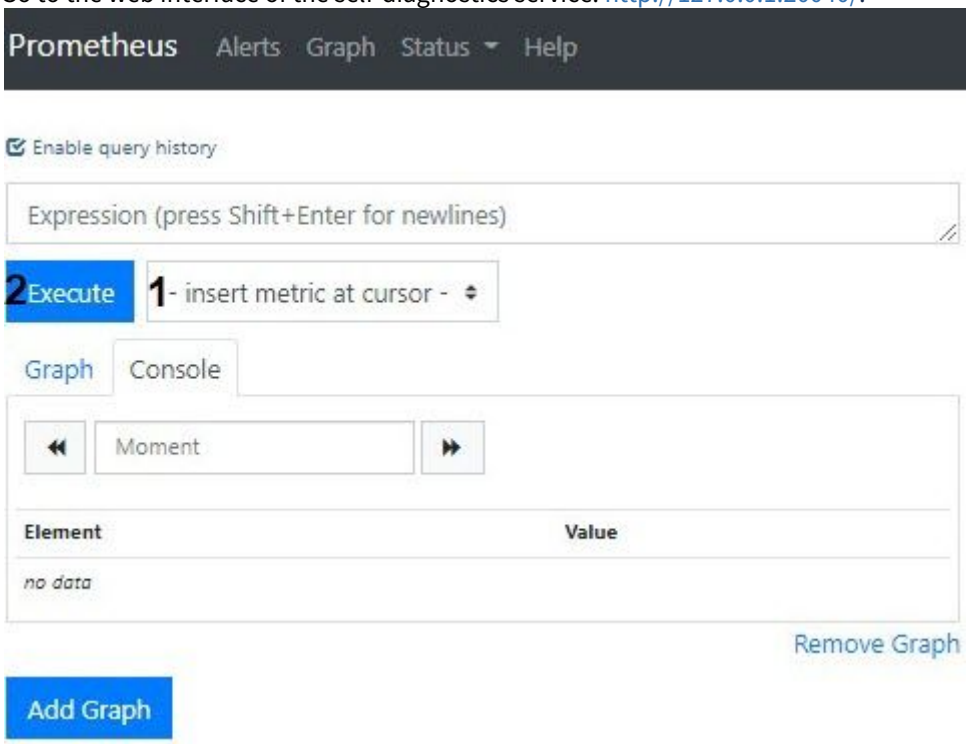
> **Note**
>
> In a failover system, the self-diagnostics service is activated/de-activated in cluster settings (see Configure a Failover System Cluster(see page 595)).

Starting and stopping the Axxon One self-diagnostics service in Linux OS(see page 932)

15.12.3 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.

Description of useful metrics

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(see page 619)): • **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[178].
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:
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:
The graph of RAM usage by the AppHost processes and a total memory space in bytes:

```
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:

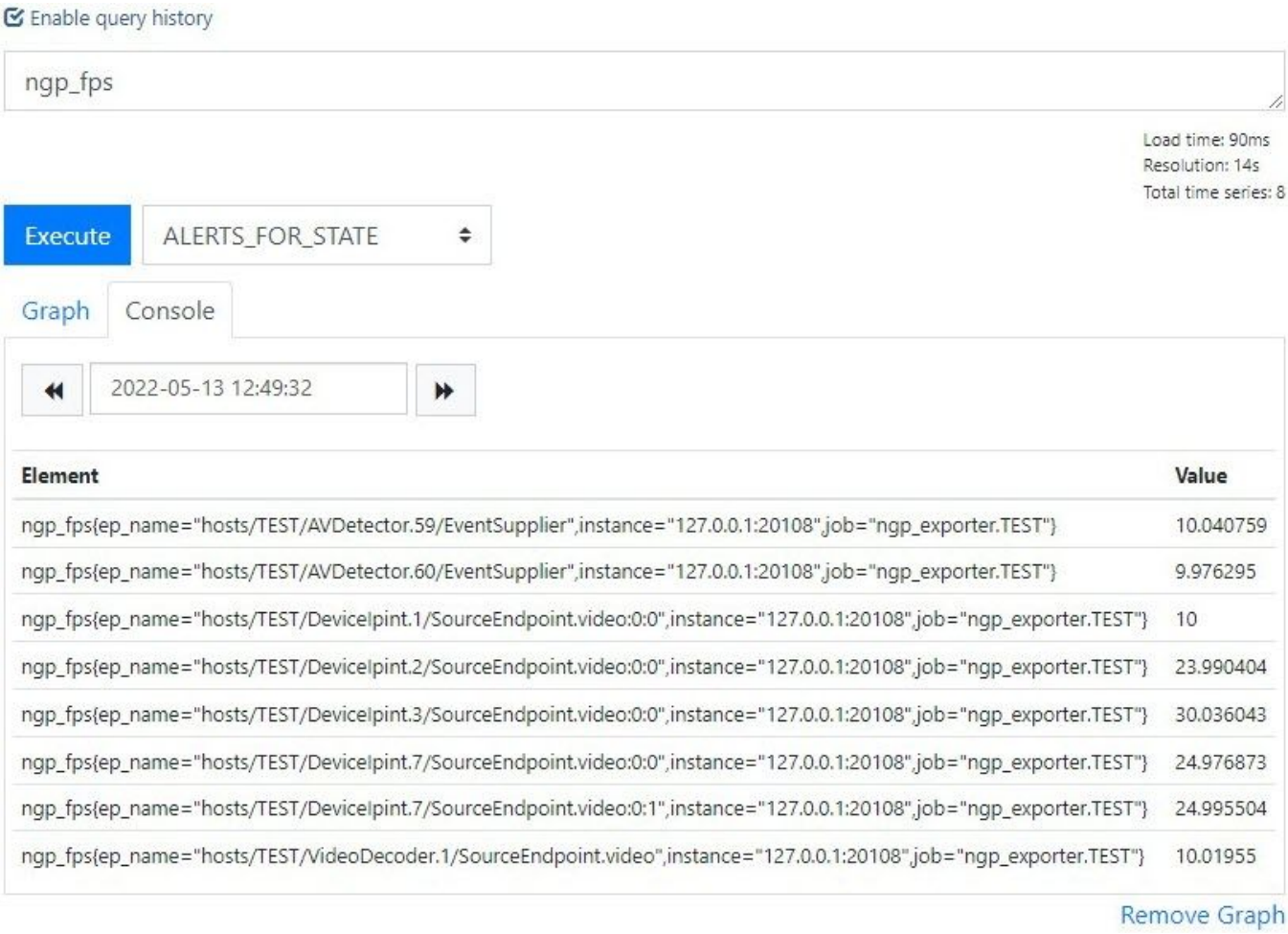
```
sum by (object_id)
(rate(namedprocess_namegroup_cpu_seconds_total{groupname="AppHost"}[1m])) * 100
```

The graph of the CPU load as a percentage:

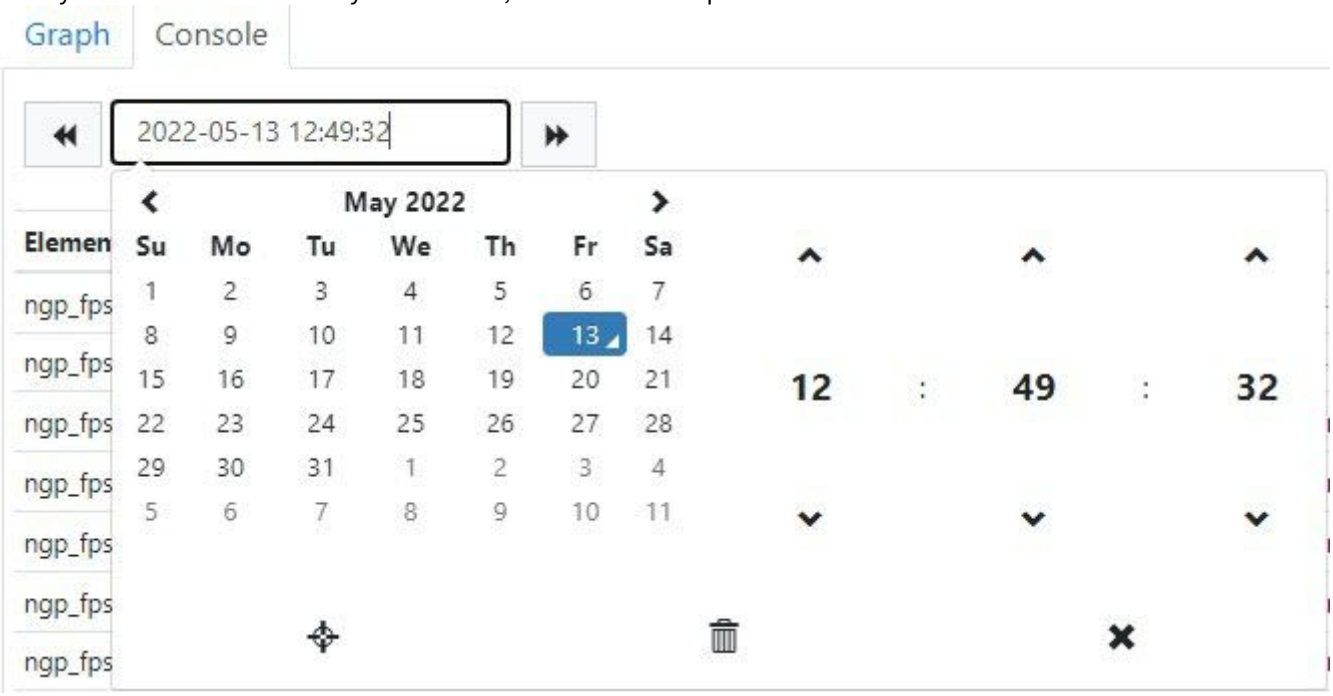
```
100 * avg without (cpu) (1 - rate(node_cpu_seconds_total{mode="idle"}[1m]))
```

3. Click the **Execute** button (**2**).
The **Console** tab will display all possible values of all elements at the time the query is completed.

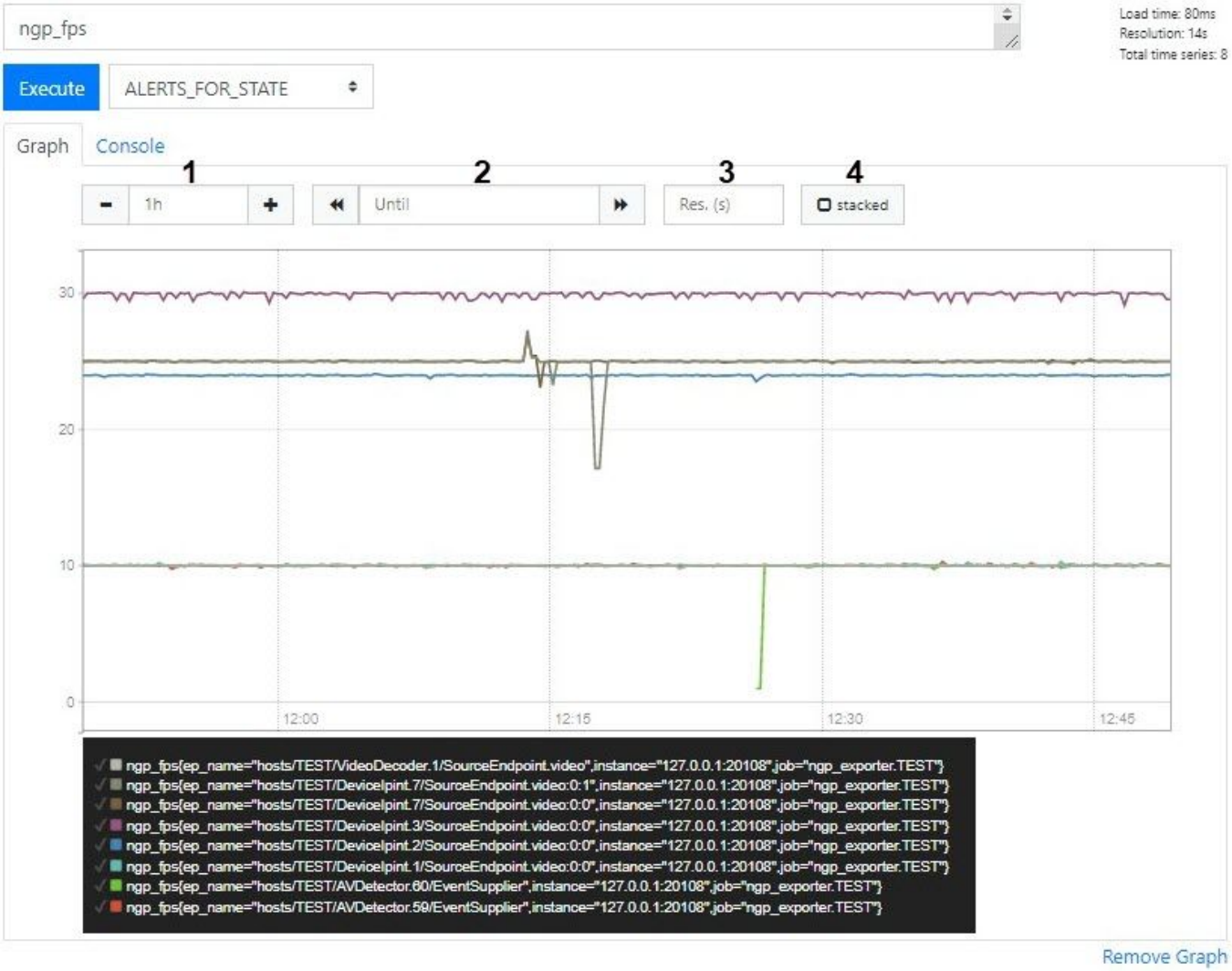
178 https://prometheus.io/docs/prometheus/latest/querying/operators/



4. When you set a date and time in your calendar, the data will be updated.



5. 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.

15.12.4 Viewing self-diagnostics metrics using third-party Grafana | Prometheus software

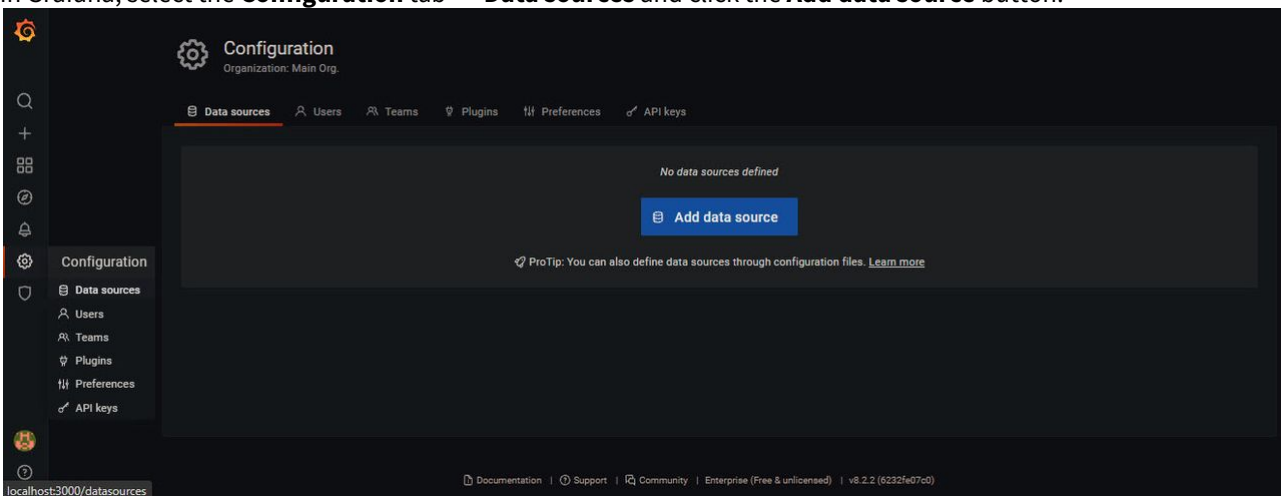
> **Attention!**
>
> AxxonSoft isn't a developer and doesn't provide technical support for Grafana | Prometheus[179] software.

To view the self-diagnostics metrics using third-party Grafana | Prometheus software, do the following:

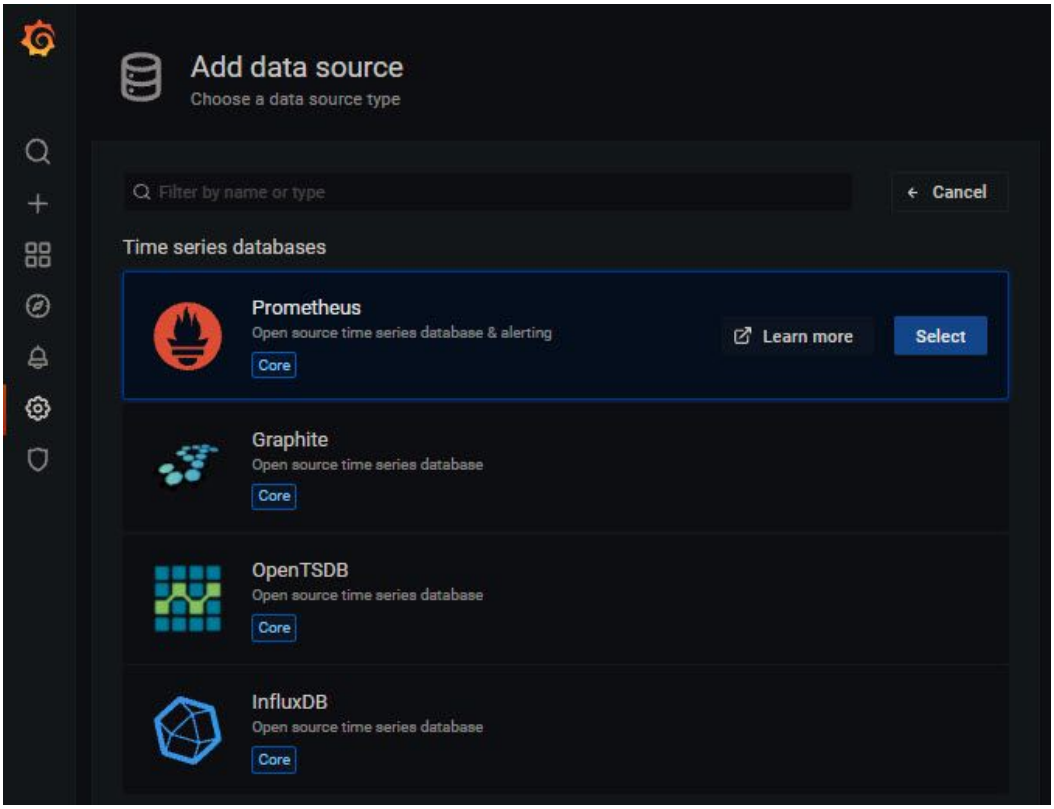
1. Download and install Grafana[180].
2. Go to the web interface of Grafana self-diagnostics service: http://localhost:3000.
3. Add Prometheus as a data source in Grafana:

179 https://prometheus.io/docs/visualization/grafana/
180 https://grafana.com/grafana/download?platform=windows

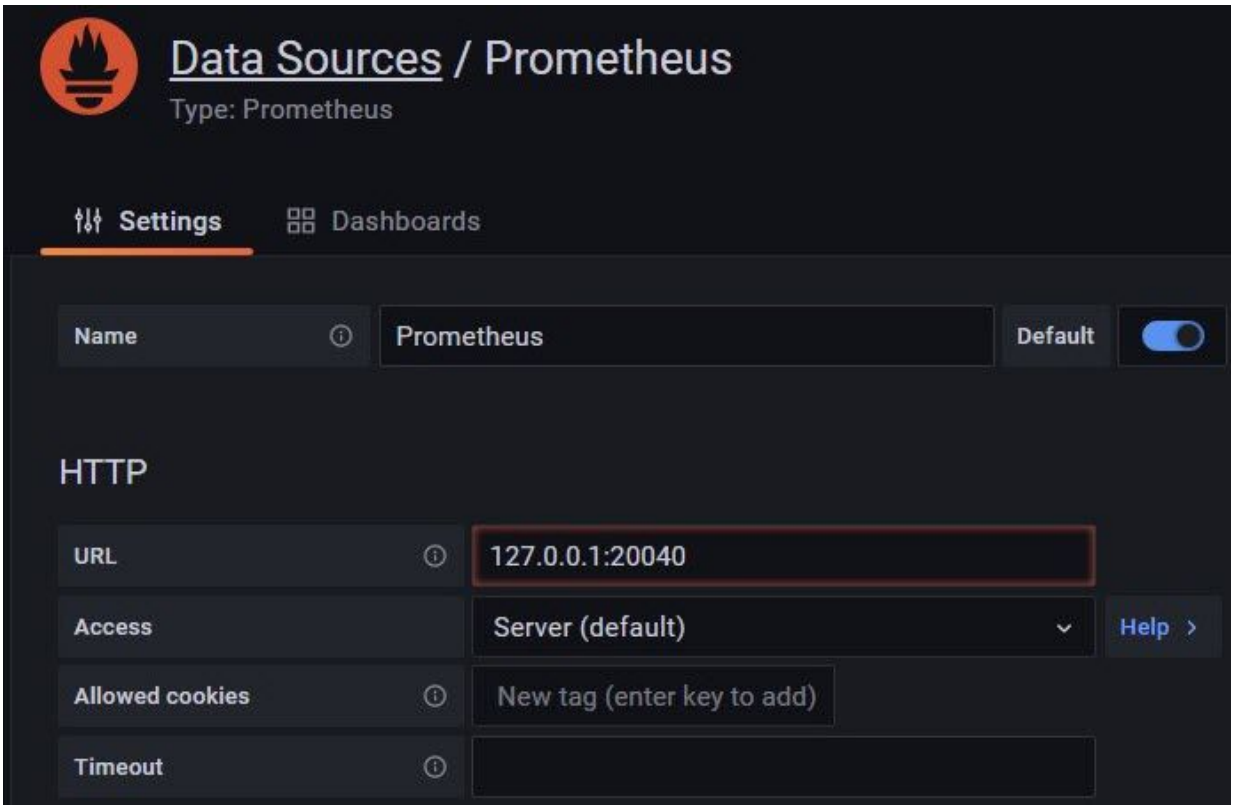
a. In Grafana, select the **Configuration** tab → **Data sources** and click the **Add data source** button.



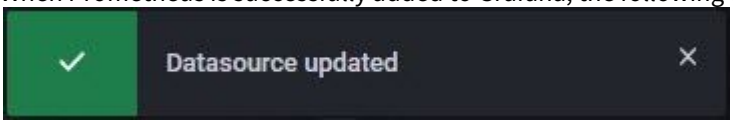
b. Select **Prometheus** and click the **Select** button.



c. Specify the URL address and Prometheus port and click the Save & test button. The default is port 20040.



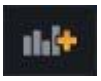
When Prometheus is successfully added to Grafana, the following window will be displayed:

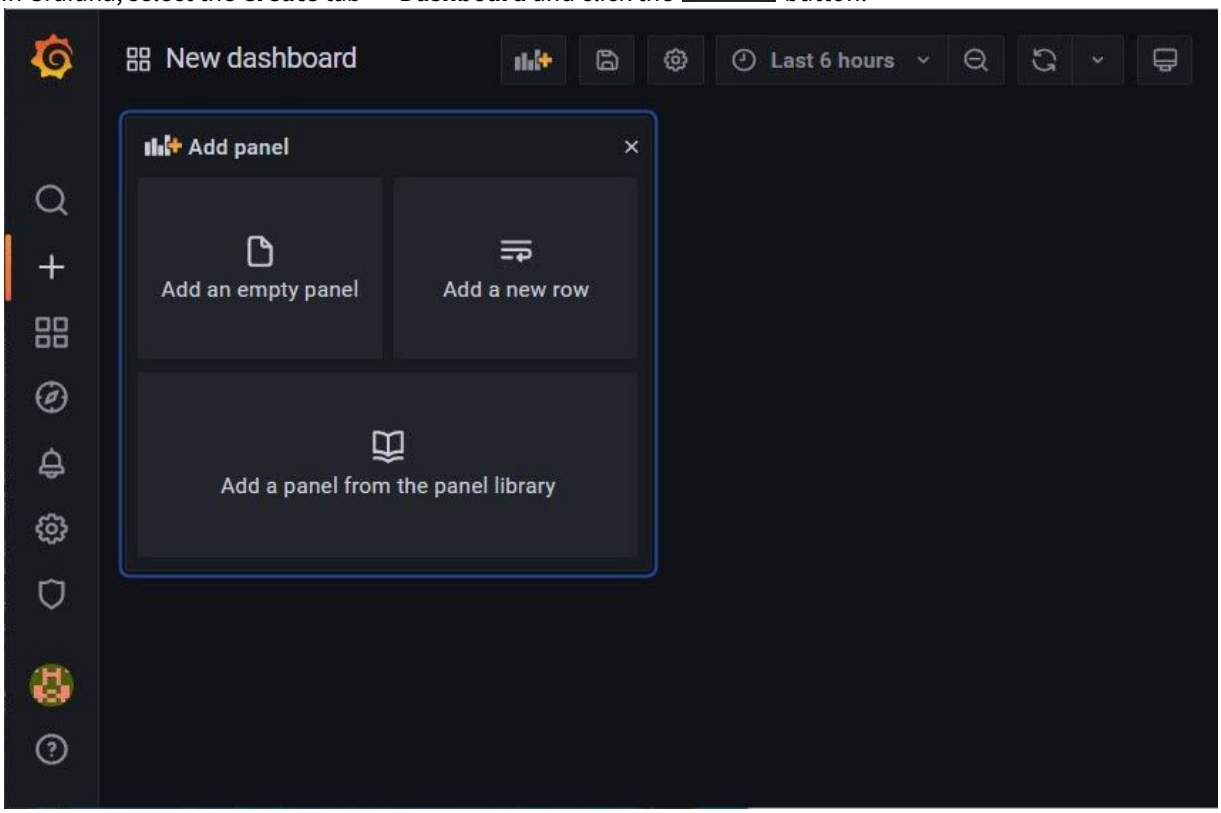


4. Configure the display of dashboards in Grafana.

Querying Prometheus[181]

181 https://prometheus.io/docs/prometheus/latest/querying/basics/

a. In Grafana, select the **Create** tab → **Dashboard** and click the  button.



b. Configure the dashboards to display the necessary information (see documentation[182]).

After configuring dashboards in Grafana, you will be able to view the self-diagnostics metrics.

182 https://grafana.com/docs/grafana/latest/dashboards/

16 Working with the Axxon One Software Package

16.1 Main Elements of the User Interface

16.1.1 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(see page 558)):

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.

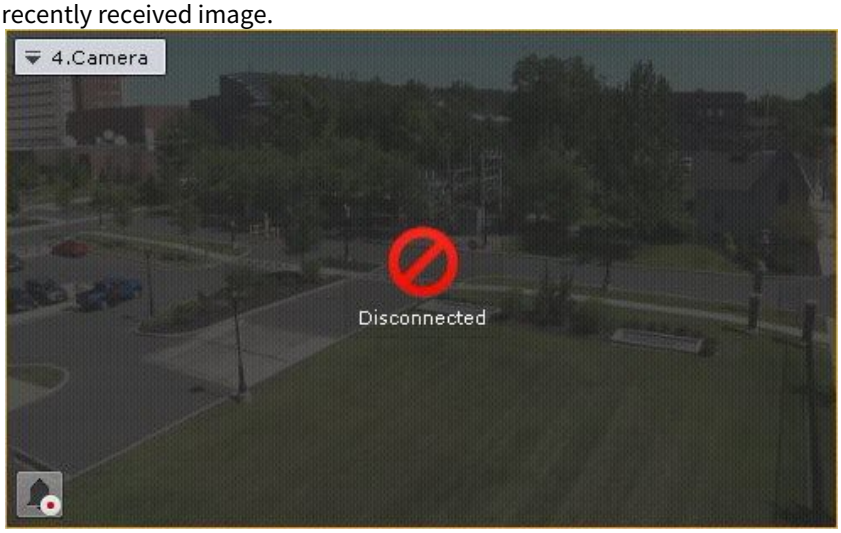
There are two states of a surveillance window within the layout: active or inactive.

A window in active state includes an additional navigation panel (see Advanced Archive Navigation Panel(see page 633)) and video mode selection tabs (see Video Surveillance Mode Selection Tabs(see page 633)).

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(see page 653).

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

.

16.1.1.1 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
Yellow	Camera armed
Gray	Archive mode

16.1.1.2 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.

16.1.1.3 Time Display

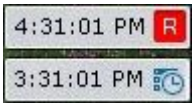
The time display appears in the upper right-hand corner of the viewing tile.

Note

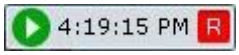
Depending on the settings (see Configuring time display(see page 559)), the indicator may show the date 5/19/2022 4:17:55 PM R.

Current time of Client is displayed on the indicator in real-time mode: 4:19:13 PM R.

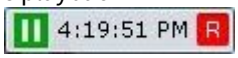
If the Client's time is different from the Server time, the Server time will also be displayed below the indicator.



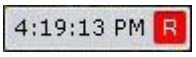
In archive, alarm, and video frame search modes, it shows the time of the fragment being viewed and the playback mode:

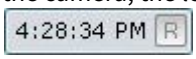
1. Forward playback 

.
2. Reverse playback

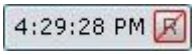
.
3. Pause 

.

If the video is currently being recorded from the camera, the letter **R** is displayed in red to the right of the clock: 

. Otherwise, the letter **R** is displayed in gray: 

.

If the camera is not linked to the archive, the letter **R** is crossed out: 

.

16.1.1.4 Display of Video Statistics

You can display video statistics in the viewing tile (see the section titled Configuring display of video statistics(see page 555)). 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.

16.1.1.5 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(see page 715)).

16.1.1.6 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 alarm status or detection tool activation:

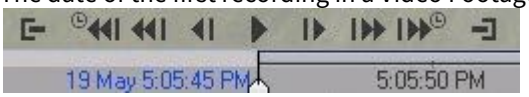
Condition	Track color
Archive absent (**1**)	Gray
Archive (**2**)	White
Archive present, alarm active (**3**)	Red
Archive present, detection tool activated (no alarm) (**4**)	Yellow

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 portion left of the marker contains videos shot when the camera was not linked to this particular Archive.

The playback control buttons on the advanced Navigation Panel are the same as the buttons on the Playback Panel (see The Playback Panel(see page 643)). 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.

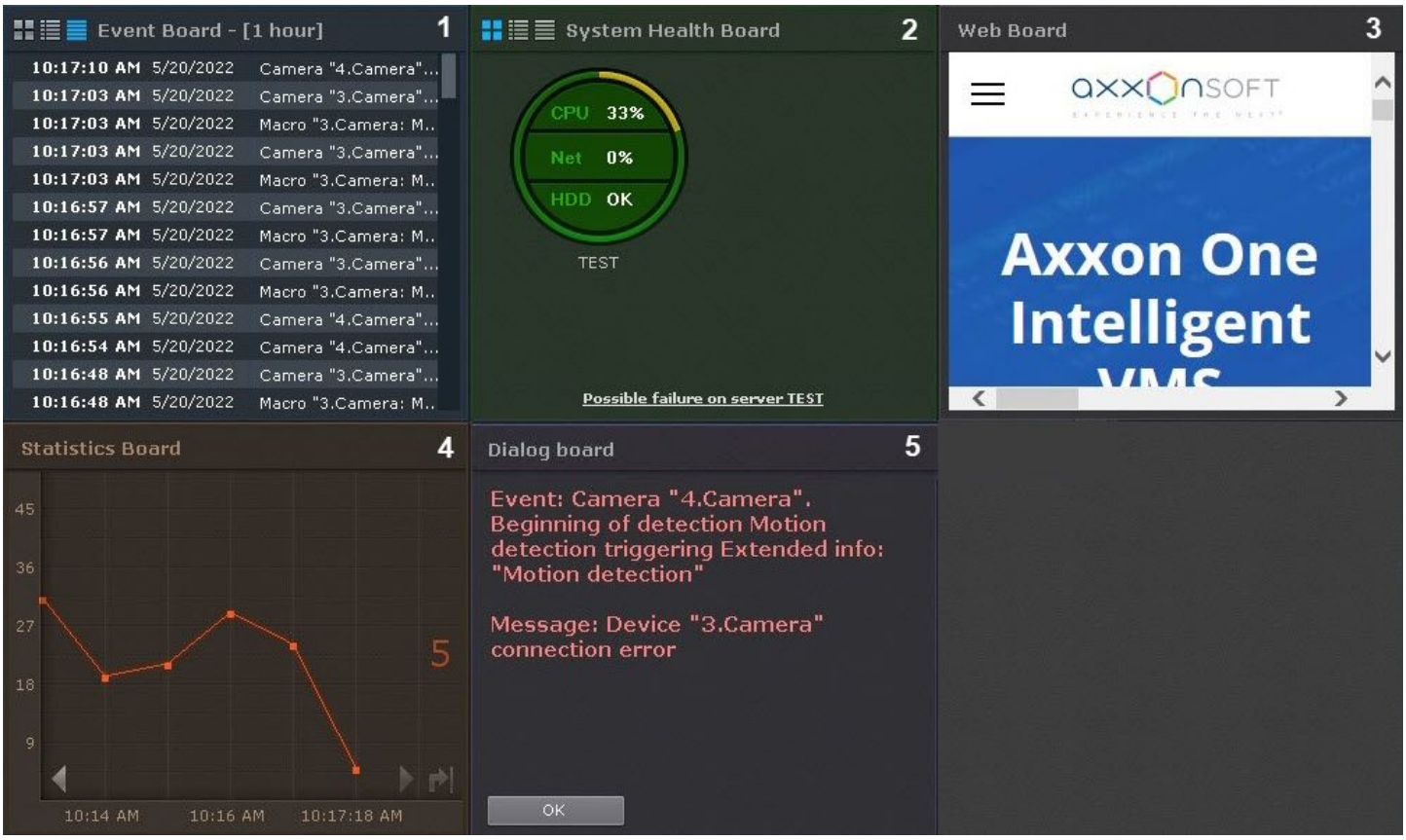
The advanced Archive Navigation Panel works completely in sync with the Playback Panel and the timeline:

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.

16.1.2 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(see page 772) (**1**).
2. System Health Board(see page 774) (**2**).
3. Web Board(see page 781) (**3**).
4. Statistics Board(see page 779) (**4**).
5. Dialog board(see page 782) (**5**).

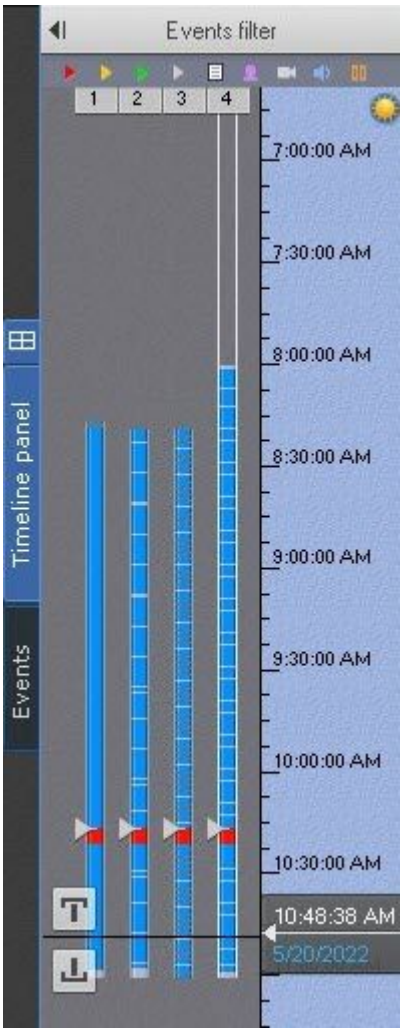


To learn about information boards, consult the relevant section(see page 771).

16.1.3 The Archive Navigation Panel

16.1.3.1 Show and Hide the Archive Navigation Panel

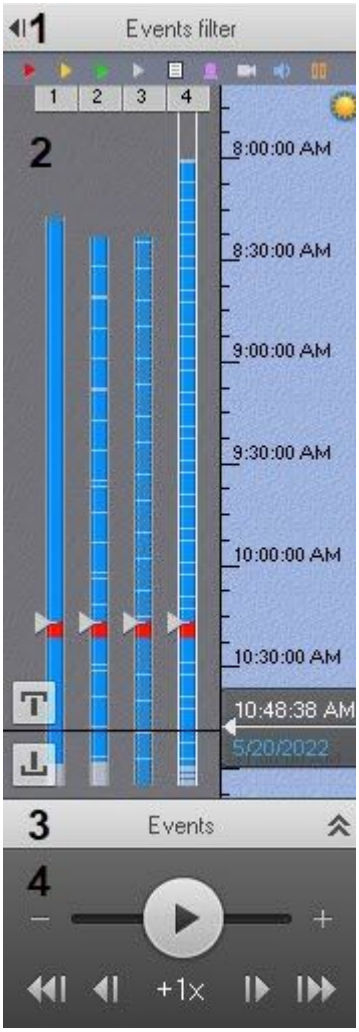
The Archive Navigation Panel is located on the right side of the screen and is automatically displayed when you switch to Archive mode (see Switching to Archive Mode(see page 695)).



To show/hide the panel, press the **Timeline panel** button.

16.1.3.2 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(see page 638) (**1**).
2. Timeline(see page 639) (**2**).
3. Events List(see page 641) (**3**).
4. Playback panel(see page 643) (**4**).

The archive navigation panel is used for the following functions:

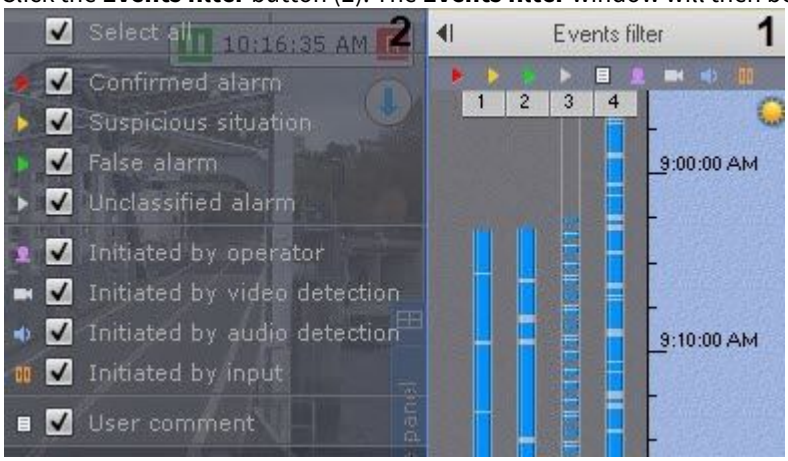
1. Navigating through the archive.
2. Playing back recordings.
3. Selecting playback mode: forward or backward.
4. Setting playback speed.
5. Selecting events for display on the timeline and in the events list.
6. Viewing the list of events of the selected type.

16.1.3.3 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.

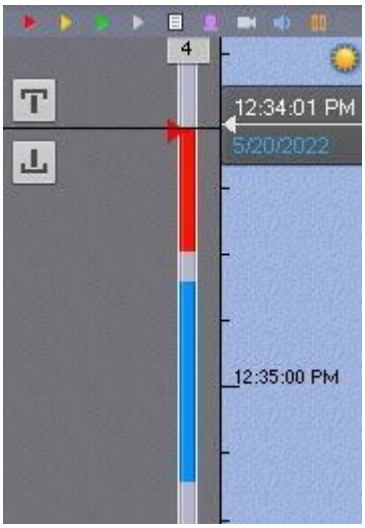
> **Note**
>
> To close **Events filter**, click to same button again.

Selection of events is now complete.

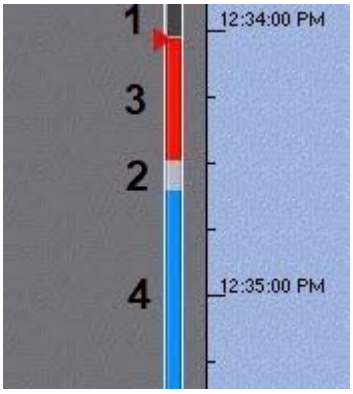
Events of the selected type are now displayed on the timeline (see The Timeline(see page 639)) and in the events list (see Events List(see page 641)).

16.1.3.4 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 alarm status or detection tool activation:

Condition	Track color
Archive absent (**1**)	Gray
Archive (**2**)	White
Archive present, alarm active (**3**)	Red
Archive present, detection tool activated (no alarm) (**4**)	Blue

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. Grey footage takes priority over dark grey.

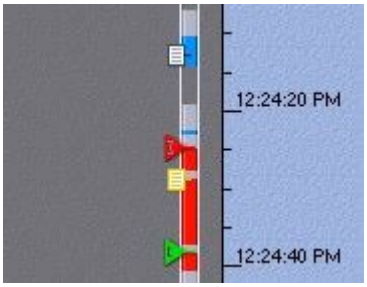
At the moment when an alarm is assigned a status (critical, non-critical, false, or unclassified), a flag is added to the track. A flag is added to the point on the timeline when the alarm began.

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(see page 638)).

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.

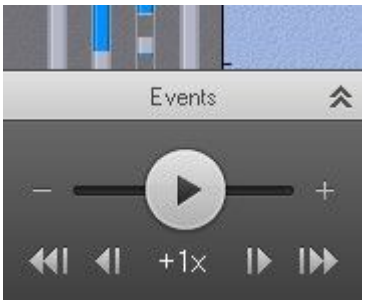
If there is no recording in the selected position, the indicator will automatically move to the position corresponding to the nearest recording.

> **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(see page 705)).
> You can also position the timeline indicator with the help of the events list (see the section Events List(see page 641)).

16.1.3.5 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(see page 638)).

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(see page 708).

16.1.3.6 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.

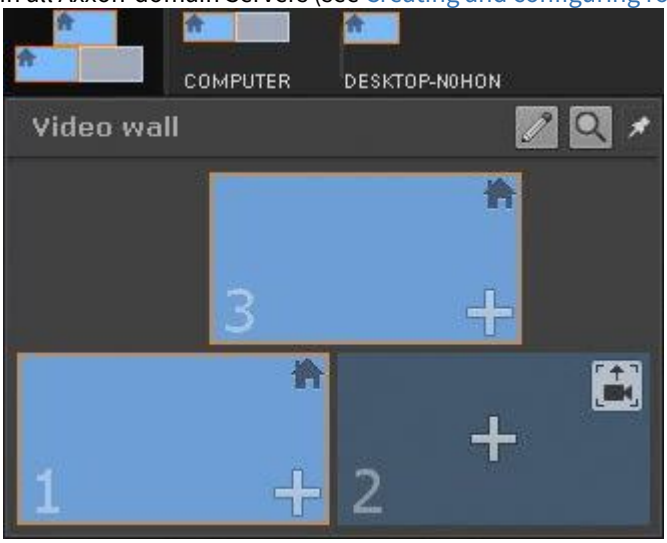
> **Note**
>
> Use of the playback panel is described in detail in the section Navigating Using the Playback Panel(see page 708).

16.1.4 Video Wall Panel

> Configuring Videowall(see page 508)

The Video Wall panel is automatically displayed at the top of the screen.

The panel is used to set up a video wall from all monitors currently connected to Axxon-domain Servers on which video walls management is permitted for the given User. The panel is hidden from users with no permissions for management of video walls in all Axxon-domain Servers (see Creating and configuring roles(see page 452)).



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.

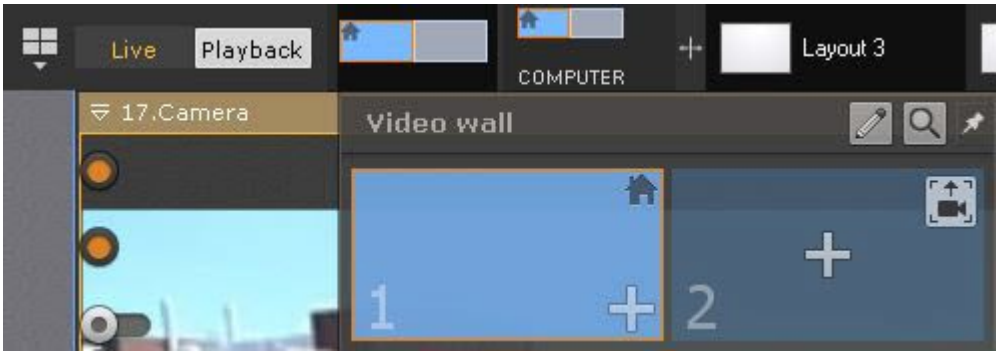
> **Note**
>
> To hide the panel, click the button.

16.1.5 Monitor Panel

The Monitor panel is automatically displayed at the top of the screen.

The panel shows thumbnail views of Client monitors currently connected to Axxon domain Servers on which video walls management is permitted for the given User (see Creating and configuring roles(see page 452)).

To open an expanded monitor view, click on its thumbnail.



If you need to always display expanded monitor views, click .

> **Note.**
>
> To disable expanded views, click .

You can change width of the Monitor panel. To do it, click and drag the panel border .

When you resize the Monitor panel, the Layout panel is automatically changed.

16.1.6 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(see page 786)

16.1.7 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[183] 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.

183 http://www.openstreetmap.org/copyright

Please refer to the section titled Working with the interactive map(see page 795) for further details on how to work with the 3D map.

16.1.8 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(see page 648)), 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.

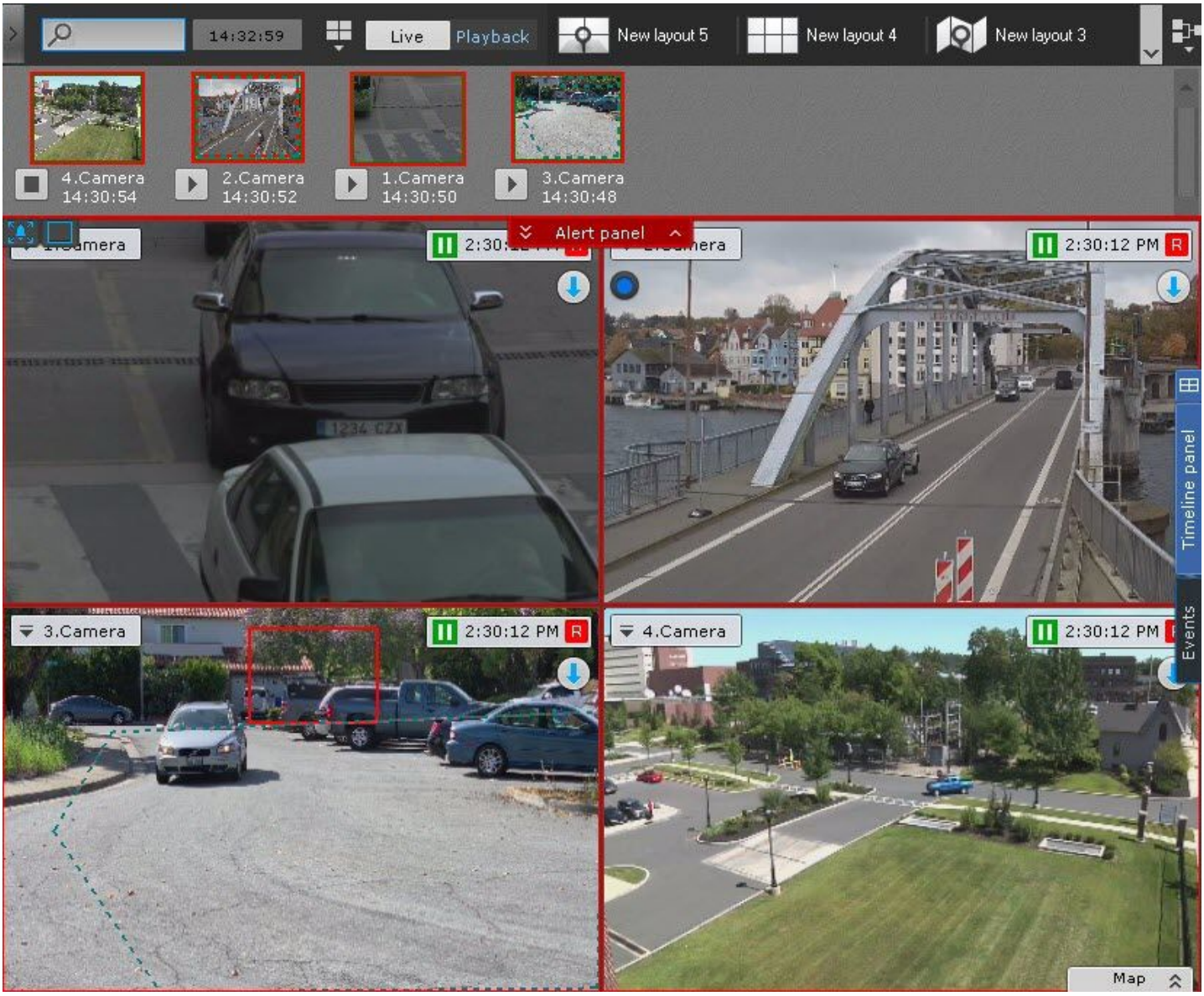
If there is no layout with the selected video camera, a new layout with a single cell is created.

16.1.9 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.

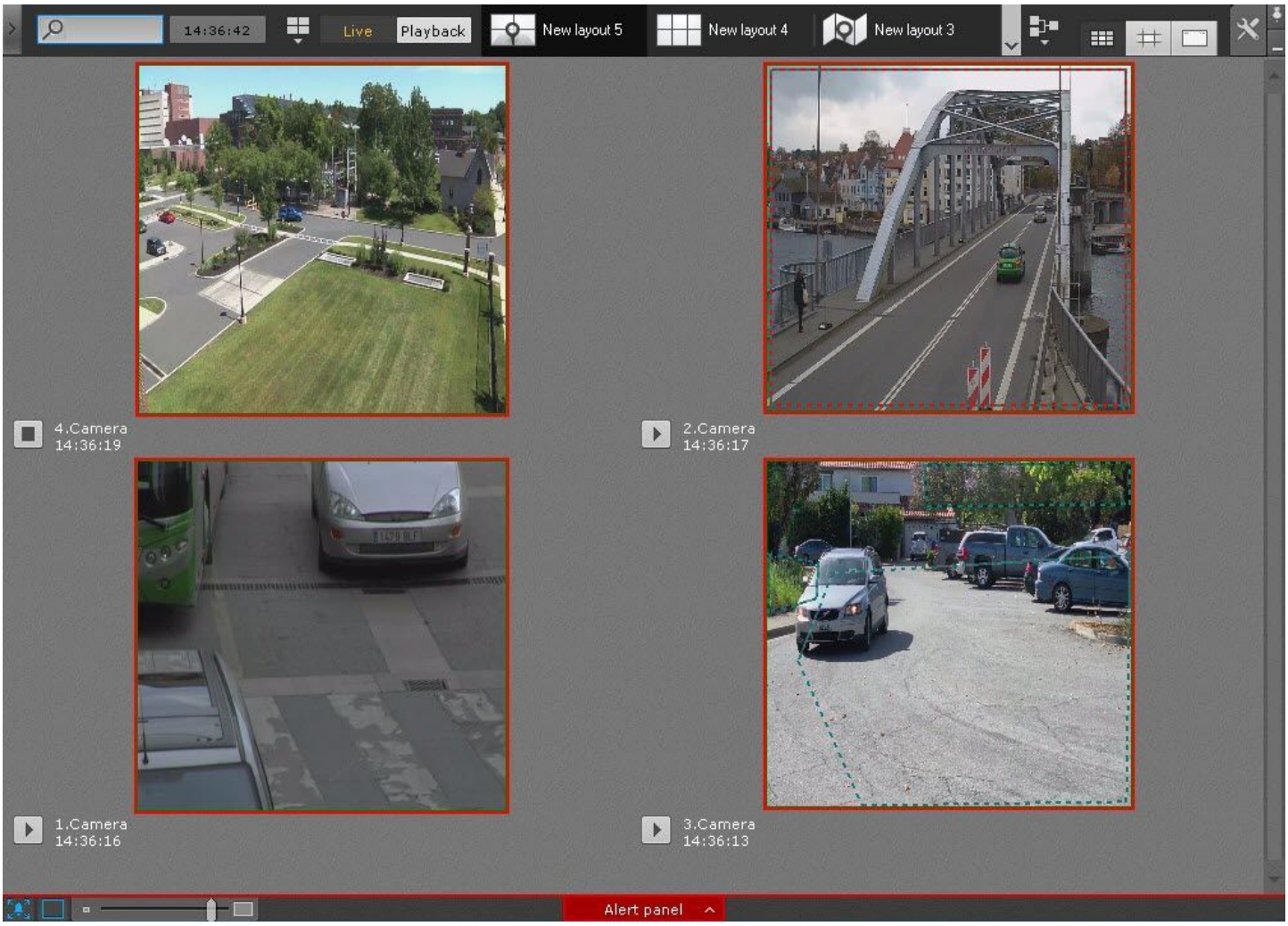
Alert panel is located at the top of the screen and is hidden by default. To open the Alert panel, click the Alert panel button.



The size of the Alert panel is adjustable from 10% to 50% of the screen vertically.

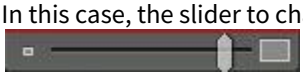
To resize the panel, left-click the **Alert panel** button and, holding it, move the cursor up or down.

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.

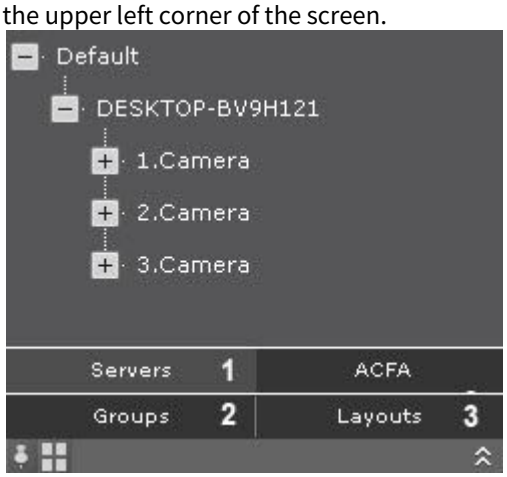
> **Note**
>
> The Alert panel button isn't displayed in the Videowall mode.

16.1.10 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(see page 790)), 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(see page 200));
- Layouts (**3**): all available layouts with video cameras added to them are displayed (see Creating and deleting layouts(see page 471)).

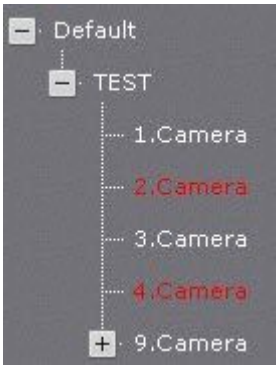
When you click on a layout name in the object tree, the corresponding layout is selected from the list. When you click on the camera name, if it is absent on the current layout, the layout with the selected camera will open.

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(see page 646)).

Note

To search for objects inside the panel, use the search bar, same as the search panel for video cameras (see Camera Search Panel(see page 646)).
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(see page 646)).
On the Objects panel, the cameras can be sorted either by name or short name (see Configuring camera sorting on Objects Panel(see page 564)).

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.

16.1.11 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(see page 164)).

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.

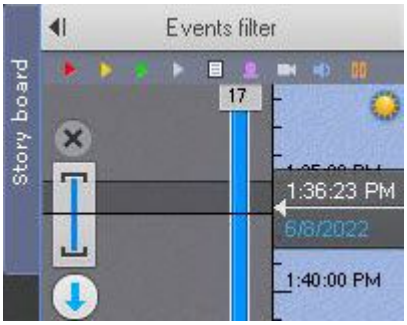
> **Note**
>
> The type of virtual 3D joystick and adjustment scale depend on the type of PTZ cameras: discrete or continuous control of Pan, Tilt, Zoom, Focus, and Iris.
>
>
>

6. Patrol button.

> **Note**
>
> Use of the dialer, PTZ controls, joystick, and patrol button is described in the section Controlling a PTZ Camera(see page 675).

16.1.12 Story board

The Story board becomes available after you set a time interval on the timeline (see Standard video recordings export(see page 809)).



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 Exporting all event videos(see page 814)S(see page 813)).

To hide the board, click once more the **Story board** button.

16.2 Video Surveillance

16.2.1 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.

16.2.2 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.

16.2.2.1 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.

16.2.2.2 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.

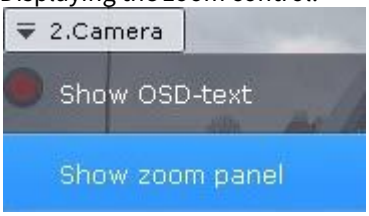
The video image can be enlarged using the following tools:

1. Digital zoom scale.
2. Area selection.
3. Mouse scroll wheel.

16.2.2.2.1 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.

16.2.2.2.2 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.

16.2.2.2.3 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.

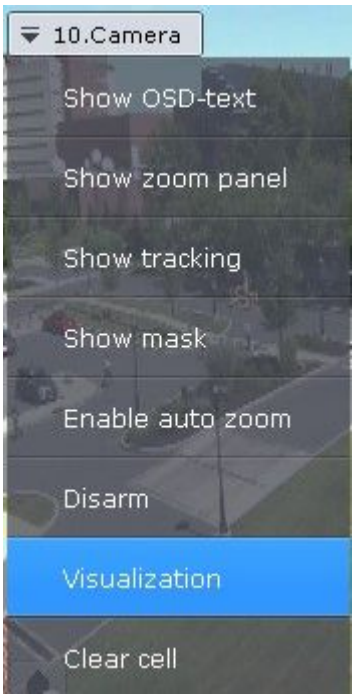
Action	Executed function
Mouse wheel is scrolled forward by one level	The video image is enlarged by 2x
Mouse wheel is scrolled backward by one level	The video image is reduced by 2x

16.2.2.3 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.

16.2.2.3.1 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.

16.2.2.3.2 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.

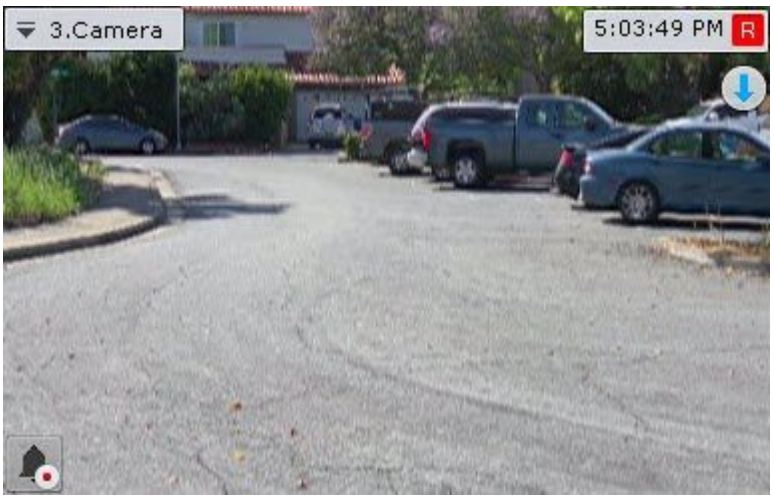
The image in the following picture shows an example of use of the **Sharpness** tool.

To return to the original image, use the **Sharpness** function again.

16.2.2.3.3 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.

16.2.2.4 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.

16.2.2.5 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 Scene Analytics detection tools(see page 254));
2. the Video Motion Detection tool is activated (see Configuring VMD(see page 250));
3. at least one of the Embedded Analytic tools is activated (see Embedded Detection Tools(see page 393)).

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(see page 255)), then you can see the detection parameters (areas, lines) in Live Video mode along with object tracking in the camera window.

Note

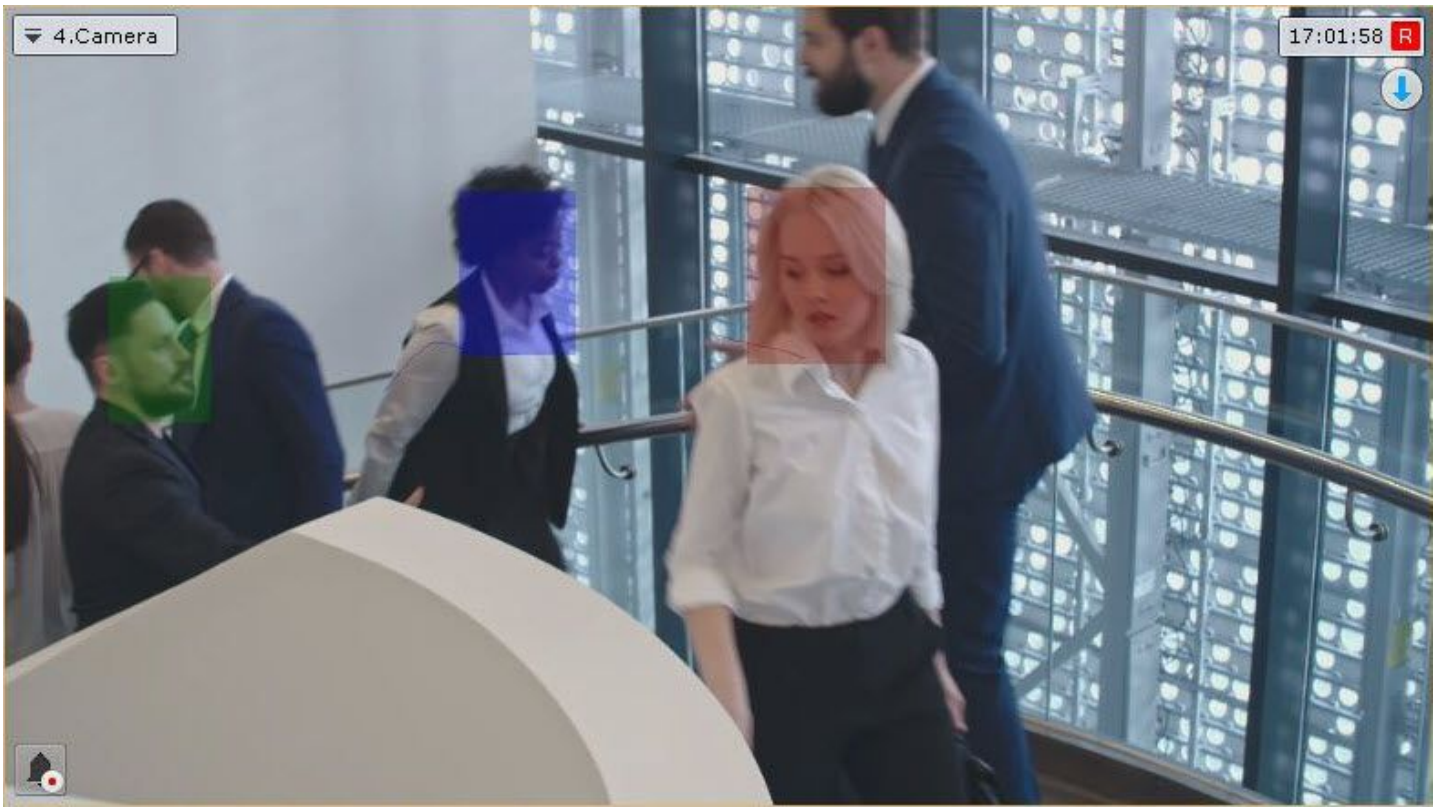
Areas to be excluded from surveillance are outlined in dotted black and green line while detection areas are outlined in black and gray.

If an ANPR detection tool has been created for a camera, the license plates within the video image will be outlined (see Automatic Number Plate Recognition (LPR/ANPR) tools(see page 308)).

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(see page 122)).

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 Configure Pose detection tools(see page 373)) has been created for a camera, a human skeleton is highlighted over the video image.

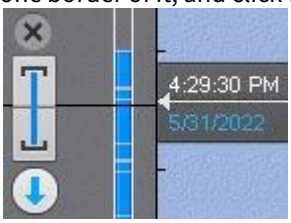
16.2.2.6 Operator comments

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(see page 702)) and are marked with tags on the timeline (see The Timeline(see page 639)). Comments can also be searched (see Searching comments(see page 729)).

16.2.2.6.1 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.

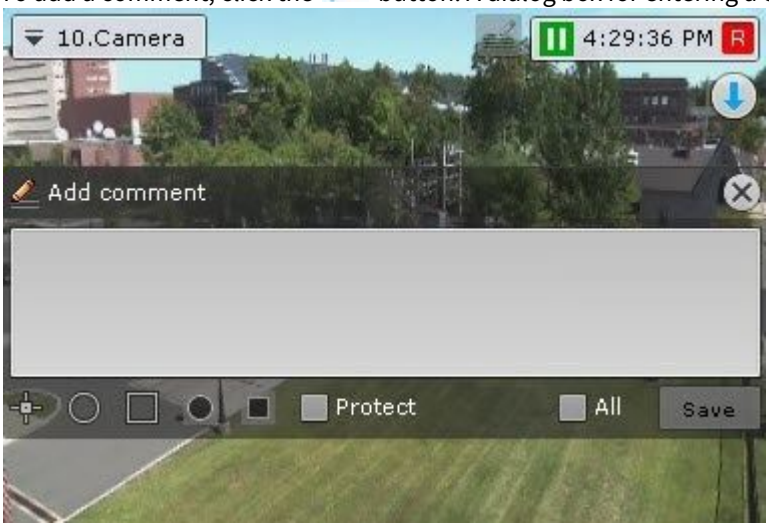


> **Note**
>
> If comments are added during playback in Archive or Archive Analysis mode, playback is paused after the button is clicked.

In Alarm Management mode, operators can be required to give comments after classifying an event (see Configuring Alarm processing(see page 540)) 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.

16.2.2.6.2 Adding a comment

To add a comment, click the button. A dialog box for entering a comment will open.

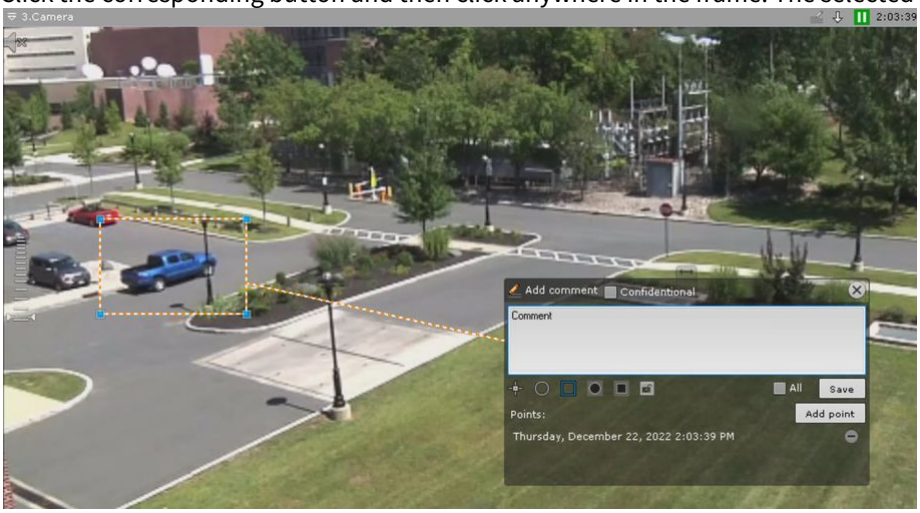


The number of characters in the comment is limited.

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:

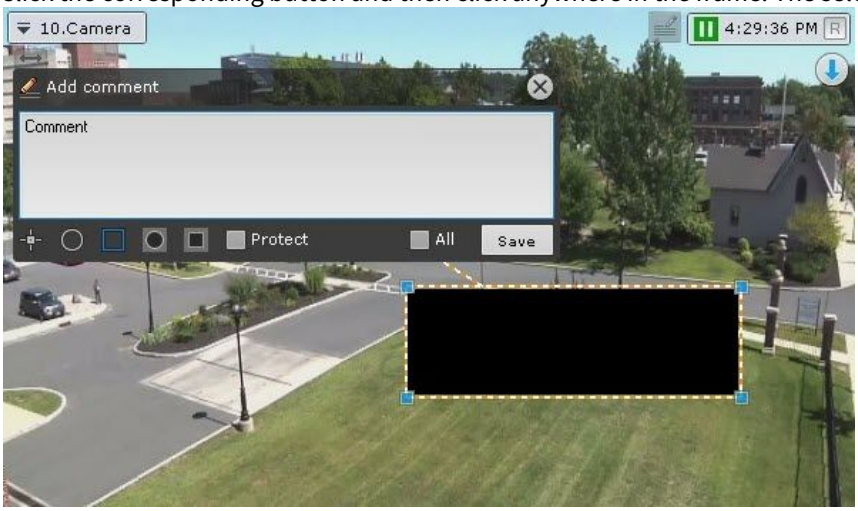
a. Click the corresponding button and then click anywhere in the frame. The selected element will be displayed.



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.

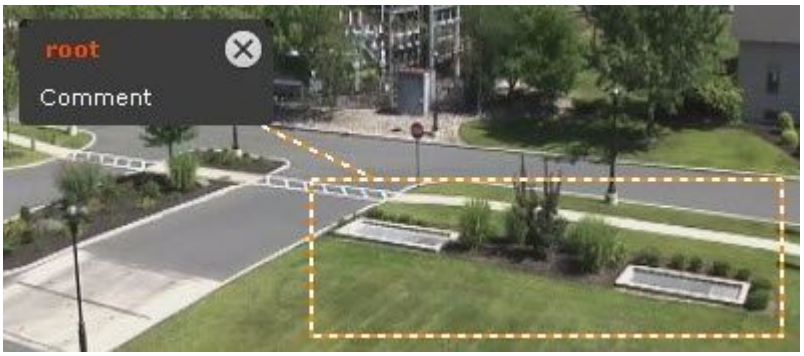
> **Note**
>
> The privacy zone cannot be set in real time.

> **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(see page 230)).
6. Adding a comment to all cameras on the layout—set the **All** checkbox.

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.



16.2.2.7 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(see page 488)).

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.

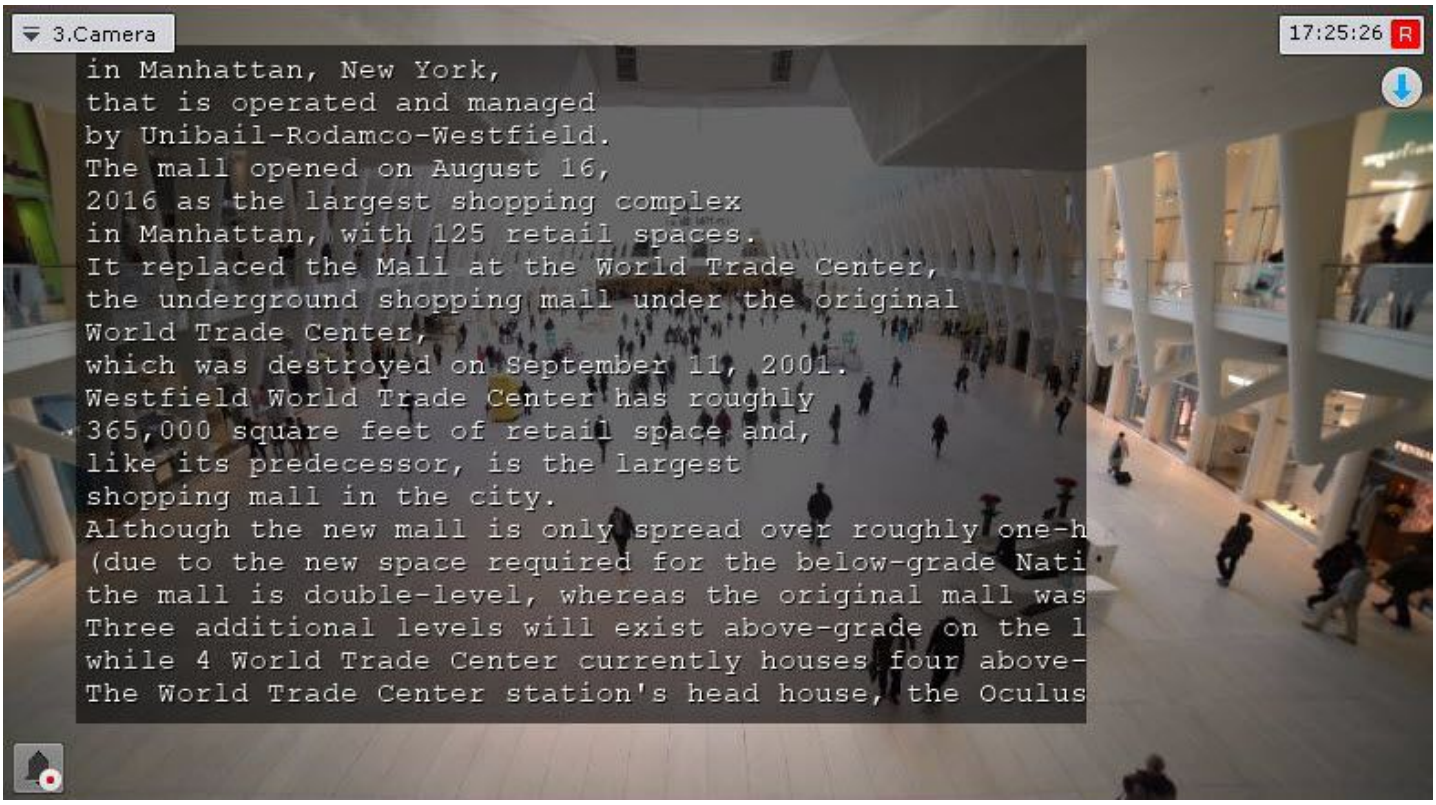
16.2.2.8 Viewing titles from POS terminals

If you have configured the titles overlay, the video tiles show titles superimposed on video (see Configuring titles view(see page 194)).

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

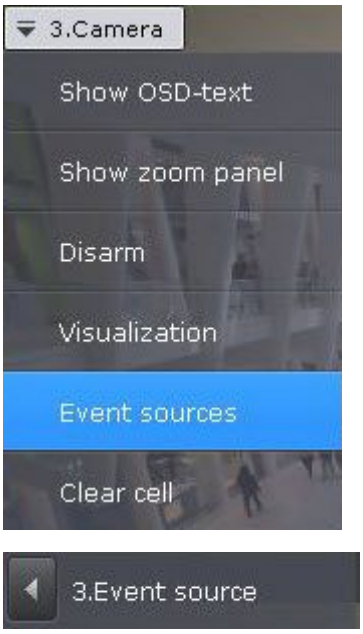
Keywords or lines can be highlighted according to the settings (see Configuring keywords(see page 196)).

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(see page 194)) 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.



16.2.2.9 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.

16.2.2.10 Displaying information from a detection tool (mask)

Some detection tools can superimpose different information on the video image:

1. Motion detection (VMD)(see page 249)—motion mask.
2. Equipment detection tool (PPE))(see page 358) and Person-based Privacy Masking(see page 366)—segments of the human body.
3. Fire and Smoke Detection Tools(see page 349) and Object presence detection tool(see page 352)—the sensitivity scale of the detection tool.
4. Neural Counter(see page 344)—highlighting of the recognized objects.
5. Water Level Detection(see page 390)—the water level indicator.
6. Queue Detection(see page 386)—highlighting of the queue.
7. People masking detection tool(see page 382)—masking people.
8. Privacy masking detection tool(see page 368)—hides moving objects.

To enable displaying information from a detection tool, select the **Show mask** item in the context menu of the surveillance window.

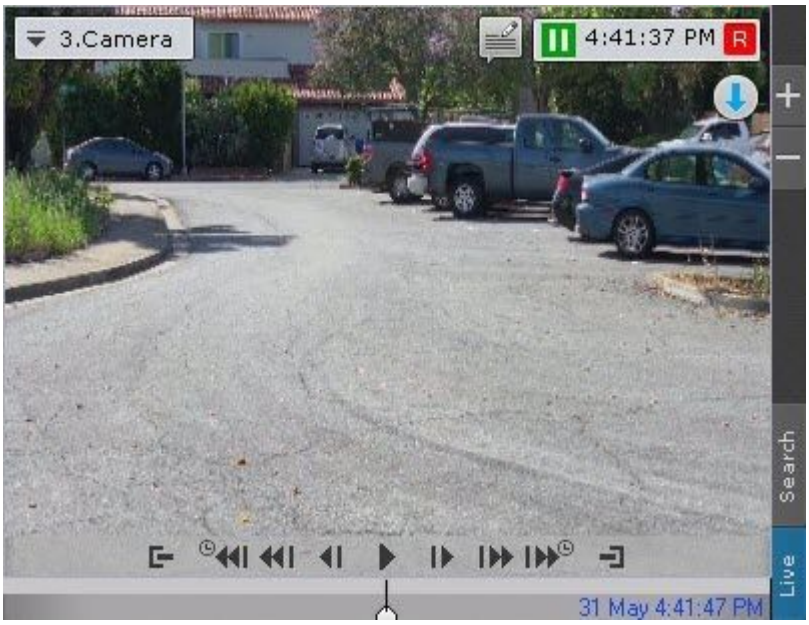
> **Note**
>
> This item is available only if you have created one of the above mentioned detection tools for this camera.

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.

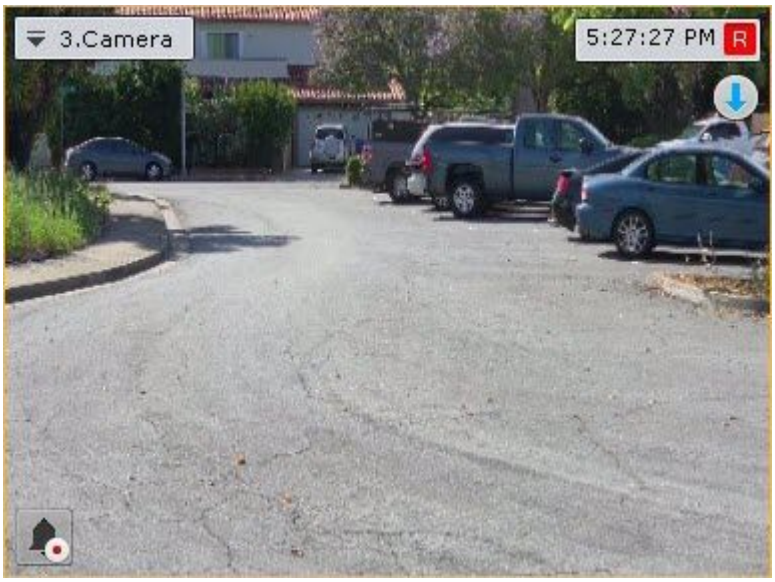
16.2.3 Real-time video surveillance

16.2.3.1 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.



16.2.3.2 Video Surveillance Functions Available in Live Video Mode

In Live Video mode, the following video surveillance functions are accessible:

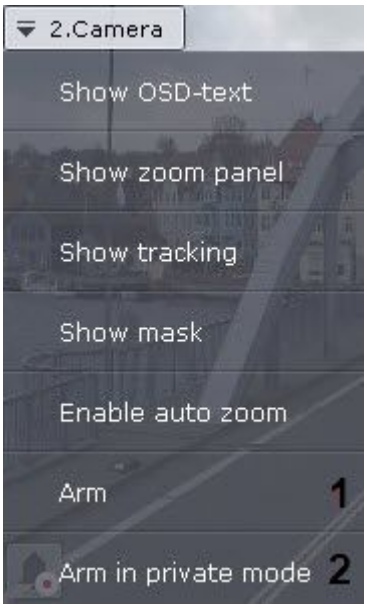
1. Selecting video stream quality in a viewing tile.
2. Autozoom.
3. Functions for tracking of moving objects.
4. Arming/disarming a video camera.
5. Controlling a PTZ Camera.
6. Controlling outputs.
7. Displaying the input status.
8. Autoreplace offline cameras on layouts.
9. Snapshot.
10. Functions Available in All Video Surveillance Modes(see page 654).

16.2.3.3 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.

16.2.3.4 Controlling a PTZ Camera

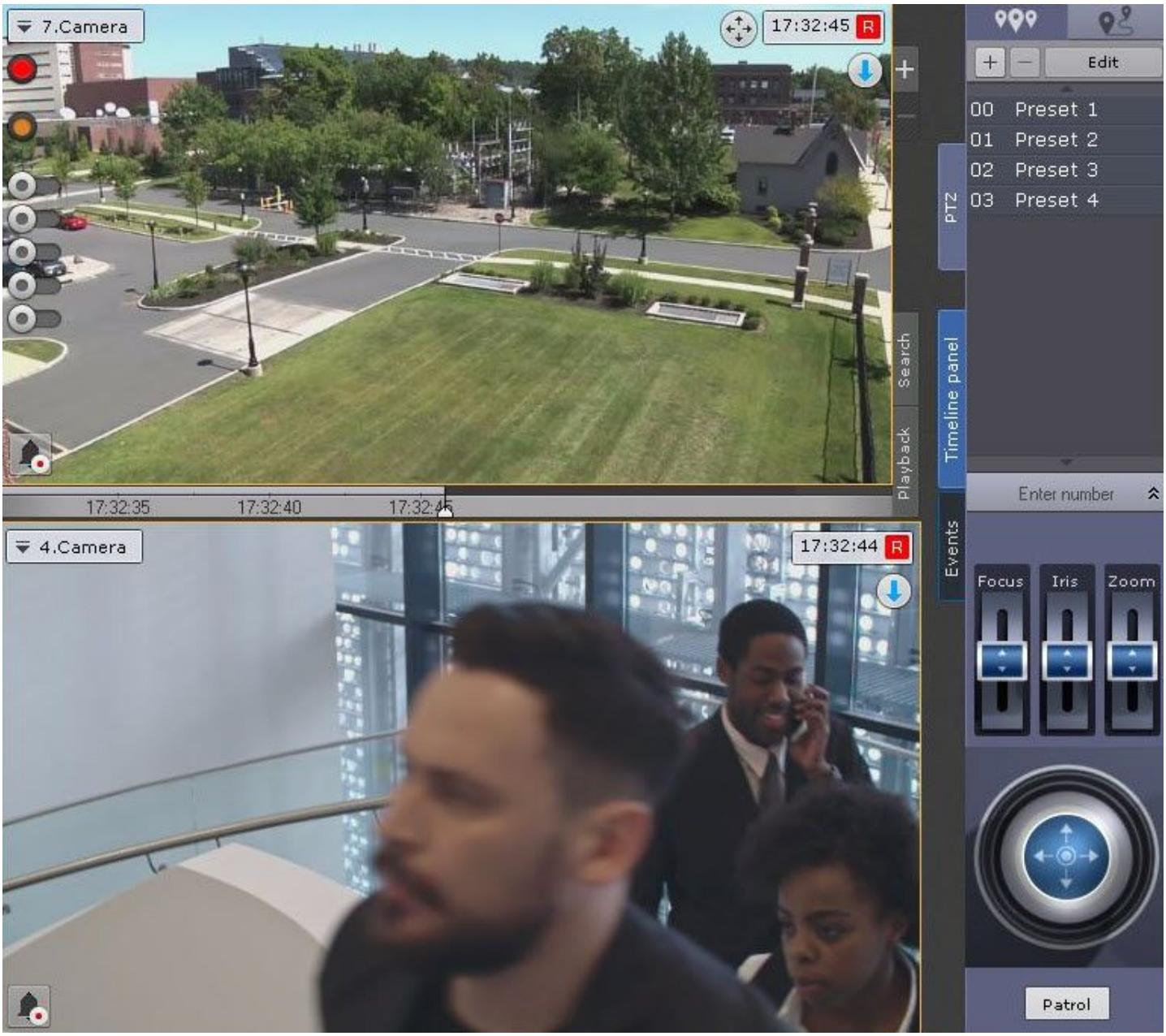
PTZ video camera can be controlled with the PTZ Control Panel or directly in the Viewing Tile (see Controlling a PTZ Video Camera in the OnScreen PTZ Mode(see page 683), Control using Areazoom(see page 684), Control using Point&Click(see page 684)).

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(see page 452)). 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(see page 540)), 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(see page 650).
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(see page 164)).

16.2.3.4.1 Presets

16.2.3.4.1.1 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 Edit. 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(see page 679).

16.2.3.4.1.2 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.

16.2.3.4.2 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)(see page 134)).

The presets list created for a selected video camera is displayed in the upper part of the PTZ control panel in the tab.

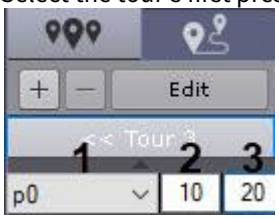
16.2.3.4.2.1 Creating and editing PTZ tours

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 .

16.2.3.4.2.2 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.

16.2.3.4.3 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(see page 164)).

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(see page 129)).

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.

16.2.3.4.4 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(see page 422), Wait for timeout(see page 414), Cyclical macros(see page 448)).

Patrolling must be activated in camera settings (see The PTZ Object(see page 164)). 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(see page 452)) 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(see page 540)).

16.2.3.4.5 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(see page 683)), otherwise the zooming will be digital (see Digitally Zooming Video Images(see page 655)).

16.2.3.4.6 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(see page 684)).

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.

16.2.3.4.7 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(see page 683)).

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.

16.2.3.4.8 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(see page 683)).

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.

16.2.3.5 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.

16.2.3.5.1 Tag&Track Pro

Tag&Track functionality depends on the PTZ mode that is specified in the settings.

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[184].
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.

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(see page 663) section).

- 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(see page 650) 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(see page 683)).

16.2.3.5.2 Tag & Track Lite

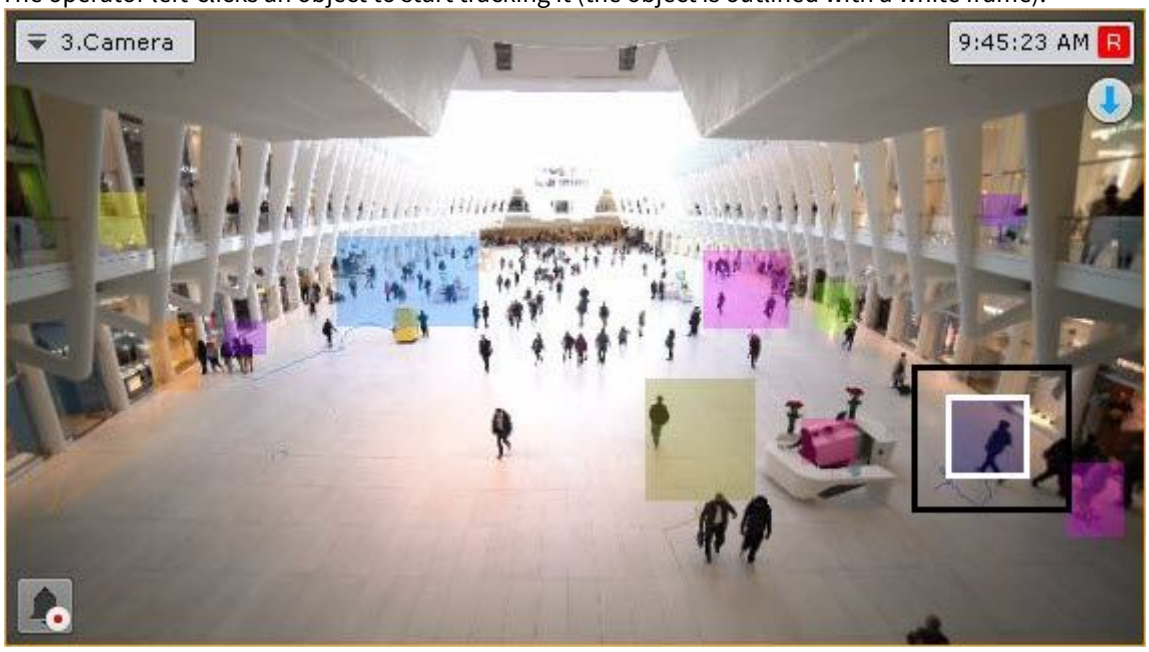
Attention!

For Tag & Track Lite to work, you must activate object tracking in the viewing tile (see the Tracking objects(see page 663) section).

Tag & Track Lite works as follows:

184 https://docs.axxonsoft.com/confluence/display/DDP

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.

16.2.3.5.3 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.

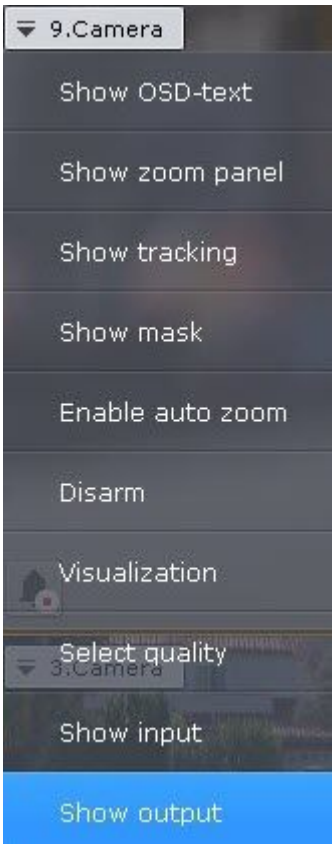
In this case, both features are active: the object will be tracked by the PTZ camera and its trajectory will be used to predict the camera in front of which it will appear next.

16.2.3.6 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

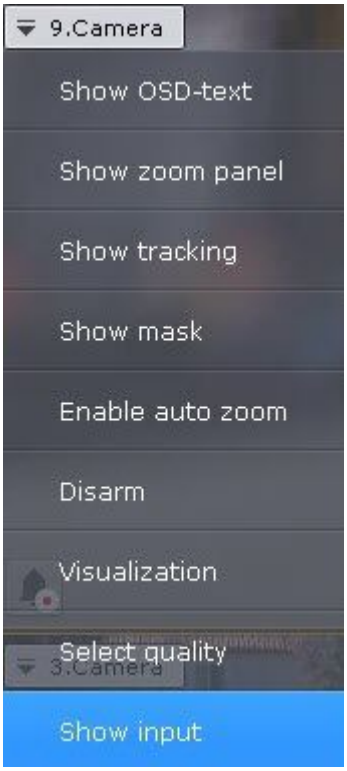
If a output is controlled by several operators simultaneously, the output will remain activated as long as at least one operator requires it.

Output Switch	Output status
	Normal
	Activated

16.2.3.7 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

Input status	Description
	Video camera is disarmed, input is in alarm status

16.2.3.8 Selecting video stream quality in a Surveillance window (GreenStream)

The Camera object(see page 122)

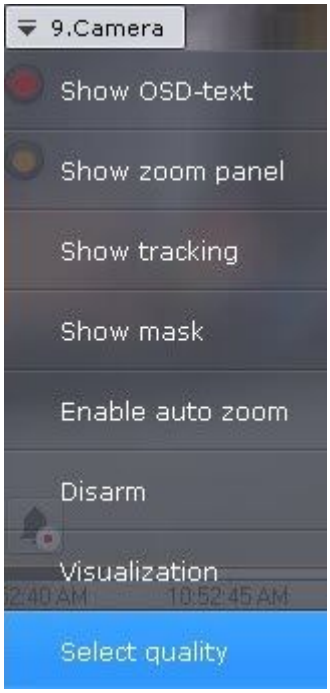
If the video camera supports multistreaming, you can select the quality of the video stream that you want to display in viewing tiles.

Note

If the video camera is not configured for multiple video streams, this action is not available.

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.

Item	Description
Auto (GreenStream, default)	The camera has two video streams: high quality video stream and low quality video stream. If the size of the cell where the video image from the camera is displayed is close to the low quality resolution with a 10% height or width margin, the video image will be displayed using the low quality stream. In other cases, the high quality video stream will be displayed.

Item	Description
High quality	A high quality video stream is used in the video surveillance window.
Low quality	A low-quality video stream is used in the video surveillance window. When you enlarge the surveillance window, the video stream switches to a high quality video stream.

> **Note**
>
> The automatic video stream selection (the **Auto** item) is unavailable, if automatic resolution selection is set for any stream.

3. Click in the area between the tiles.

Selection of the video stream quality in the viewing tile is complete.

The HQ symbol in the video surveillance window indicates high quality stream.

16.2.3.9 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.

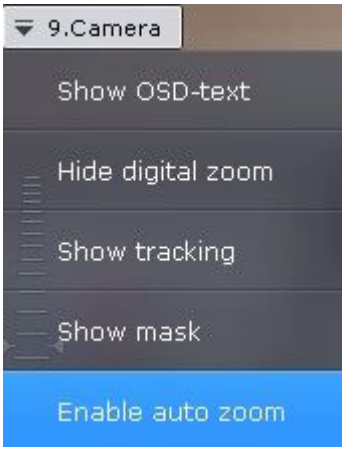
Autozoom can be enabled both for a single camera and for all video cameras in a layout.

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 Scene Analytics detection tools(see page 254)).
2. the Video Motion Detection tool is activated (see Configuring VMD(see page 250)).
3. at least one of the Embedded Analytic tools is activated (see Embedded Detection Tools(see page 393)).

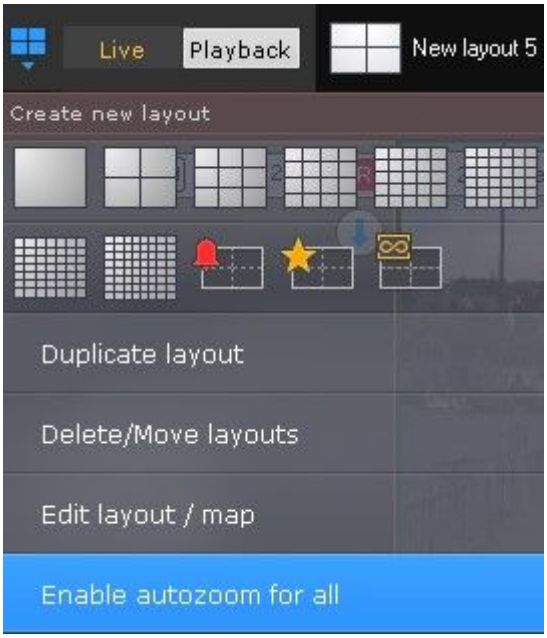


Note

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.

16.2.3.10 Autoreplace Offline Cameras on Layouts

If the main camera goes offline and a sub camera is defined in the settings (see The Camera object(see page 122)), 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.

16.2.3.11 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.

16.2.3.12 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(see page 772)) opens containing detection tool triggering events for this

camera only.

To hide the panel, click again the **Events** button.

16.2.3.13 Removing a camera from a layout

You can remove a camera from any given layout.

> **Attention!**
>
> These changes are not saved, and the camera will reappear when you call the layout again, or relaunch the Client.

To do it, follow the steps below:

1. Open the Camera Window context menu.

2. Select **Clear cell**.

The corresponding layout cell becomes empty.

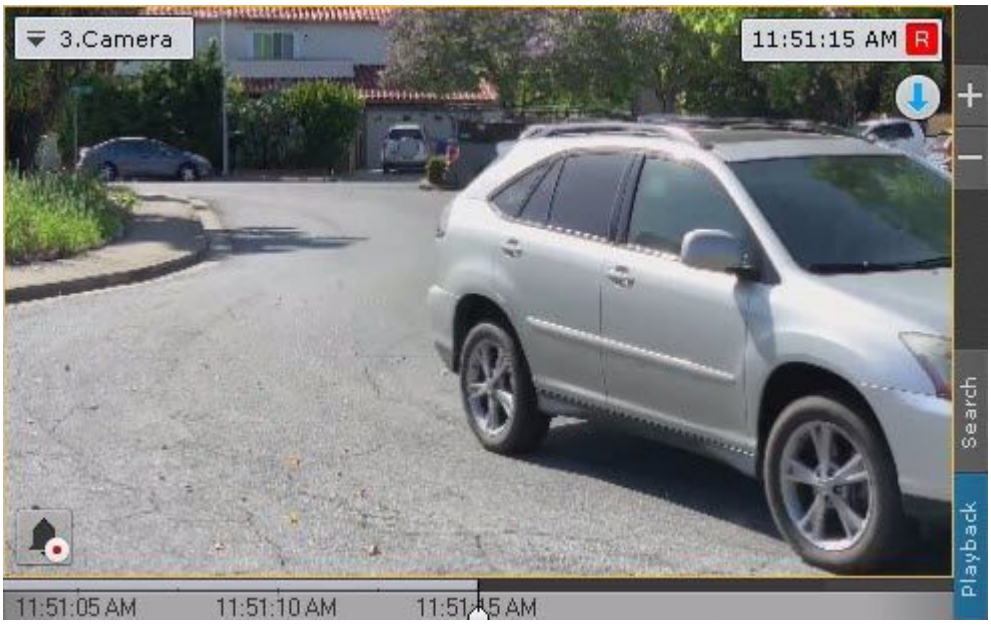
You can further drag and drop a camera from the Objects panel (see Objects Panel(see page 648)) or Camera search panel (see Camera Search Panel(see page 646)).

16.2.4 Video surveillance in archive mode

16.2.4.1 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.

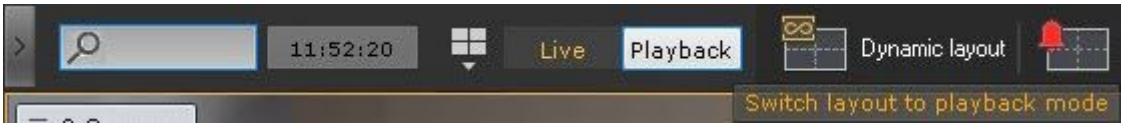
> **Note**
>
> If a camera is not linked to a video archive and has no on-board storage, this tab will be not available.



You can also switch from Live Video mode to Archive mode if you select a position on the advanced archive navigation panel (see Advanced Archive Navigation Panel(see page 633)).

> **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 activate, click the viewing tile.

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(see page 636)).

> **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(see page 484)).

On first access to Archive mode, the most recently recorded video will be selected on the timeline (see The Timeline(see page 639)). 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.

16.2.4.2 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(see page 673) 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(see page 713).
12. Functions Available in All Video Surveillance Modes(see page 654).

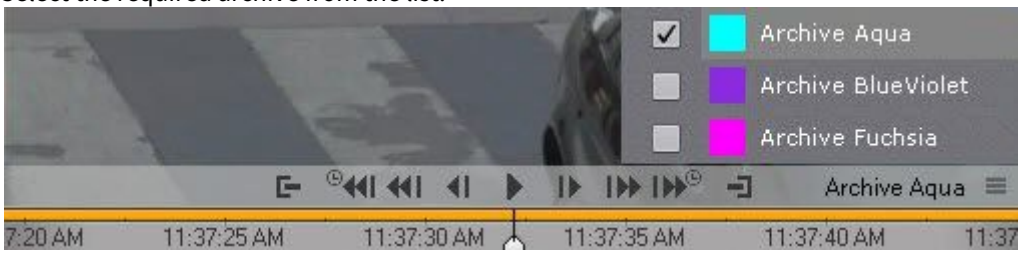
16.2.4.3 Selecting an Archive

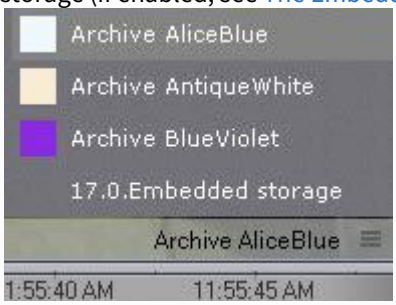
You can select video footage to view only if the camera is recording to several archives.

If you do not select an archive, the default archive is played back (see Configuring recording to an archive(see page 224)).

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(see page 226)) and on-board storage (if enabled, see The Embedded storage object(see page 174)).
>
> 
>

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.

16.2.4.4 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(see page 697)).
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:

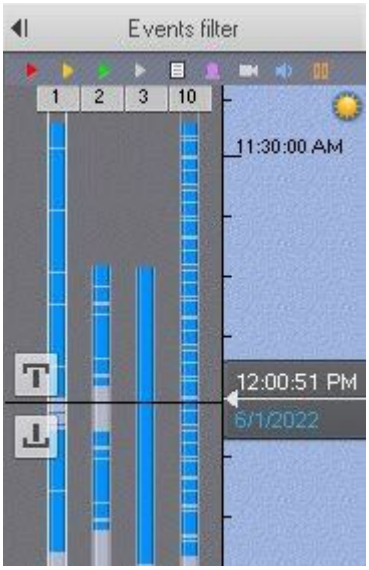
- a lower quality video stream is permanently recorded into Archive #1,
- and a high quality video stream is recorded into Archive #2 by VMD,

then the combined Archive will consist of high quality motion-triggered records and low quality "other" videos.

16.2.4.5 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.

16.2.4.6 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(see page 224)).
2. The camera must have at least one active source of metadata (Object Tracker, Video Motion Detection, Embedded Analytics).

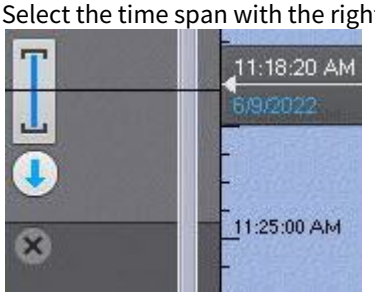
Attention!

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(see page 260)).

16.2.4.6.1 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(see page 705)).
   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(see page 751)).

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 .

16.2.4.6.2 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

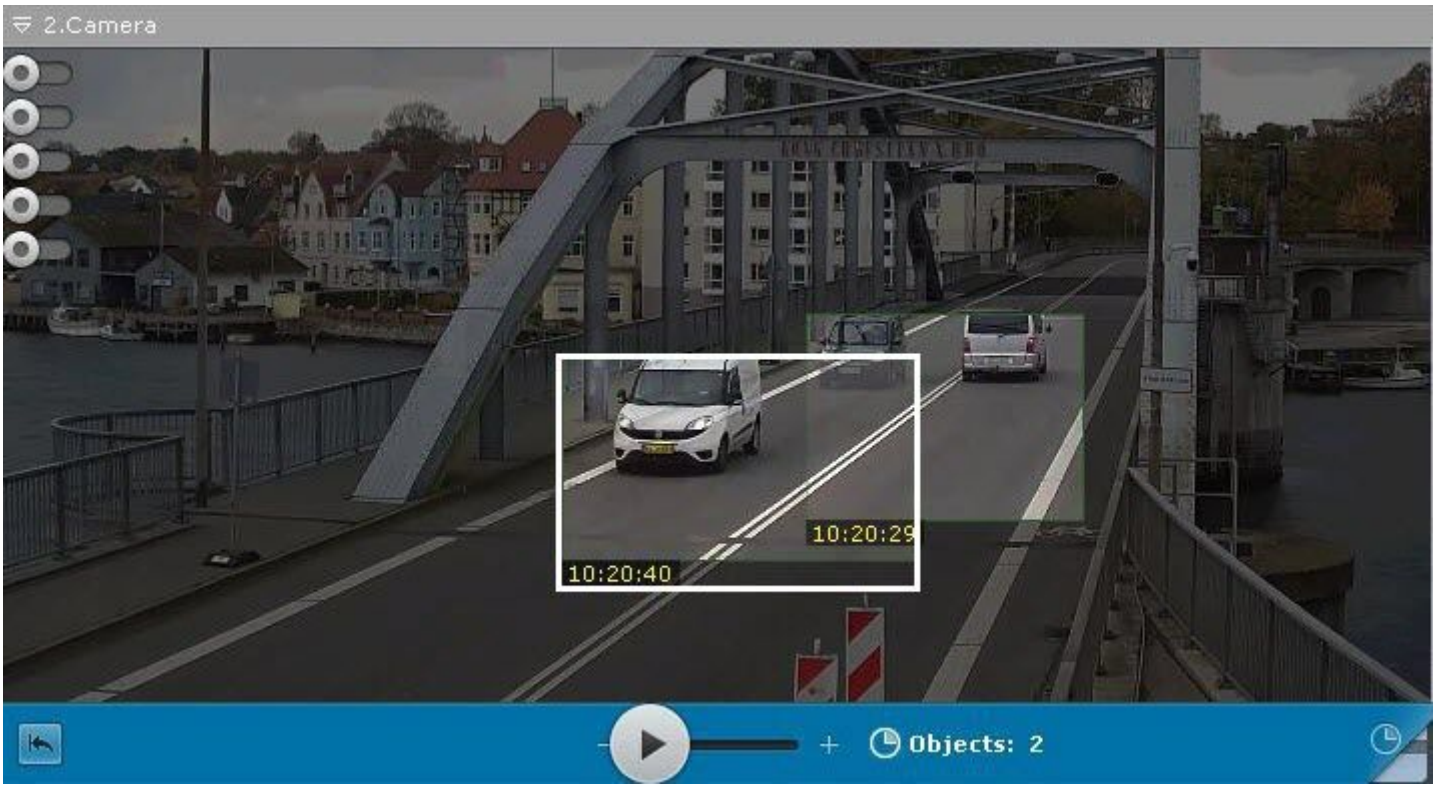
However, according to the logic of the algorithm, the number of displayed objects may be greater.

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**).

16.2.4.6.3 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.

16.2.4.7 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.

16.2.4.8 Viewing External Archives

External Archive is time-referenced video footage (see Importing video to Axxon One(see page 531)).

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.

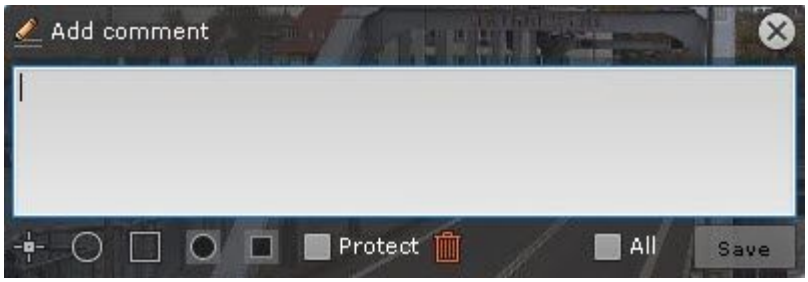
If video recordings overlap, they are displayed as one track that spans from the beginning of the first video clip to the end of the second.

If you want to watch this track, both video clips are played sequentially and in full.

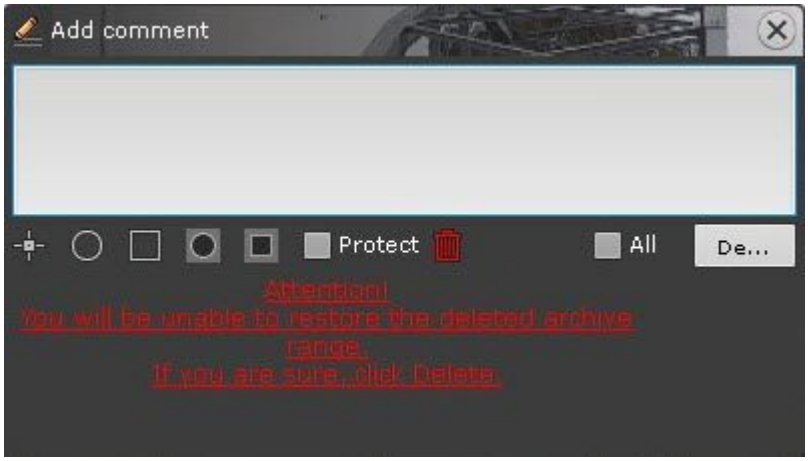
16.2.4.9 Delete a part of an archive

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(see page 698)), 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.

16.2.4.10 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.

16.2.4.10.1 Navigating Using the Timeline

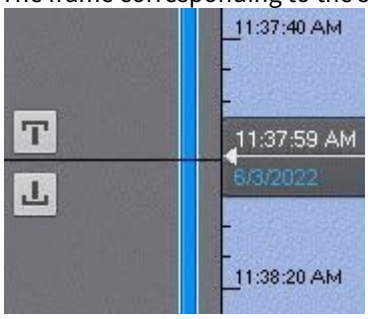
> **Note**
>
> Use of the timeline is described in detail in the section The Timeline(see page 639).

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.

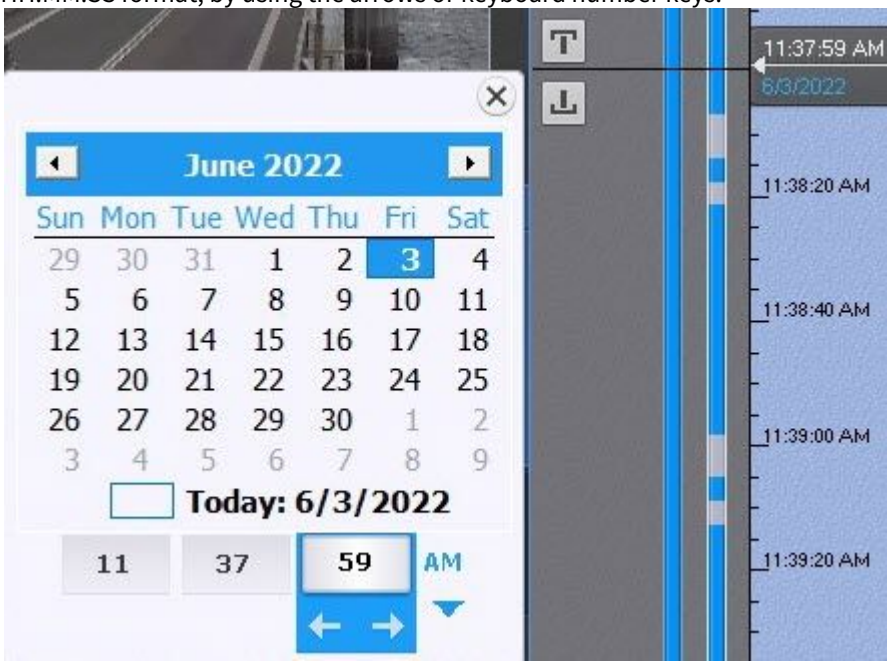
   > **Note**
   >
   > The position on the timeline is a graphical representation of a specific moment in time.

   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(see page 708)).

16.2.4.10.2 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(see page 708)) 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(see page 706).			

Attention!

Click and hold the button to jump to the end of the archive.

16.2.4.10.3 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(see page 641).

16.2.4.10.4 Navigating using the Playback Panel

To navigate in the archive using the playback panel, you must first select a recording for playback.

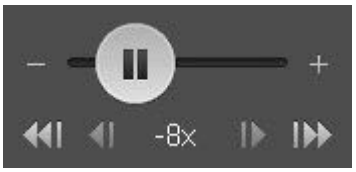
Once a recording is selected, the following operations are accessible:

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.

16.2.4.10.5 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.

16.2.4.10.6 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

16.2.4.11 Displaying the causes of triggered Scene Analytics detection tools

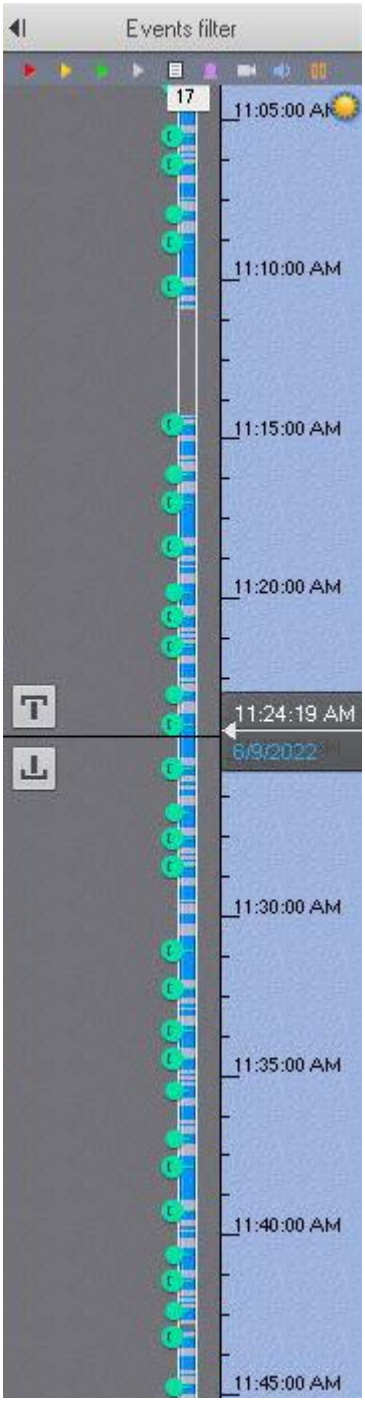
When positioning the archive in the range [-1 sec.; +1 sec.] from when the Scene Analytics detection tool was triggered, the objects that triggered the detection unit will be marked on the video frame.

16.2.4.12 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(see page 705)).

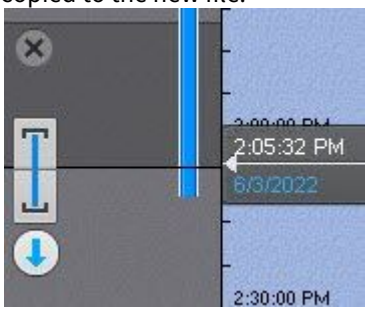
> **Note**
>
> To search in standard archive mode without displaying search results, click the corresponding tab in the viewing tile.

The parameters for the search are displayed when switching from search results to Archive Analysis mode.

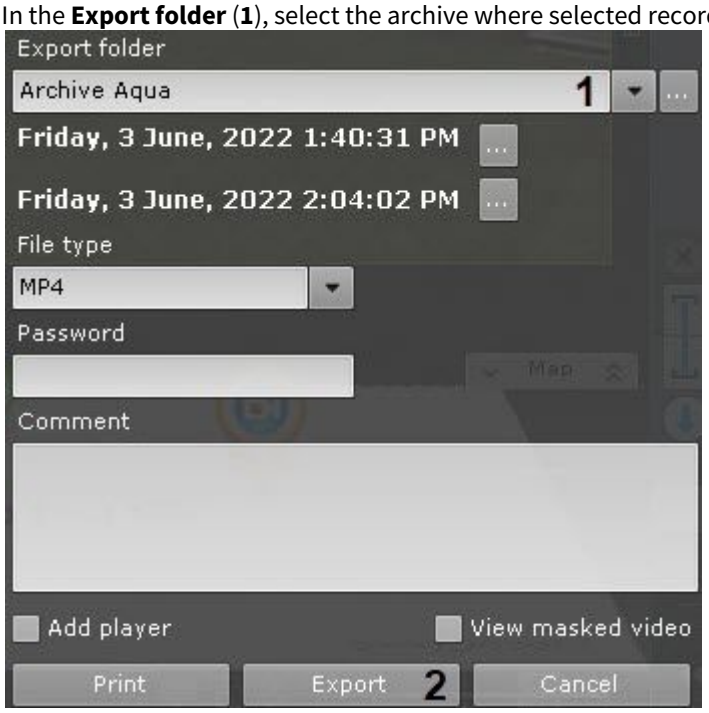
16.2.4.13 Manual Archive Replication

You can protect selected video recordings from being overwritten. To do this:

1. Create a new archive (see Creating archive[185]) and configure on-demand replication for it (see Configuring data replication(see page 226)).
2. Switch to Archive Mode (see Switching to Archive Mode(see page 695)).
3. Set the time interval on the timeline (see Standard video recordings export(see page 809)). 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.

16.2.4.14 Tag & Track Lite in Archive mode

Configuring Tag & Track Lite(see page 189)
Tag & Track Lite(see page 686)

185 https://docs.axxonsoft.com/confluence/display/one20en/Creating+archive

Attention!

For Tag & Track Lite to work, you must activate object tracking in the viewing tile (see the Tracking objects(see page 663) section).

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.

16.2.5 Video surveillance in alarm management mode

16.2.5.1 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(see page 654).

16.2.5.2 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.

16.2.5.3 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.

16.2.5.3.1 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(see page 646)). 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.

16.2.5.3.2 Automatic Initiation

Automatic rules or macros can be configured to initiate an alarm (see the section titled Initiating an alarm in the system(see page 420)).

If an alarm is initiated automatically, the **Alert panel** tab is color-coded

.

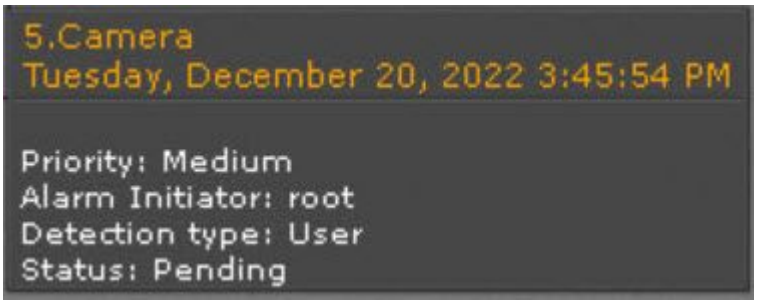
To evaluate the situation, click the Alert panel tab, select the event and classify it in Alarms Management (see the section titled Selecting an alarm event for Alarm Management(see page 717)).

16.2.5.4 Working with an assessment of an alarm event

16.2.5.4.1 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.

16.2.5.4.2 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.

16.2.5.4.3 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).

16.2.5.5 Working with the Alarm Management window

16.2.5.5.1 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.

16.2.5.5.2 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(see page 420)).

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(see page 706)) or the Playback panel (see Navigating using the Playback Panel(see page 708)).

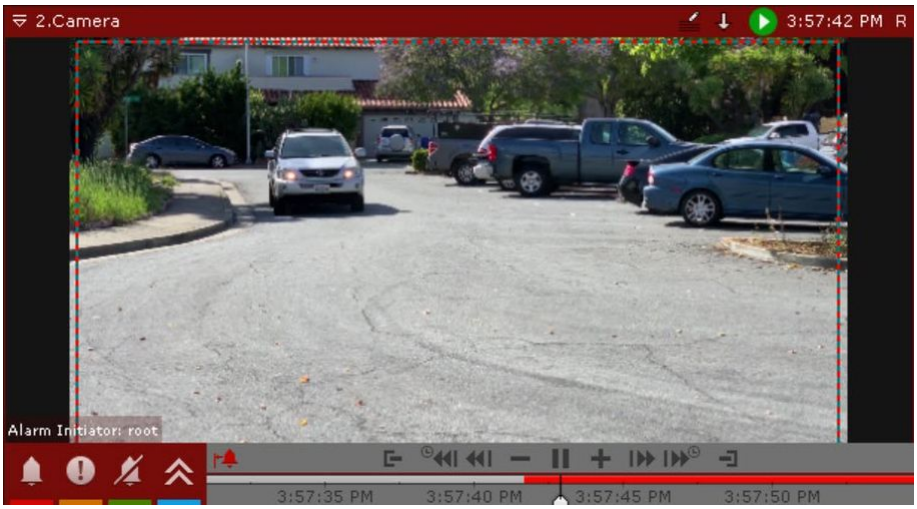
To go to the required fragment of an alarm event in order to play it again, hold the timeline pointer with the left mouse button and drag it to the required position.

To go to the beginning of the alarm event, click the button.

16.2.5.5.3 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

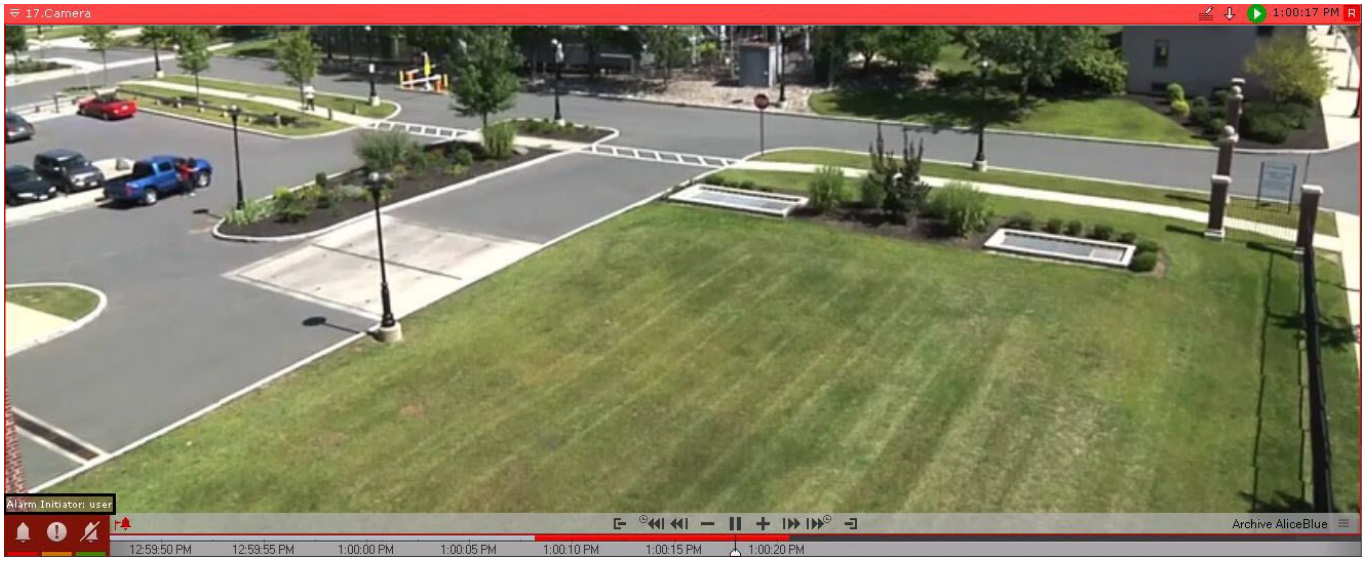
It is possible to specify the time within which the alarm event should be taken into processing, otherwise it will be assigned the **Skipped** status (see Configuring Alarm processing(see page 540)).

> **Note**
>
> The statuses of alarm events are displayed on the timeline using color indicators (see The Timeline(see page 639)).

16.2.5.6 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 mode with limited functions for the purpose of playing back the alarm. This can be done in one of two ways:

1. Click the button (see the section Video surveillance in alarm management mode(see page 714)).
2. Switch to the **Alarms** tab and select the alarm from the alarms list.



In Alarm Management mode with limited functions, the Alarm Management buttons are not displayed. Instead, the name of the operator who is currently processing the alarm is displayed. The other functions of the alarm handling tile remain unchanged.

After processing of the alarm on another client, on the given client the status assigned to the alarm is displayed in place of the name of the operator.

If a user has accepted an alarm for processing and leaves Alarm Management mode (going to Live Video mode, Archive or Archive Search mode, the viewing tile for another camera, etc.), after an amount of time equal to the operator's idle time after leaving, other users will also have the opportunity to accept the alarm for processing.

If more than one alarm appears for one camera, any operator may access all alarms not yet accepted for processing.

16.2.6 Video surveillance in archive search mode

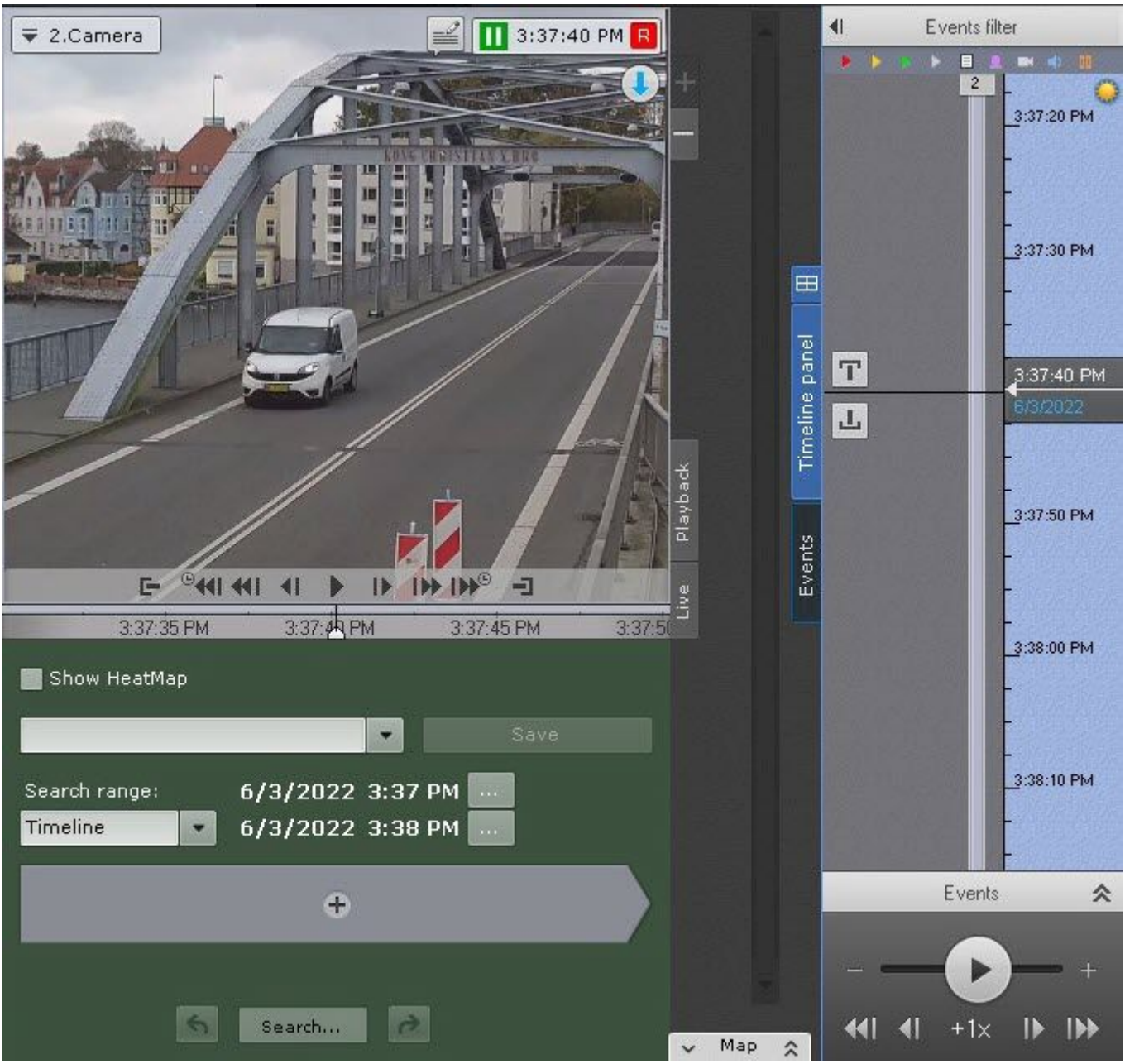
16.2.6.1 Switching to Archive Search mode

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.

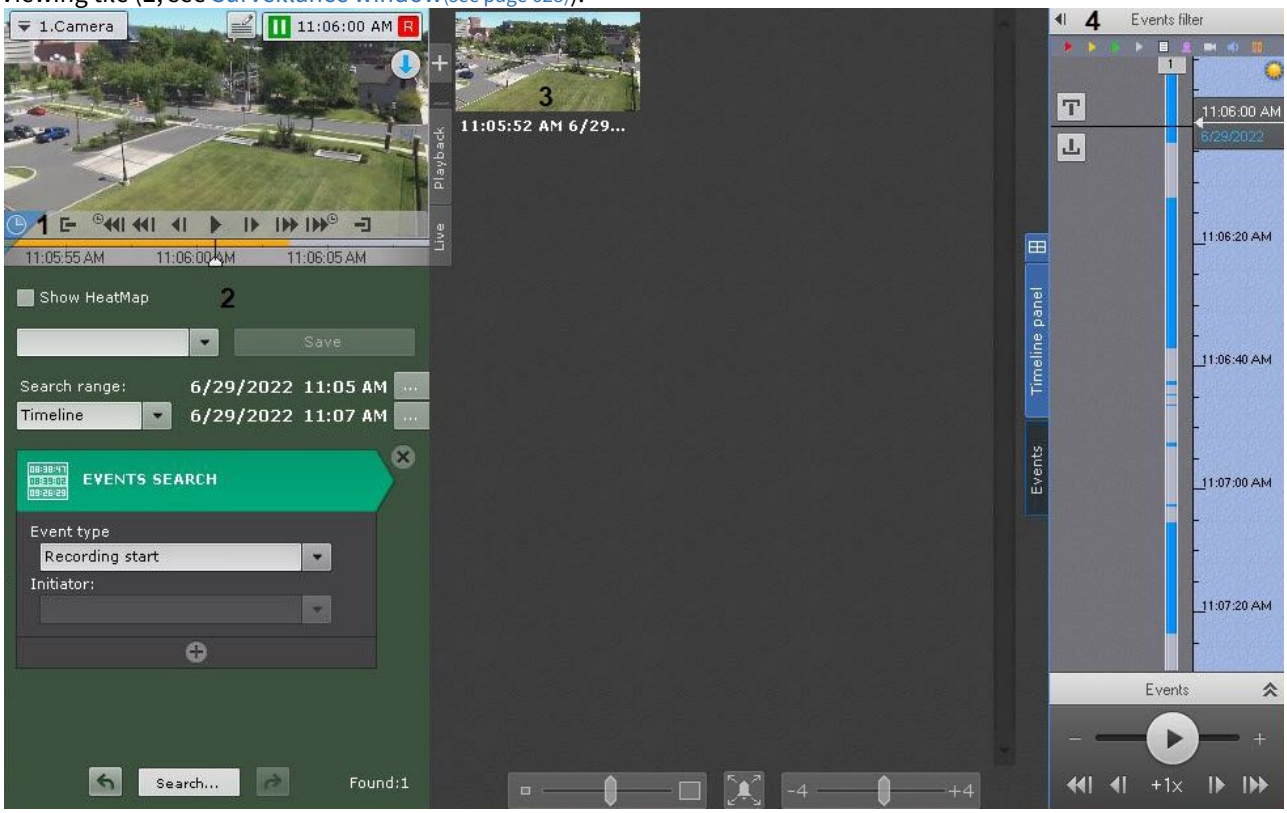
The archive analysis interface will then appear.



16.2.6.2 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(see page 628)).



2. Search control panel (**2**, see Search in an archive of a single video camera(see page 725)).
3. Search results panel (**3**, see Viewing search results(see page 750)).
4. Archive navigation panel (**4**, see The Archive Navigation Panel(see page 636)).

You can hide search parameters for a portrait-oriented camera. To do so, click the button.

To unhide, press the button.

16.2.6.3 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(see page 654).

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(see page 695). The Autozoom function is described in the Real-time video surveillance(see page 673) section.

16.2.6.4 Search in an archive of a single video camera

16.2.6.4.1 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

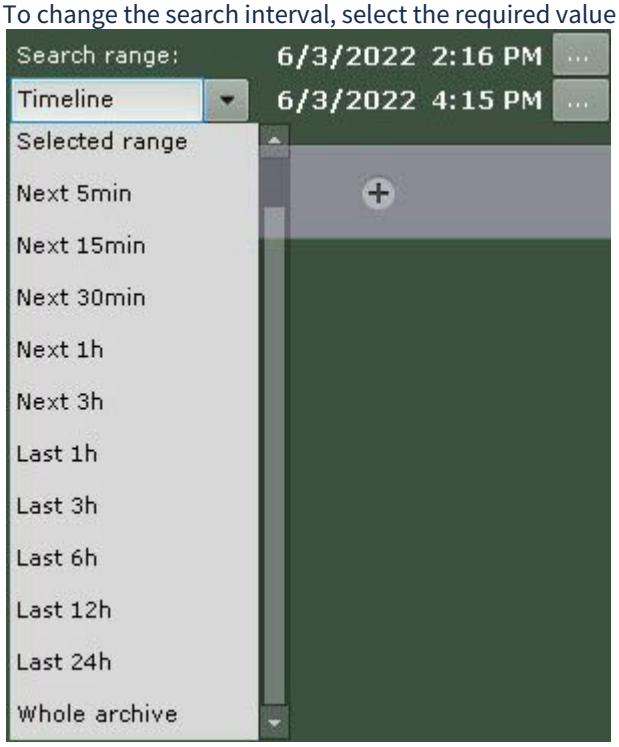
In the on-board storage of the camera, you can only find video episodes with thumbnail search (TimeSlice).

16.2.6.4.2 Setting a search interval

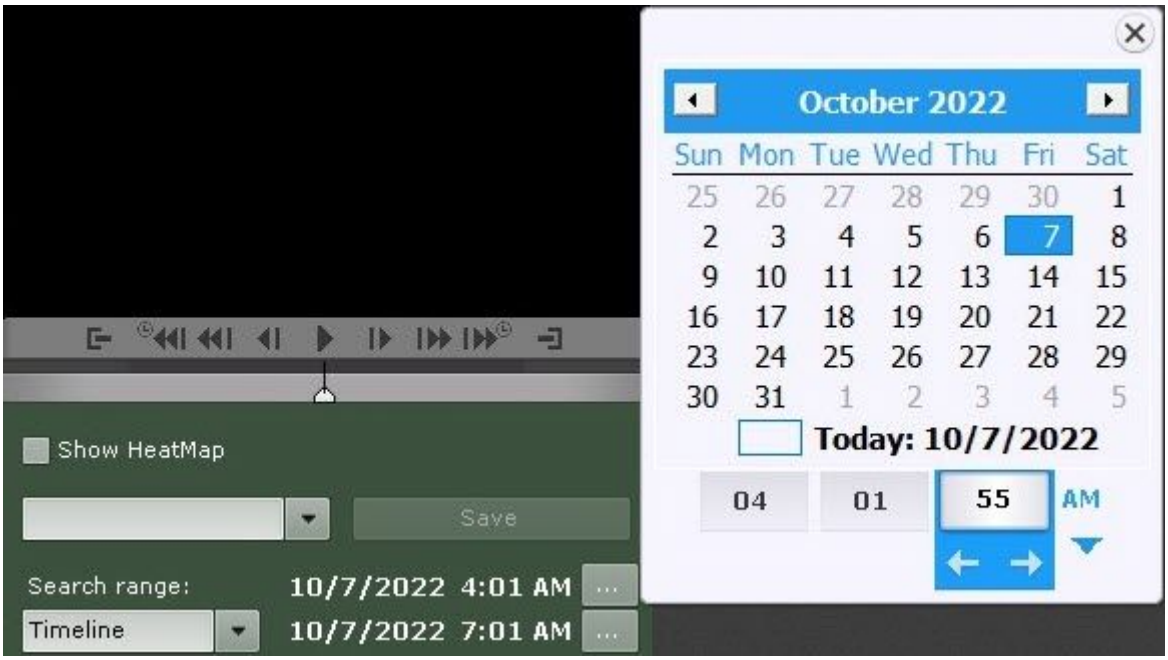
Setting a search interval is a common procedure for all types of the archive search.

By default, the search spans across the part of the archive that is displayed on the timeline (see Navigating Using the Timeline(see page 705)).

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.

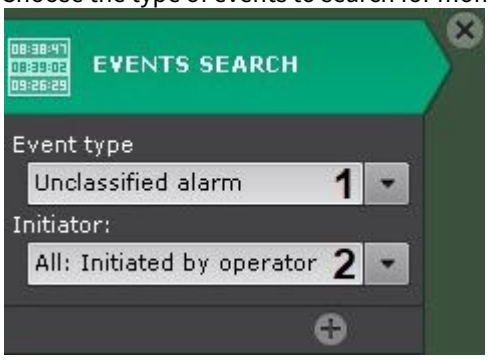


16.2.6.4.3 Events search

This type of search lets you select events in the archive based on the type of event.

To do this, complete the following steps:

1. Choose the type of events to search for moments (**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 units were triggered
Recording start	The search finds the beginning and end of recordings from the specified video camera regardless of the initiator

2. Select an event initiator from a list with the same name (**2**).

> **Note**

An event initiator could be an operator, a video camera input, or any detection unit that is activated in the system. The search results will show the moments in time containing the events that were triggered by the initiator.
To search for face recognition and ANPR events, select **Realtime recognition**.

3. If necessary, click + and add more similar search conditions.
4. Set the search interval (see Setting a search interval(see page 725)).
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 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 unit, select the **Expand alarm object** check box in the lower portion of the search results panel.

16.2.6.4.4 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(see page 725).
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(see page 752).

16.2.6.4.5 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(see page 725)).
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.

16.2.6.4.6 Forensic Search for Fragments (MomentQuest)

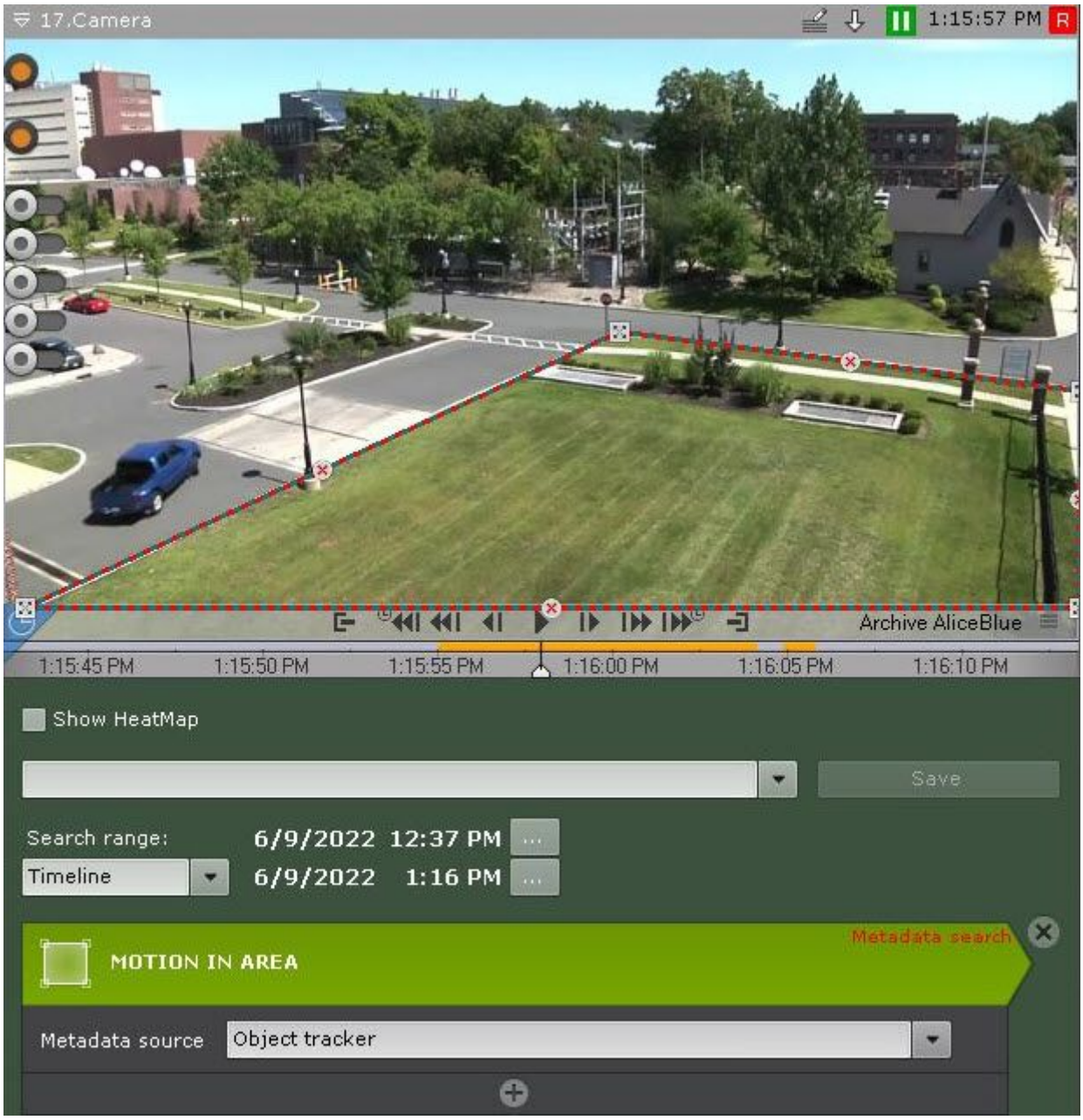
Forensic Search lets you search for moments in the archive using the following criteria:

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.

16.2.6.4.6.1 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(see page 735)).
4. Set the search interval (see Setting a search interval(see page 725)).
5. Click the **Search** button.

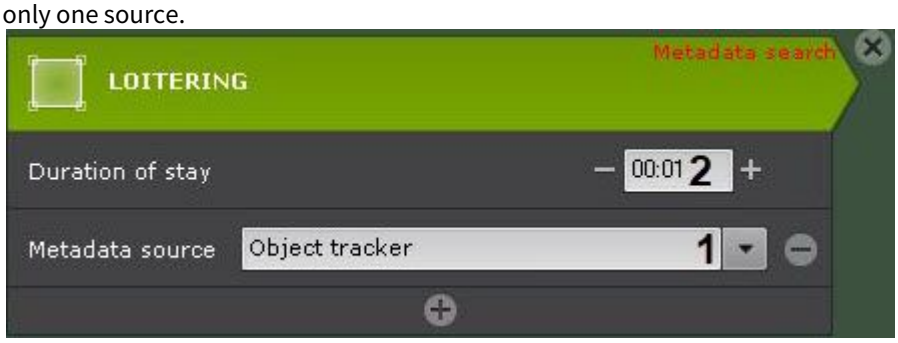
> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

The found moments will be displayed in the search results panel.

16.2.6.4.6.2 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(see page 730)).
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(see page 735)).
5. Set the search interval (see Setting a search interval(see page 725)).
6. Click the **Search** button.

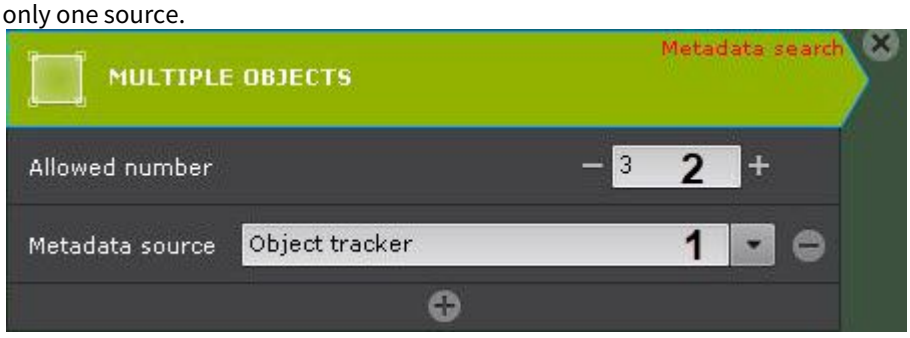
> **Note**
>
> Once launched, the search can be stopped at any time. To do this, click the **Stop** button which appears instead of the **Search** button.

The found moments will be displayed in the search results panel.

16.2.6.4.6.3 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(see page 730)).
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(see page 735)).
5. Set the search interval (see Setting a search interval(see page 725)).
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.

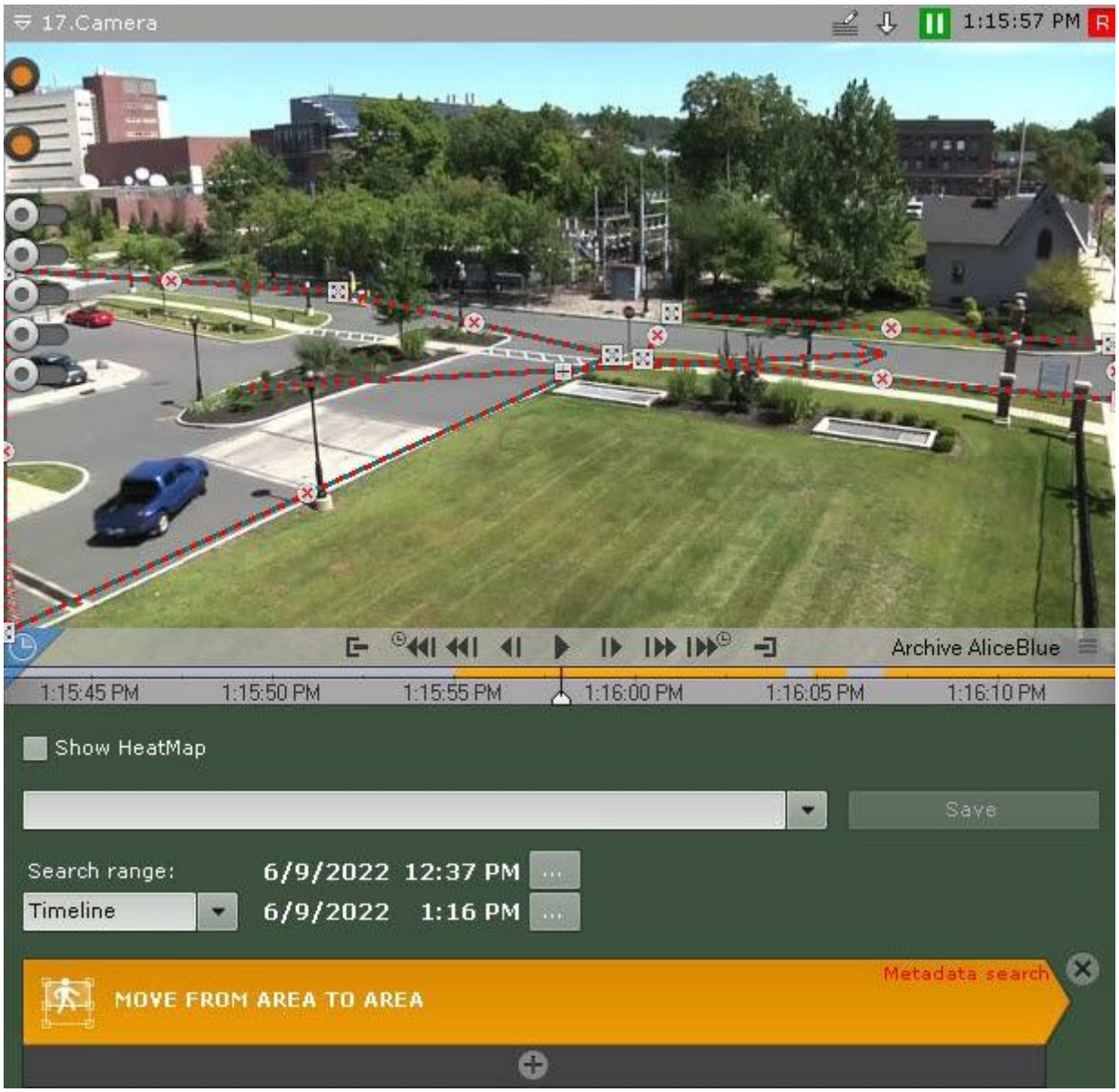
The found moments will be displayed in the search results panel.

16.2.6.4.6.4 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(see page 730) 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(see page 735)).
4. Set the search interval (see Setting a search interval(see page 725)).
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.

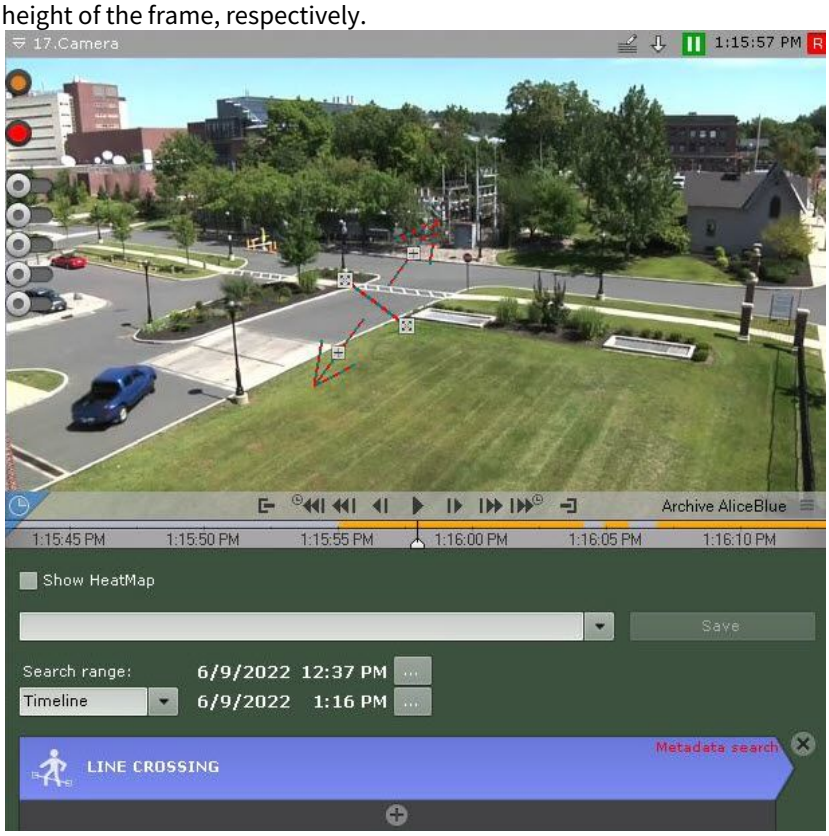
The found moments will be displayed in the search results panel.

16.2.6.4.6.5 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(see page 735)).
4. Set the search interval (see Setting a search interval(see page 725)).
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.

16.2.6.4.6.6 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

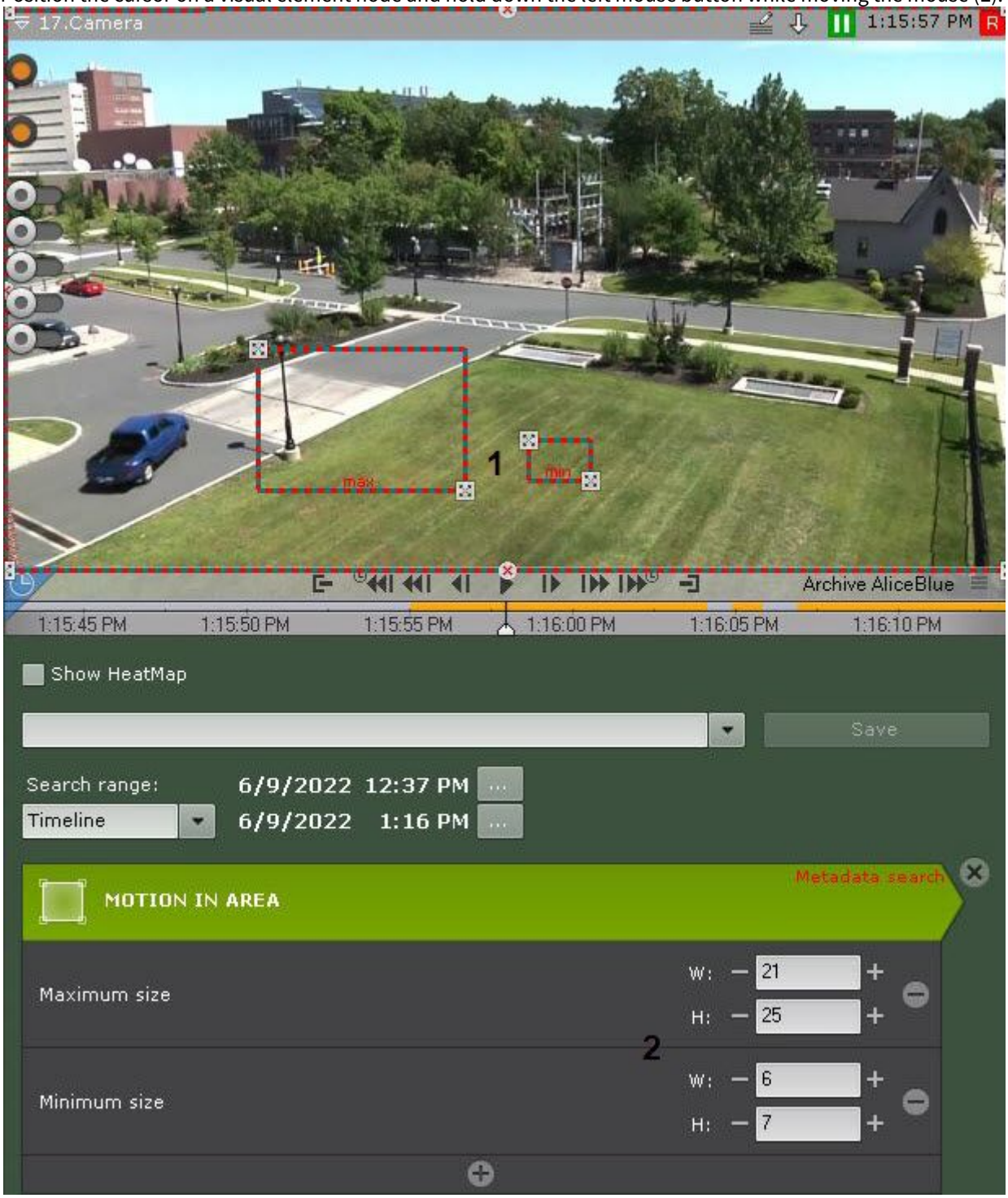
Configuring minimum and maximum object size

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.

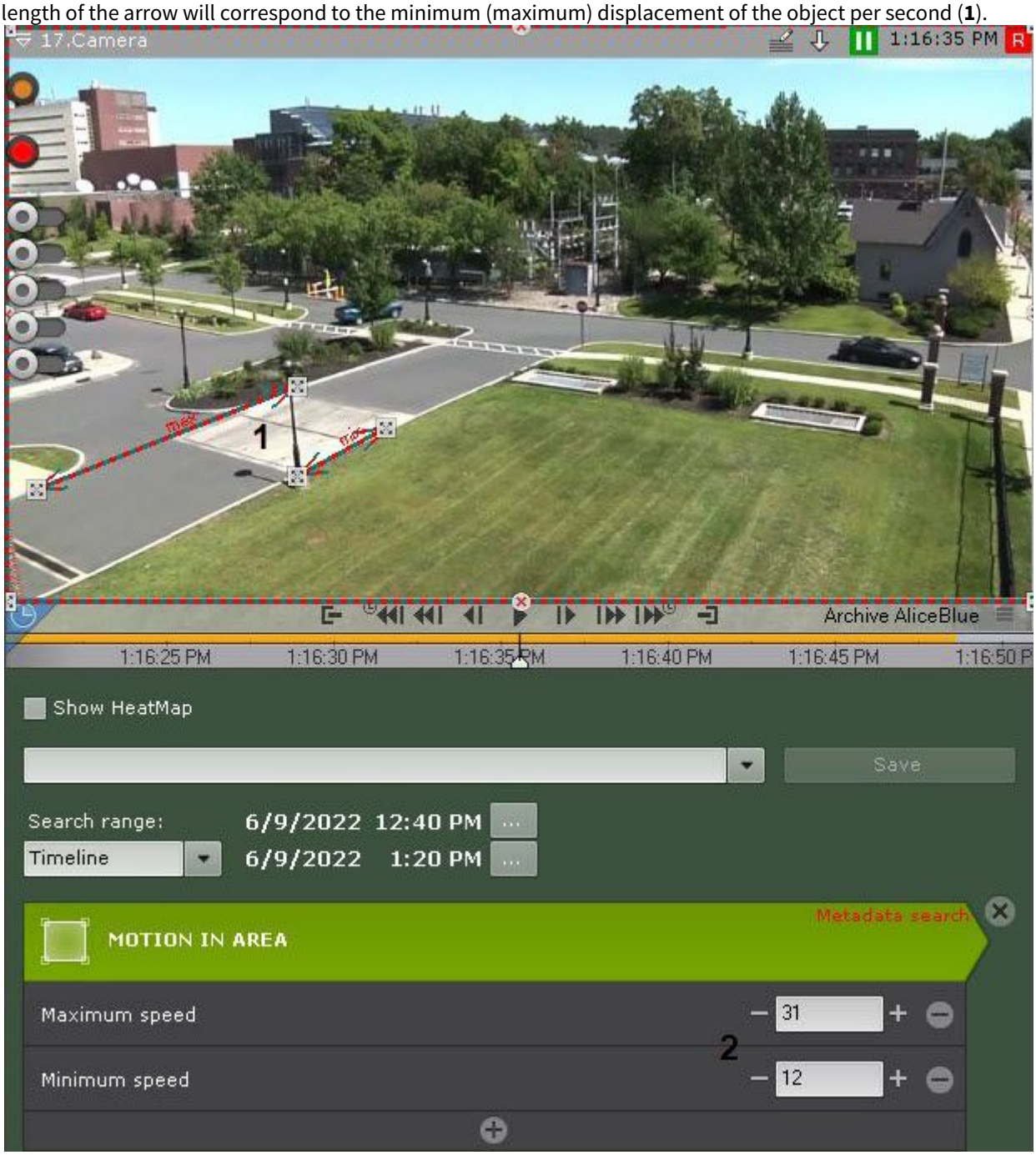
Configuring minimum and maximum object speed

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**).

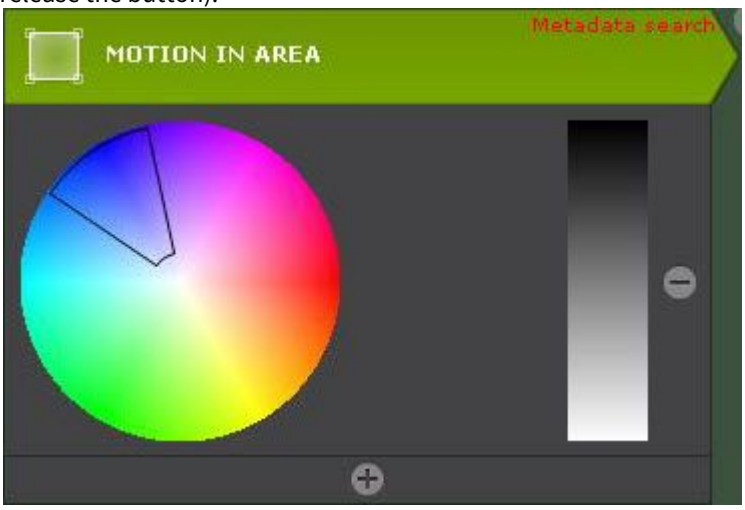
The minimum (maximum) speed of a moving object is now set.

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(see page 277)).

Configuring direction of object movement

By default, when searching the archive, the system searches for motion in all directions. It is possible to prevent searching for motion in one or several specific directions.

Click with either mouse button to designate a direction in which you do not want to perform movement search (privacy mask). The sector corresponding to the direction is then colored gray. If necessary, repeat this action for other directions. To reactivate searches for a masked (gray) direction, click it again with either mouse button.

The required directions of an object's movement are now set.

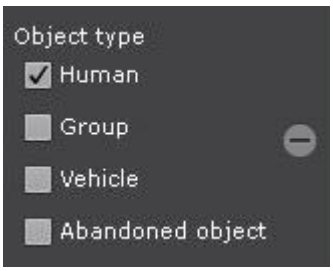
Configuring object entry/exit from area

"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(see page 277)).

16.2.6.4.7 Titles search

Titles search allows you to find the necessary words in the titles DB received from the POS devices.

To search the titles DB, do as follows:

1. Set a time interval for your search (see Setting a search interval(see page 725)).
2. Enter the text that you want to find in the titles. You can search the whole word or part of it.

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

There is no search by empty string.

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 titles containing the search text.

> **Attention!**
>
> When you search for events, the event time corresponds to the start time of the receipt, rather than the time of occurrence of the search text.

16.2.6.4.8 LPR search

With LPR search you can find video footage of the vehicles with recognized number plates, as well as filter them according to specified criteria.

To search recorded video for LPR results:

1. Set a time interval for your search (see Setting a search interval(see page 725)).
2. Select the detector from the list (**1**), by which you want to search.
3. Enter the number plate (**2**). Fuzzy search supported if you enter the number with the **?** mask for any one character, and the ***** mask for any number of characters) For example, a search query **?20*** will show all vehicles with license plate containing **2** and **0** in the second and third position respectively. The total number of characters in number plates will be variable.

> **Note**
>
> To search for all recognized number plates, enter ***** (asterisk).

4. If necessary, set additional search criteria by clicking the button:

> **Note**
>
> To remove a search criterion, click .

> **Note**
>
> To search by additional criteria, the **Vehicle recognition** option should be enabled in the **License plate recognition (RR)** settings (see Configuring License plate recognition (RR)[186]).

186 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=202673284

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, LADA, Hyundai.
c. **Model** (**5**): enter full name of the car model in Latin letters, case-insensitive. Correct spelling examples: Outlander, XRAY, Creta.

> **Note**
>
> A complete list of models and vendors is given here.

d. **Color** (**6**): set the color of the vehicle (see Configuring object color(see page 738)).
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) (see page 330)):
   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.

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 for video fragments based on the defined 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 number plate will be highlighted by a red frame in the Viewing Tile.

16.2.6.4.9 Face search

Face detection tool (see Face detection tools(see page 278)) 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 Requirements for face detection tools(see page 279)), 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.

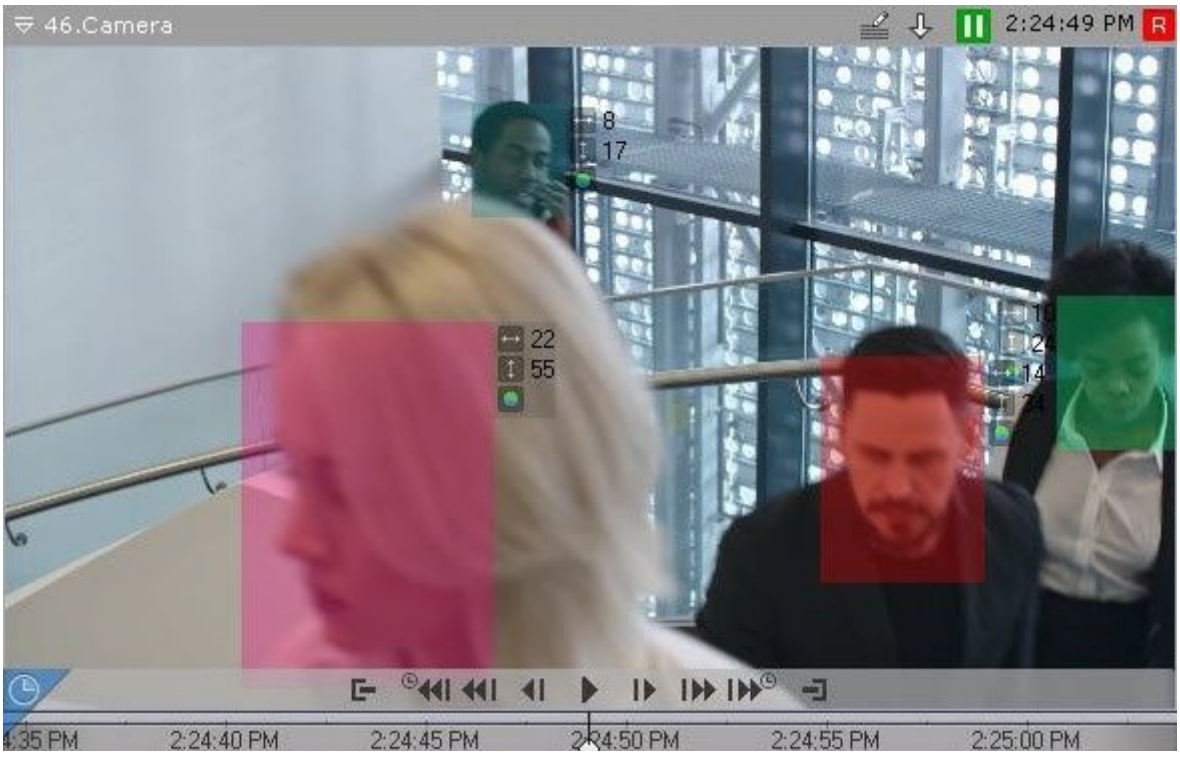
The information about the biometric vectors stored in the database on the selected cameras for the specified time interval (see Setting a search interval(see page 725)) is uploaded to the RAM on the Server side and compared with the biometric vector created on the basis of the image received from the 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(see page 744)).
2. Recognized faces (see Search for all recognized faces(see page 746)).
3. Face contacts (see Search for face contacts(see page 747)).

Face track and face size are always highlighted in the surveillance window during face search.



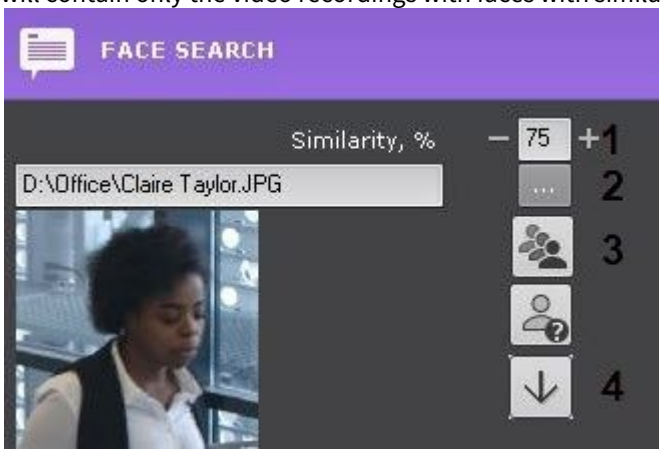
16.2.6.4.9.1 Search for similar face

Face search allows you to find faces similar to a given photo in the archive.

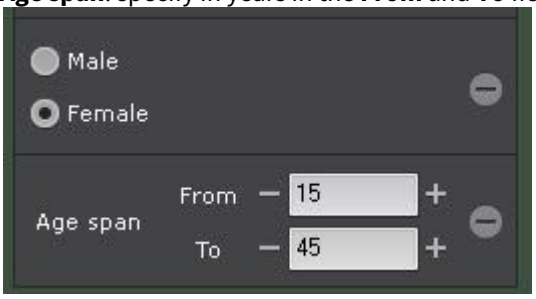
To perform face search:

1. Set the search interval (see Setting a search interval(see page 725)).

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[187]).
>
> 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.

187 https://docs.axxonsoft.com/confluence/display/next46en/Configuring+Face+detection

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(see page 572)).

16.2.6.4.9.2 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(see page 725)).
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 Face detection(see page 280)).
>
> 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(see page 572)).

16.2.6.4.9.3 Search for face contacts

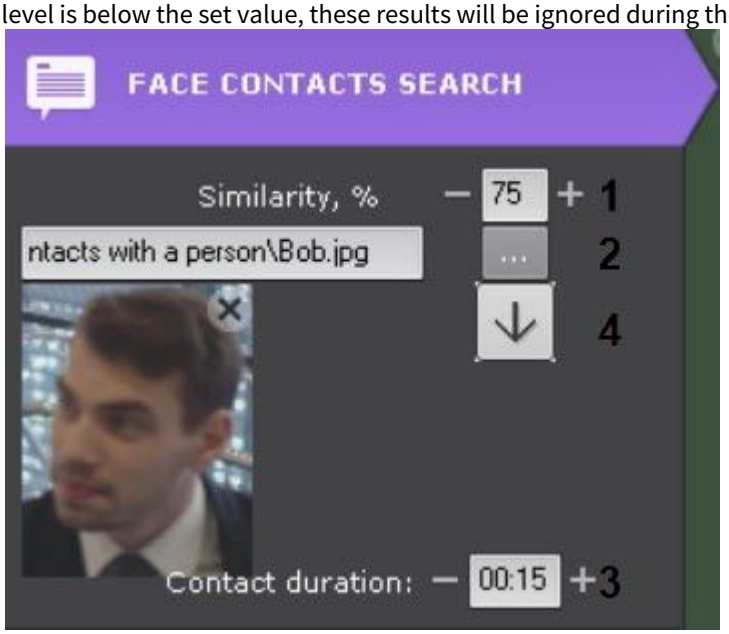
Face contacts search allows you to find in the archive all people who contacted with any person for a specified time.

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(see page 725)).
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.



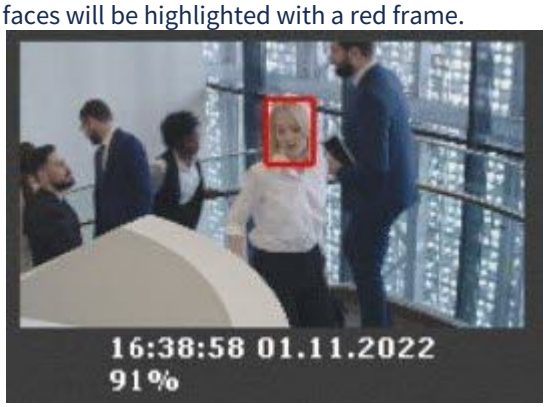
3. Select a photo of the person whose contacts you want to find (**2**). Supported formats: **png**, **jpg**, **jpeg**, **jpe**. When you click the face in the surveillance window, this face will be selected for search. If you do not select a photo, then all faces recognized during the specified time 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:

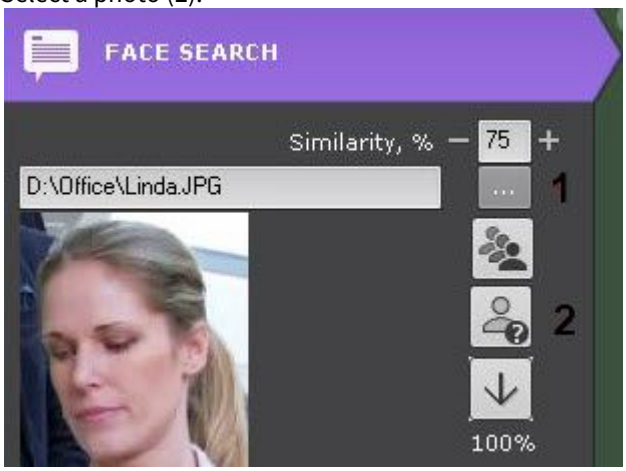
1. Click a face track in the surveillance window.
2. Click the button (**4**).

The face image will be saved to the folder specified in the settings (see Configuring export options(see page 572)).

16.2.6.4.9.4 Identifying "friend" or "foe" from a photo

To identify the "friend" or "foe" 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 "foe".

The algorithm is as follows:

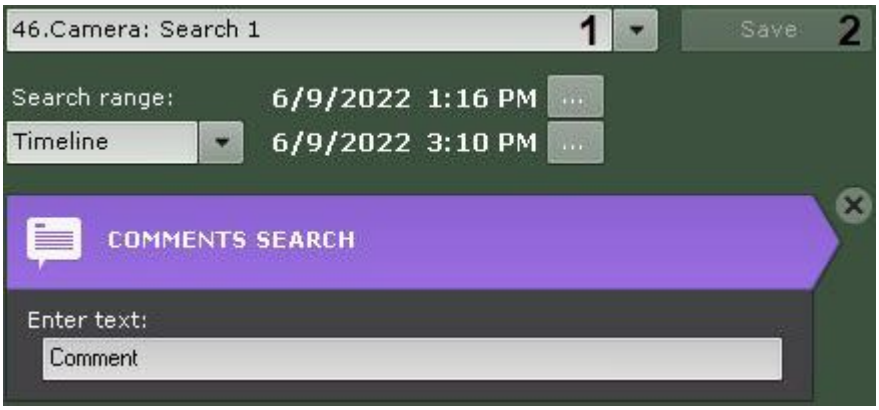
1. The person is compared to all recognized persons in the last 30 days.
2. The number of days (**N**) in which the person was captured by camera and recognized is calculated.
3. The probability is calculated according to the formula (1−**N**/30)*100.

16.2.6.4.10 Saving search queries

Saving a search query allows you to:

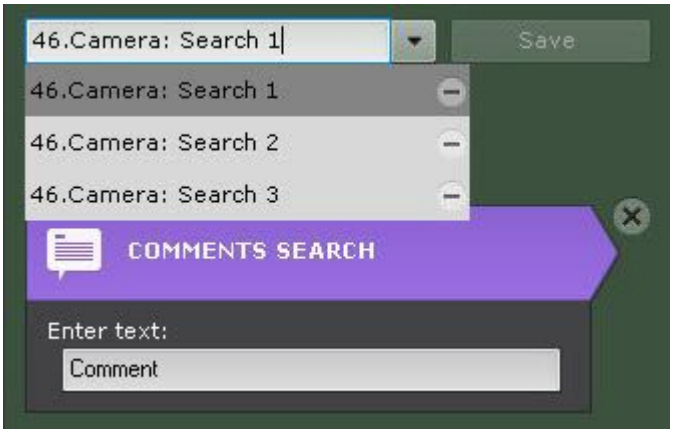
- quickly retrieve its results;
- apply search criteria to other cameras.

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(see page 710)).



> **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.

16.2.6.4.11 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.

16.2.6.4.12 Working with search results

16.2.6.4.12.1 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(see page 705)), 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(see page 725)), 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.

16.2.6.4.12.2 Viewing Search Results In TimeCompressor

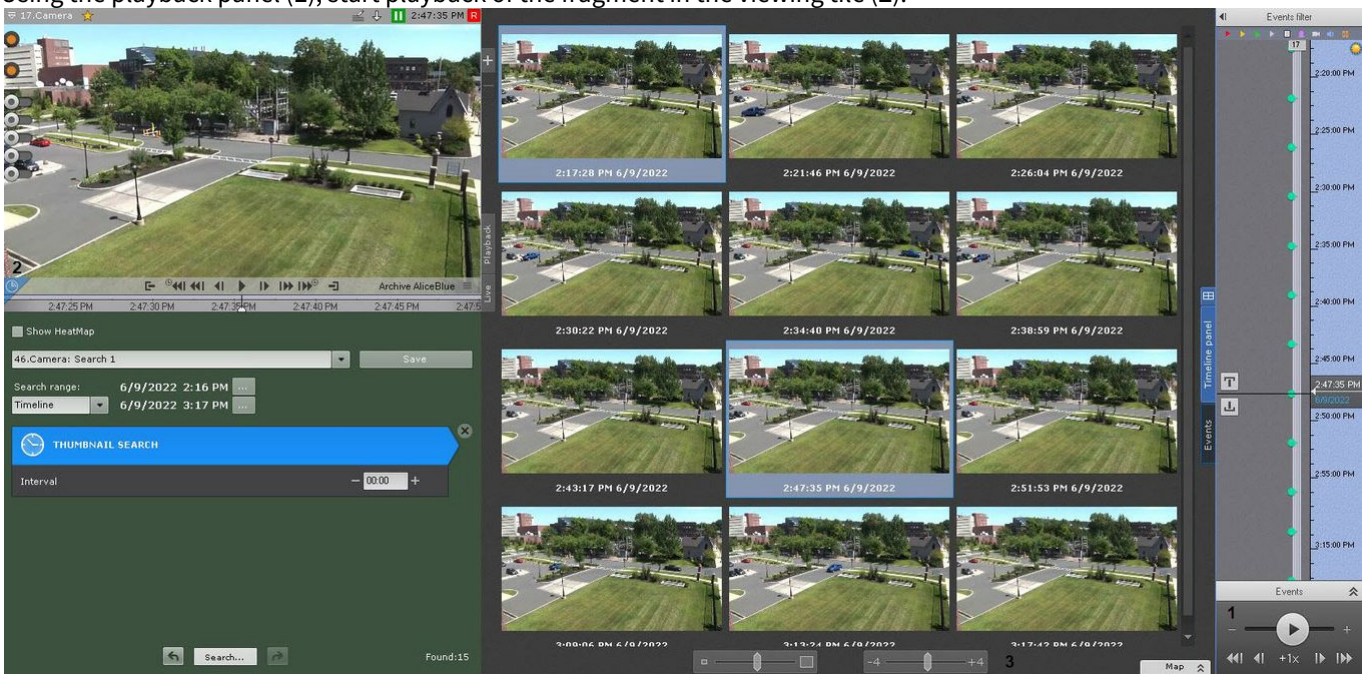
When you search recorded video for motion events by metadata (LPR search(see page 741), Face search(see page 744), Forensic Search for Fragments (MomentQuest)(see page 730)), you can view results in the TimeCompressor mode(see page 699).

To do this, click the button on the timeline in the camera window.

16.2.6.4.12.3 Playback of video fragments

To view the video fragment corresponding to a found moment in the archive, complete the following steps:

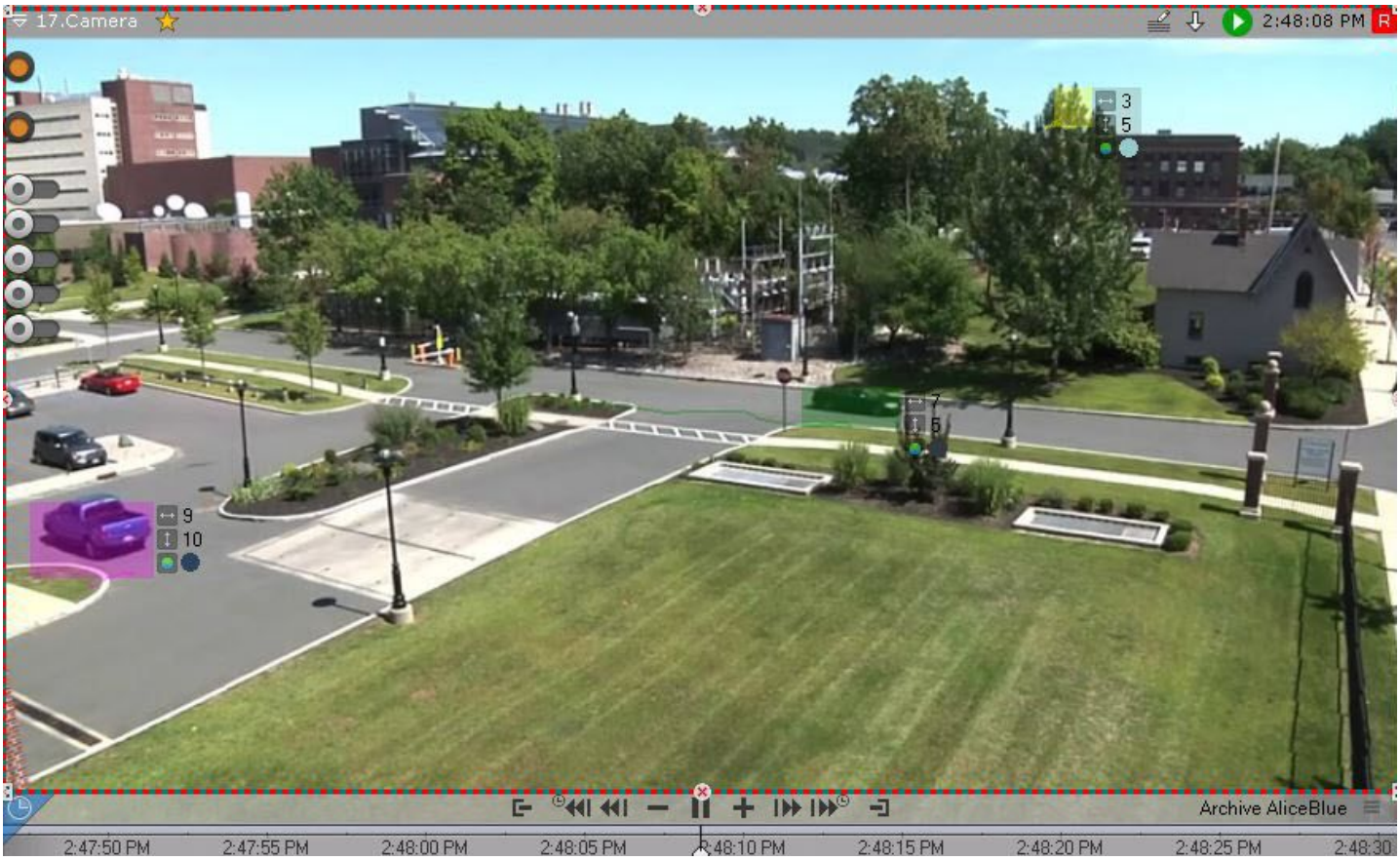
1. Left-click the found moment on the search results panel.
2. Using the playback panel (**1**), start playback of the fragment in the viewing tile (**2**).



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

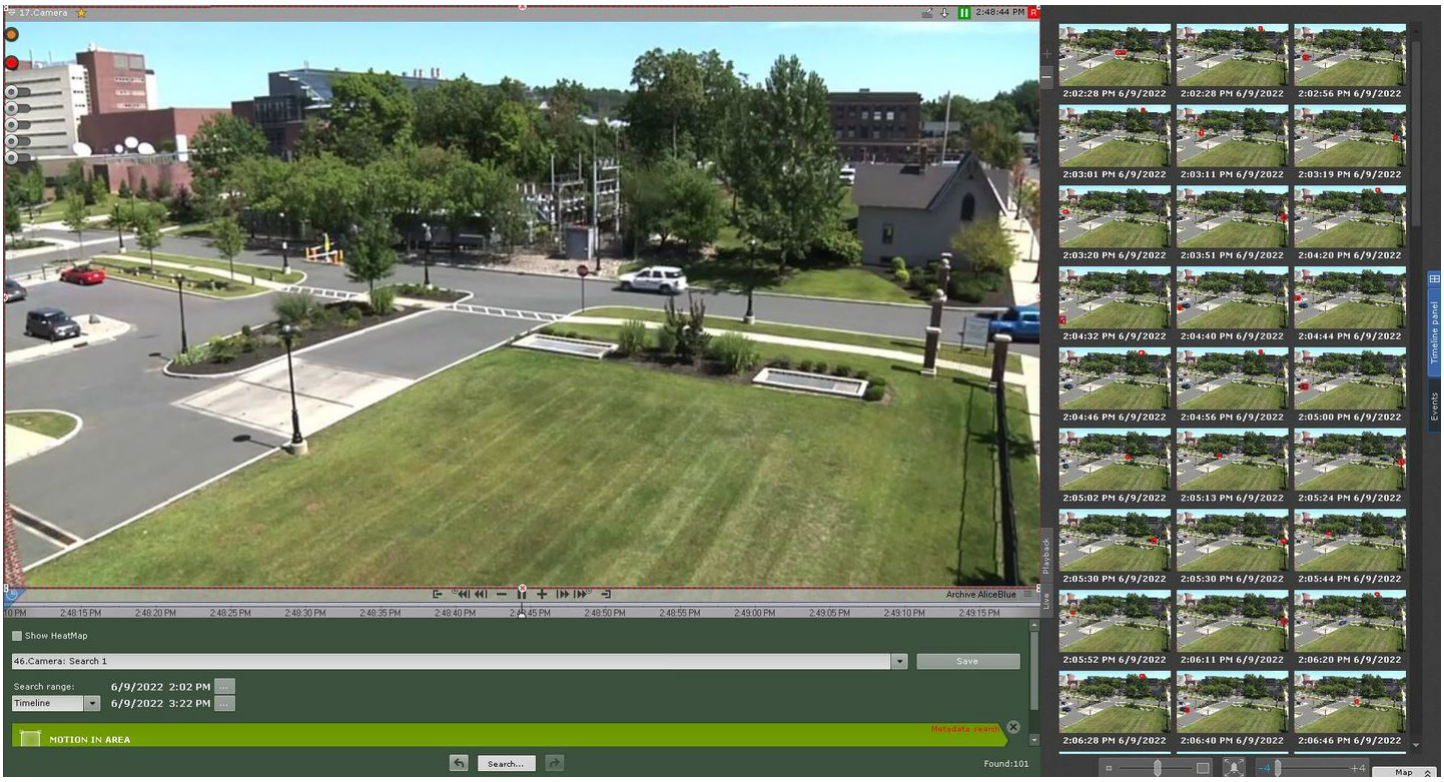
If object tracking is activated in the viewing tile, then the properties of tracked objects (width and height as a percentage of the width or height of the frame) are displayed when viewing video fragments found through forensic search.



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(see page 706) and Navigating using the Playback Panel(see page 708)).

Extreme zooming a camera window makes the Search Conditions and Archive Navigation panels become hidden (see Scaling the surveillance window(see page 654)).



16.2.6.4.12.4 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.

16.2.6.4.12.5 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(see page 809)).

16.2.6.4.13 Heat map

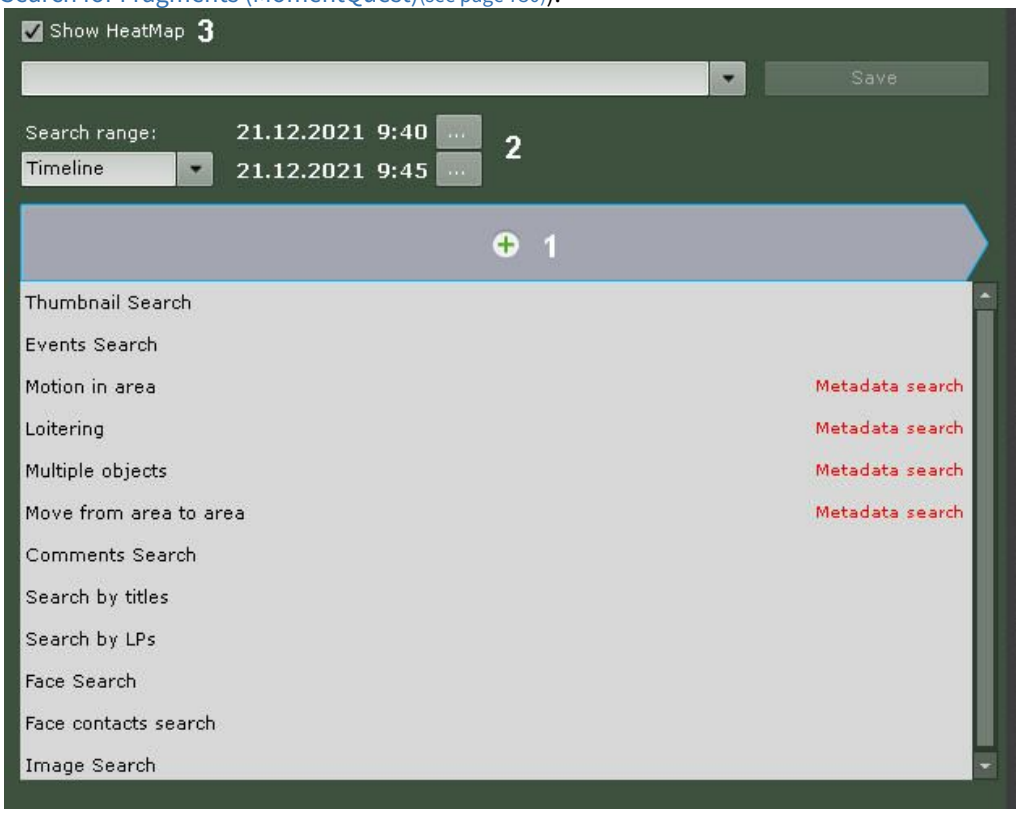
Attention!

At least one metadata source is required for displaying a heat map (for example, an object tracker — see General information on metadata(see page 237)).

The heat map allows you to check the movement activity in the frame and determine the areas where the objects move mostly.

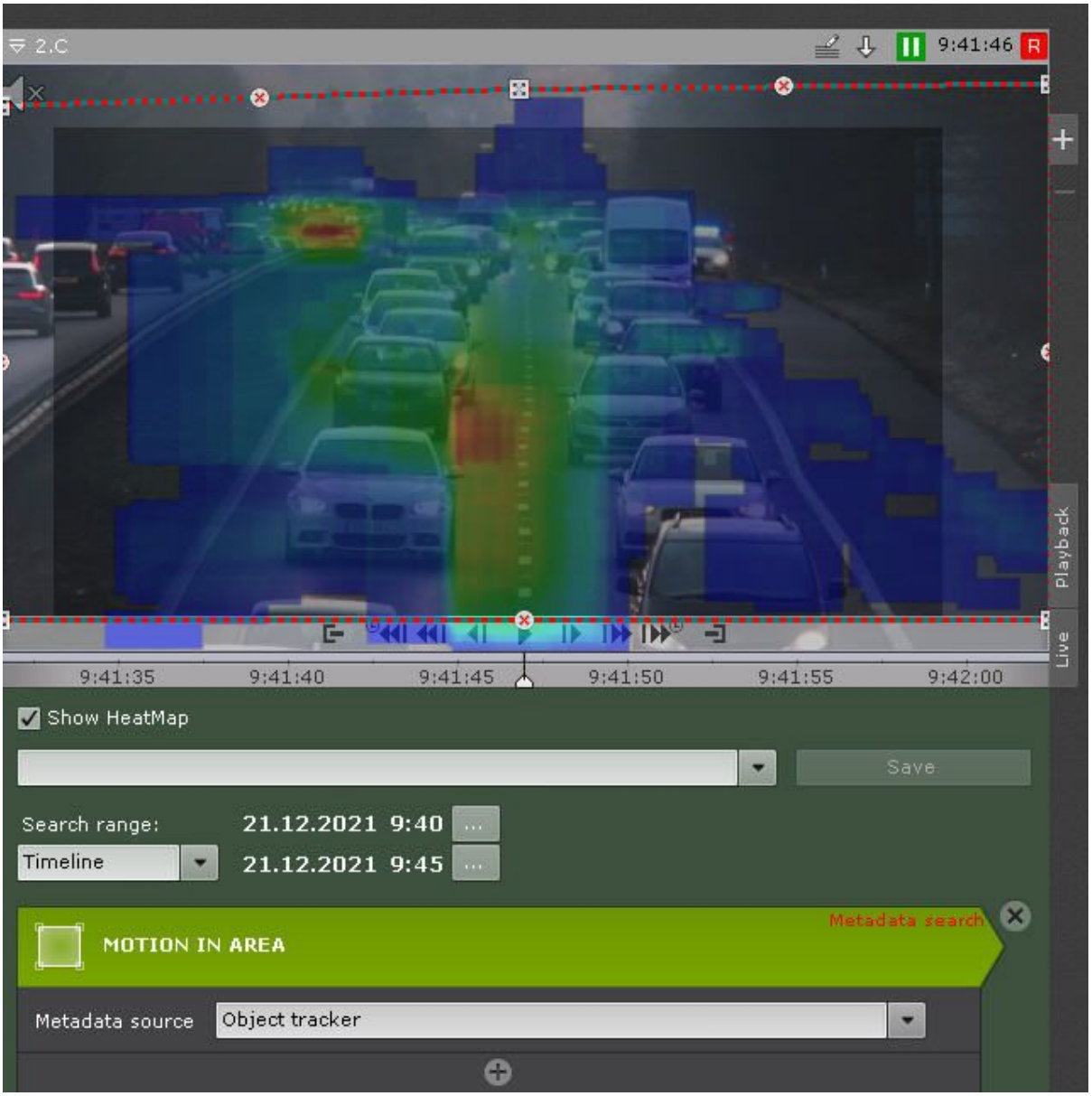
To display a heat map, do the following:

1. Select the type of search using metadata (**1**, see LPR search(see page 741), Search for similar face(see page 744), Forensic Search for Fragments (MomentQuest)(see page 730)).



2. Set the time period, according to the data from which the heat map should be generated (**2**, see Setting a search interval(see page 725)).
3. Set the **Show HeatMap** checkbox (**3**).
4. Click the **Search** button.

When the search is completed, a heatmap 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.

16.2.6.4.14 Image Search

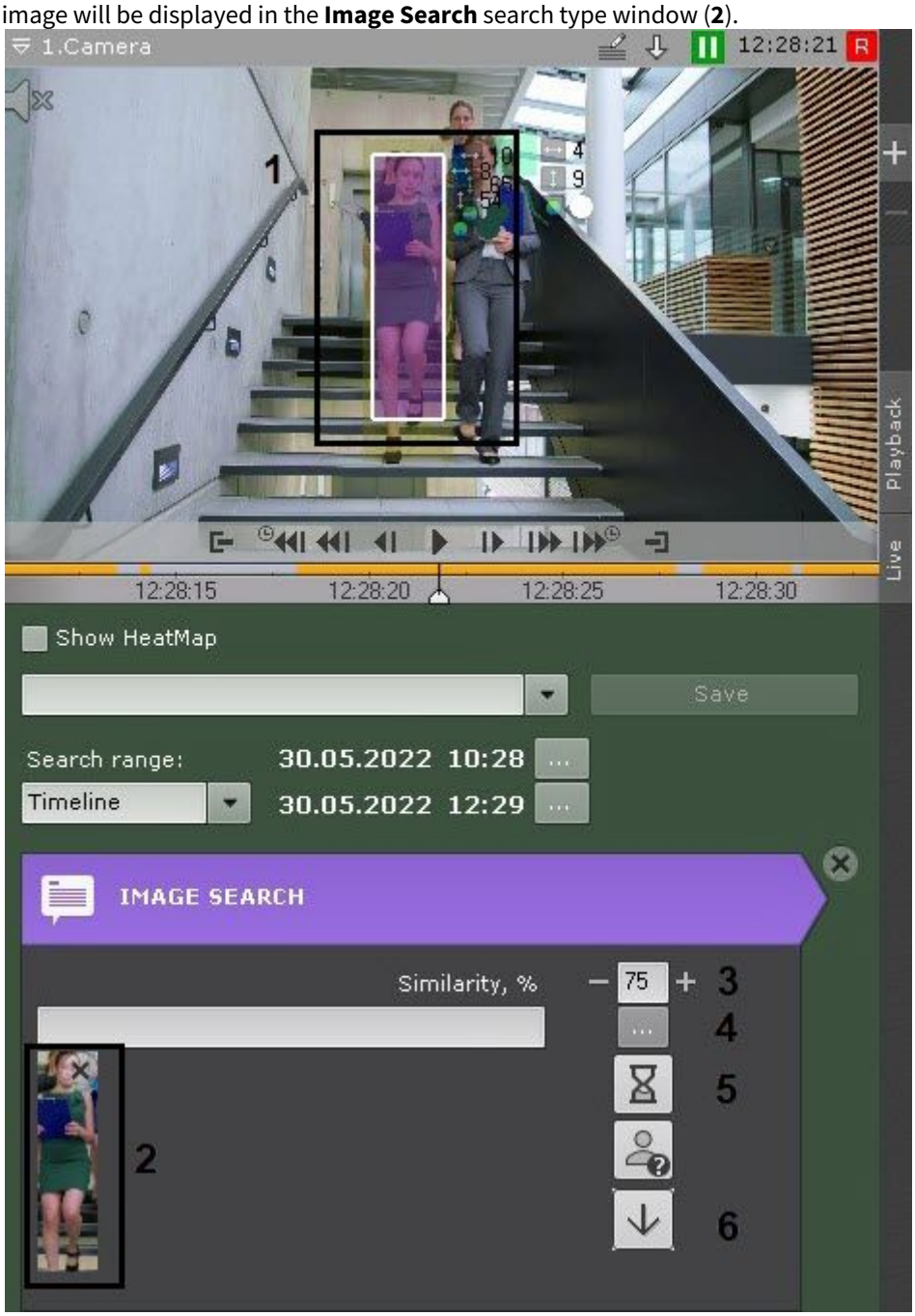
Image Search allows you to find in the archive similar images using a certain track or an image.

Attention!

To use Image Search, it is necessary to configure the neurotracker(see page 274) 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(see page 725)).
2. Select the **Image Search** search type (see Selecting the search type(see page 725)).
3. Select a search method:
    a. Search for a similar image by track:
        i. Select a track by left-clicking on an object in the video surveillance window (**1**). When you use image search, the image track is highlighted and its dimensions are displayed in the video 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.

> **Note**
>
> 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 3 minutes).
> Next times, 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(see page 572)).

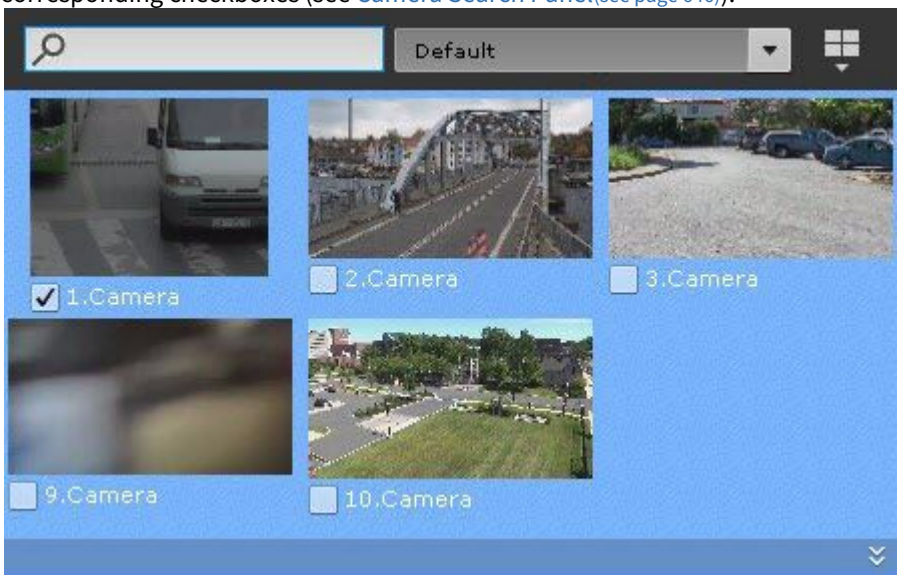
16.2.6.5 Simultaneous search in an archive of several video cameras

> **Attention!**
>
> The number of video cameras for search is not limited.

To search in the archive of several video cameras simultaneously, do the following:

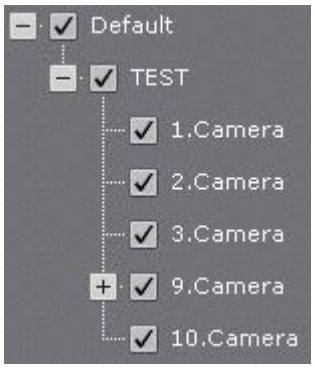
1. Choose the search type and set its parameters (see Search in an archive of a single video camera(see page 725)).

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(see page 646)).



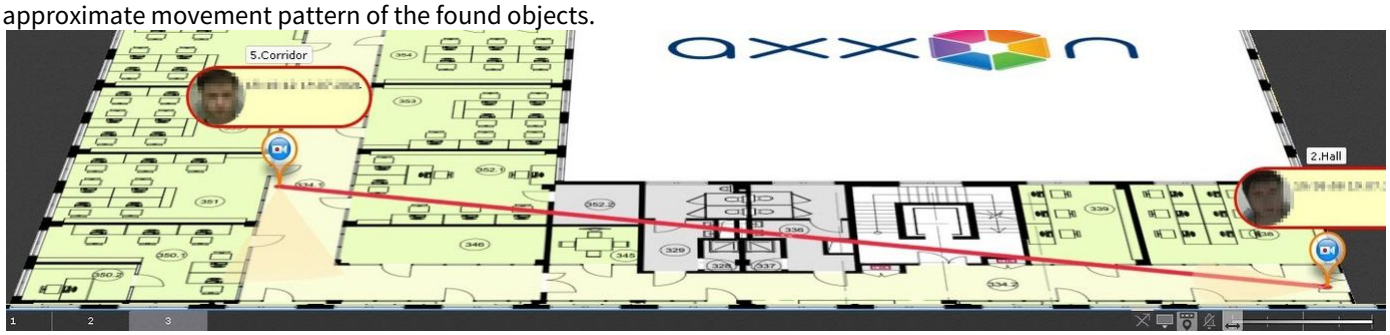
> **Note**
>
> By default, the checkbox is set next to the camera which was switched to the archive search mode. If you want to change the active camera in the archive search mode, clear the checkbox next to the current active camera and set it next to the required camera.

To search all video cameras in an Axxon-domain, open the Objects Panel (see Objects Panel(see page 648)) 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(see page 744)) or for LPs (see LPR search(see page 741)) in the archive of several video cameras simultaneously, the interactive map (see Opening and closing the map(see page 796)) 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(see page 639)) 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.

16.2.7 Working with fisheye cameras

16.2.7.1 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:

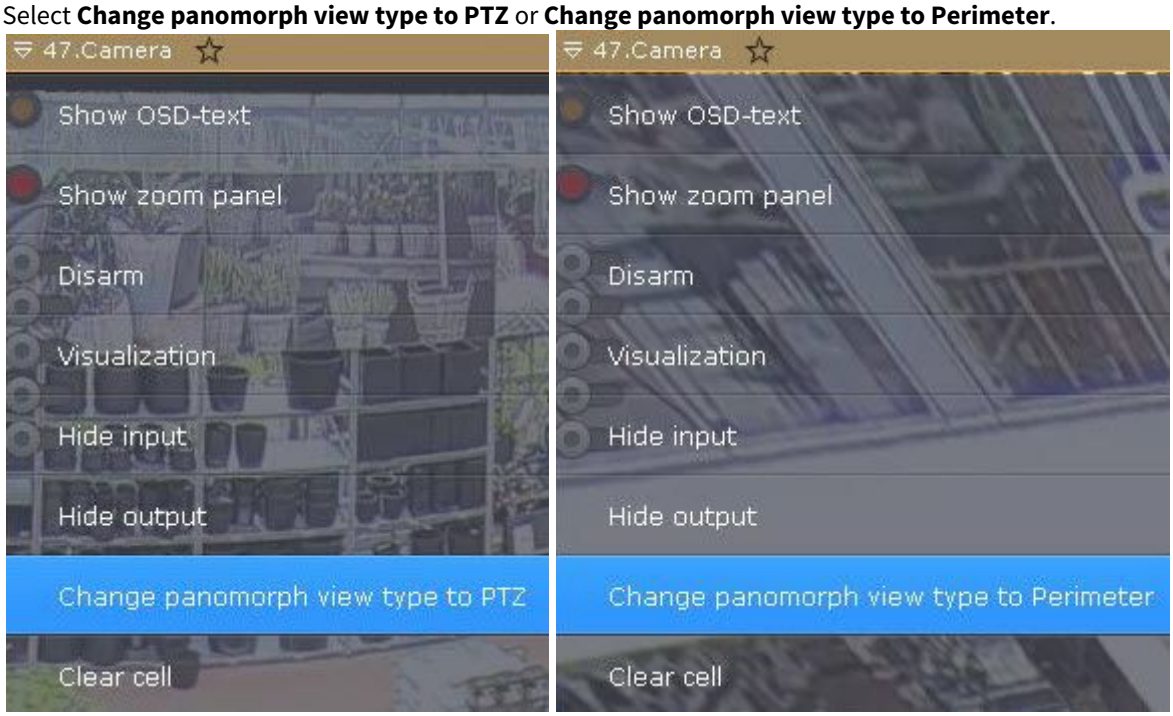
1. 360° panorama.
2. Regional view.
3. 180° panorama (for video camera with an Immervision lens).

16.2.7.1.1 Selecting viewing mode for videos from a fisheye camera

By default, fisheye camera video viewing mode setting is taken from device settings (see Configuring fish-eye cameras(see page 127)), or from layout settings (see Selecting default functions for viewing tiles(see page 484)).

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.

16.2.7.1.2 360 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[188]) by one notch or more, regional viewing begins.

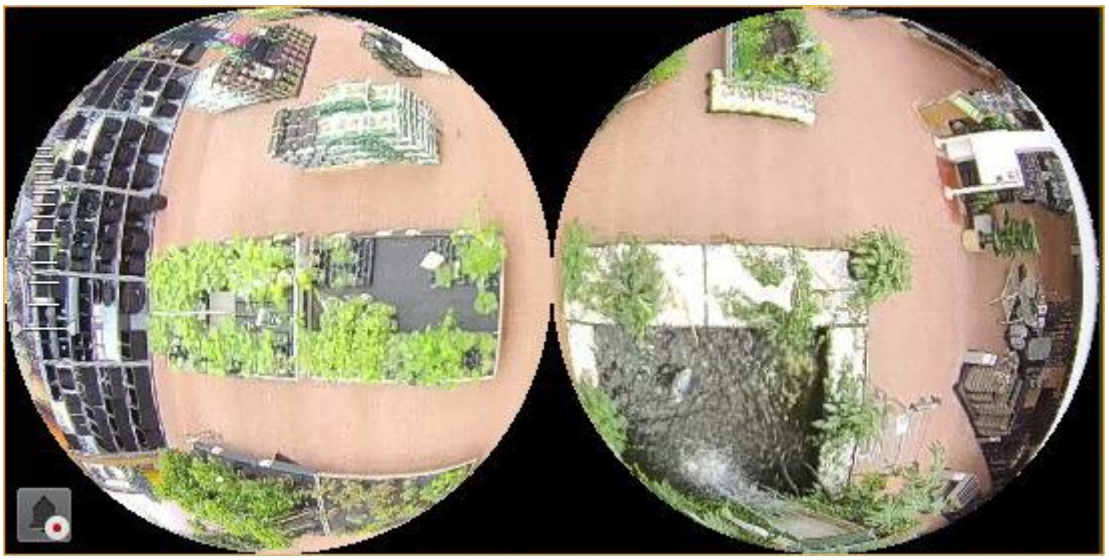
The following actions are available when viewing video in this format:

1. Point & Click functionality (see Control using Point&Click[189]).
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.

188 https://docs.axxonsoft.com/confluence/display/next36en/Digitally+Zooming+Video+Images
189 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=108299719



When you zoom in one of the images, both views will be merged into a single panoramic view.

16.2.7.1.3 180 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 fish-eye cameras(see page 127)).

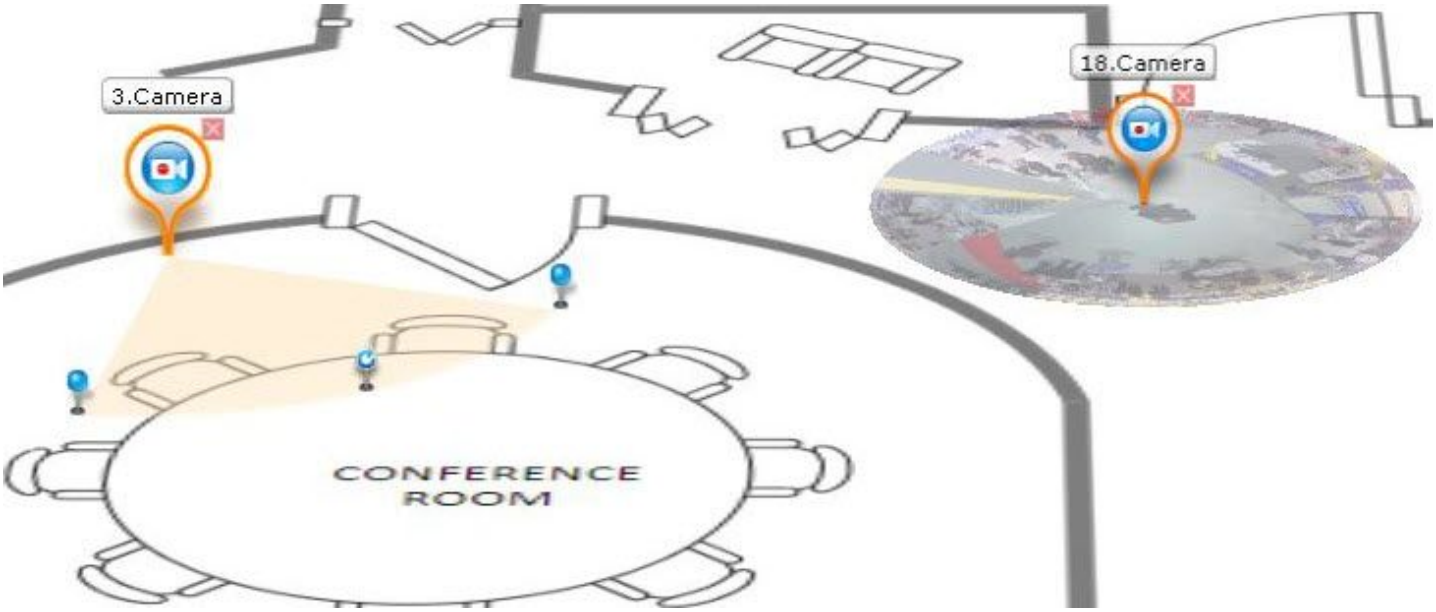
To set the viewing angle, click and hold the button while moving the cursor to the left or right.

Point&Click (see Control using Point&Click(see page 684)) and all standard video viewing functions are available when viewing video in this format.

16.2.7.2 Fisheye cameras on an interactive map

16.2.7.2.1 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 fish-eye cameras(see page 127)) 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[190]).

Note

190 https://docs.axxonsoft.com/confluence/pages/viewpage.action?pageId=226953016

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.

16.2.7.2.2 Fish-eye cameras in immersive mode

In immersive mode (see Immersive mode(see page 802)), 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(see page 761)).

In immersive mode, only the following video surveillance functions are available for fish-eye cameras.

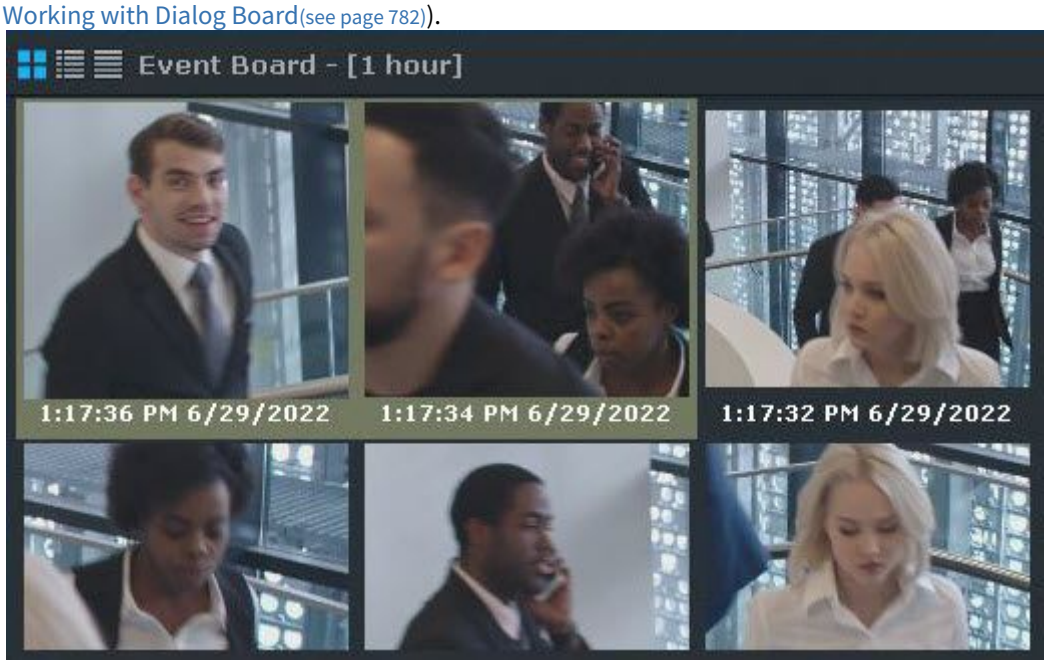
1. Digital zoom via mouse scrolling (see Enlarging a video image using the mouse scroll wheel(see page 657)).
2. Point&Click functionality (see Control using Point&Click(see page 684)).
3. To change the angle of view of a fish-eye camera, move the mouse around the video image while holding down the left mouse button.

To exit immersive mode, click the button.

16.2.8 Face recognition and search

Face recognition events are registered in the System Log (see The System Log(see page 819)).

These events can as well be displayed on the Events Board (see Working with Event Boards(see page 772)) or Dialog Board (see Working with Dialog Board(see page 782)).

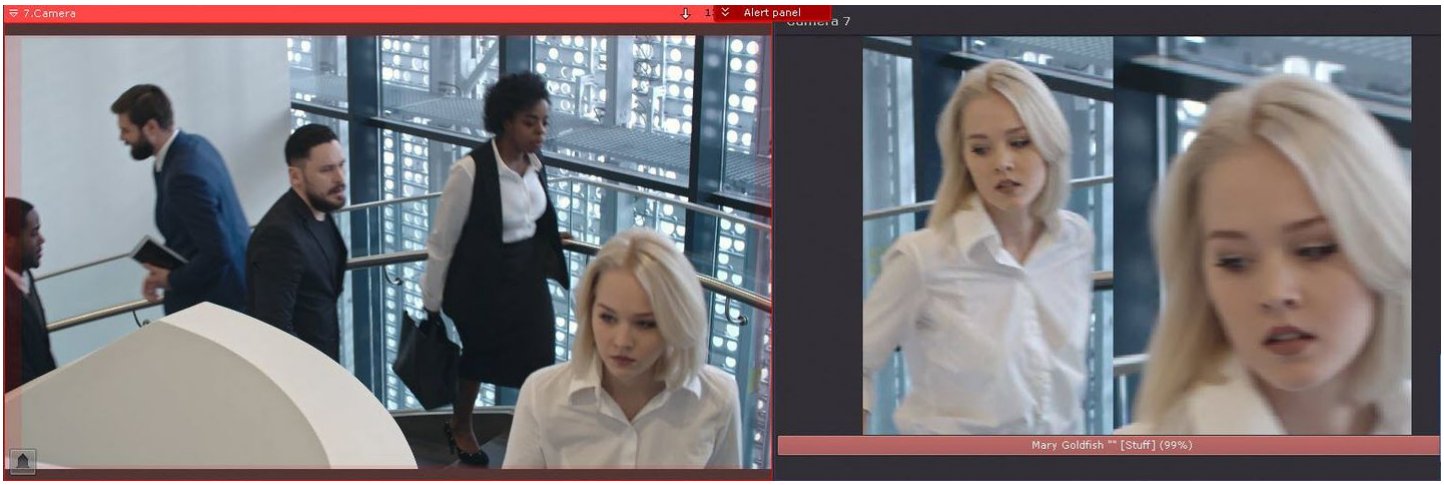


If you activate the age and gender information collection, its results will be displayed on the panel and saved into the System Log (see Configuring Face detection(see page 280)).

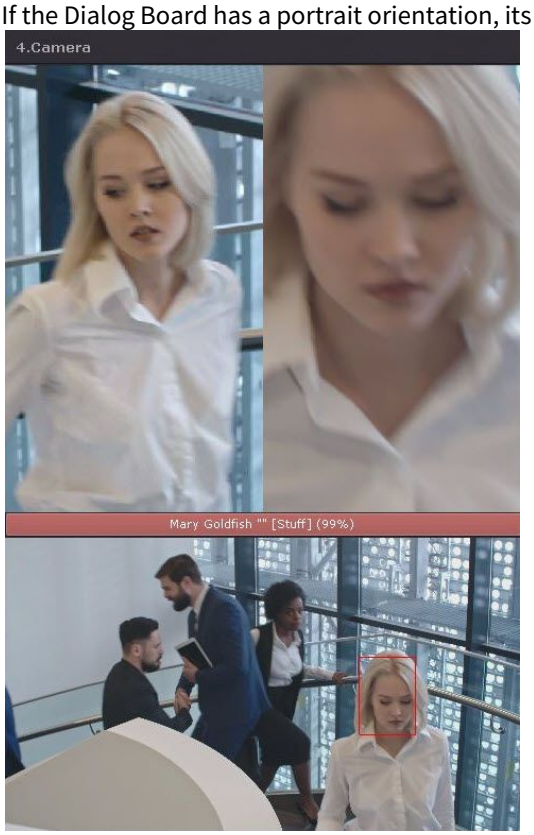
If the Camera window is linked to the Event Board (see Linking cells(see page 481)), you can double click on an event to start the Video Footage search for sequences containing the recognized face.

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.

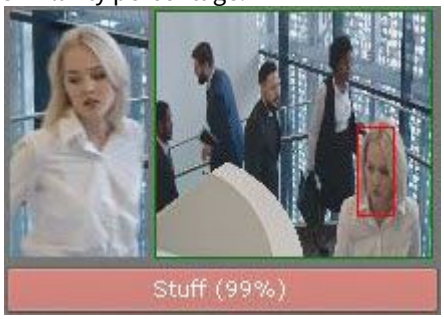


If the Dialog Board has a portrait orientation, its lower part will display the alarm video.



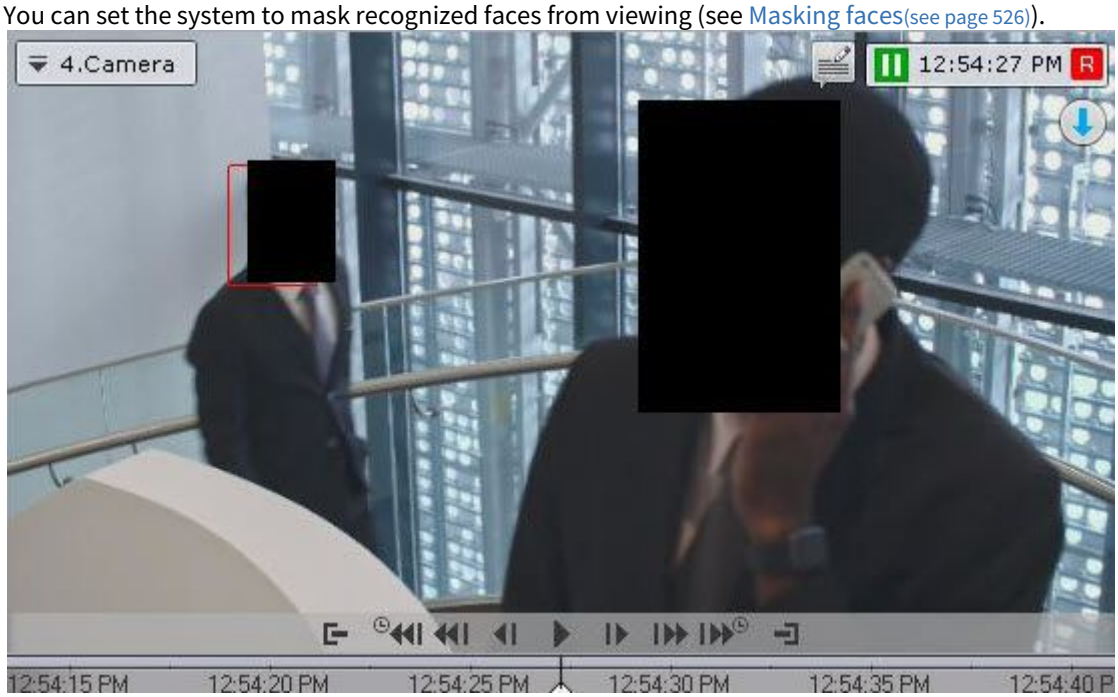
The Alarm notification panel will also include:

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(see page 744)) or multiple cameras (see Simultaneous search in an archive of several video cameras(see page 759)).

You can set the system to mask recognized faces from viewing (see Masking faces(see page 526)).



16.2.9 Vehicle number plate recognition and search

VMS logs every ANPR number (see The System Log(see page 819)).

Attention!

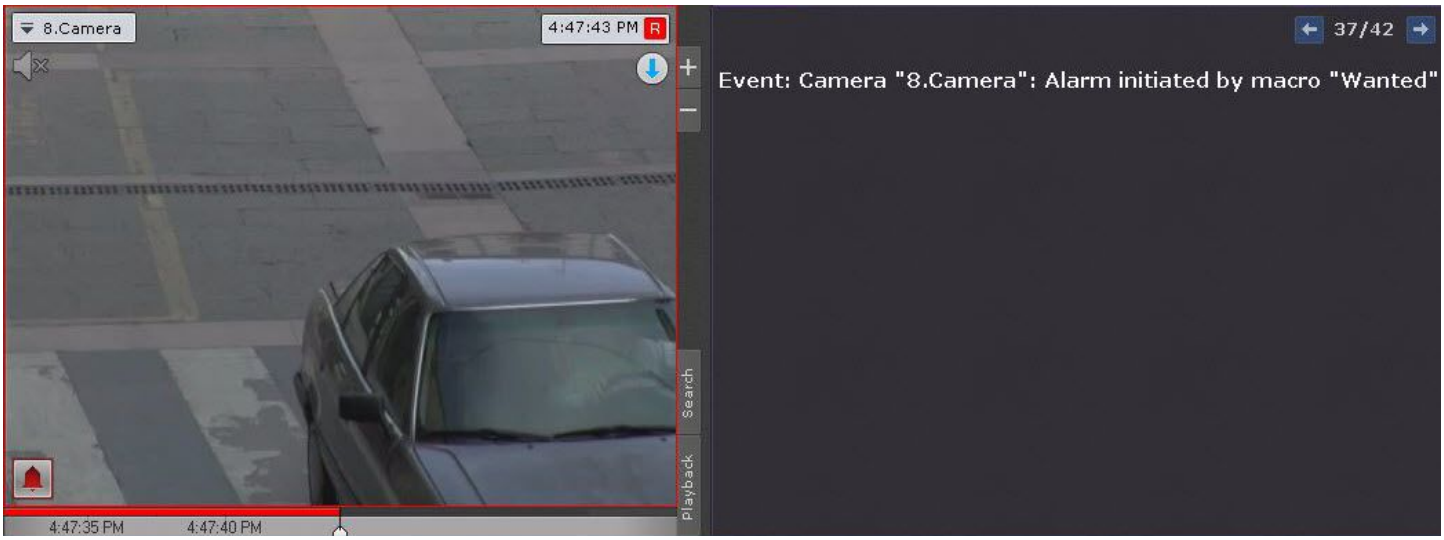
Depending on detection tool settings, a delay may occur between the number recognition and the registration of the corresponding event (see Configuring License plate recognition (VT)(see page 314), Configuring License plate recognition (IV)(see page 326)).
The event is time-stamped with the time of recognition, 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)(see page 314).

All relevant events can be displayed on the Event Board (see Working with Event Boards(see page 772)) or Dialog Board (see Working with Dialog Board(see page 782)).

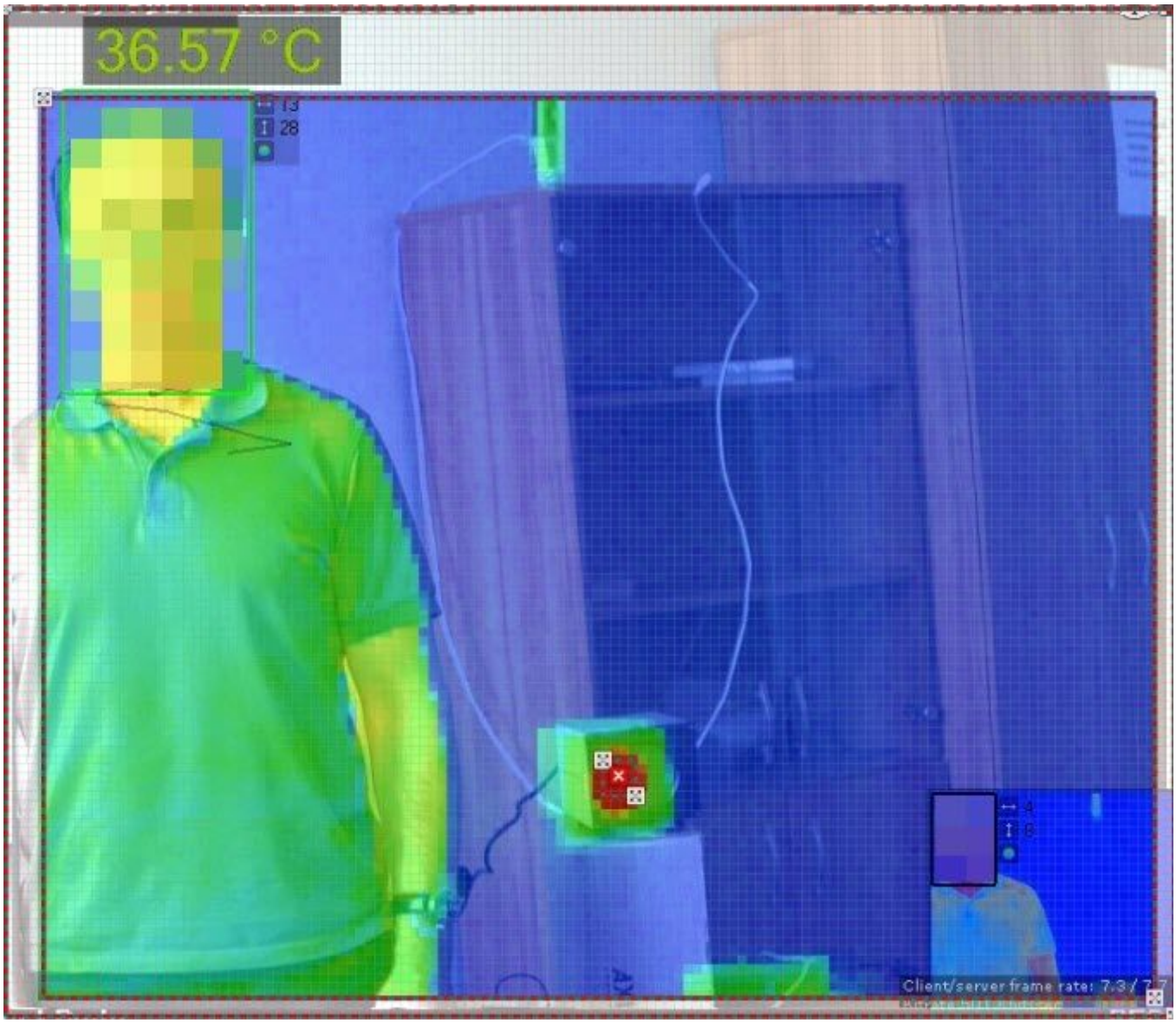
If you have created any LP lists in your system, you can program automatic responses (e.g. alarm triggering) to LP recognition events related to list's entries (see Configuring real-time vehicle license plate recognition(see page 337)).



16.2.10 Temperature screening

In *Axxon One*, only two methods of temperature screening are available:

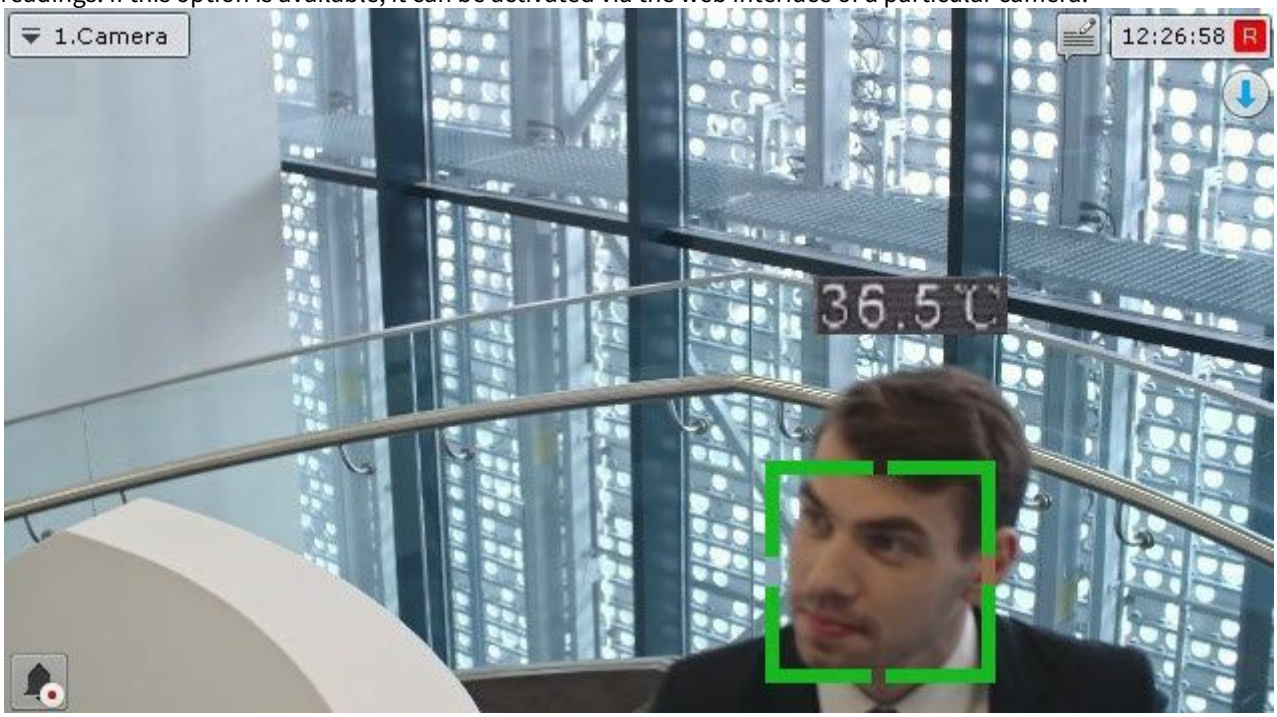
1. With the use of Mobotix M16 TR cameras. In this case, temperature values are displayed next to each recognized face's bounding box (see Face Detection and Temperature Control with Mobotix M16 TR cameras(see page 293)).



Each face recognition event contains thermal measurement data which can be displayed on the Events Board (see Working with Event Boards(see page 772)).

2. With the use of built-in detection tools of selected camera models (see Embedded Detection Tools(see page 393)). 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.



16.3 Working with information boards

16.3.1 Resizing information boards

You can resize information boards in the same way as viewing tiles (see Scaling the surveillance window(see page 654)).

> **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.

16.3.2 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(see page 495)).

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

16.3.3 Automatically switching to layouts with information boards

Automatic switching to a layout with an information board is possible for Event Board, Health Board and Dialog Board (if it is set up to Automated Responses to Events). This option is available when configuring boards of these types.

Automatic switching to a layout with Event Board or Dialog Board occurs when all of the following conditions are met:

1. The current layout does not contain Event/Dialog Board.
2. An event matching the board filtering settings has occurred in the system.

Automatic switching to a layout with a Health Board occurs when the following conditions are met:

1. The current layout does not contain a Health Board.
2. The status of a monitored server or camera worsens.

The layout with the smallest number of cells is chosen for display. If there are multiple layouts with identical numbers of cells, the layout that comes first in the alphabet is chosen.

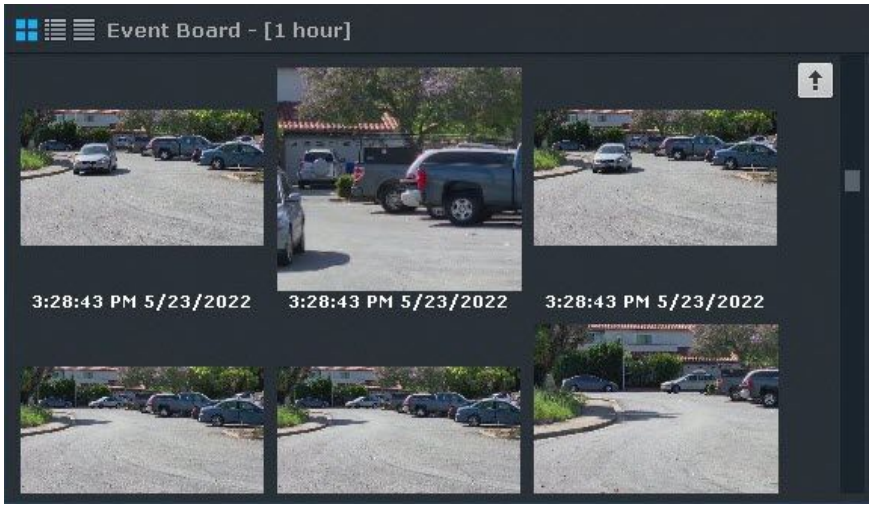
16.3.4 Working with Event Boards

16.3.4.1 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(see page 490).

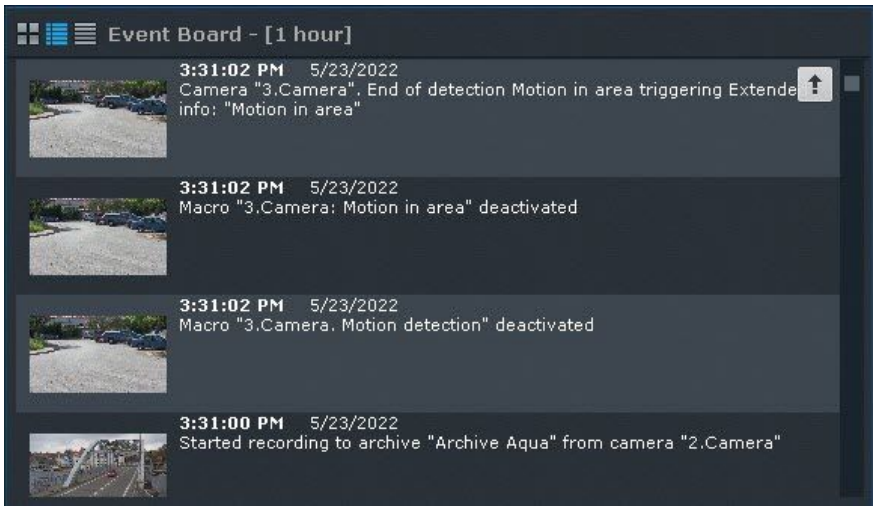
Events on the board can be displayed in three ways, chosen via the buttons in the upper-left corner of the board:

1. First frame of events and their time:

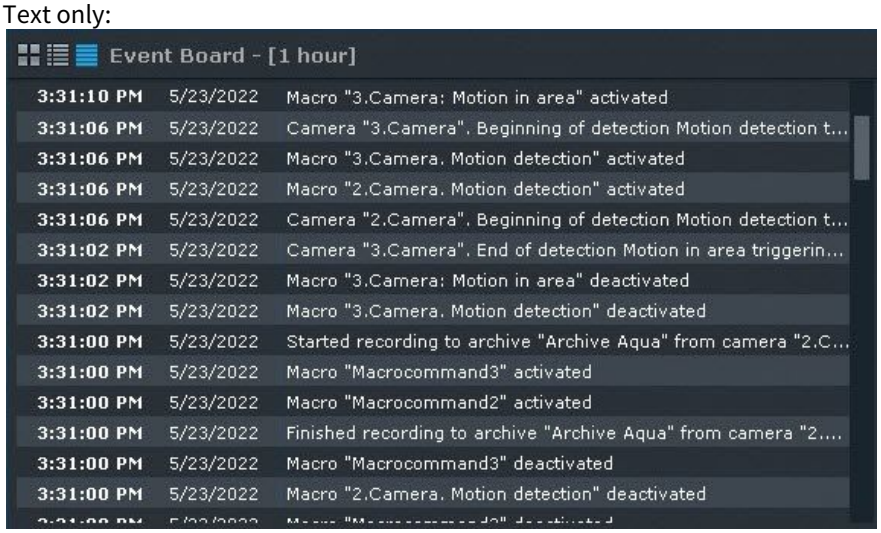


> **Note**
>
> The frame is not displayed when there is no recording in the archive.

2. First frame of events and text:



3. Text only:



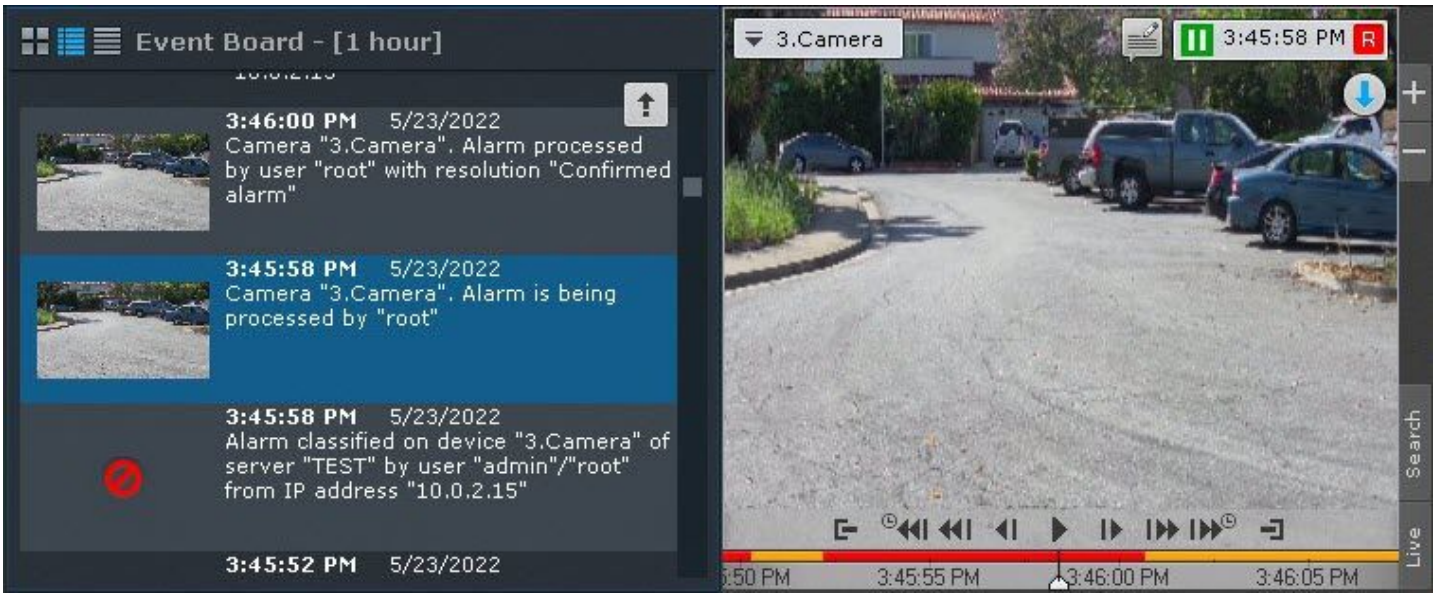
When a layout is switched to, by default the **Events Boards** is displayed as configured in the settings.

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(see page 693)). In this case, it includes only detection events for a selected camera.

16.3.4.2 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.



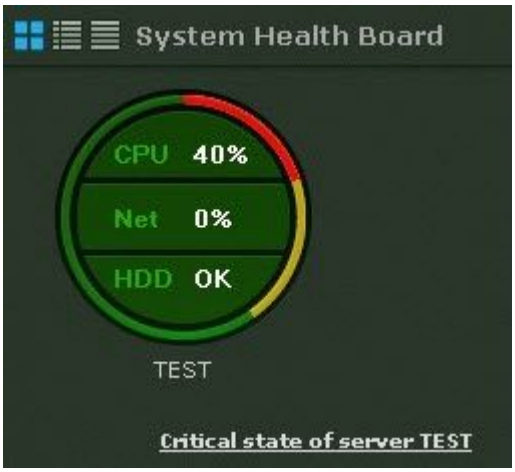
> **Note**
>
> If there is no archive for a camera when an alarm occurs, the archive is positioned at the closest recorded archive entry.

> **Note**
>
> If an Event Board is linked to several cameras, all cameras transition to Archive mode.

16.3.5 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

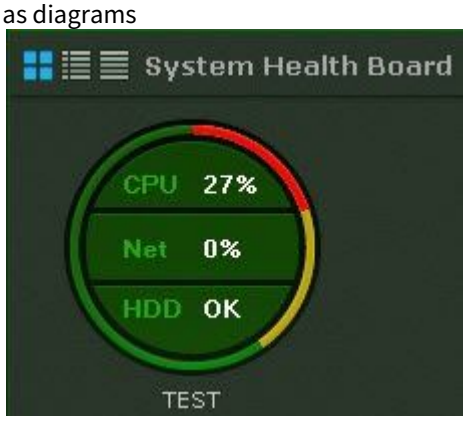
In table mode, you can view server status by clicking the relevant line in the table.

To switch to a view of server status, click the button.

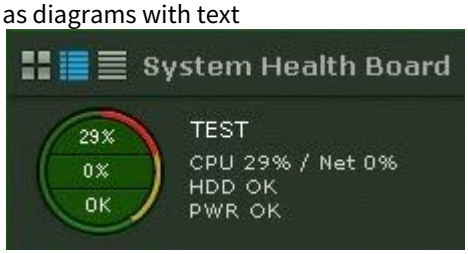
16.3.5.1 Viewing server status

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)

When you switch the server to reserve power, an icon is added to the chart. The icon disappears when you restore the main power.

The edge of the diagram changes color based on the status of the connected cameras (see Viewing camera status(see page 777)).

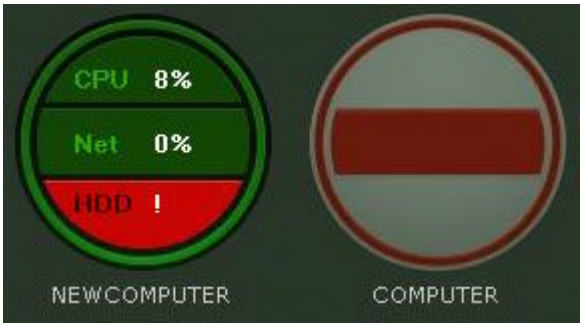
If the entire edge is green, all cameras are in normal condition. If part of the edge is yellow or red, some cameras have borderline or critical status.

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 ten 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).

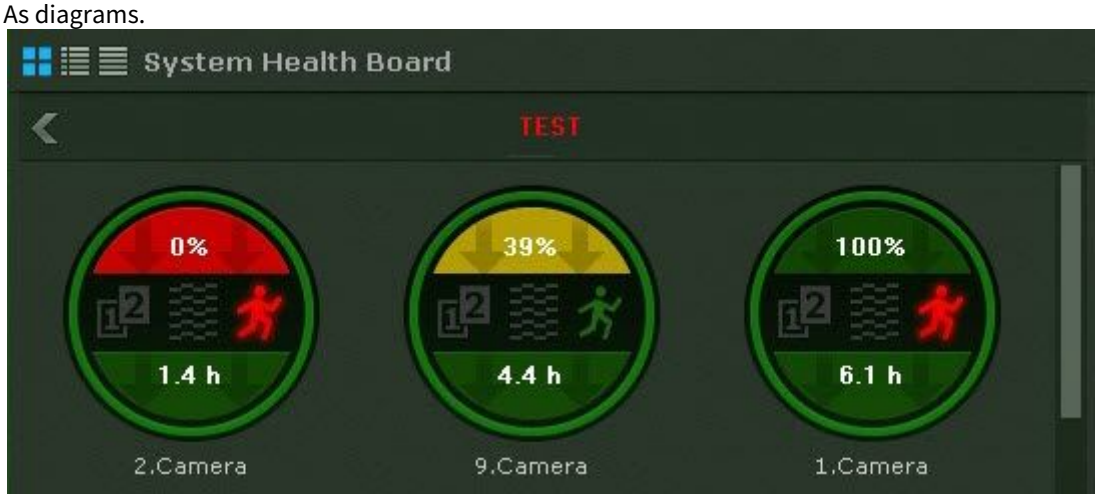
The message then closes and the status bar again appears.

> **Note**
>
> If the status of several servers worsens, a message is shown for the last one.

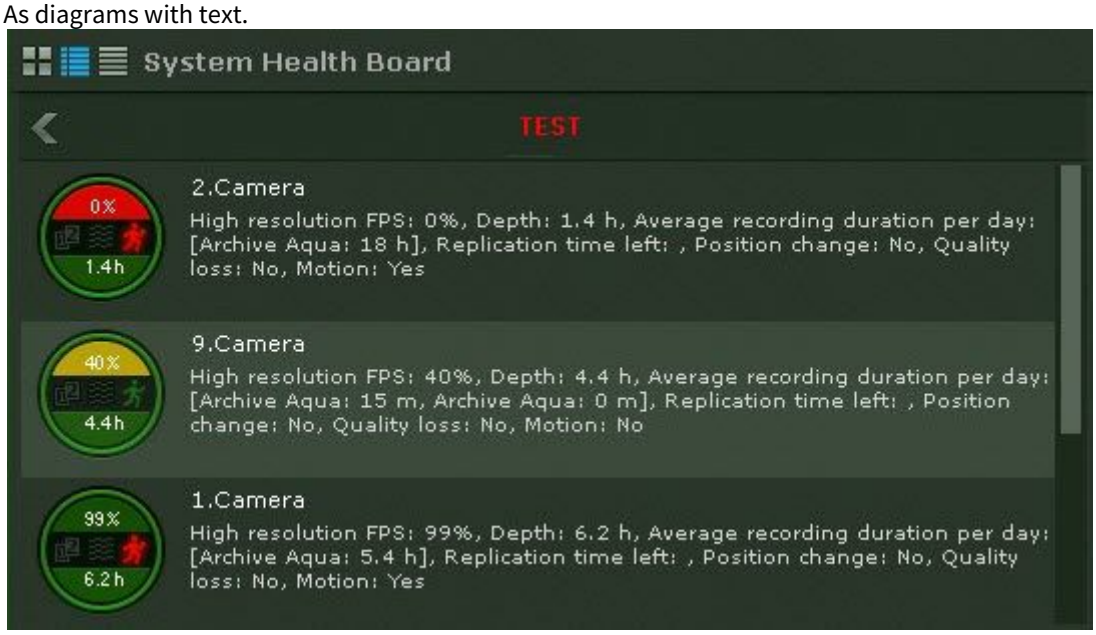
16.3.5.2 Viewing camera status

Information about the status of cameras can be displayed in three ways, chosen via the buttons in the upper-left corner of the board:

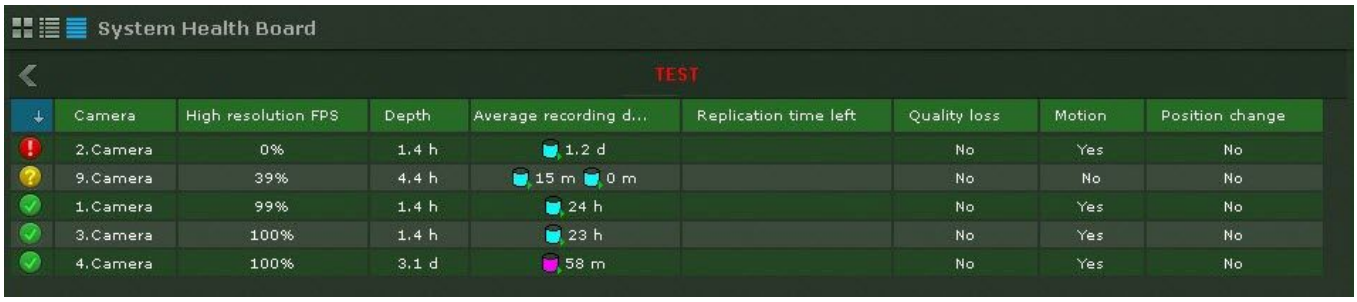
1. As diagrams.



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(see page 122)).
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.

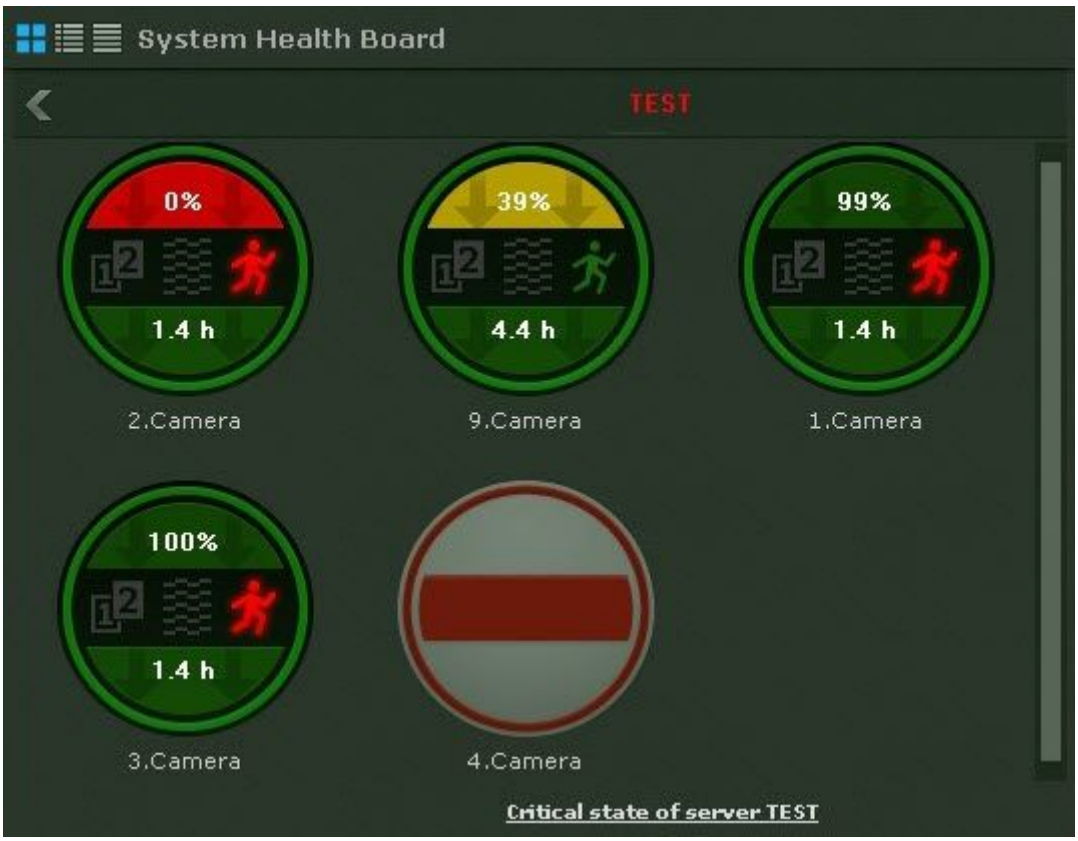
The camera status is measured based on the signal from the camera and stream rate:

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.

16.3.6 Working with Statistics Boards

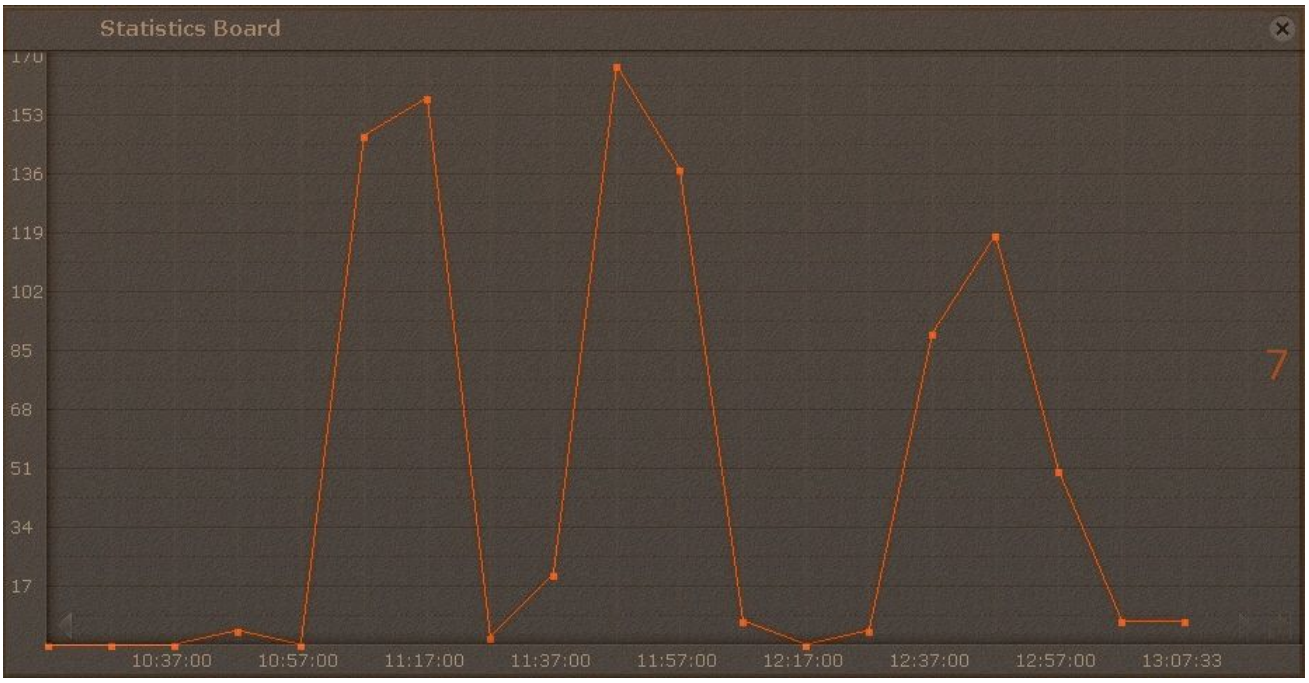
The Statistics Board is a graph of the number of events of a certain type for a specified timeframe. The type of events and amount of time between the points of the graph are configured in the board settings (see Configuring a Statistics Board(see page 492)).

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.

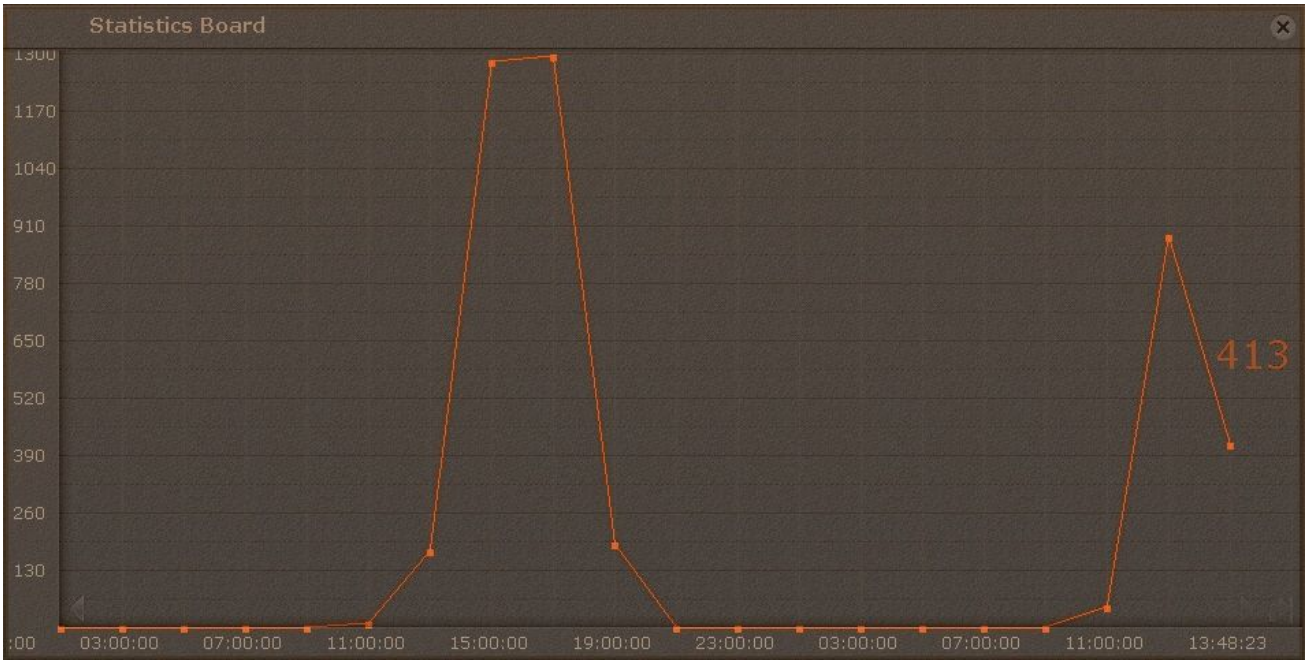
For example, the interval is set to **10** minutes on this sample graph here. The current time (**1:07:33 p.m.**) is the last point on the graph, so after rounding this to the next whole minute we get the value for the next-to-last point: **1:07:00 p.m.** Correspondingly, the points before it are **12:57:00 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.

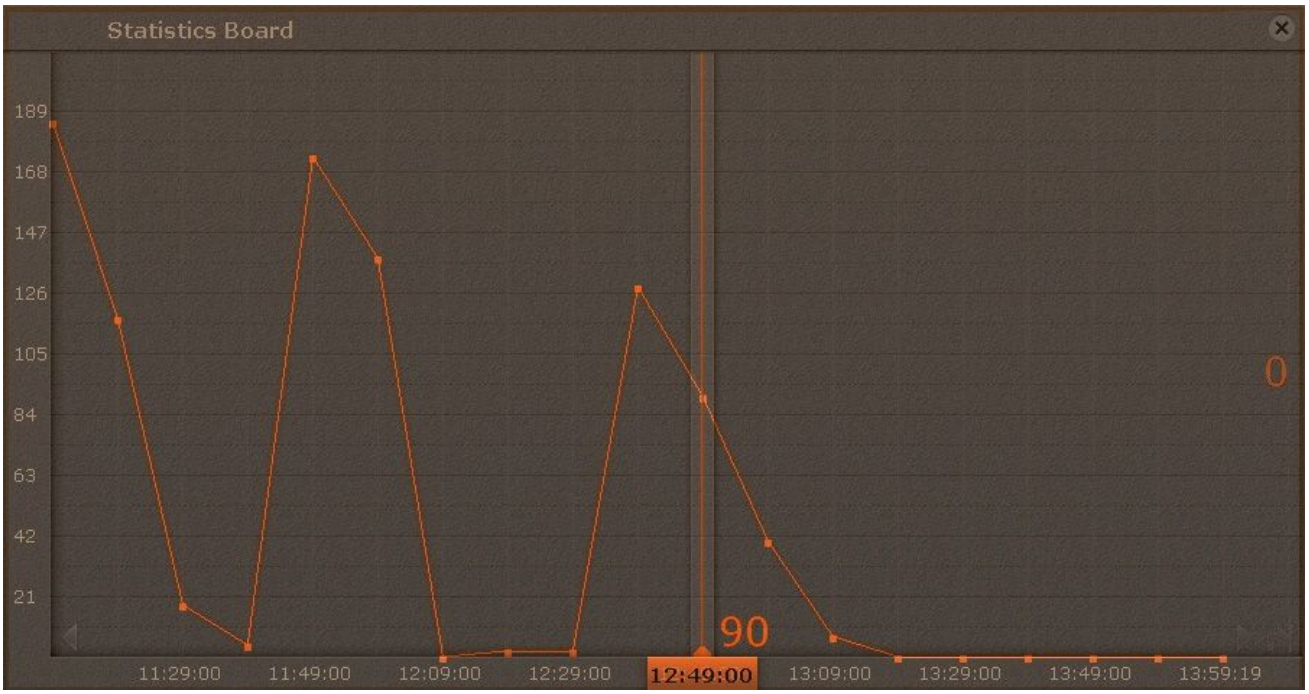
The graph displays the current number of events. The number of events is recalculated every minute and does not depend on the interval chosen.

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 **413**, 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.

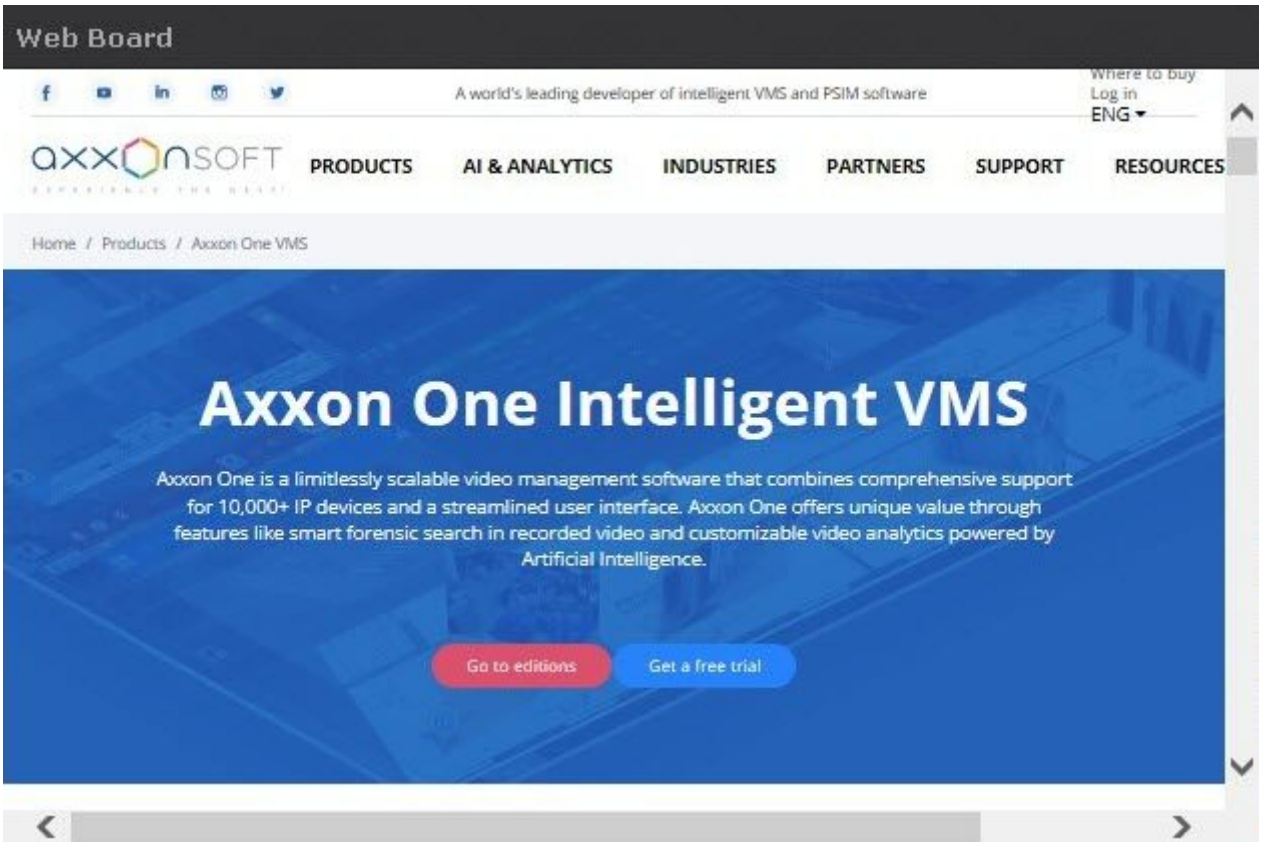
Clicking anywhere on the graph jumps to the nearest point and the relevant value is indicated.



16.3.7 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.

16.3.8 Working with Dialog Board

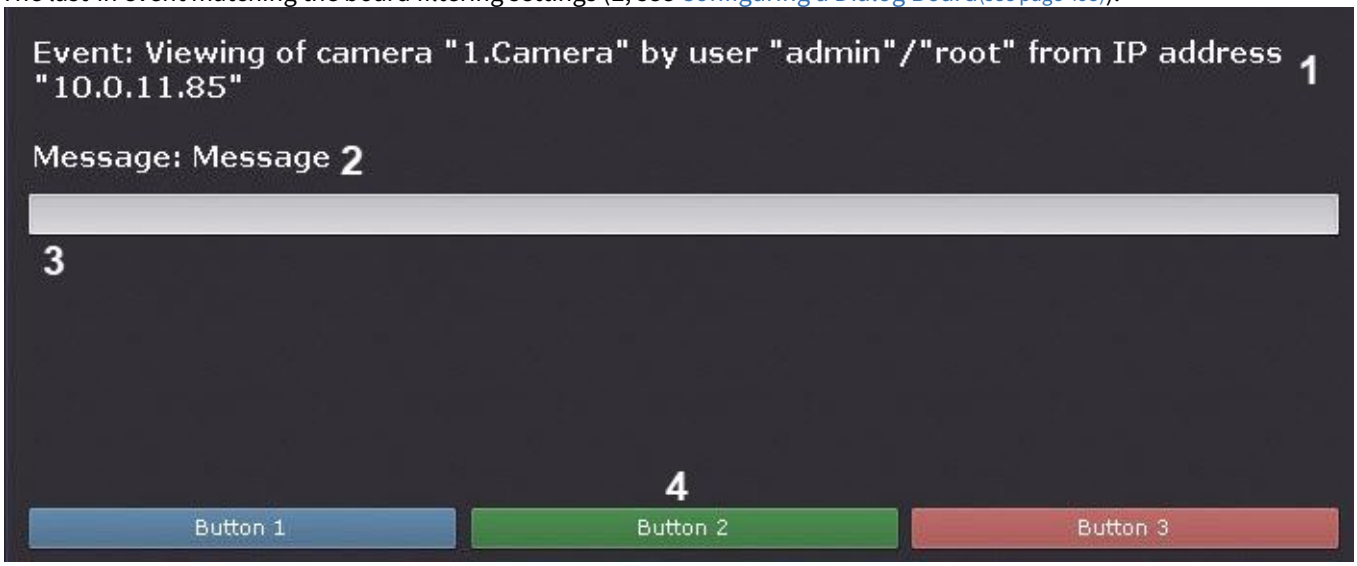
> Configuring a Dialog Board(see page 495)

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:

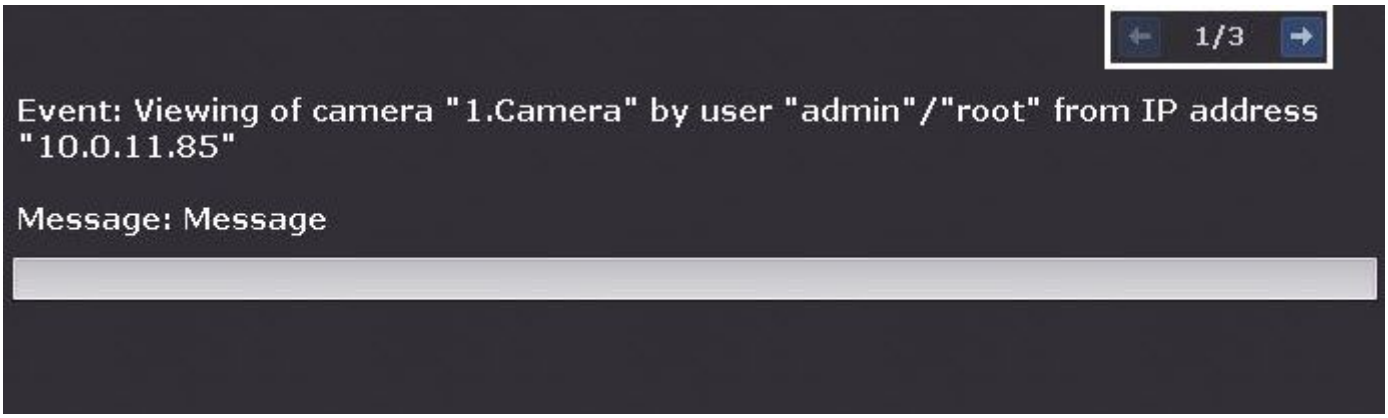
1. The last-in event matching the board filtering settings (**1**, see Configuring a Dialog Board(see page 495)).



> **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(see page 819), 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(see page 771)).

If the pane has a history of events (see Configuring a Dialog Board(see page 495)), 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.

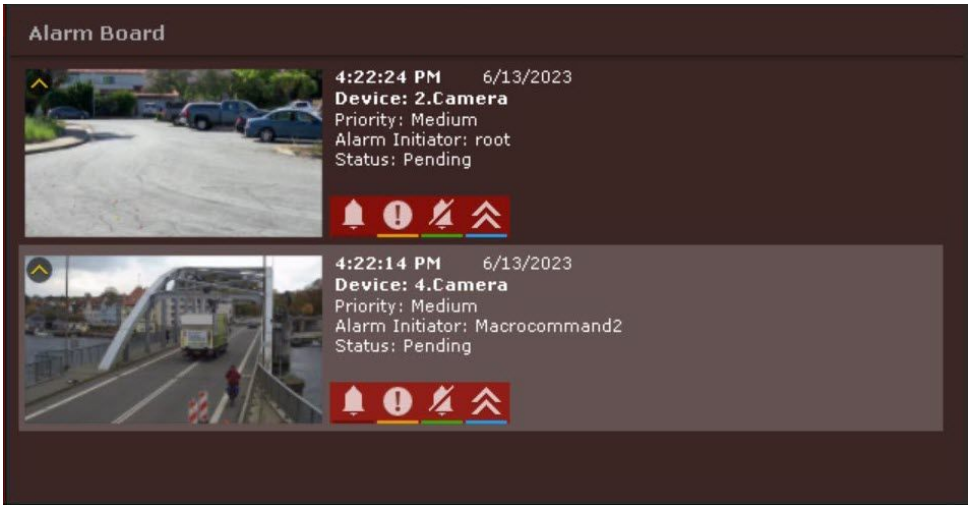
You can select a camera if you click on its tile on a layout, in the Objects panel (see Objects Panel(see page 648)) or on the map (see Working with the interactive map(see page 795)).

The panel can also display a selected still image.

16.3.9 Working with an Alarm Board

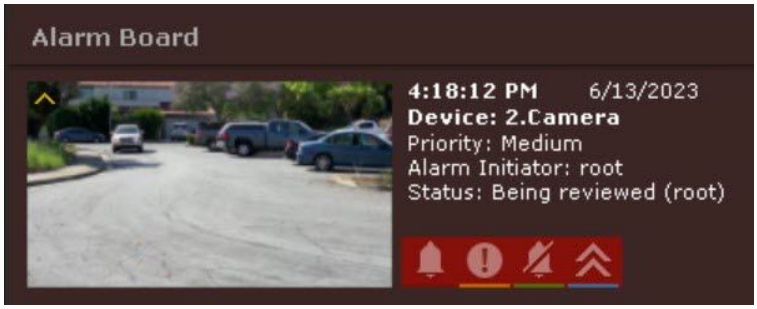
Configuring an Alarm Board(see page 498)

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.

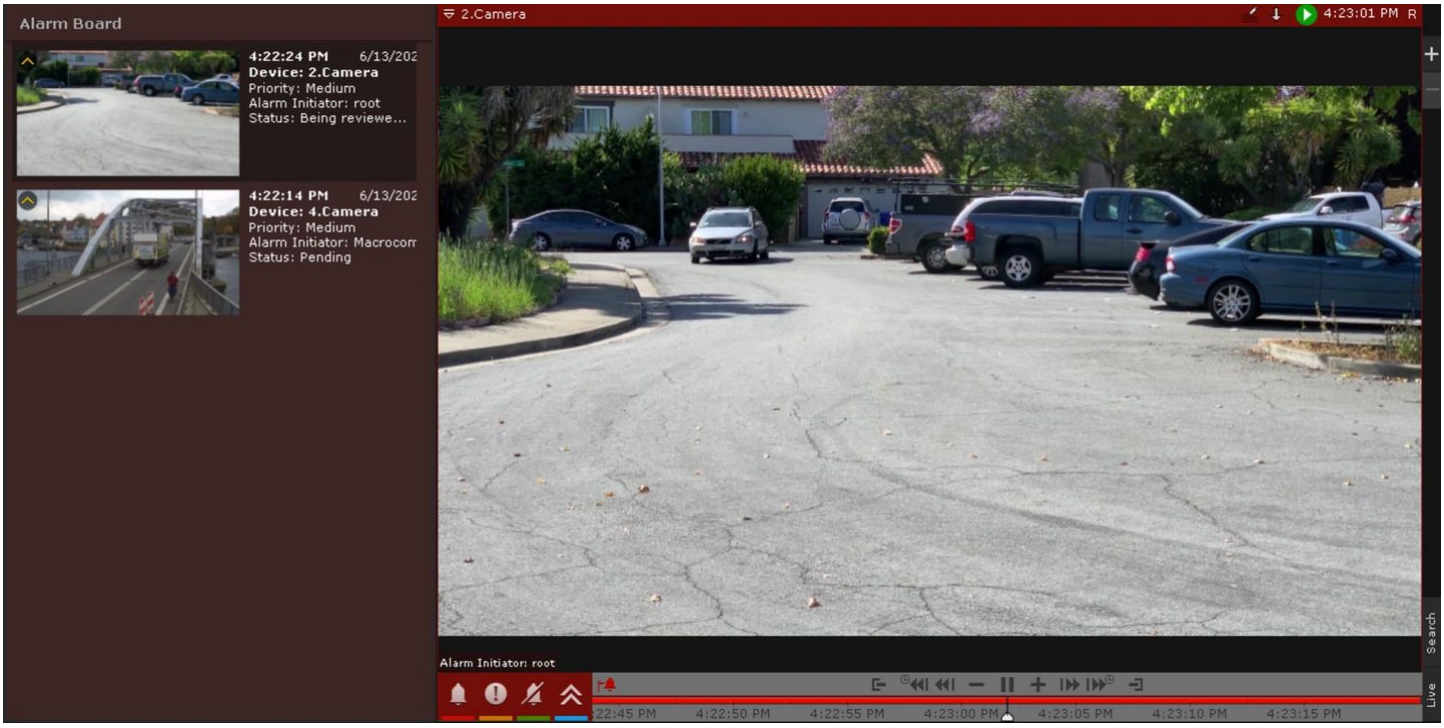


Note

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**.

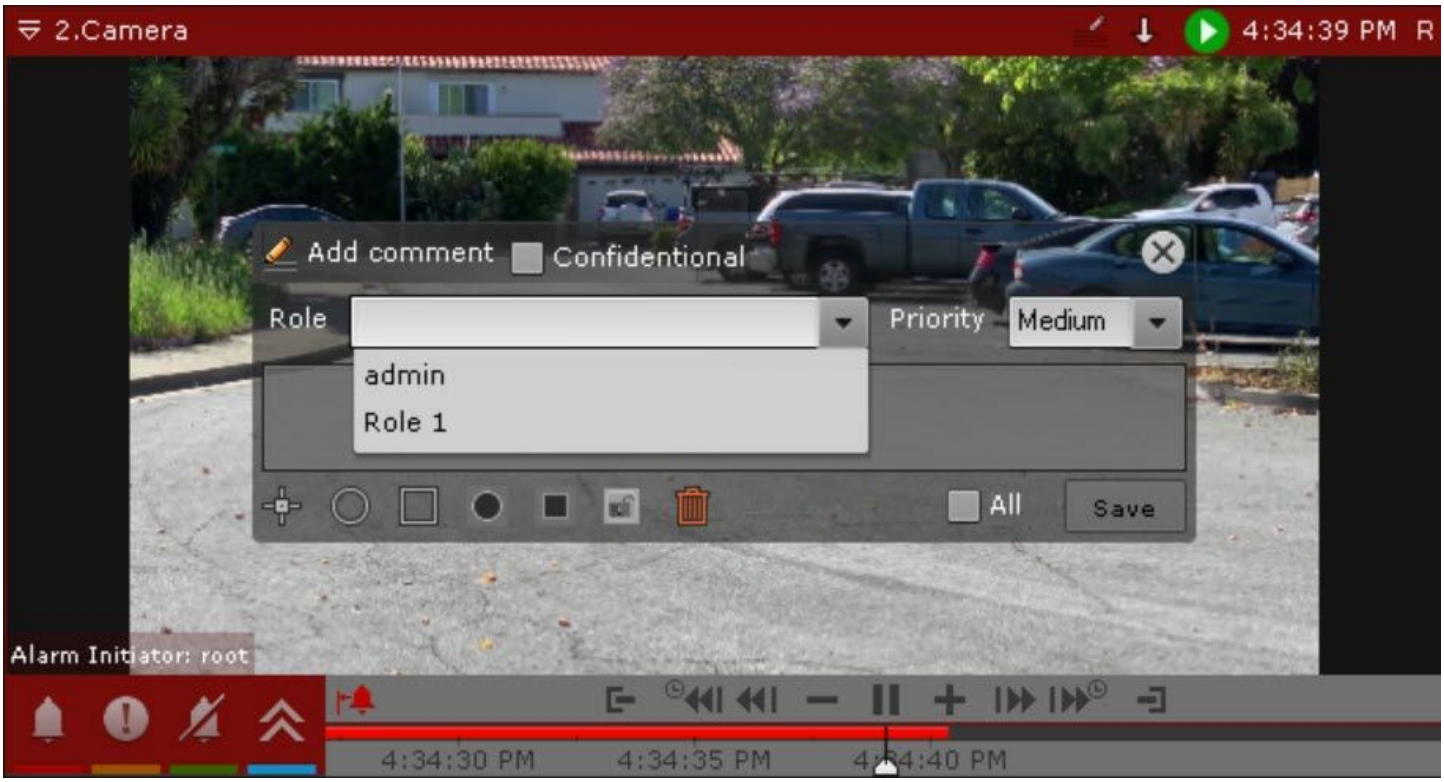


To open a detailed view of an alarm event, double-click the alarm event window on the **Alarm Board**. A detailed view of the alarm event will open. There you can assess the alarm event (see Assessing an alarm event(see page 719)).



Alarm events are displayed in order of priority on the **Alarm Board** (see Initiating an alarm in the system(see page 420)).

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.



16.4 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(see page 644)).

16.4.1 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(see page 648)) or from the Camera Search Panel (see Camera Search Panel(see page 646)) 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(see page 695)), 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.

16.4.2 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(see page 646).

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.

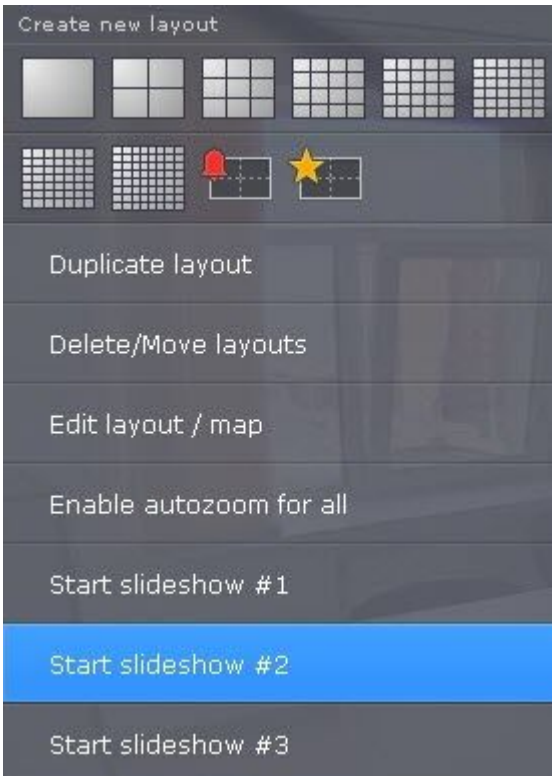
To launch a slideshow, click the button, and select **Start slideshow** in the context menu of the layout panel.

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(see page 554)). Special layouts (see Working with Special layouts(see page 788)) 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(see page 790)), select the required monitor in the Video Wall Management Panel (see Monitor Panel(see page 644)).

To turn off Slideshow mode, select **Stop slideshow** in the context menu of the layouts panel or left-click any viewing tile.

16.4.3 Working with Special layouts

Configuring special layouts(see page 501)

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(see page 719)).

2. After the timeout expires (see Configuring Alarm processing(see page 540)).

> **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

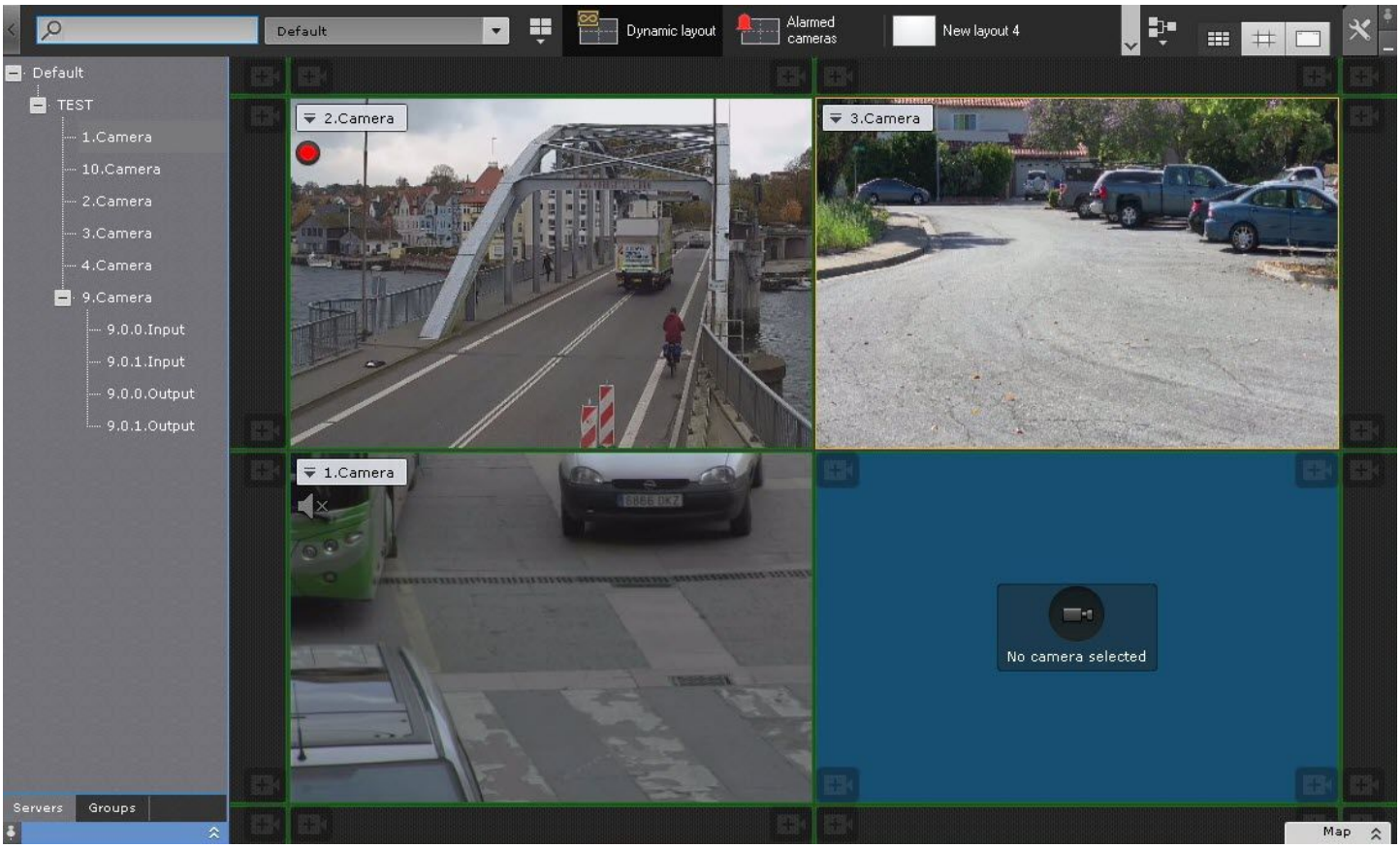
Selected Cameras layout

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(see page 648)) 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(see page 473)).

16.5 Monitor management

16.5.1 Managing monitors on a local Client

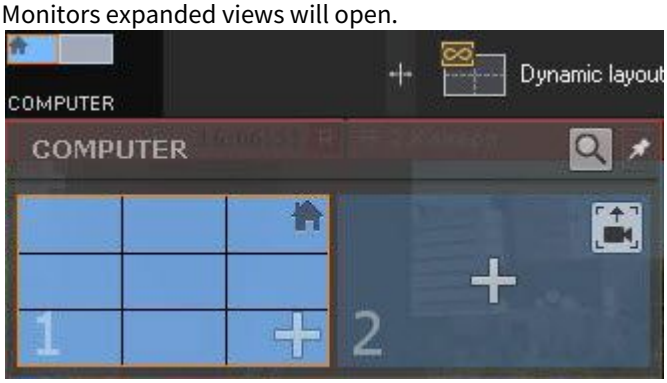
16.5.1.1 **Displaying layouts on monitors**

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(see page 644)).

> **Note**
>
> Client monitor management is regulated by the user rights (see Creating and configuring roles(see page 452)).

Monitors expanded views will open.

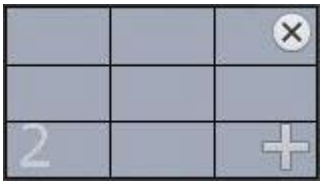
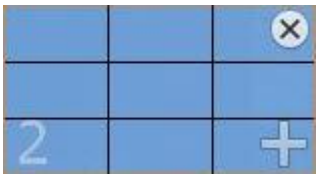


> **Note**
>
> All connected Clients have the NetBiosName name.

> **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

Thumbnail	Monitor status
	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(see page 471)). 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.

16.5.1.2 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.

16.5.1.3 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[191] them:

1. in the cell of the main or additional monitor diagram from the Objects Panel (see Objects Panel(see page 648));
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(see page 795));

191 https://en.wikipedia.org/wiki/Drag_and_drop

3. in the cell of the main or additional monitor diagram from the Camera Search Panel (see Camera Search Panel(see page 646)).

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.

16.5.1.4 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.

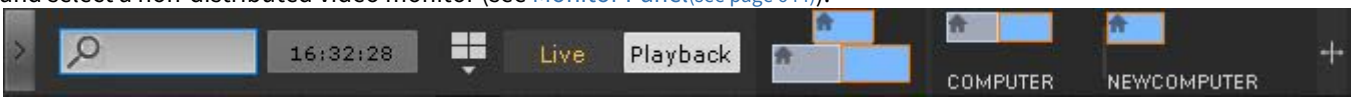
16.5.2 Managing monitors on remote Clients within the Axxon-domain

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(see page 452)).

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(see page 644)).



> **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(see page 790)).

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(see page 786)).
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(see page 644)) or configure (see Creating and deleting layouts(see page 471)) 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(see page 644)).
2. Open the Objects Panel (see Objects Panel(see page 648)).
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[192]).

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.

16.6 Audio Monitoring

16.6.1 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:

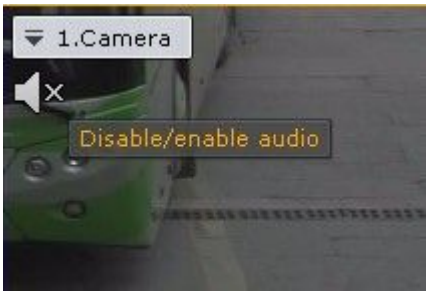
1. Live playback mode – listening to sound from a microphone in real time; playing back sound from Client microphone on camera speakers.
2. Archive mode, Alarm Management mode, Archive Search mode – playback of sound recorded from a microphone.

> **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.

16.6.2 Listening on the Client to sound from a camera microphone

> **Attention!**
>
> The **Microphone** object must be enabled (see the section titled The Microphone Object(see page 163)).

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

192 https://docs.axxonsoft.com/confluence/display/one1en/Working+with+the+interactive+map

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 10. Creating system variable(see page 951)).

16.6.3 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(see page 950)

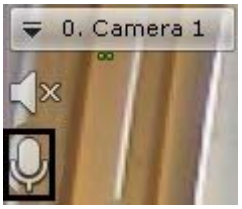
Sound from the Client microphone can be broadcast both on a single camera and on all cameras in a layout.

Attention!

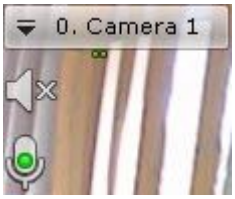
To use this option:

1. Configuration of audio on the Client is now completed (see Configuring audio on the Client(see page 577)).
2. **Speaker** objects are activated for the corresponding cameras (see The Speaker Object(see page 170)).

To broadcast sound on the speaker of a single camera, left-click the microphone icon in the viewing tile.

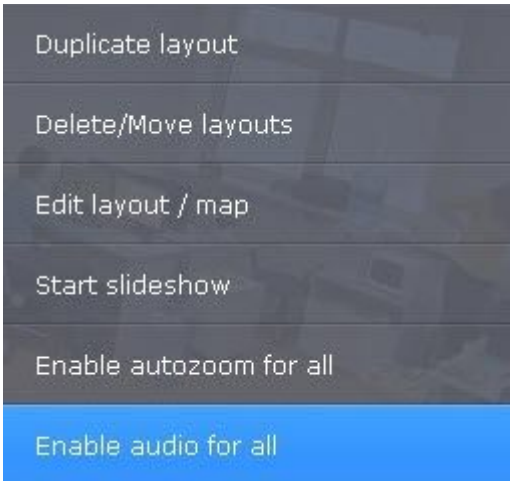


The microphone icon now becomes active.



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**.

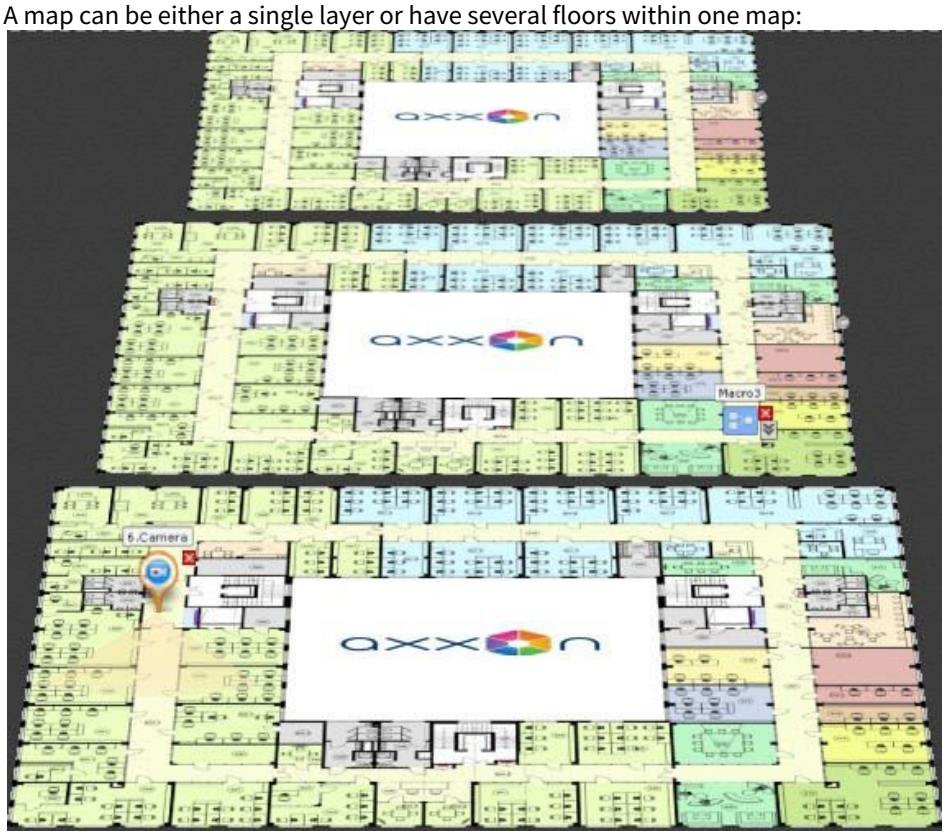
16.7 Working with the interactive map

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:



16.7.1 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(see page 654)).

> **Note**
>
> When you minimize the tile, the map appears again.

16.7.2 Geo map search

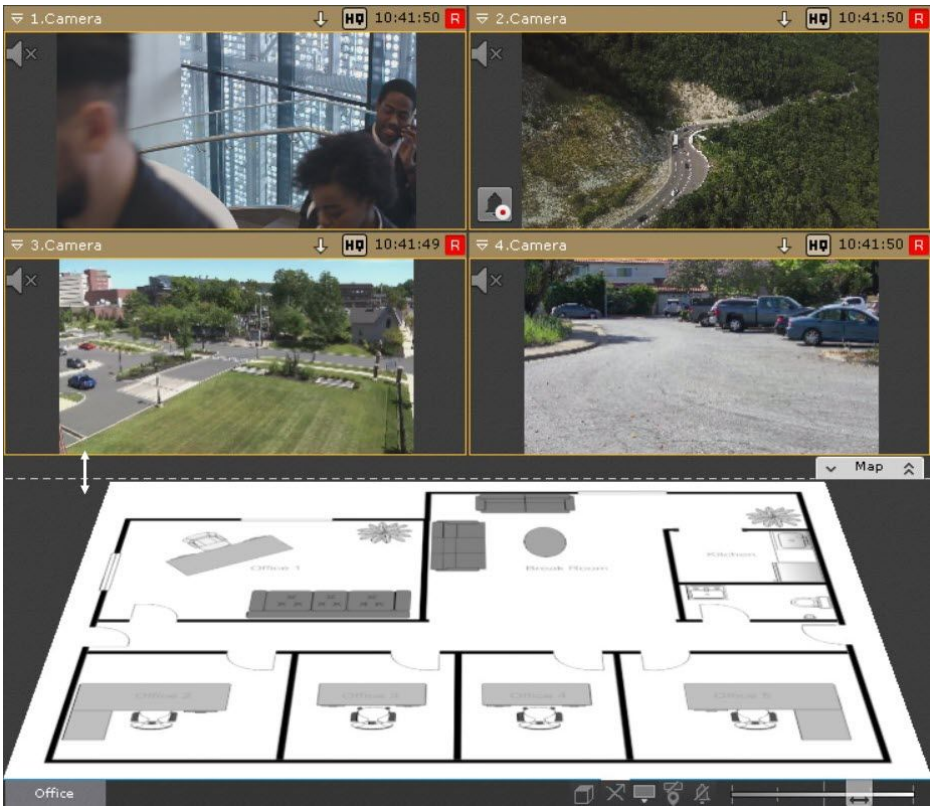
Using the OpenStreetMap web service, you can search for sites or streets within a pre-defined city/town (see Setting keywords for geo map search(see page 523), refer to the provider's website[193] for details).

To do so, enter the street name in the corresponding field, and press **Enter**.

193 https://wiki.openstreetmap.org/wiki/Main_Page

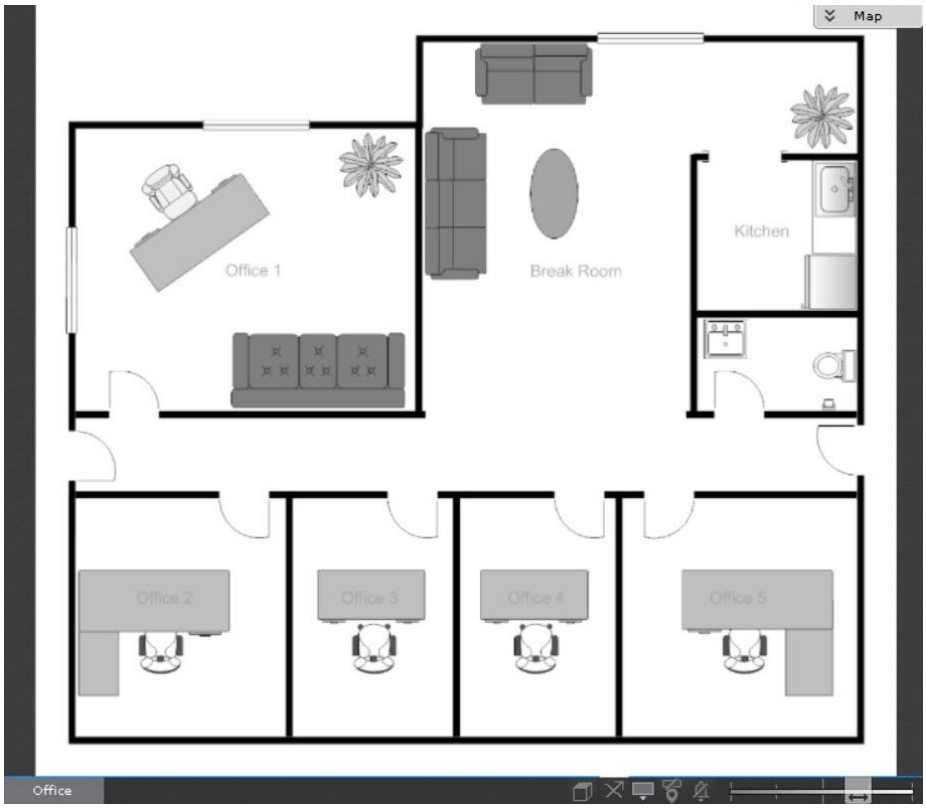
16.7.3 Changing the map tilt

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 .

16.7.4 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(see page 557)).

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.

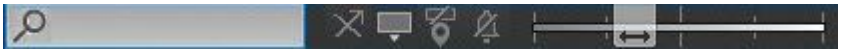
Automatic scaling and focusing of the map stops when the user clicks to select the icon of a video camera on the map or viewing tile.

To manually adjust the map scale, use the mouse scroll wheel (the cursor must be above the map) or use the map scale slider.

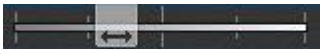
After increasing the scale, you can refocus the map with the mouse (by clicking and holding the left mouse button) in the direction of your choice.

16.7.5 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 adjust transparency of video display in the Map View using a dedicated slider in the bottom right corner.



The leftmost position corresponds to no video, the rightmost makes the video opaque.

Use the / button to toggle the display of devices' names and their IDs.

To enable/disable camera icon fluttering on alarm, use the / button.

To change the action when you click on the video camera icon on the map, use (takes you to the layout with the camera)/ (switches to immersion mode (see Immersion mode(see page 802))).

To change map view, use the button (3D view)/ (flat view).

Video in 3D view:

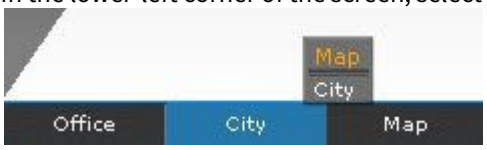
Video in flat view:

16.7.6 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(see page 513)). The icon header shows the name of the destination map.

16.7.7 Immersion mode

In Immersion mode, video from a selected camera is overlaid on the map display.

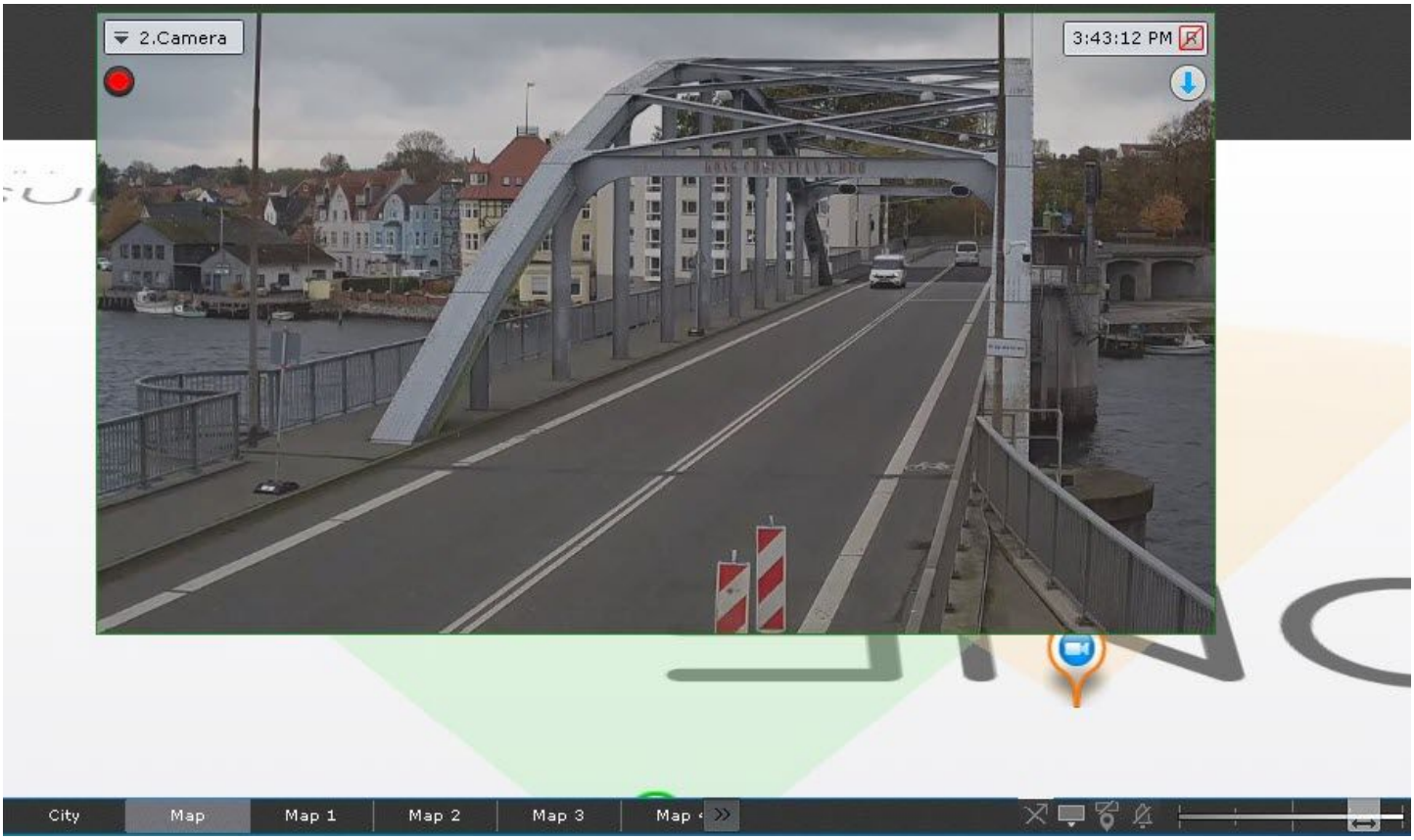
If links have been created between video and the map (see Configuring cameras in immersion mode(see page 517)), an angle will be chosen so that objects in the video match the objects as depicted on the map.

If links have not been created, the map is shown so that the video is located in the field of view specified for the camera on the map. The field of view is oriented upwards.

To switch to Immersion mode, click the button on the right border of the viewing tile or, on the map, left-click a video icon, field of view, or video display area.

Note

The second method is possible if the button is not pressed (see Customizing an Interactive Map(see page 801)).



In Immersion mode you can view video from only one video camera at a time.

To select another video camera, do one of the following:

1. Click the video camera icon or its field of view on the map, if possible.
2. Exit Immersion mode and select the necessary video camera on the map.

To exit Immersion mode, do one of the following:

1. Click the button.
2. Minimize the viewing tile by clicking the button.
3. Click a part of the map that does not contain the camera field of view.

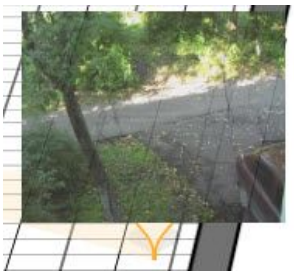
Note

Actions 2 and 3 do not apply if a fisheye camera is in Immersion mode (see Fish-eye cameras in immersive mode(see page 765)).

16.7.8 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(see page 674))	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(see page 807)
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

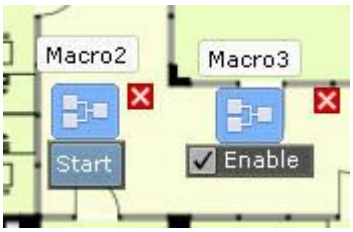
You cannot switch the status of the Output from the map if there are macros with the corresponding action running in the system (see Switch output(see page 422)).

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

16.7.9 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.

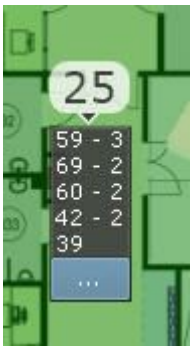
Map icon	Input status
	Video camera is armed, Input is in normal status
	Video camera is armed, Input is in alarm status
	Video camera is disarmed, Input is in normal status
	Video camera is disarmed, Input is in alarm status

Inputs (sensors) connected to Tibbo boards also show temperature/humidity values on the map (see Setting up Tibbo relay/loop boards(see page 187)).

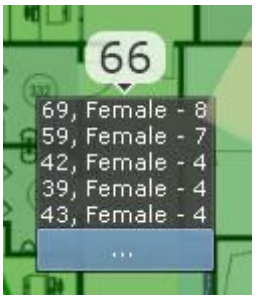
16.7.10 Displaying the counters

Counters on the map show the results of counting some values using events (see Adding counters(see page 513), Creating and configuring counters(see page 405)):

If grouping by events is configured for the counter, then in addition to the total number of events, the results of counting by groups will be displayed. In this case, the names of the groups correspond to the specified properties of the grouping. In the example below, the **Age** property is set:



If multiple properties are specified for a grouping, then the groups that combine these properties will be displayed. In the example below, the **Gender** and **Age** properties are set:



In the example above, **69** in the first line is the age, **Female** is the gender, and **8** is the number of women at the age of 69. The same goes for the rest of the lines.

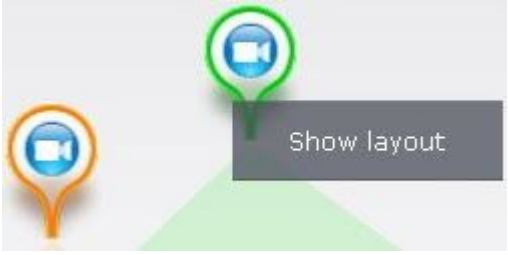
To view all lines, click the button.

16.7.11 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.

16.8 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(see page 875) 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.

16.8.1 Frame export

You can export snapshots at any time when working with a camera in *Axxon One*.

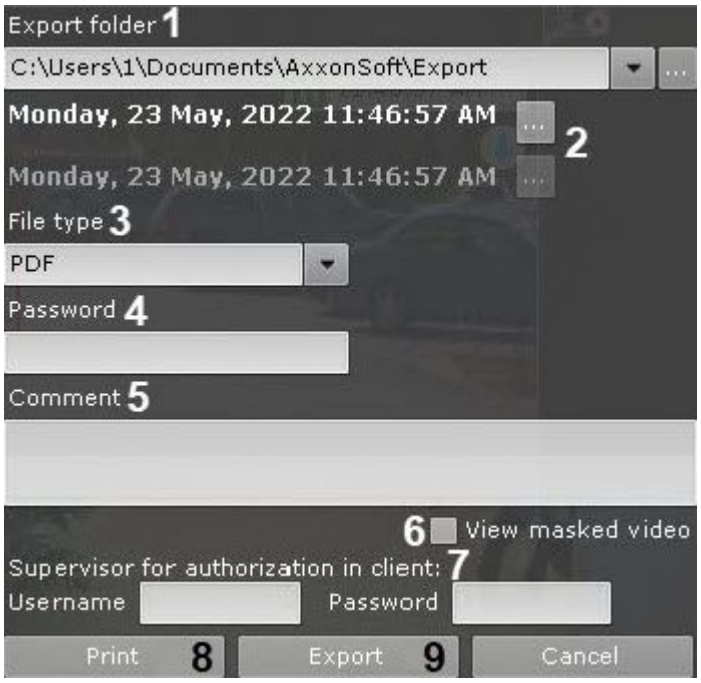
To export a snapshot:

1. If exporting from archive mode or archive analysis mode, specify an export area and mask if necessary (see the Configuring export area and masks(see page 816) section).
2. In the viewing tile, in the upper-right corner, click the button.

   > **Attention!**
   >
   > To instantly export a frame with standard settings, right-click the button.

3. Specify the folder to which you want to export the snapshot (**1**).

   > **Note.**
   >
   > By default, snapshots are exported to the folder specified in the export settings (see the Configuring export(see page 572) section).
   > If you change this folder, the new path to exported files will be kept in memory until the Client restarts.



4. Select the date and time for a snapshot (**2**). The default setting is the frame currently displayed in the viewing tile. If you are watching recorded video, then the snapshot with the frame displayed at the time when you hit the button.

> **Note.**
>
> If you are watching live video, then the snapshot with the frame displayed at the time when you hit the button. Date and time fields are not displayed.

5. Select the snapshot format: PDF or JPG (**3**).
6. If you want to export a snapshot to an encrypted zip archive, set a password (**4**).

> **Attention!**
>
> This setting may be overridden by the user role settings (see Creating and configuring roles(see page 452)).

7. If exporting a snapshot to PDF format, you can add comments (**5**).
8. To export unmasked frames from the Video Footage, the user must have appropriate access rights. To perform such an export, check the **View masked video** box (**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 rights settings. If no export confirmation is required, these fields will not be displayed.

10. If exporting to PDF, you can immediately send the file to print (**8**). In this case, the snapshot is not saved to disk.
11. To export the snapshot, click the corresponding button (**9**).

Export begins. Progress is shown in the export panel (see the Viewing export progress(see page 817) section).

Export of the frame is now complete. The frame exported to JPG will also be placed on the Clipboard.

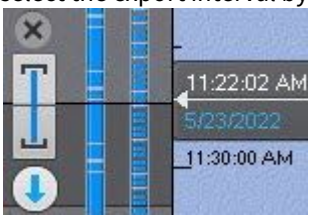
16.8.2 Exporting Video Recordings

16.8.2.1 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;

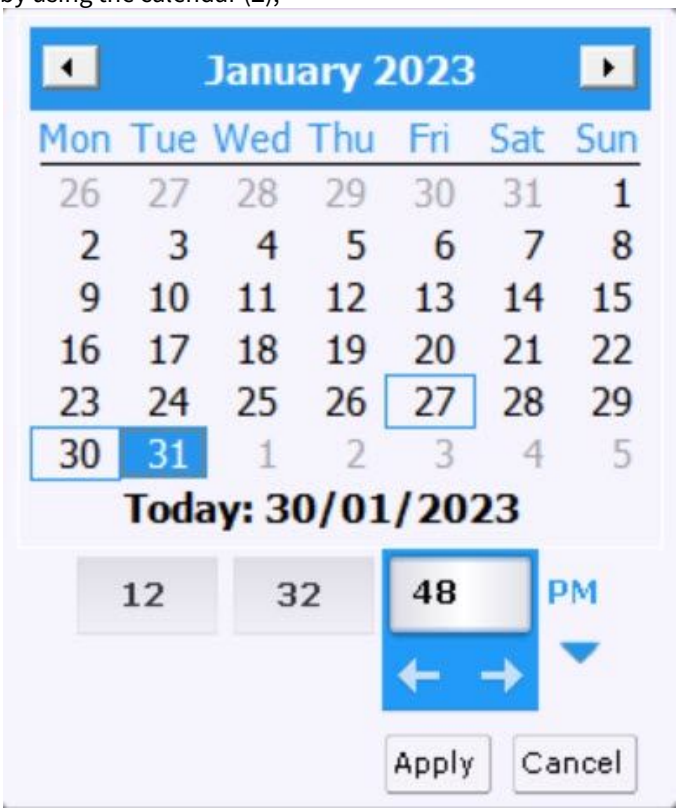
   b. you can specify the interval on the additional navigation panel in the same way, by clicking the buttons. You cannot use the mouse to select the export interval on the additional navigation panel.

2. Setting the export area and masks (see the Configuring export area and masks(see page 816)).
3. Setting the export format.

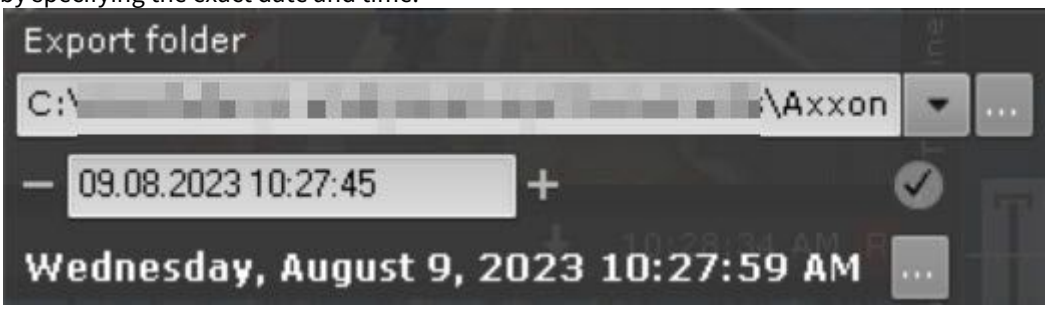
   a. Click the button on the timeline or in the surveillance window.
   The export window opens.

   b. If necessary, change the export path (**1**). By default, the file is exported to the folder specified in the settings (see Configuring export(see page 572)). 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.

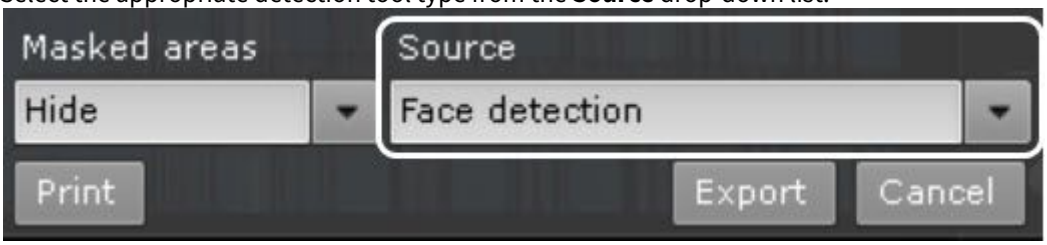
> **Note**
>
> Video recordings are exported into the MKV format without recompression.
> Video recordings are exported into the AVI format with recompression by the codec selected in the settings. Export into the AVI format may take longer because of recompression. In addition, the AVI format export increases the CPU load, especially when you export several files at once (see Simultaneous export of video from multiple cameras(see page 813), Exporting all event videos(see page 814)).
> 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.

> **Attention!**
>
> If you export video recordings from the fish-eye 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[194]) 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(see page 452)).

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 appropriate detection tool type 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.
    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(see page 452)). 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(see page 817)).

> **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.

16.8.2.2 Instant video export

You can instantly export video without specifying an export range. To do so, click the button in the surveillance window at any time.

> **Note.**

194 https://docs.axxonsoft.com/confluence/display/player/The+Axxon+Player+User+Guide

Then specify export settings, as described in Standard video recordings export(see page 809).

If export is performed from the Live Video mode, the first frame of the exported video will be the moment when the button was clicked. Export will continue for 10 minutes or until the **Stop** button on the export panel is clicked (see Viewing export progress(see page 817)).

If export is performed from 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 was clicked. Export will continue for 10 minutes, or until the end of the archive, or until the **Stop** button on the export panel is clicked (see Viewing export progress(see page 817)).

The length of the exported video recording will depend on the time of export and resources of the Server.

Note.

If export is performed from the archive mode or the archive analysis mode, you can pre-configure an export area and masks (see Configuring export area and masks(see page 816)).

If you right-click on the button in the surveillance window at any time, the frame will be exported in JPG format.

16.8.2.3 Simultaneous export of video from multiple cameras

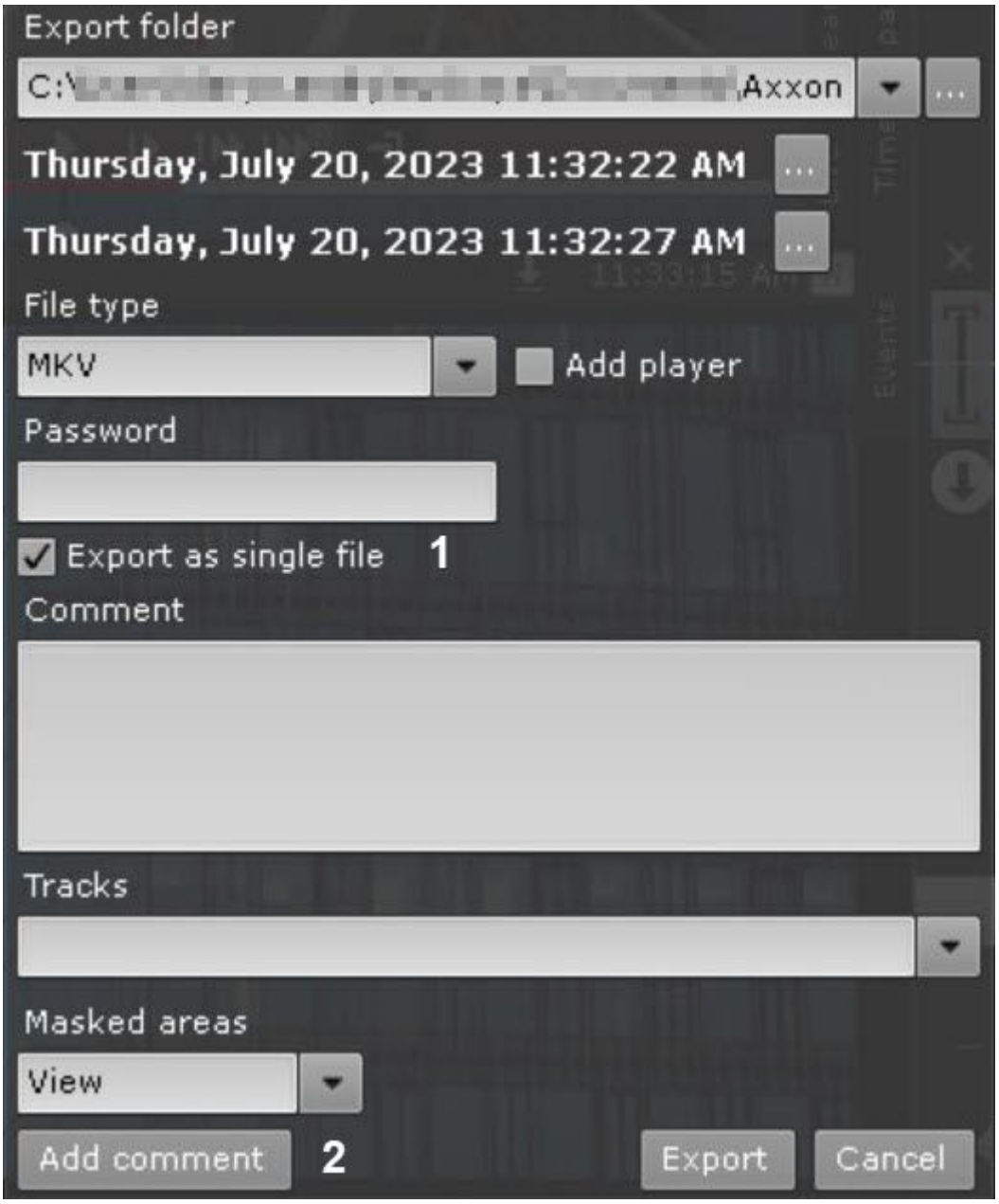
If multiple cameras in a layout have been switched to Archive mode, you can simultaneously export video from all of them.

To do this, select the export interval on the primary timeline or in the calendar and start exporting (see the Standard video recordings export(see page 809) section).

By default, the video is exported to a single file. To export video from different video cameras to separate files, deselect the **Export as single file** check box in the export window (**1**).

Note.

When you export to one file, the streams are written in parallel. To view exported video, use a player that allows playing multiple instances and different streams in each (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 the Configuring export area and masks(see page 816) section).

16.8.2.4 Exporting all event videos

You can use the Story board (see Story board(see page 652)) for one-click export of an event video from multiple cameras' Video Footage.

To do so, follow the steps below:

1. Click on the thumbnail of interest.

2. Set a time interval on the timeline for export.
   This will add the thumbnail of the selected video clip to the Story board.

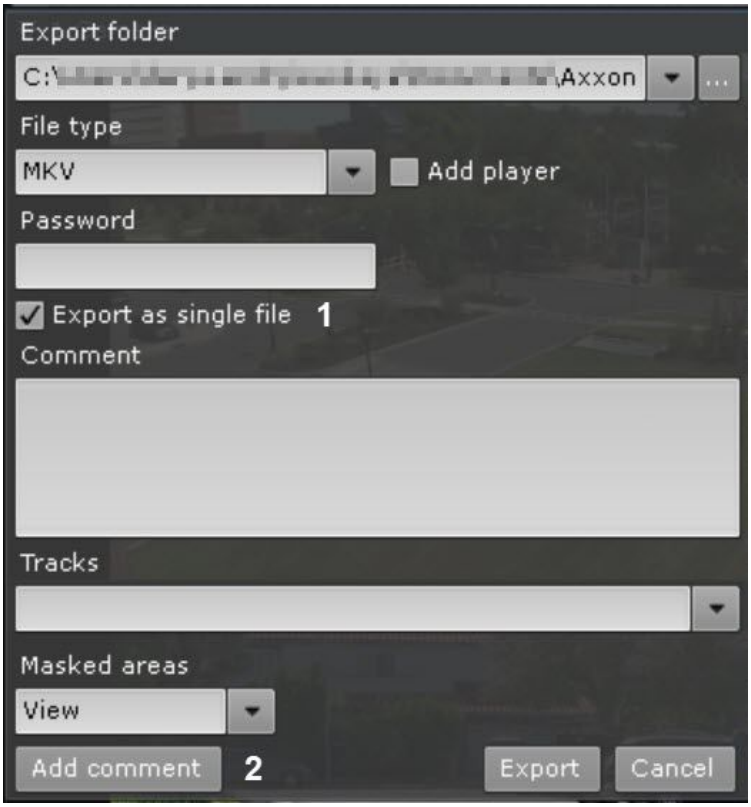
3. Click the **+** button in the middle of the thumbnail. The video clip will be added to the export batch.

> **Note**
>
> To remove it from the batch, click the button.

4. Repeat these steps for all videos of interest.
5. Click the button to export all selected clips.

By default, the video is exported to a single file. To export video from different video cameras to separate files, deselect the **Export as single file** checkbox in the export window (**1**).

> **Note.**
>
> When you export to one file, the streams are written in parallel. To view exported video, use a player that allows playing multiple instances and different streams in each (for example, VLC).



This opens the Export window. Follow the same steps as with the standard export procedure (see Standard video recordings export(see page 809)).

> **Note**

We recommend you to export to the EXE format.

Comments made during export are added to each exported video (**2**).

16.8.3 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:

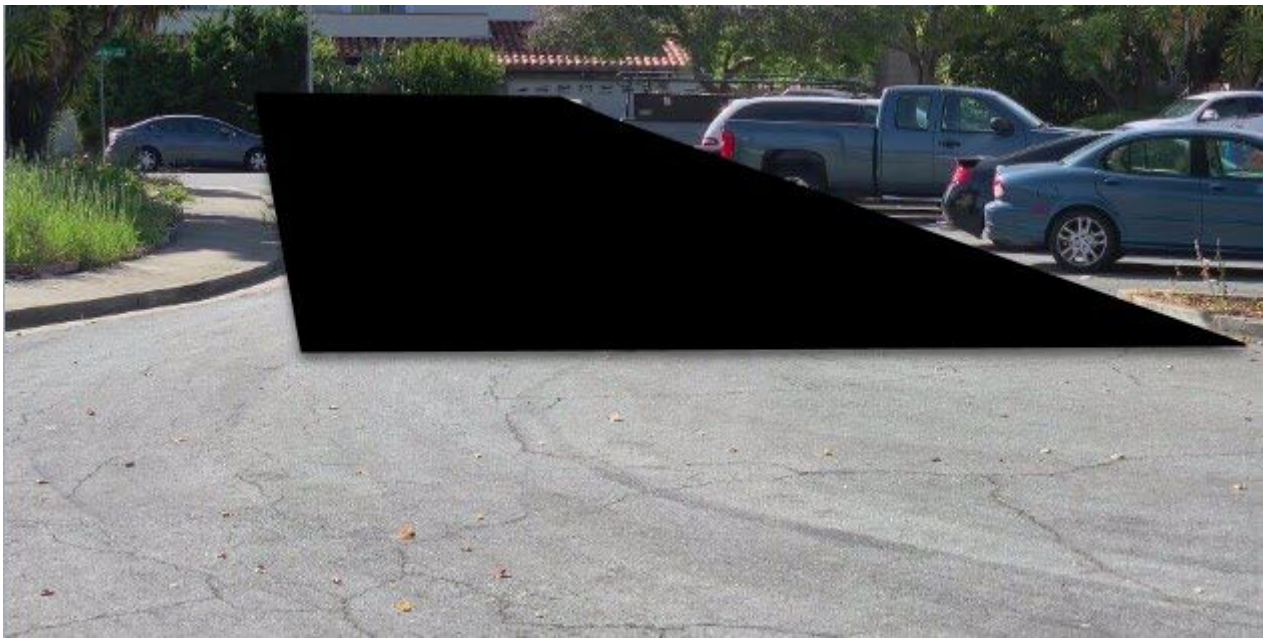
1. In a viewing tile, click the button.
2. Use the corner points to enclose the area that you want to mask. To add a corner point, left-click the video. You can add an unlimited number of corner points.

   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.



16.8.4 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(see page 818)).

16.9 Macros control

You can manage macros from the map (see Controlling devices from the map(see page 803)) or from the menu on the top panel.

A macro may include settings (see Create Macros(see page 403)) 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(see page 403)), 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(see page 782)) or by using hotkeys.

16.10 Event control

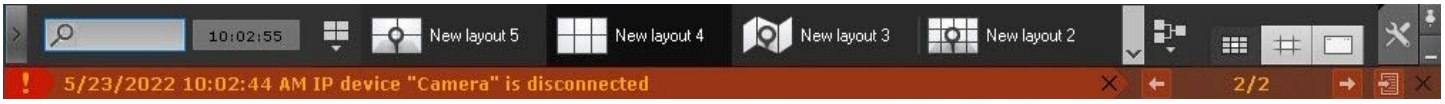
Event control in the *Axxon One* software package can be conducted in three ways:

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(see page 870)).

16.10.1 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(see page 452)).

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.

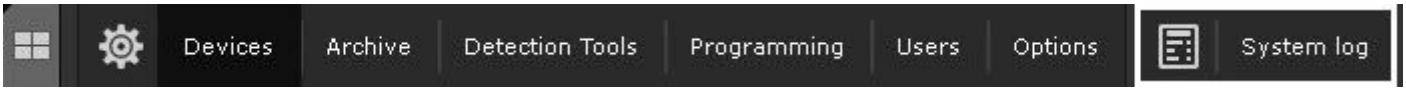
To switch between error messages, click the buttons.

To jump to System log (see The System Log(see page 819)), and open error messages, click the button.

16.10.2 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.

16.10.2.1 Setting Event Search Filters

To view and/or export system log events, first you need to perform a search for them.

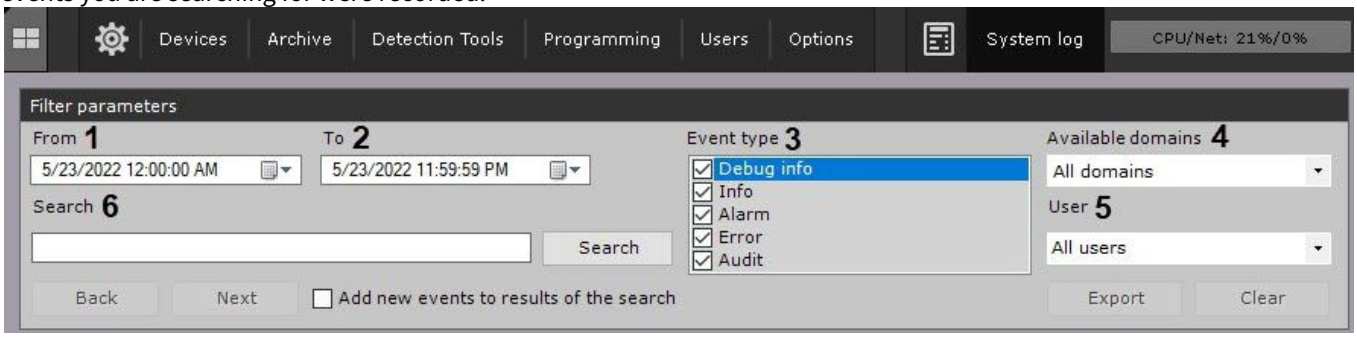
To search for system log events, you need to set one or more filters:

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!

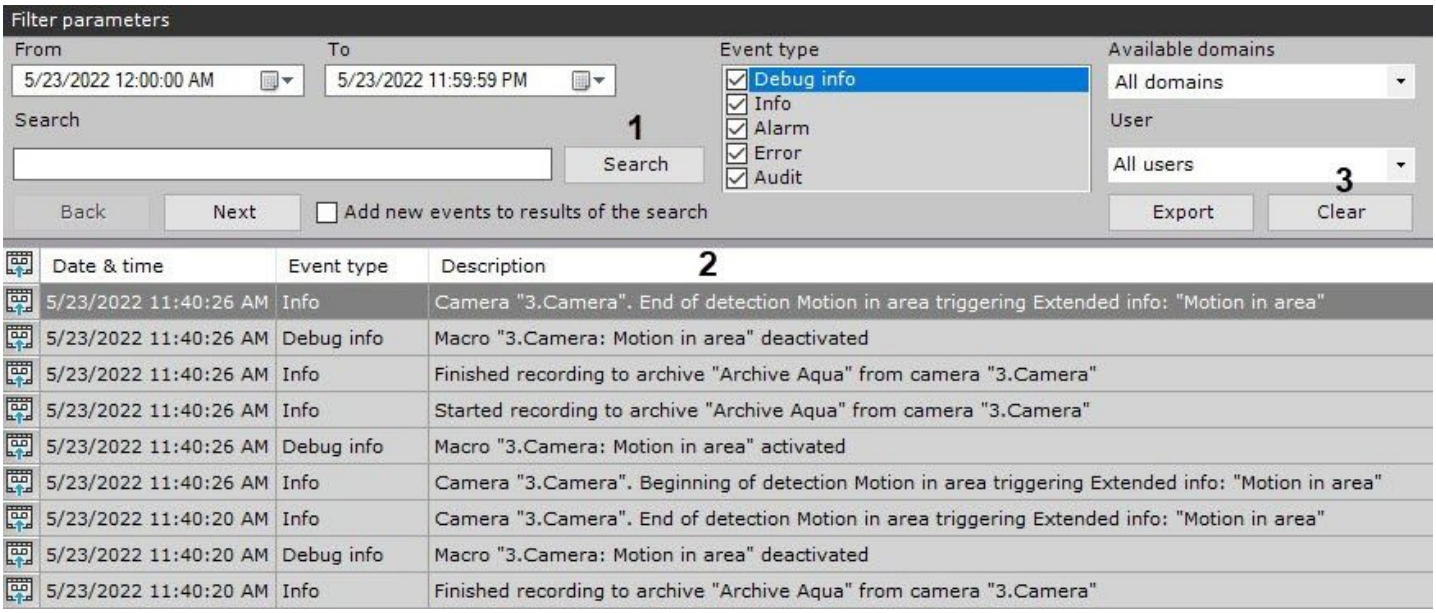
You can use OR and AND logical operators when searching data in the system log:
- to search with the OR logical operator, separate the words with the symbol "|";
- to search with the AND logical operator, use a space.

The event search filters have been set.

Next you must start the event search (see the section titled Event search procedure(see page 820)).

16.10.2.2 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(see page 819)), click the **Search** button (**1**).

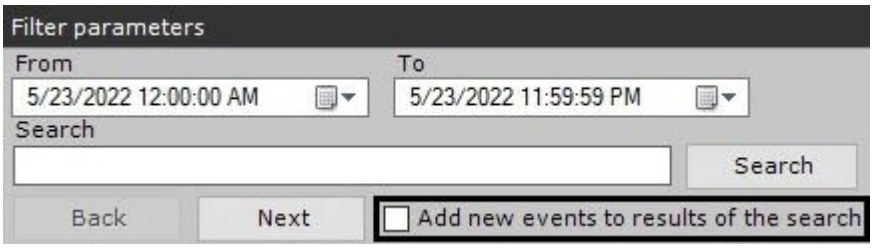


When you do that, a search results table appears (**2**).

To accept all errors and close the error panel, click the **Clear** button (**3**).

16.10.2.3 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(see page 820)). 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.

16.10.2.4 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.

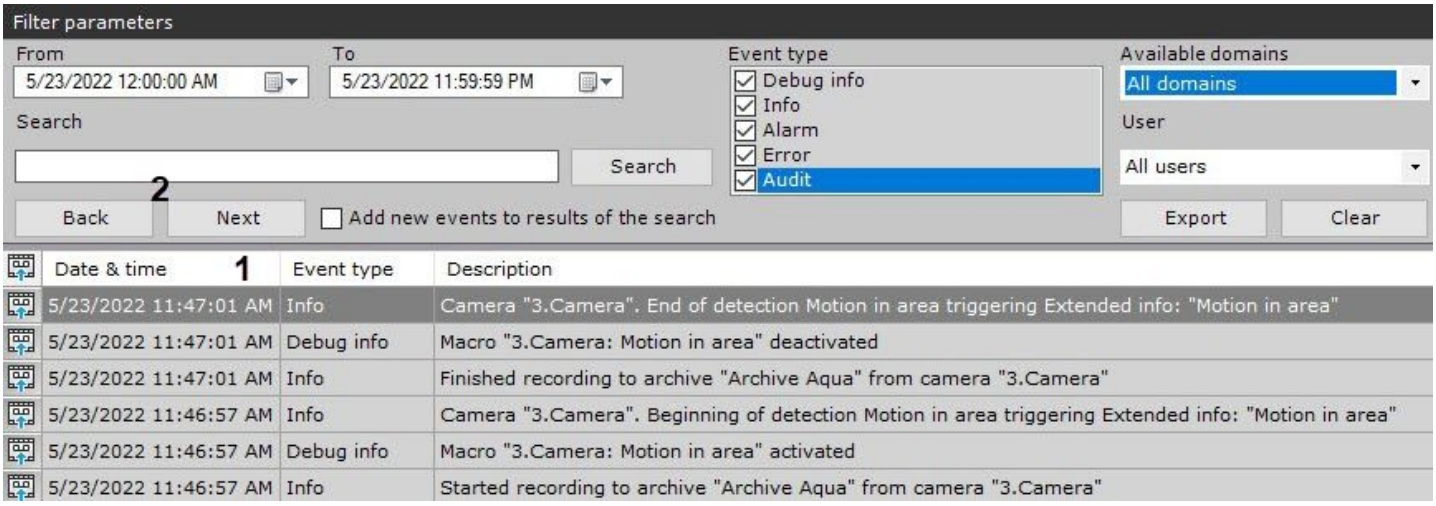


Table column	Contents of column
	Switching to archive video of specific events
Date & time	Date and time of the event was recorded in the system in the format DD.MM.YYYY HH:MM:SS
Event type	Event type (Information, Alarm, Debug info, Error)
Description	System description of the event

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**):

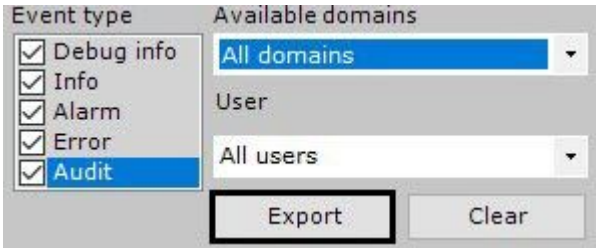
1. **Back** – go back to the previous page of the table.
2. **Next** – go to the next page of the table.

Note

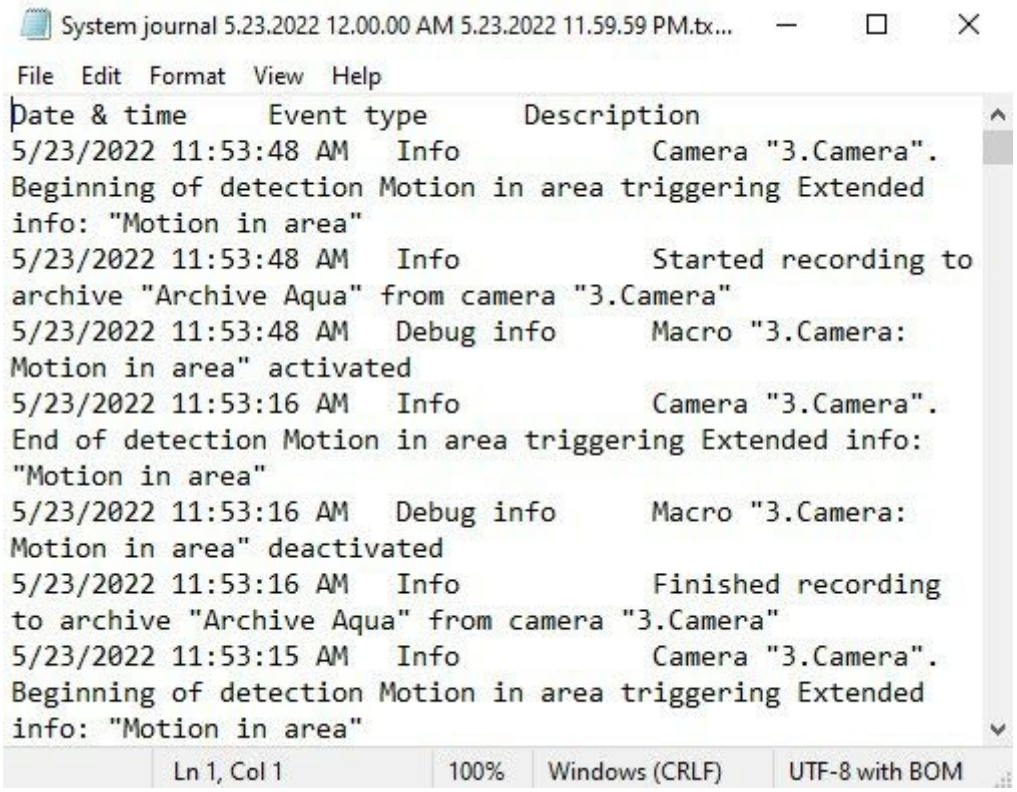
Once the *Axxon One* VMS is installed, the log may show a **Table end violation** error**.** This is part of the installation routine and not a bug.

16.10.2.5 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).



16.10.2.6 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(see page 166), The Output Object(see page 169)).

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.

16.11 Working with Axxon One through the Web-Client

16.11.1 Web-Client overview

The Web-Client offers the following options:

1. Viewing live videos(see page 838).
2. Controlling PTZ cameras(see page 841).
3. Viewing Archive(see page 843).
4. Archive search(see page 847).
5. Listening to a camera's microphone(see page 854).
6. Exporting still frames and videos(see page 854).
7. Digital zooming(see page 854).
8. Working with bookmarks(see page 857).
9. Viewing Camera and Archive Statistics(see page 856).

16.11.2 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.

16.11.3 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:

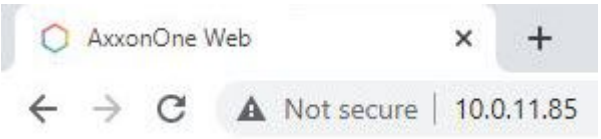
1. Start a web browser.

2. In the address bar, enter the address of the *Axxon One* Web-Server in the following format: <Web-Server IP address>:<Port>/<Prefix>.

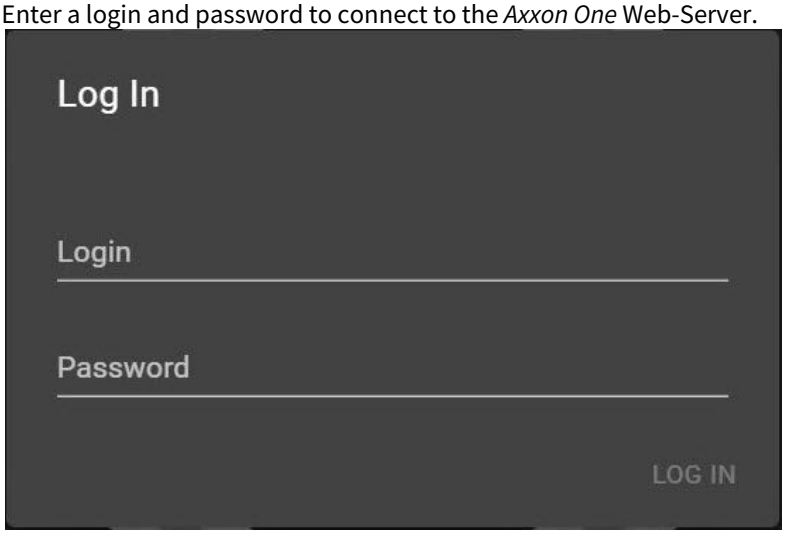
Connecting the Web and Mobile Clients to the Server behind NAT(see page 948)

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(see page 119)).
- A connection via the secure HTTPS protocol will be automatically established, if the Web-Server is configured accordingly (see Configuring the Web-Server(see page 119)).

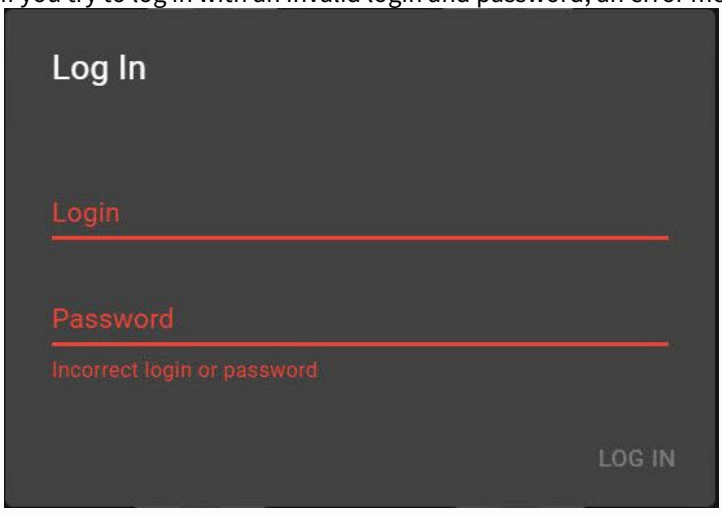


3. Enter a login and password to connect to the *Axxon One* Web-Server.



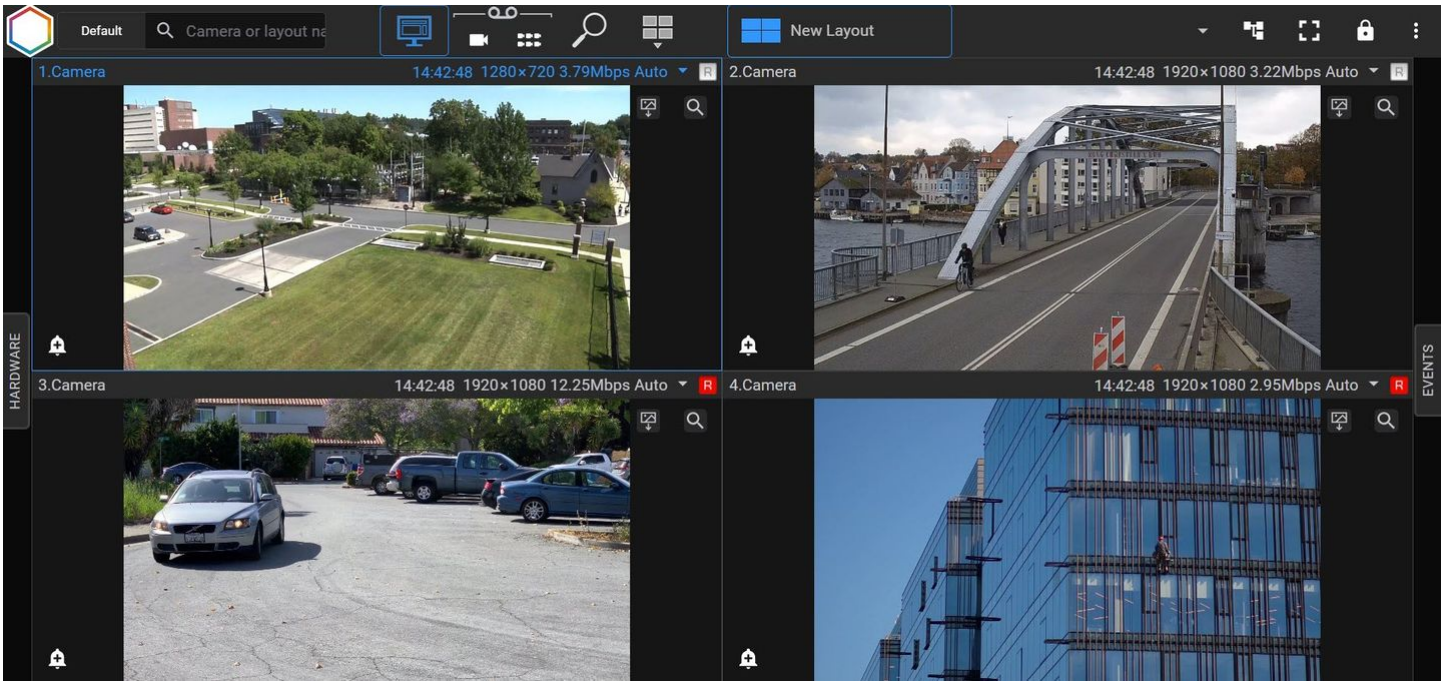
Note

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.

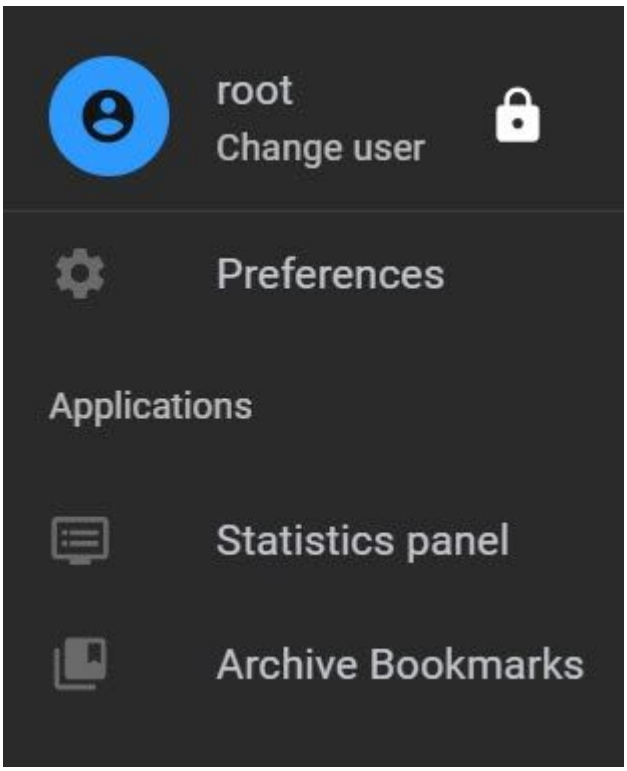
As a result, the Web-Client interface will be displayed. By default, the first listed layout will be displayed. If there are no layouts, the Cameras panel will open on the left and the video image from the first listed video camera will be displayed.



16.11.3.1 Changing the user in the Web-Client

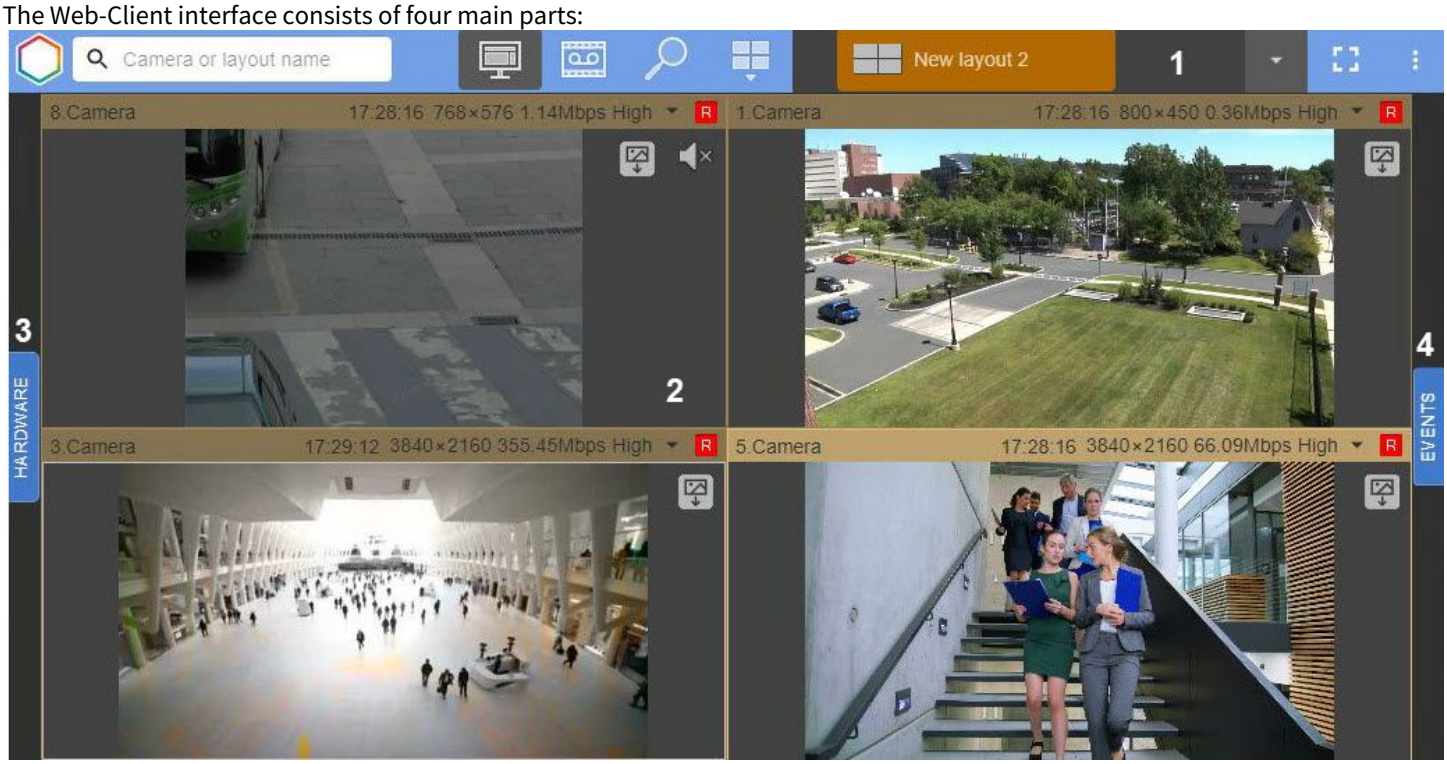
To change the user in the Web-Client, click the button in the top right corner and select the **Change user** menu item.

> **Note**
>
> The name of the current user is displayed next to this item.



16.11.4 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(see page 830));
   b. the button to go to the real-time video surveillance mode (see Real-time video surveillance in the Web-Client(see page 838));
   c. the button to view the camera archive (see Viewing video archives through the Web-Client(see page 843));
   d. the button to go to the archive search mode (see Archive search in the Web-Client(see page 847));
   e. the layouts menu and the list of available layouts (see Working with layouts in Web-Client(see page 832));

   > **Attention!**
   >
   > The Web-Client displays the layouts available to a particular user. The number of cameras on the layouts is unlimited.

   f. the full-screen mode button ;
   g. 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.
   h. the three-dot menu button (see Web-Client configuration(see page 827), Viewing Camera and Archive Statistics(see page 856)).
2. The Surveillance window (**2**), (see Surveillance window(see page 628) in the Client). Each surveillance window includes:
   a. the export button (see Export in the Web-Client(see page 854));

b. the button to go to the quick search mode (see Archive search in the Web-Client(see page 847));

c. the button to trigger an alarm (see Viewing and processing alarms in Web-Client(see page 852)).

3. The **Hardware** panel (**3**) that displays all available cameras (see Searching for video cameras in the Web-Client(see page 830)).

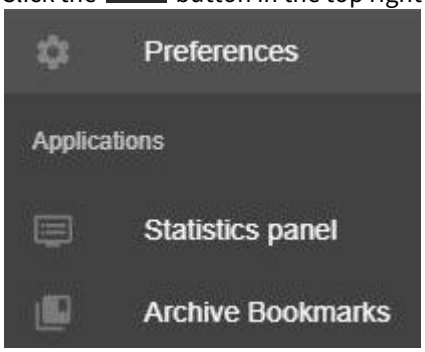
> **Note**
>
> In the Web-Client interface, you can change the width of the **Hardware** panel. To do this, point the cursor to the **Hardware** panel, hold down the cursor and drag it to the left or right.
>
>
>

4. The **Events** panel (**4**) that displays the selected system events.

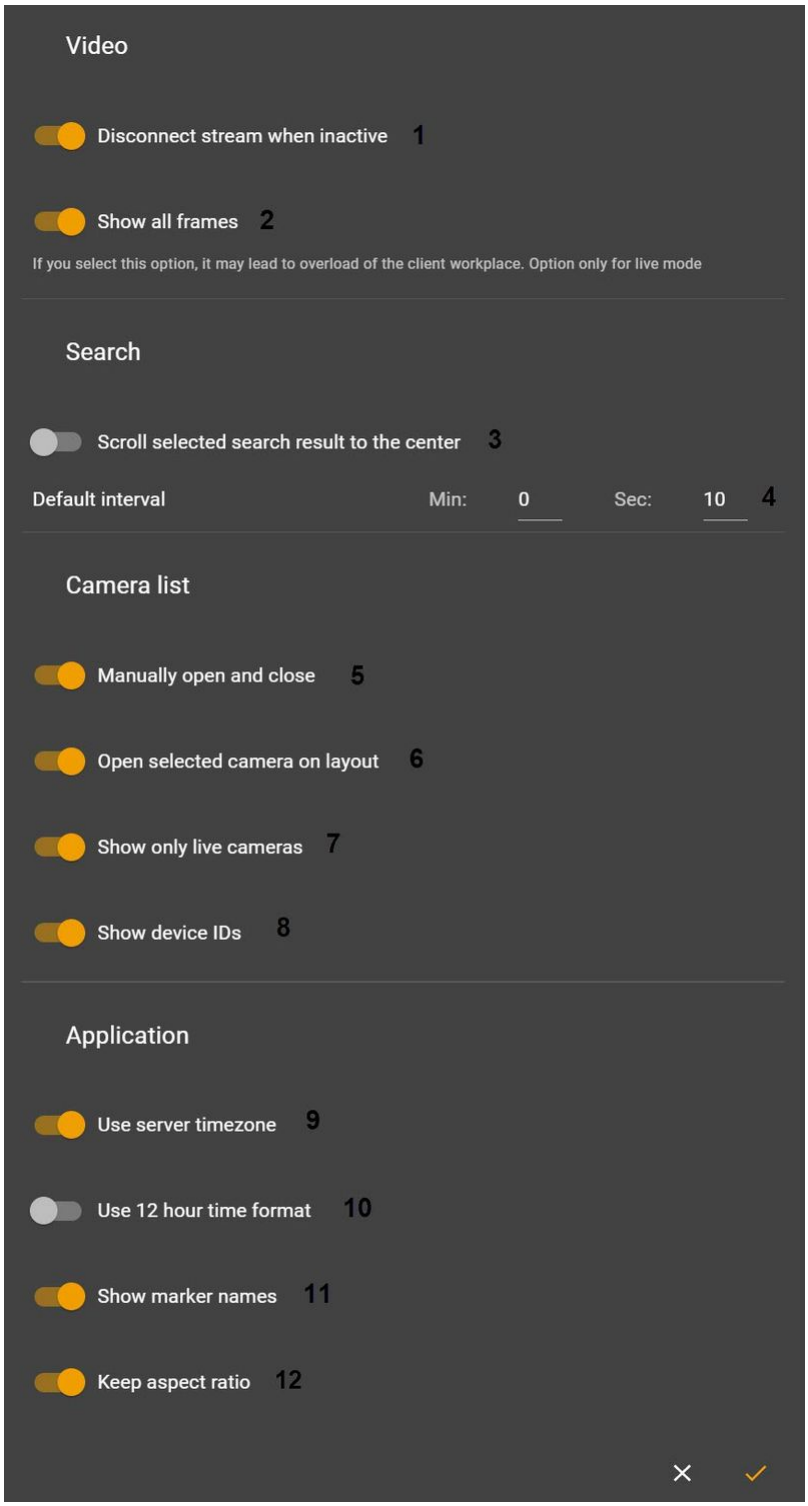
16.11.5 Web-Client configuration

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.



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.

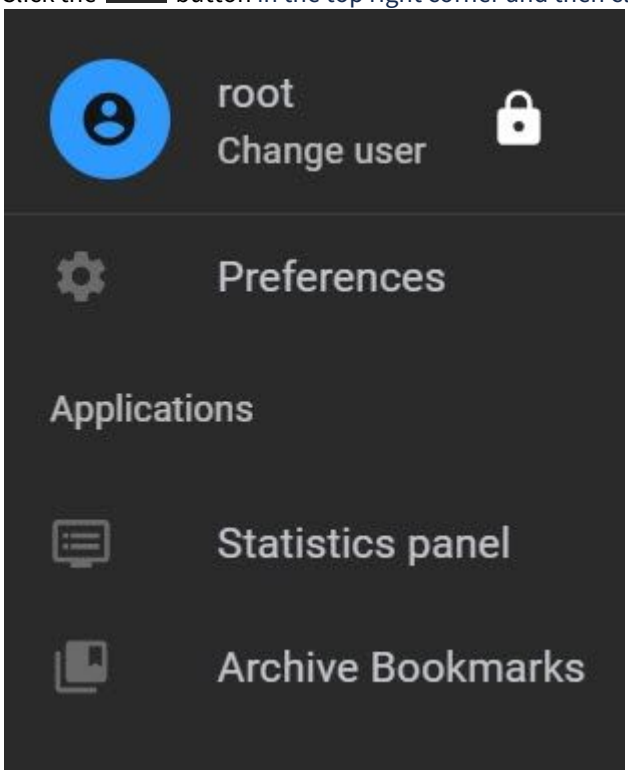
5. Set the default interval for the TimeSlice (**4**, see Types of archive search in the Web-Client(see page 849)). This setting is common to all Web-Client users in a particular browser.
6. By default, the Cameras panel does not close after you select a device. To minimize the panel, disable the **Manually 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 **Show 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. If you want the time to be displayed in the 12-hour 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.

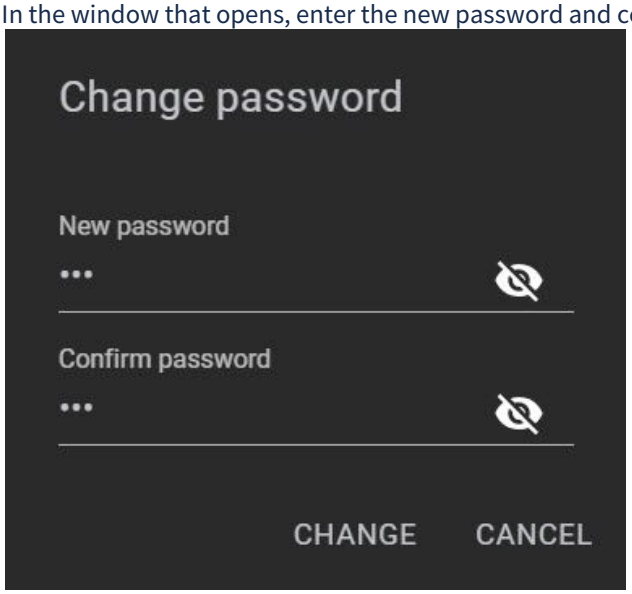
16.11.5.1 Changing the user password in the Web-Client

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.

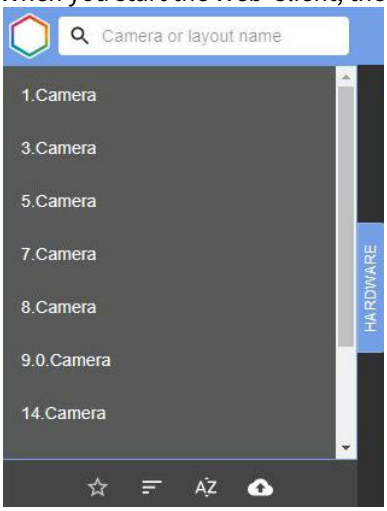


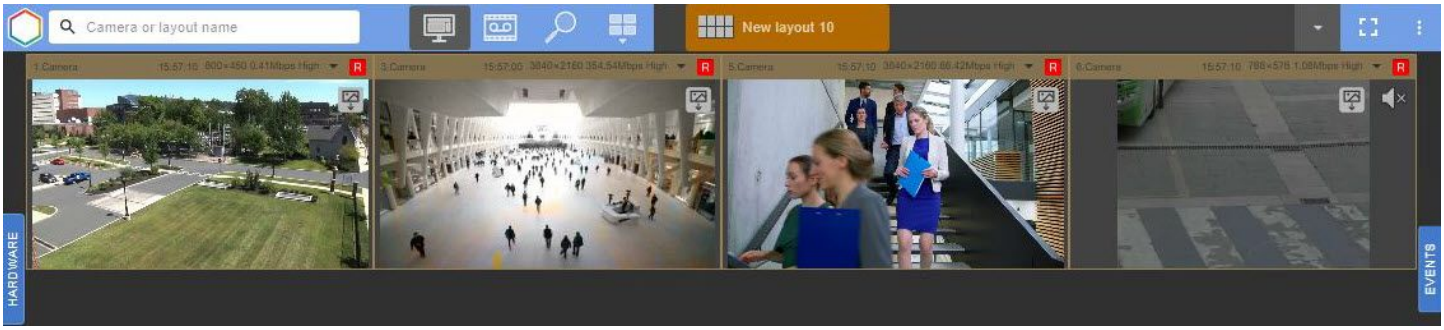
3. Click the **Change** button.

Changing the user password in the Web-Client is complete.

16.11.6 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

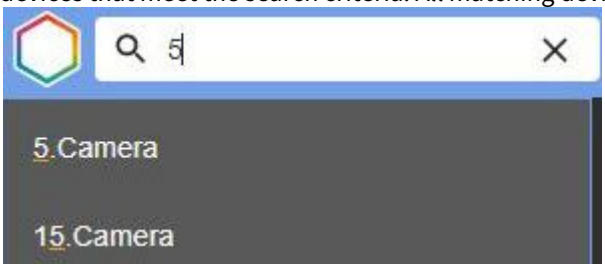
2. Click the button and select the file.

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.



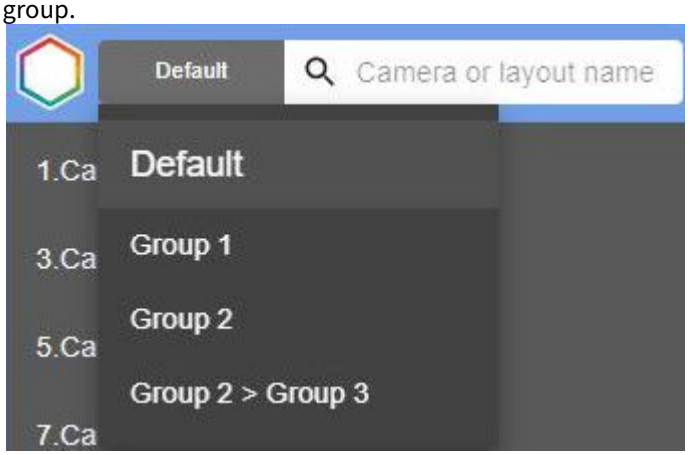
Note

The search result includes both the list of cameras and the list of layouts.

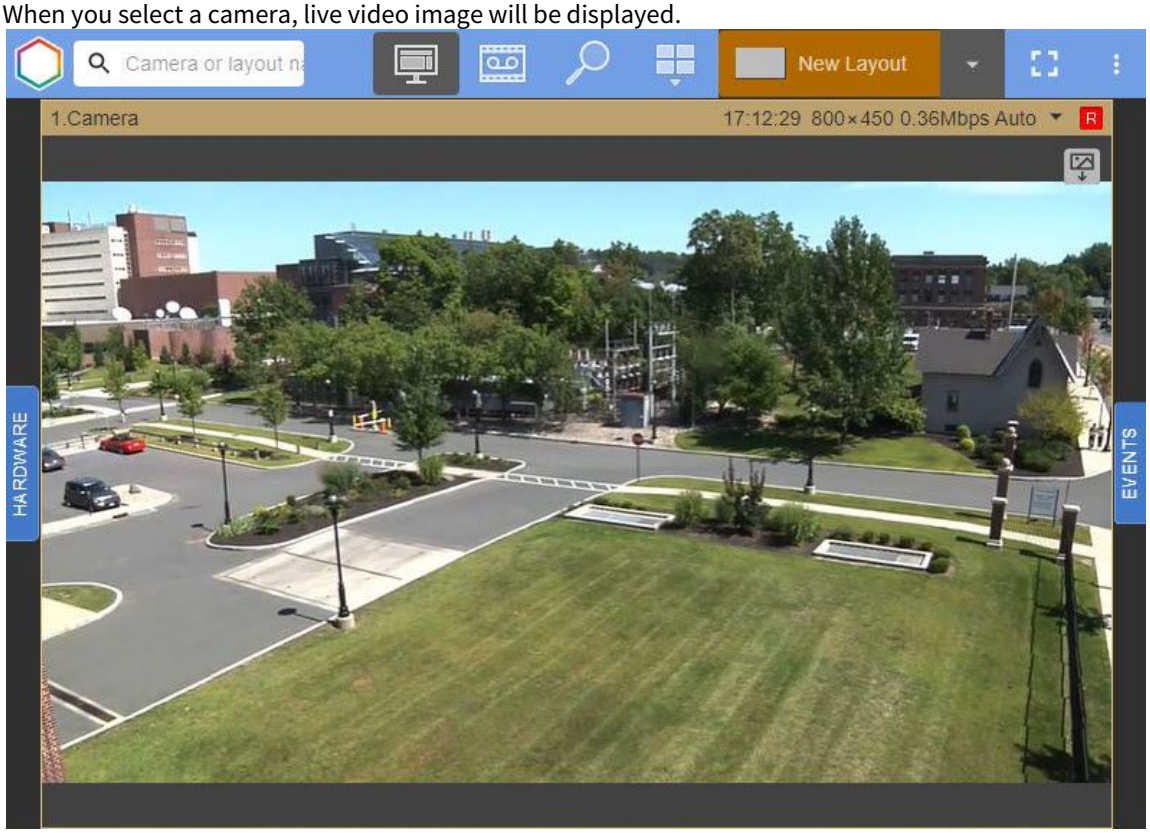
Note

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(see page 200)), 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:

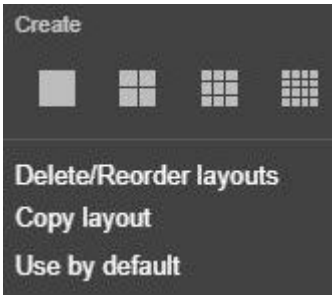
- time display (see Time Display(see page 631) in the main Client);
- video stream parameters;
- archive recording indicator.

16.11.7 Working with layouts in Web-Client

16.11.7.1 Summary of how to work with layouts in Web-Client

Configuring layouts(see page 471)

To create and edit layouts in Web-Client click to access the corresponding menu.



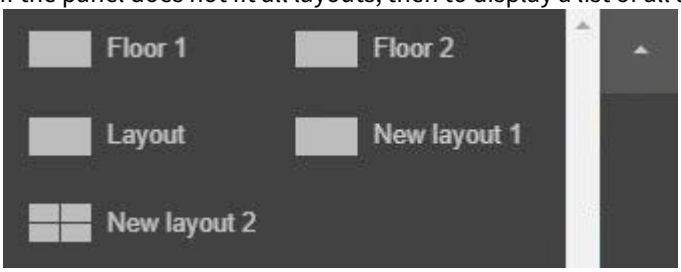
There are a number of things you need to consider when dealing with layouts in Web-Client:

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.

16.11.7.2 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 .



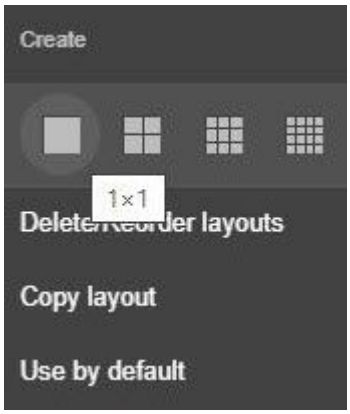
To close the layout list, you need to press a button .

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.

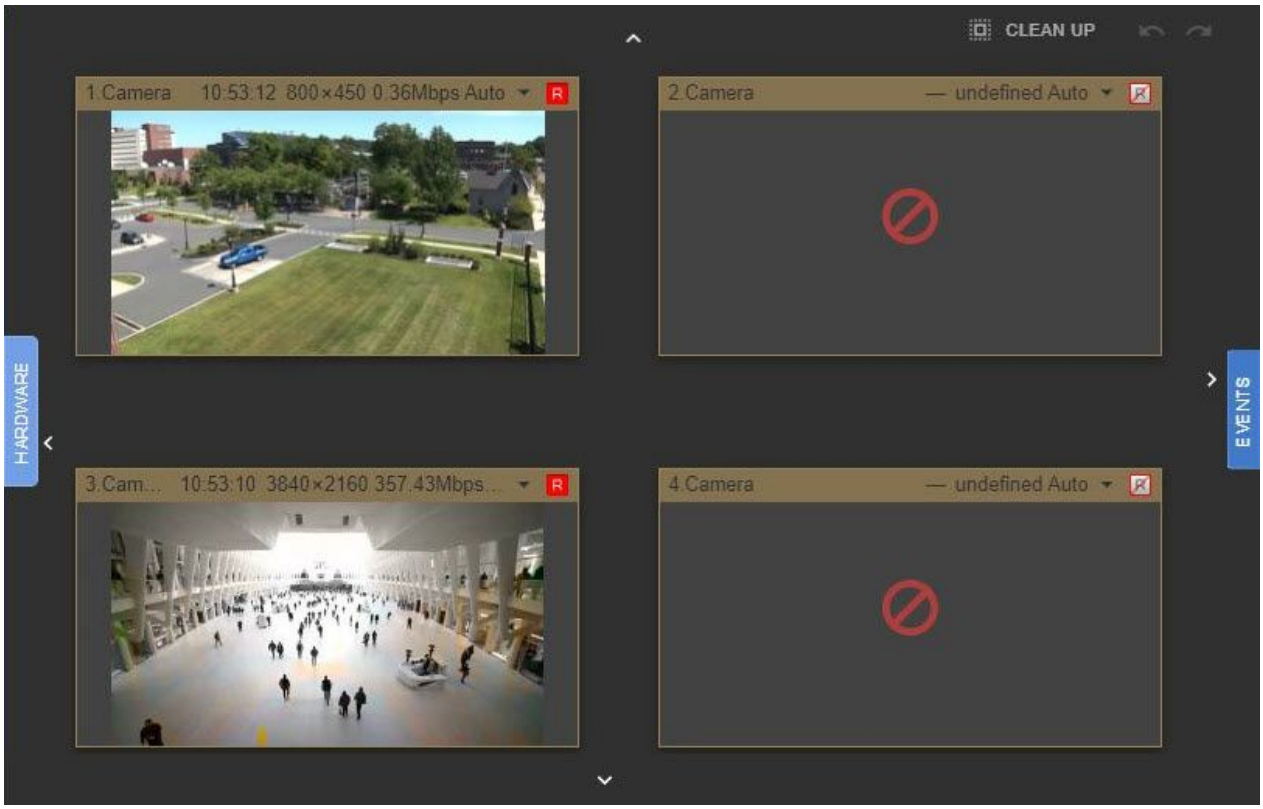
16.11.7.3 Creating a new layout in the Web-Client

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.

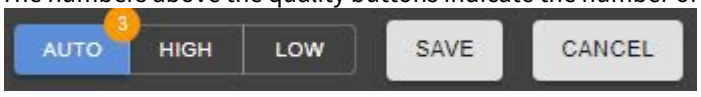


> **Note**
>
> By default, the layouts display only active cameras. if you want the layout to display all available cameras, including inactive, disable the **Show only live cameras** parameter in the Web-Client settings (see Web-Client configuration(see page 827)).

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(see page 475)).

> **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 .

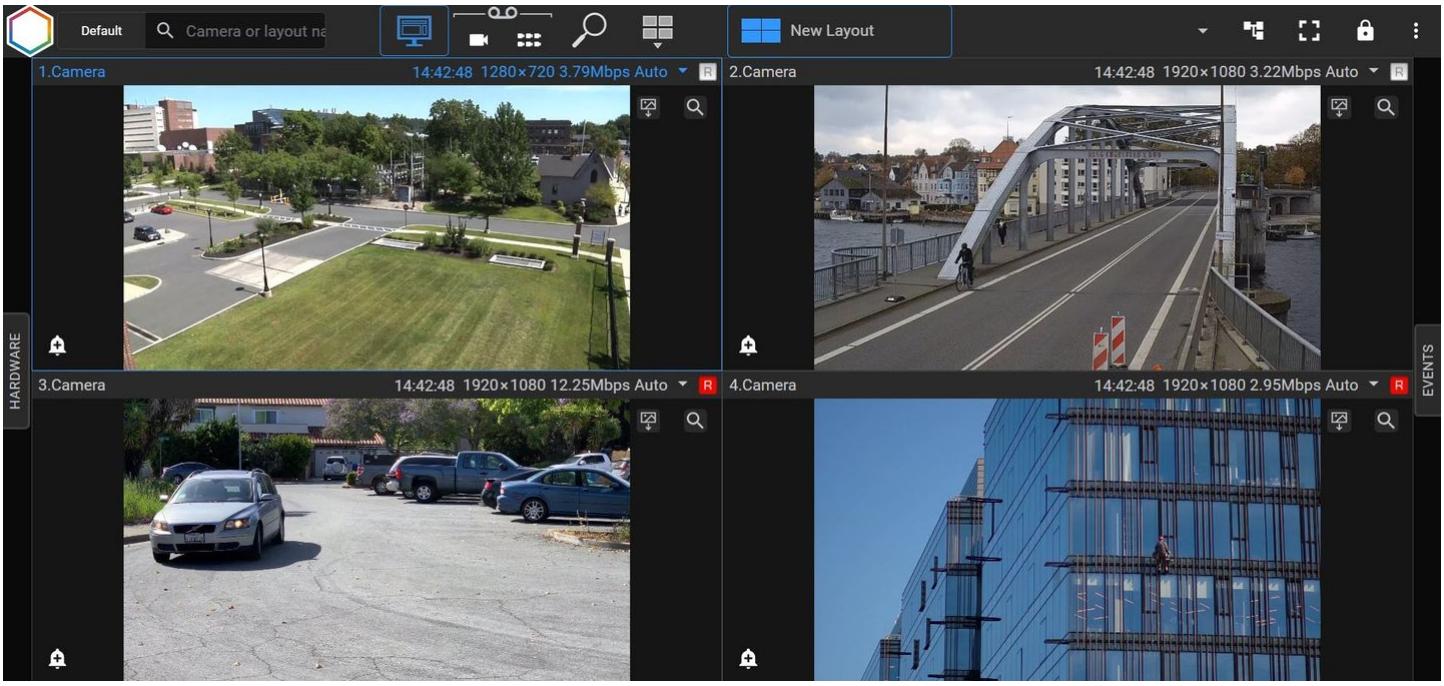
3. You can resize the cells using arrows on the cell boundaries (similar to the main Client, see Resizing cells(see page 478)).
4. Add video cameras to the cells. To do this, drag & drop a camera from the Cameras panel (see Searching for video cameras in the Web-Client(see page 830)).
5. Select the default 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.
>
> 
>

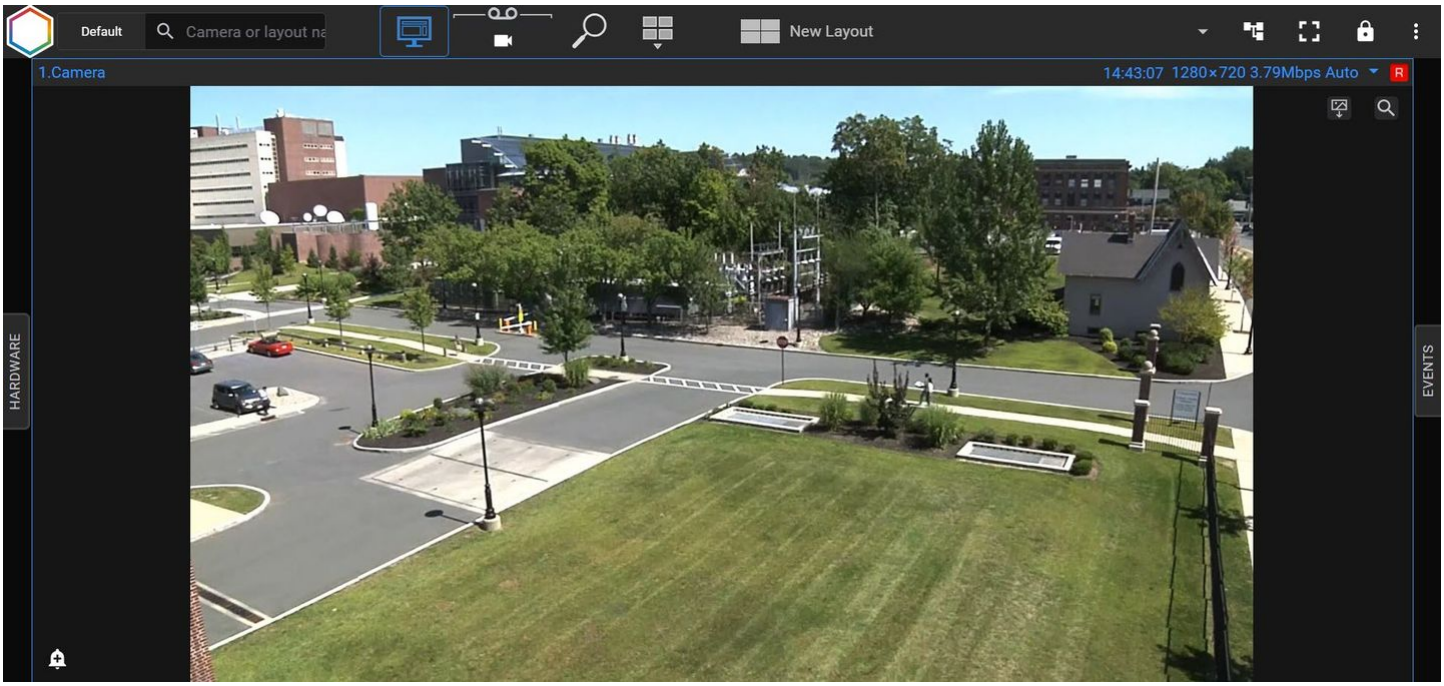
In this example, there are three **Surveillance windows** on the layout: the stream quality is automatically selected in two windows (see Selecting video stream quality in a Surveillance window (GreenStream)(see page 690)), one window displays a high-quality video stream, and another window displays 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.

16.11.7.4 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 .

16.11.7.5 Selecting the default layout in Web-Client

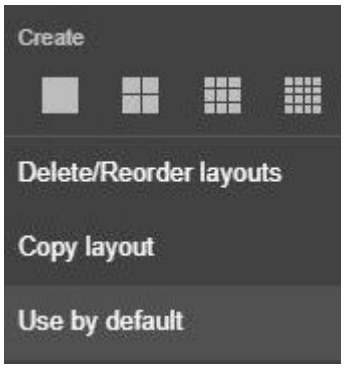
You can select the default layout for each user to be displayed after they launch Web-Client. If you don't set this layout, they'll see a blank screen.

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:

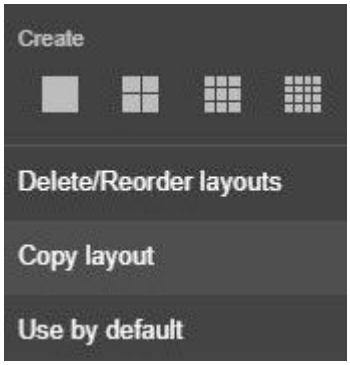
To remove the default layout, click the button and select **Do not use by default**.

16.11.7.6 Copying layouts in the Web-Client

Layout copying(see page 473)

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.

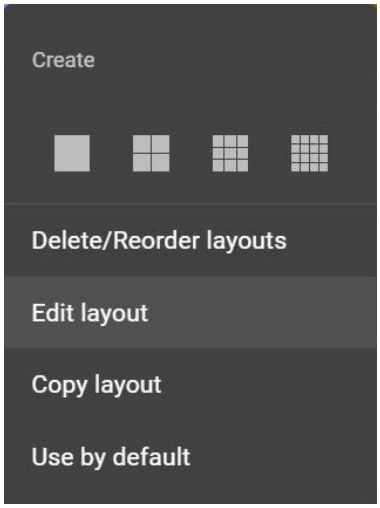
An identical layout will be created with the word "Copy" added to its name. All subsequent copies will have a copy number added to the name of the layout.

16.11.7.7 Sharing layouts in the Web-Client

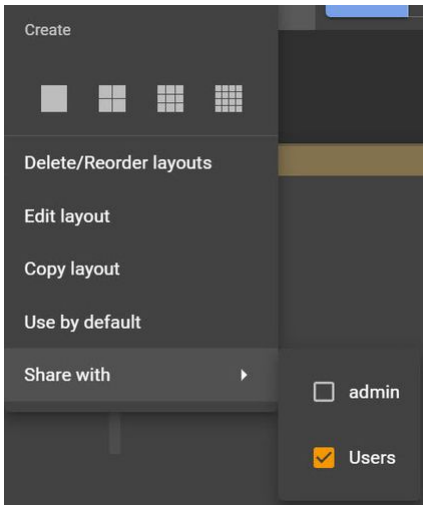
Share Layouts(see page 499)

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.



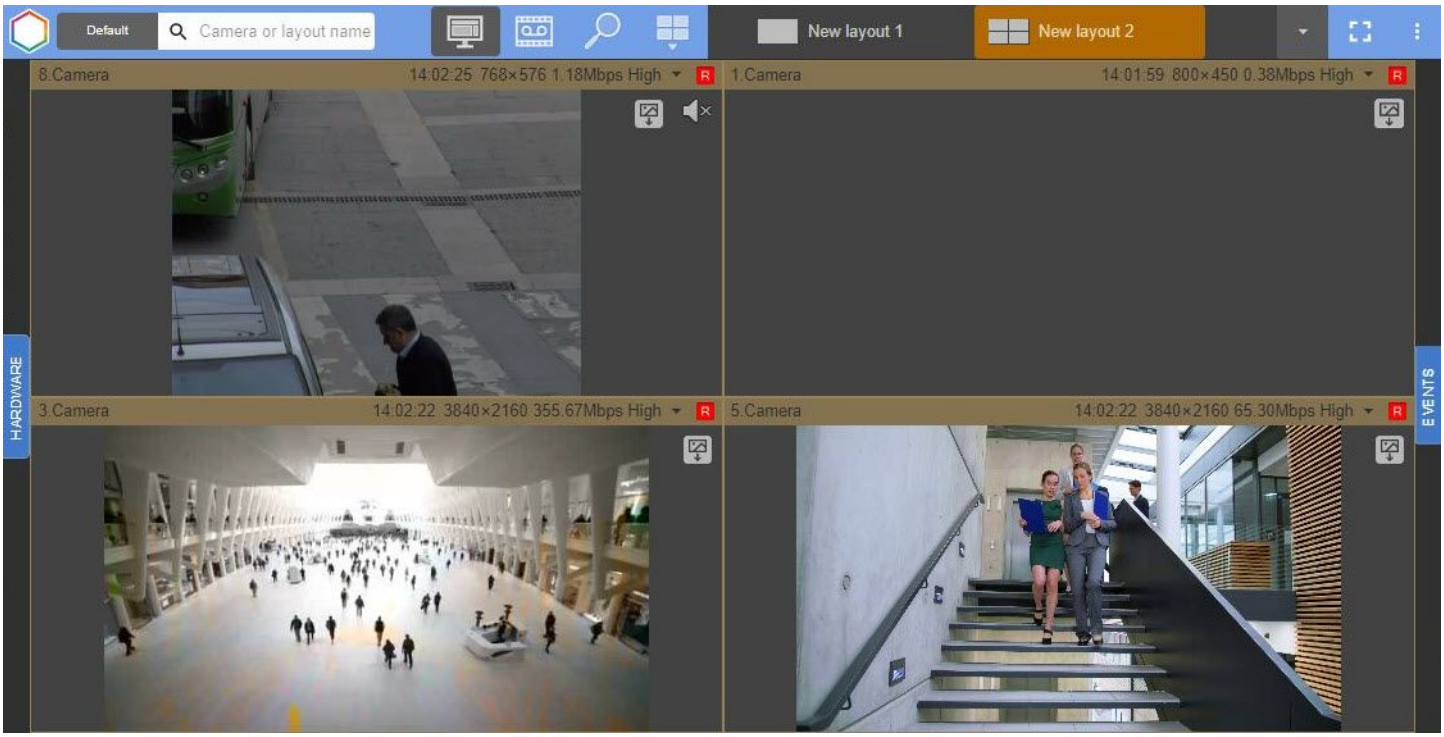
4. Click **Save**.

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(see page 835)). 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.

16.11.8 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(see page 830)), or one of the available layouts (see Web-Client GUI(see page 826)).



The Web-Client supports video playback in the following video formats: MJPEG, H.264, H.265. All other formats are transcoded to MJPEG on the Server.

Attention!

H.265 video playback is possible in the following browsers: Safari, Microsoft Edge with HEVC video extension[195] 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.

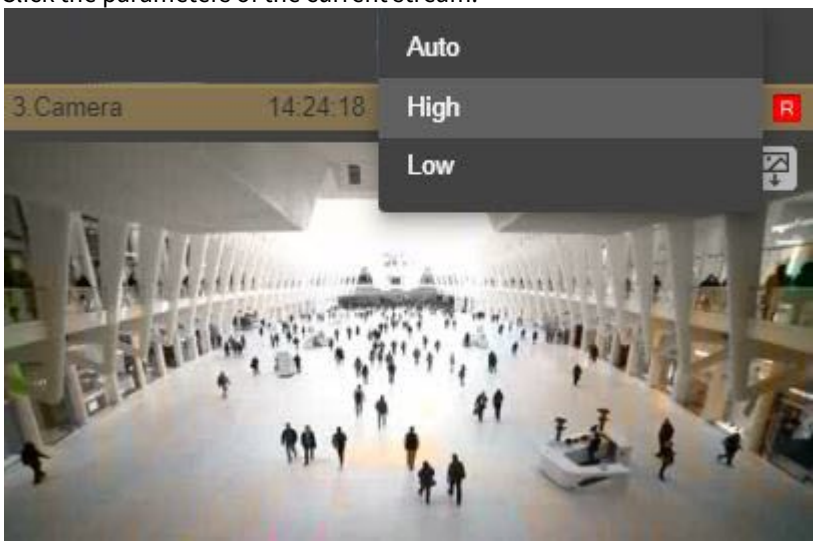
Attention!

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(see page 827)). If you select a specific camera, all frames will be displayed.
In the MJPEG video format each frame is displayed.

To select a displayed stream in the Web-Client manually (see The Camera object(see page 122)), do the following:

195 https://apps.microsoft.com/store/detail/hevc-video-extensions/9NMZLZ57R3T7?hl=en-us&gl=us

1. Click the parameters of the current stream.



2. Select a stream to be displayed.

Menu item	Description
Auto (GreenStream, default)	The camera has two video streams: high quality video stream and low quality video stream. If the size of the cell where the video image from the camera is displayed is close to the low quality resolution with a 10% height or width margin, the video image will be displayed using the low quality stream. In other cases, the high quality video stream will be displayed
High quality	A high quality video stream is used in the video surveillance window (see The Camera object(see page 122))
Low quality	A low-quality video stream is used in the video surveillance window (see The Camera object(see page 122)). When you enlarge the surveillance window, the video stream switches to a high quality video stream

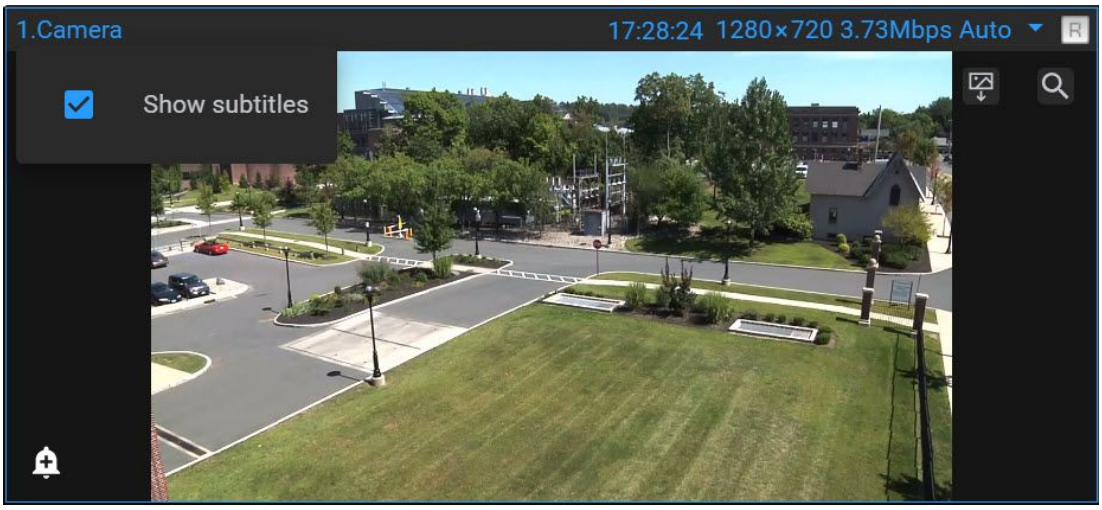
Note

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.



16.11.9 Controlling PTZ cameras through the Web-Client

A PTZ video camera is controlled through the PTZ device control panel.

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.

16.11.9.1 Controlling a PTZ camera through the Web-Client by using presets

To go to a preset, select the relevant line in the list of presets.

16.11.9.2 Changing the optical zoom of a PTZ camera in the Web-Client

To change the optical zoom of a PTZ unit, use the buttons in the **ZOOM** group.

– increase image.

– reduce image.

16.11.9.3 Changing the positioning speed of a PTZ camera in the Web-Client

To change the positioning speed of a PTZ camera, use the buttons in the **SPEED** group.

– increase positioning speed.

– reduce positioning speed.

5 – field displaying the current positioning speed.

16.11.9.4 Changing the tilt of a PTZ camera in the Web-Client

To change the tilt of a PTZ camera, use the arrows in the **PTZ Control** group.

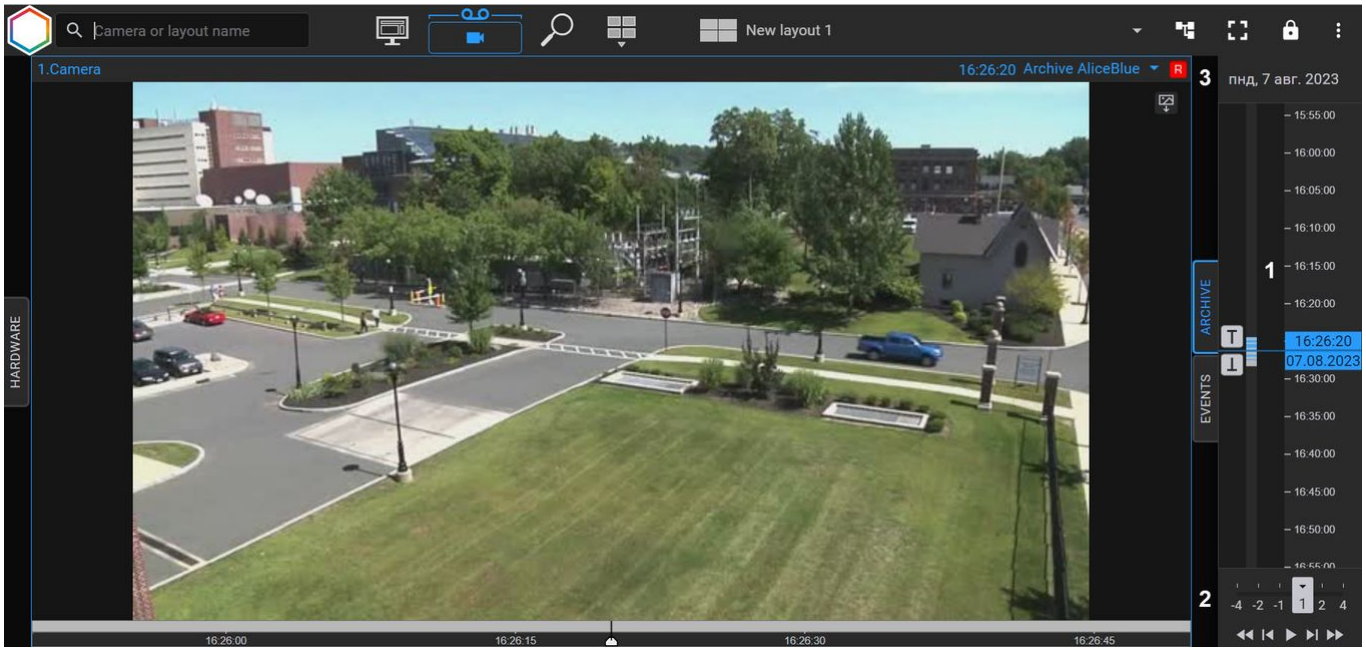
The arrow direction indicates the direction in which the camera lens will be moved when the arrow is clicked.

16.11.10 Viewing video archives through the Web-Client

16.11.10.1 **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(see page 225)).

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(see page 705)).

   > **Note**
   >
   > Similar to the Client (see The Timeline(see page 639)), 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!

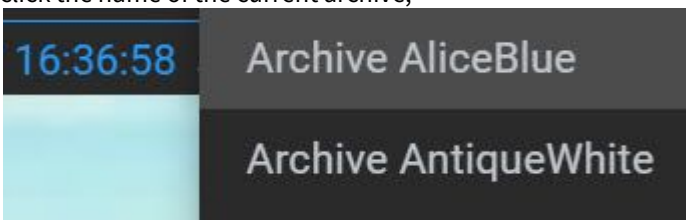
- Reverse fast-forward playback of H.264 video is based on key frames, so it will not be smooth.
- Audio is unavailable during fast forward and reverse playback of the archive video.

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(see page 846)).

Note

You can also navigate in the archive using the time indicator similar to the Client (see Navigation via the time indicator(see page 709)).

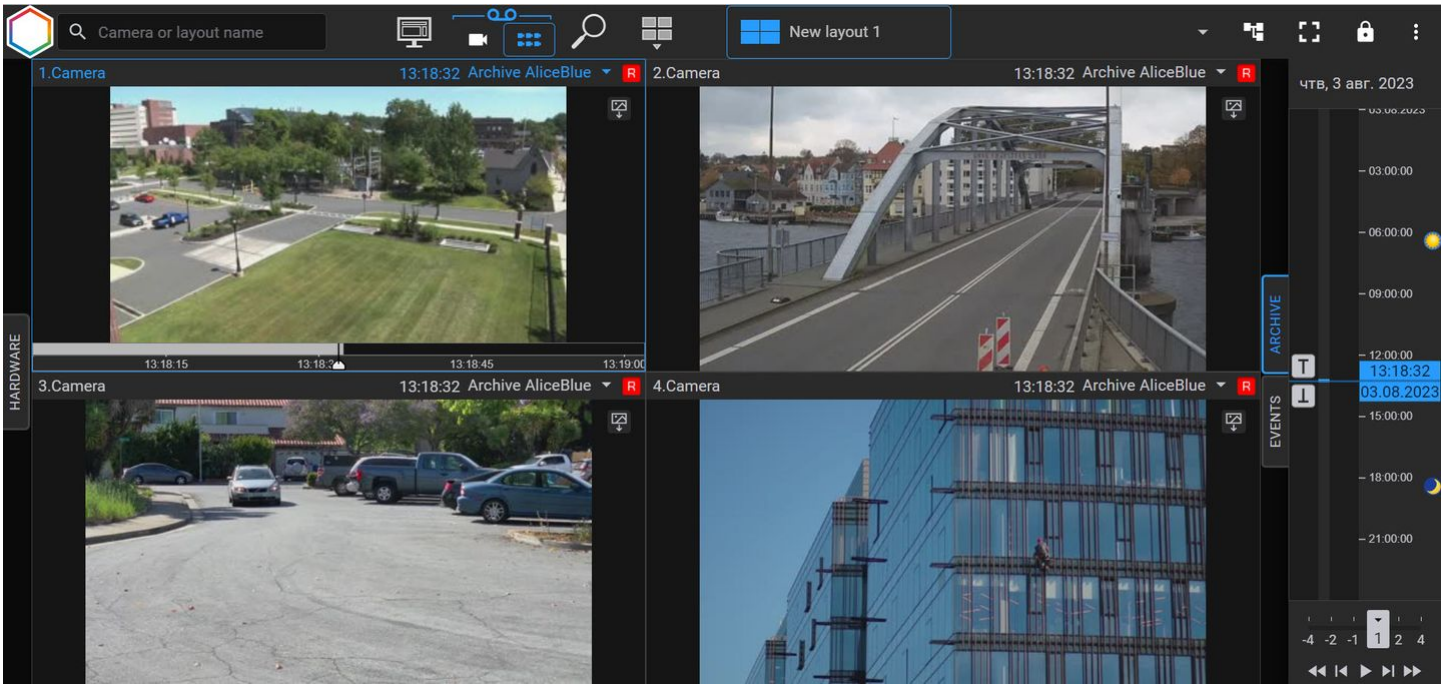
4. To select an archive, do the following:
   a. click the name of the current archive;



   b. select the required archive.

16.11.10.2 Multi-camera archive view mode

You can switch all cameras on the layout to the archive mode. To do this, click the button.

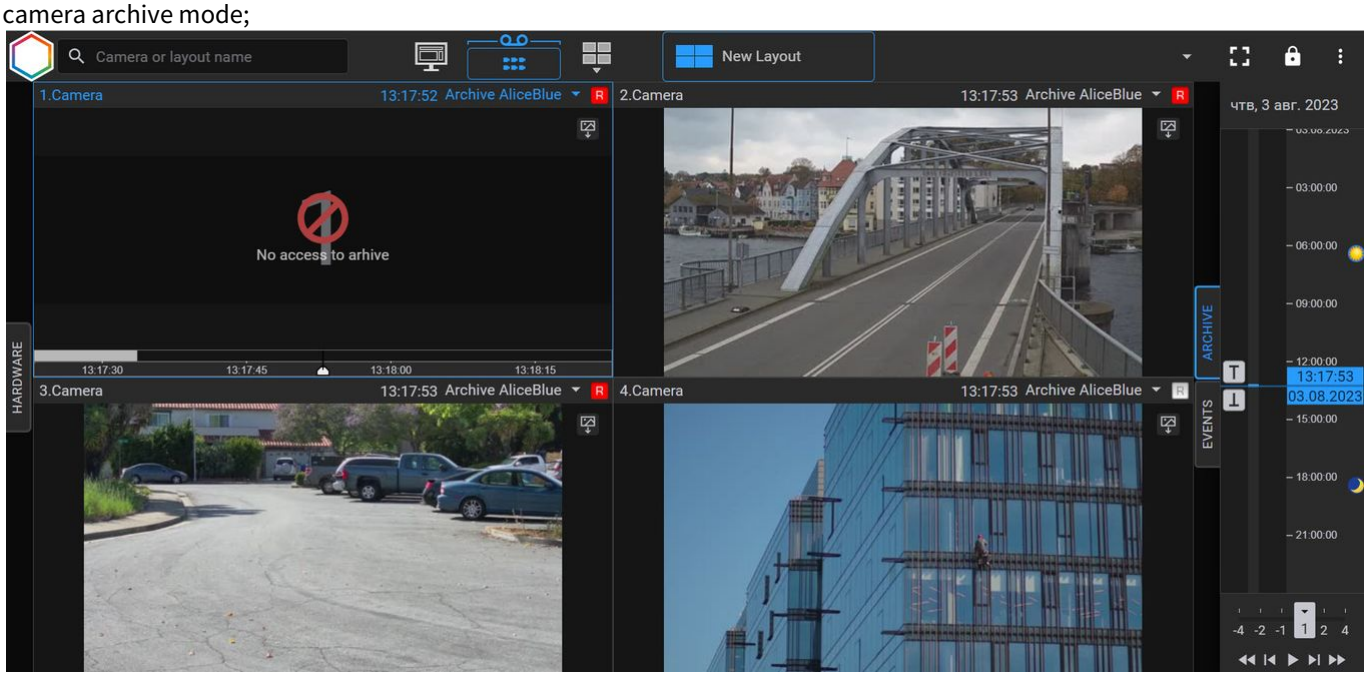


You can control the archive viewing using the playback control panel, the same as when viewing the archive of a single video camera.

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(see page 452)). 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;



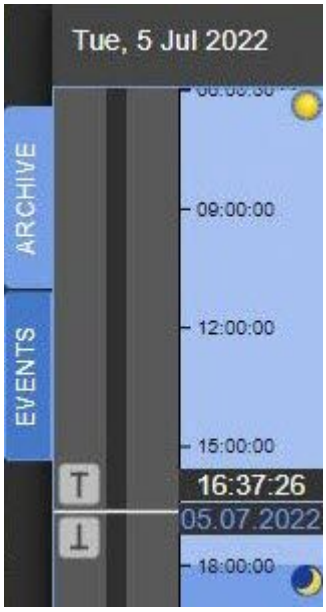
- if there is only one camera with limited access to the archive on the layout, the buttons for changing the mode (archive, search) won't be displayed;

- 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.

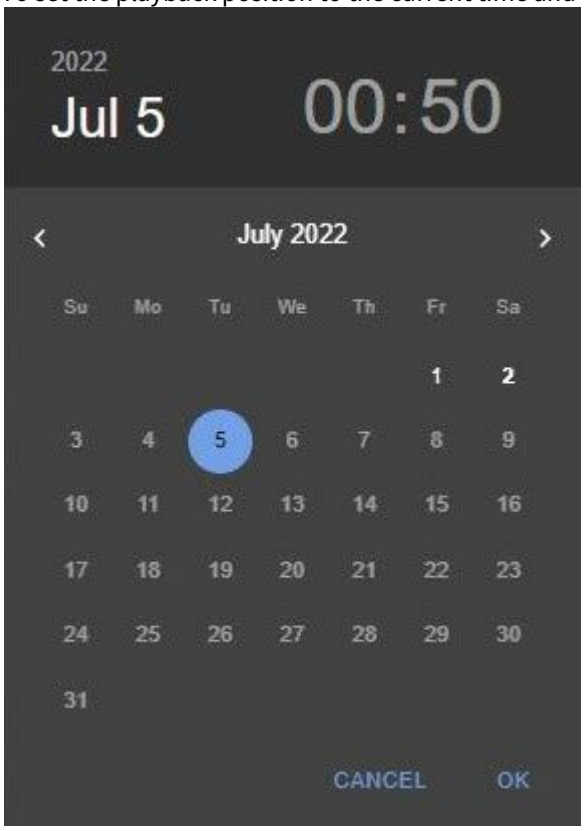
16.11.11 Archive position selection panel for the Web-Client

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.



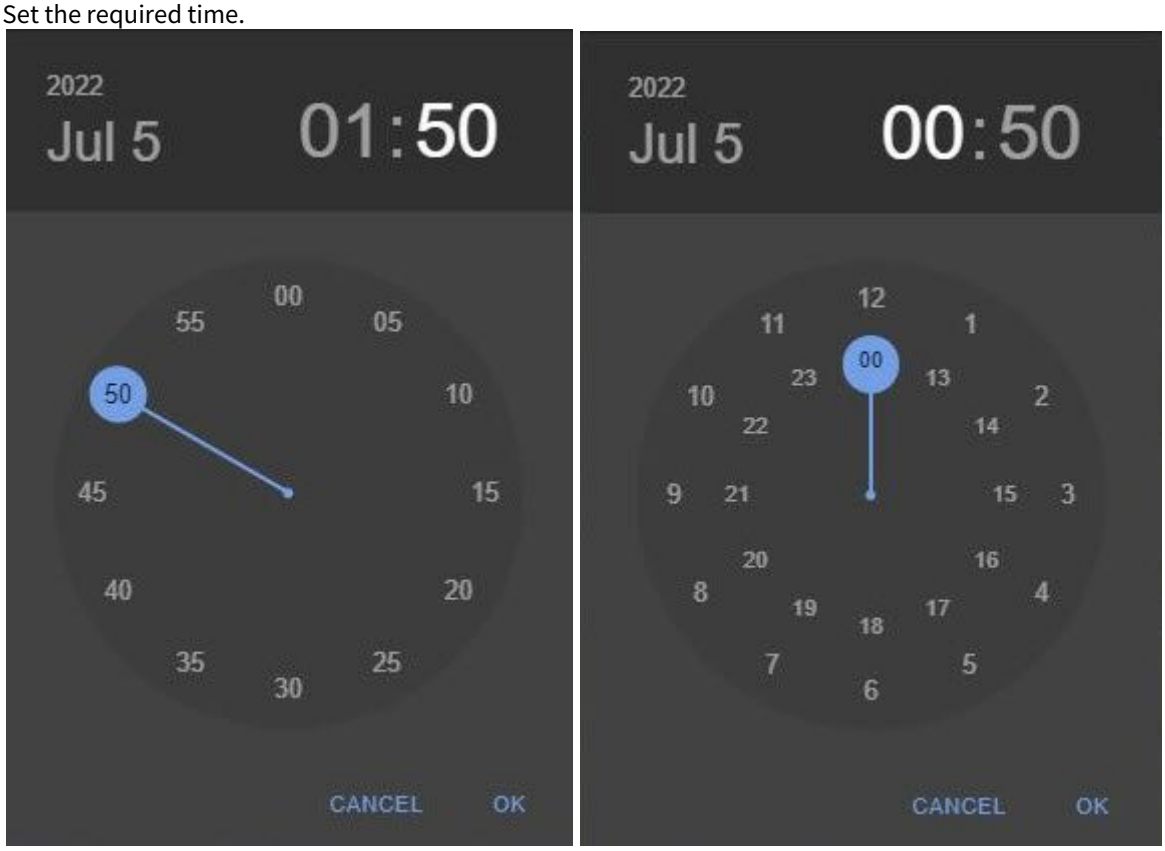
2. To set the playback position to the current time and date, go to step 6.



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.

16.11.12 Archive search in the Web-Client

There are two ways to search the archive in the Web-Client:

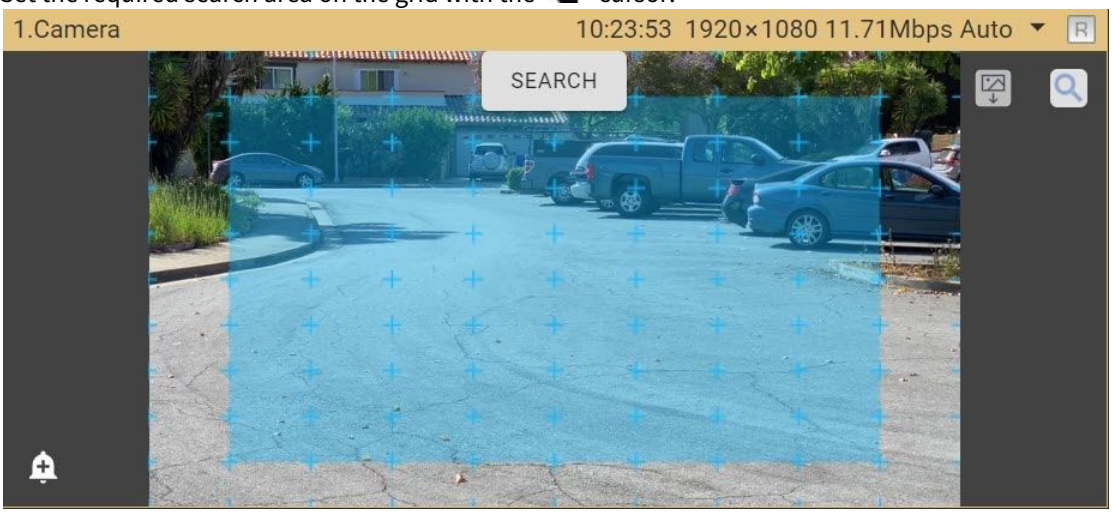
- **Standard search**. To go to the search in the archive, do the following:
  a. Select the required camera on the cameras panel or on the layout.
  b. Click the button.

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(see page 722)).

- **Quick search**. To go to the quick search in the archive, do the following
  a. Select the required camera on the cameras panel or on the layout.
  b. Click the button on the camera fold.

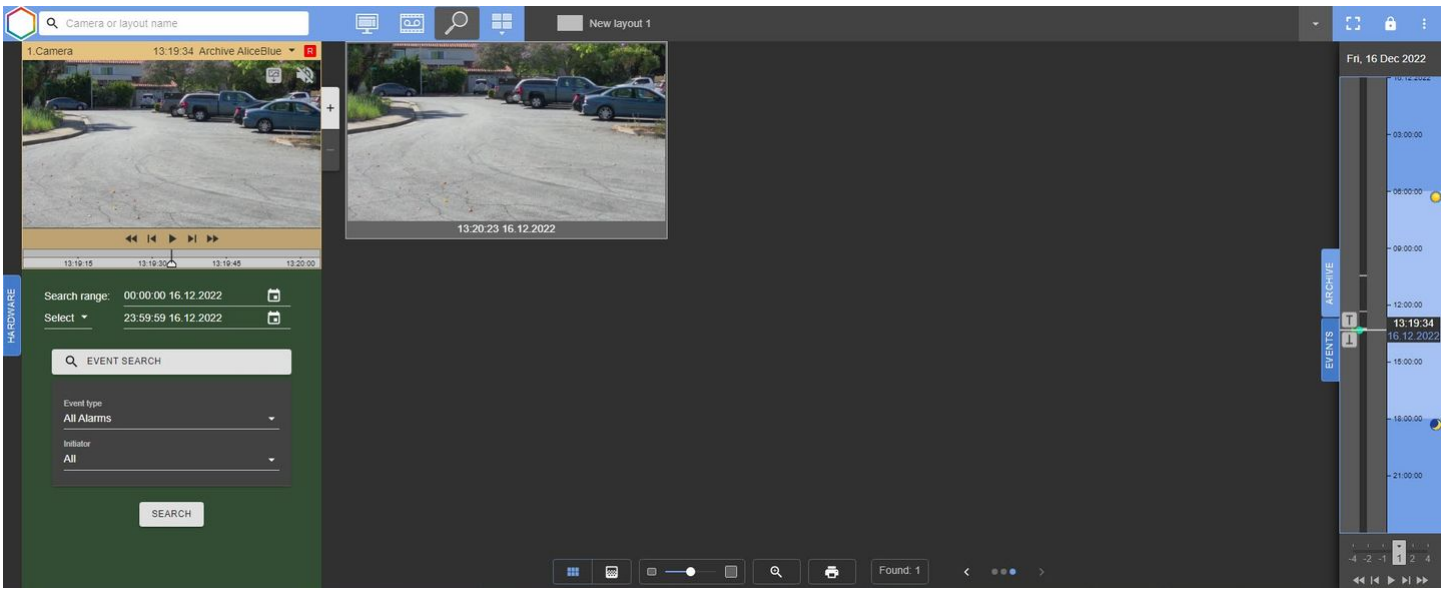
> **Note**
>
> The quick search button is displayed on the fold of the cameras, on the basis of which the detection tools with the ability to track objects are created (see Tracking objects(see page 663)).

c. Set the required search area on the grid with the cursor.



d. 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(see page 725)). 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(see page 639)). 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).

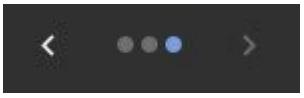
You can change the size of the Surveillance window using the buttons.

Attention!

If you select a device on the cameras panel (see Searching for video cameras in the Web-Client(see page 830)), 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.

16.11.12.1 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(see page 827)).

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(see page 721)).

You can also build a Heat Map in the Web-Client (see Building a Heat Map(see page 849)).

16.11.12.2 Building a Heat Map

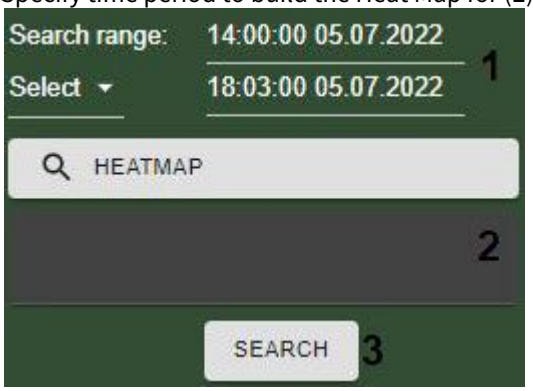
Attention!

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.

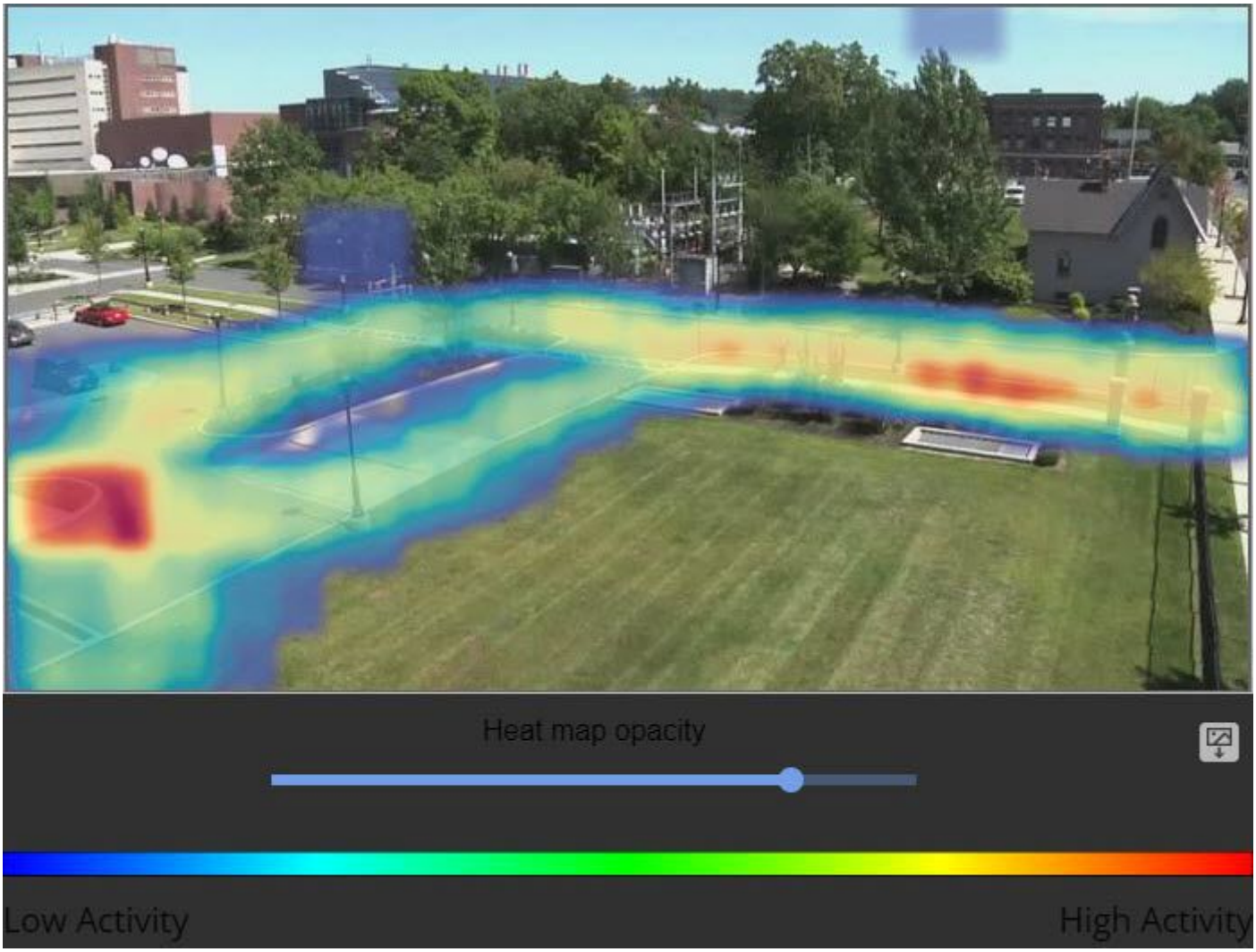
How to build a Heat Map:

1. Proceed to the Archive search.
2. Specify time period to build the Heat Map for (**1**).



3. From the **Select** drop-down list select **Heat Map**.
4. Select the source of metadata (**2**).
5. Click the **SEARCH** button (**3**).

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.

16.11.12.3 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(see page 847)).
2. Set the search criteria.
3. Open Cameras panel and select the required devices (see Searching for video cameras in the Web-Client(see page 830)).

> **Note**
>
> To select all cameras, select the appropriate box on the bottom of the page.

4. Click the **Search** button.

16.11.12.4 Reporting the search results

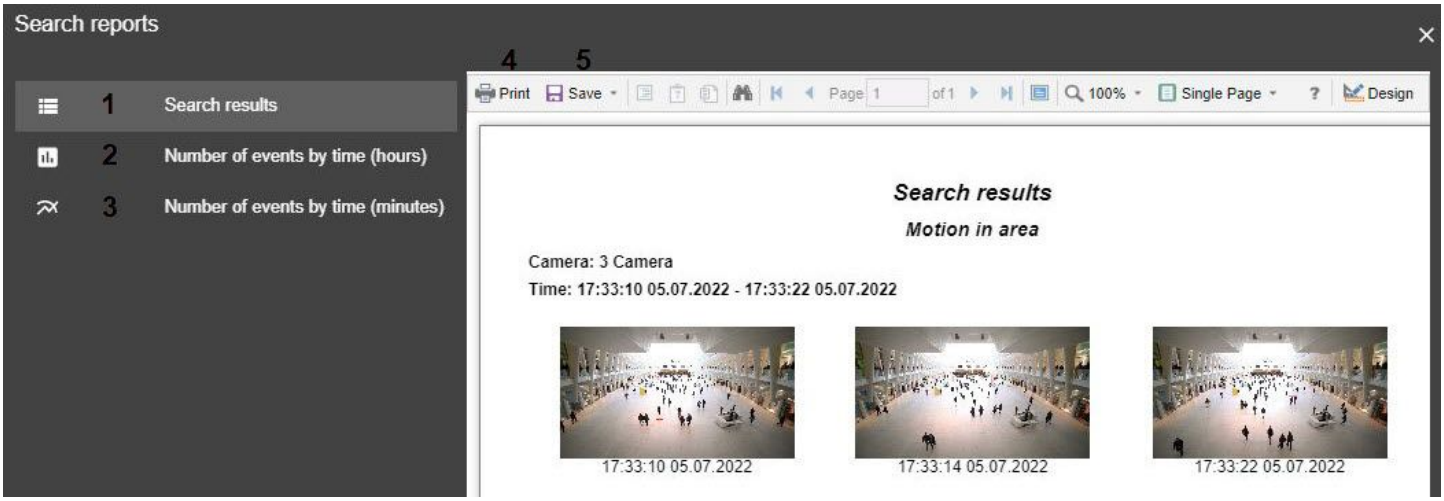
The Web-Client also includes the Stimulsoft[196] report editor for building reports on retrieved video fragments.

To build a report after you finished searching, click in the bottom part of the screen.

> **Attention!**

196 https://www.stimulsoft.com/en/documentation/online/user-manual/

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.

16.11.13 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(see page 830), Web-Client GUI(see page 826)).

Note

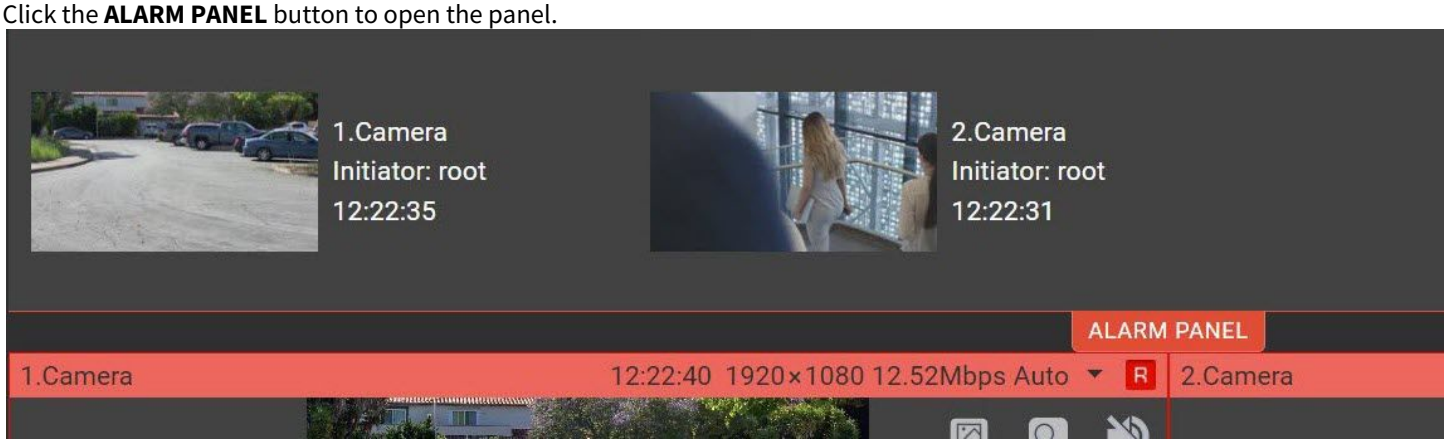
The alarms that were triggered before selecting a camera or a layout are only displayed if the user is in the workspace. After you reload the page, go to the open statistics or bookmarks sections, the panel with the current alarms will disappear.

When an alarm triggers, the alarm panel appears on top (like in the Client, see Alert panel(see page 646)).

Note

The browser tab will indicate the number of current alarms in the Web-Client.

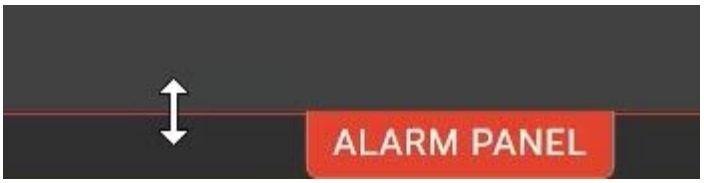
Click the **ALARM PANEL** button to open the panel.



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.

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.



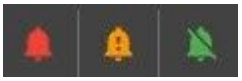
16.11.13.1 Alarm processing in the Web-Client

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:

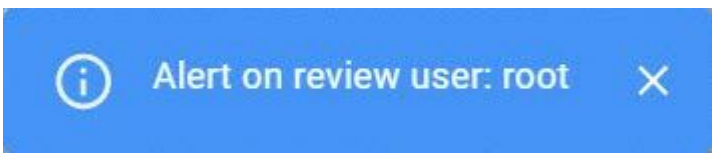
1. Initiate an alarm by clicking the button (like in the Client, see Switch to Alarm Management mode(see page 714)).
2. Click the button to go into the alarm event management mode.

As a result, the archive mode will open, and the panel for managing an alarm event will appear (see Assessing an alarm event(see page 719)).



> **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(see page 720)).

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:



16.11.14 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.

16.11.15 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.

16.11.16 Export in the Web-Client

To export a frame, click the button when viewing the video image.

> **Note**
>
> Users without export access rights won't have the access to the icon, as well as the possibility to select the export interval on the timeline (see Creating and configuring roles(see page 452)).

To export video image, do the following:

1. Switch to the archive mode (see Viewing video archives through the Web-Client(see page 843)).

2. On the timeline, set the timeline indicator to the location that matches the beginning of the export interval. Click the button. Set the indicator to the location that matches the end of the export interval. Click the button.
3. Click the button.

> **Note**
>
> To delete the export interval, click the button.

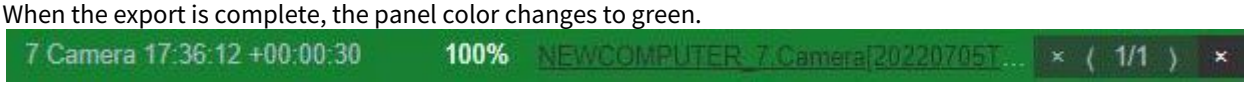
4. Select the video export format (**1**). If necessary, add comments to the export (**3**). You can export videos to the AVI, MKV, MP4 and EXE formats. The comments will be displayed as captions when the exported video is played back.

> **Note**
>
> In macOS, you can export to the AVI, MKV, MP4 formats. Files with the .exe extension are not supported in this OS.

5. If you are exporting to the AVI format, select the compression level (**2**). **Low level**—minimum compression, maximum file size; **High level**—maximum compression, minimum file size.
6. Click the **EXPORT** button (**4**).

The export progress is displayed on the drop-down panel as in the Client (see Viewing export progress(see page 817)).

When the export is complete, the panel color changes to green.

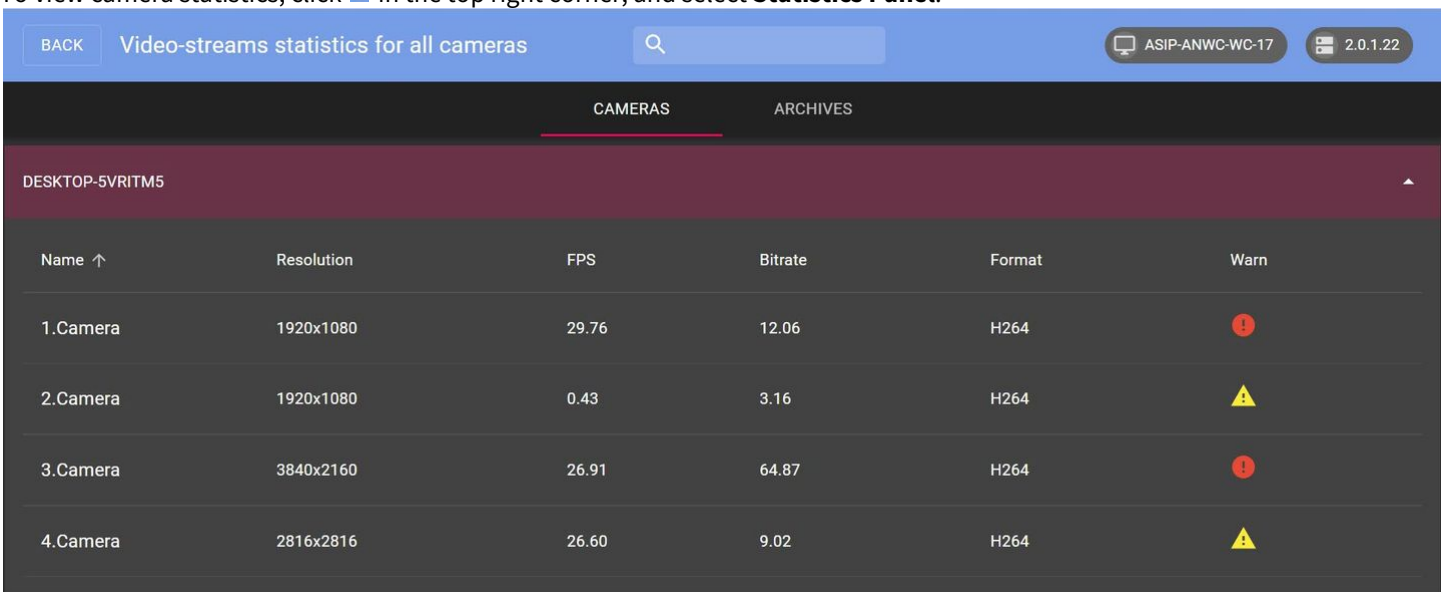


To download an exported file, click its name on the panel.

> **Note**
>
> The text of the timestamp in the exported video will depend on the language selected in the browser.

16.11.17 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.

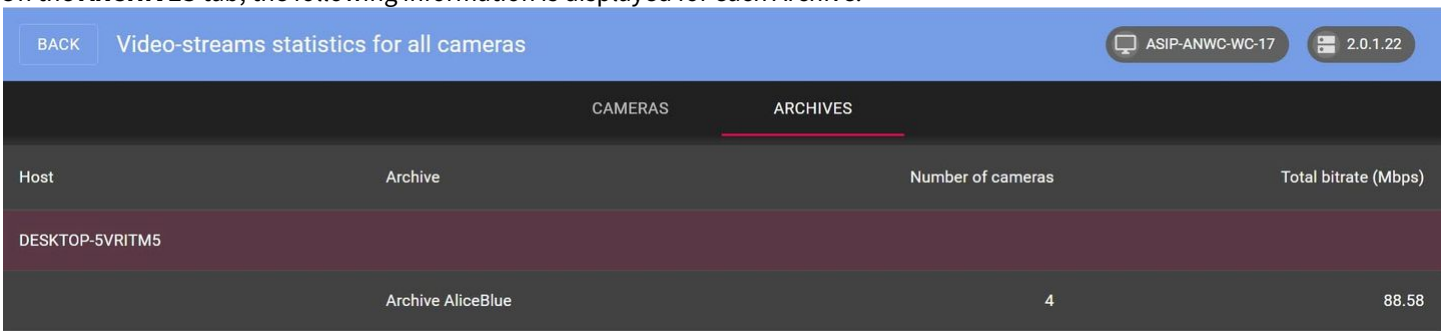
If the bit rate exceeds the expected value, and there is more than 1 Mbit per megapixel, the stream is marked with .

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:



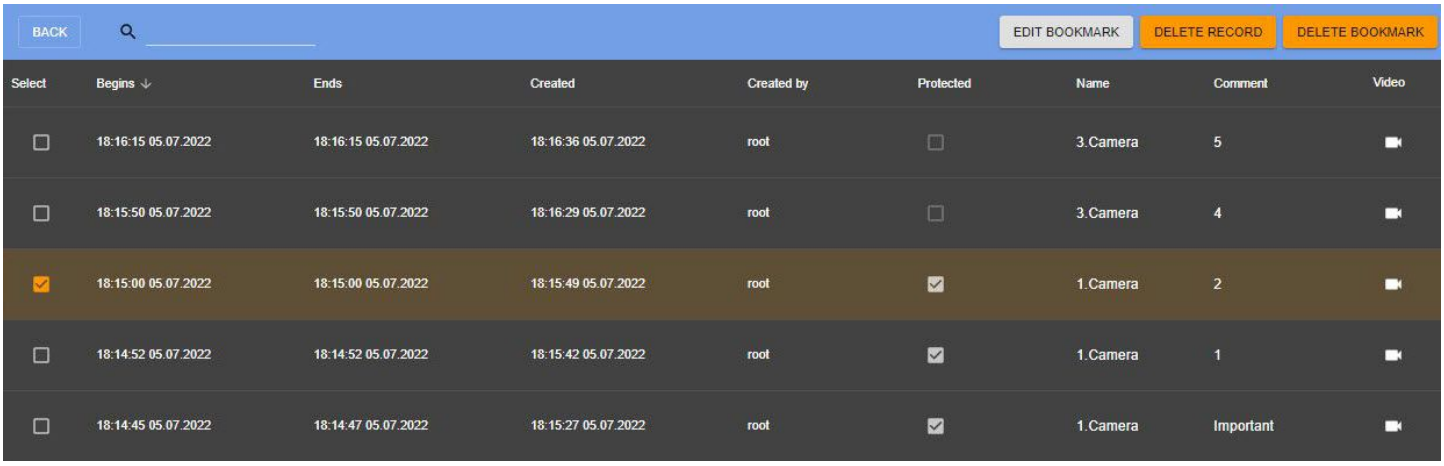
- name;
- number of linked cameras;
- cumulative bit rate of linked cameras.

To return to the previous page, click **BACK** in the left upper corner of the screen.

16.11.18 Working with bookmarks in the Web-Client

A bookmark represents either a comment in the archive (see Operator comments(see page 667)), or a protected video recording (see Protecting video footage from FIFO overwriting(see page 228)).

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(see page 227)).
> 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.

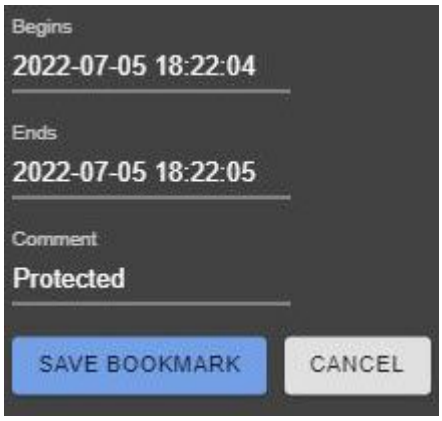
Use the search bar to locate a necessary bookmark.

To proceed to a particular video, click the button in the **Video** column. To return to a main page, click the **BACK** button.

16.11.18.1 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.

16.11.18.2 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** button.

16.11.18.3 Un-protecting a video

To un-protect a video, clear the **Protected** checkbox next the bookmark.

16.11.18.4 Deleting a protected video

To delete a protected video, select a protected bookmark and click the **DELETE RECORD** button.

16.12 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[197].

16.13 Changing user password

You can change user passwords in *Axxon One* with a few clicks.

Please follow the steps below:

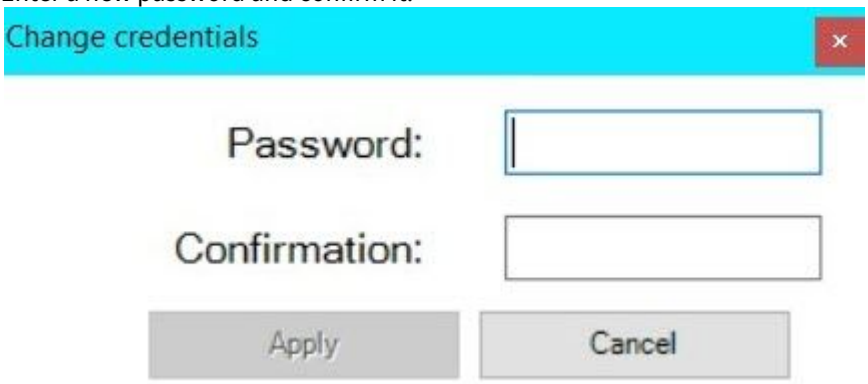
1. Go to the Settings tab .

197 https://docs.axxonsoft.com/confluence/display/mobile/AxxonSoft+mobile+Clients.+Documentation

2. In the upper-right corner, click the user name.

3. Click **Change password**.

4. Enter a new password and confirm it.



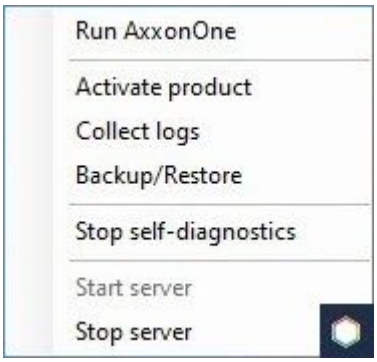
5. Click **Apply**.

The next time log in with a new password.

17 Description of utilities

17.1 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

17.2 Activation utility

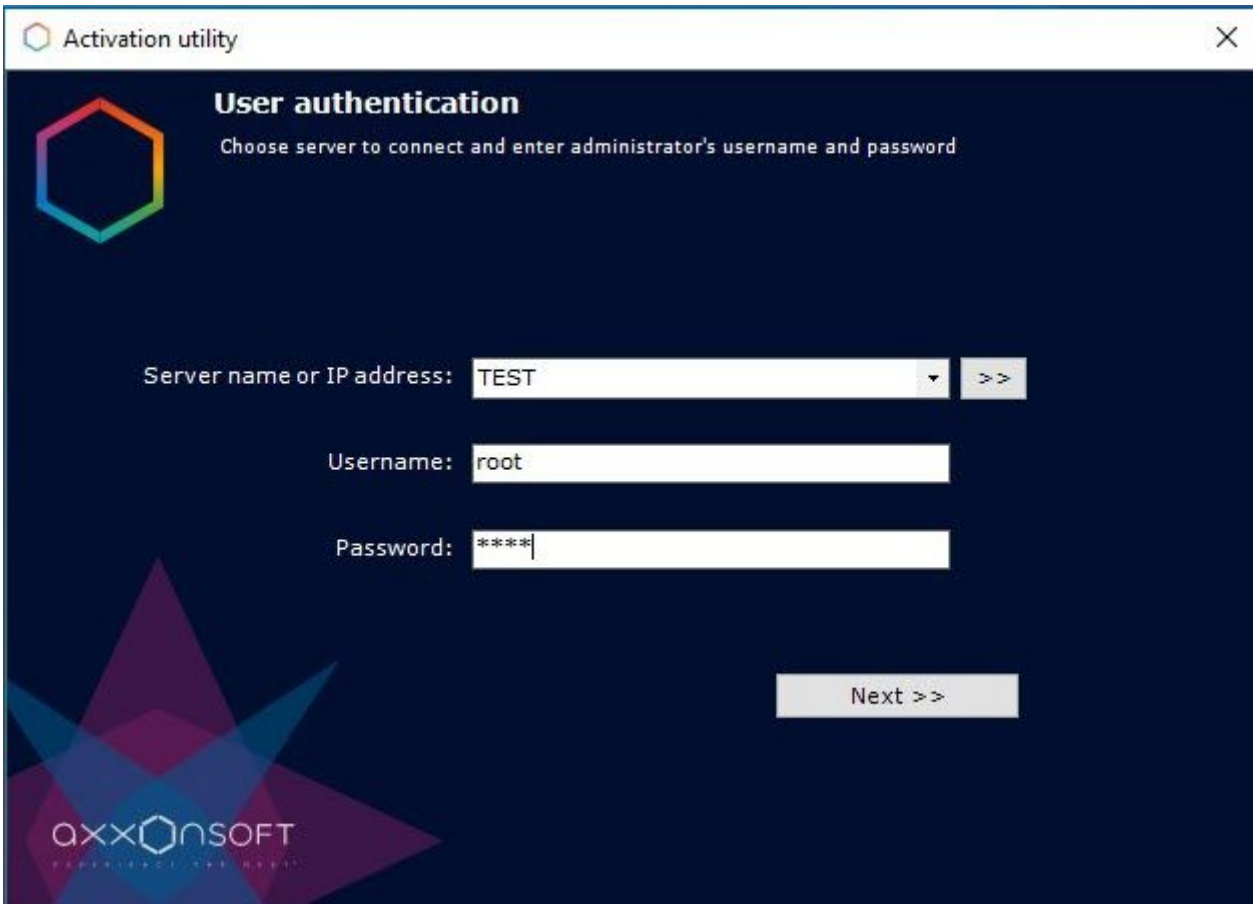
License activation for the *Axxon One* software package is carried out through the product activation utility.

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(see page 860) 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\

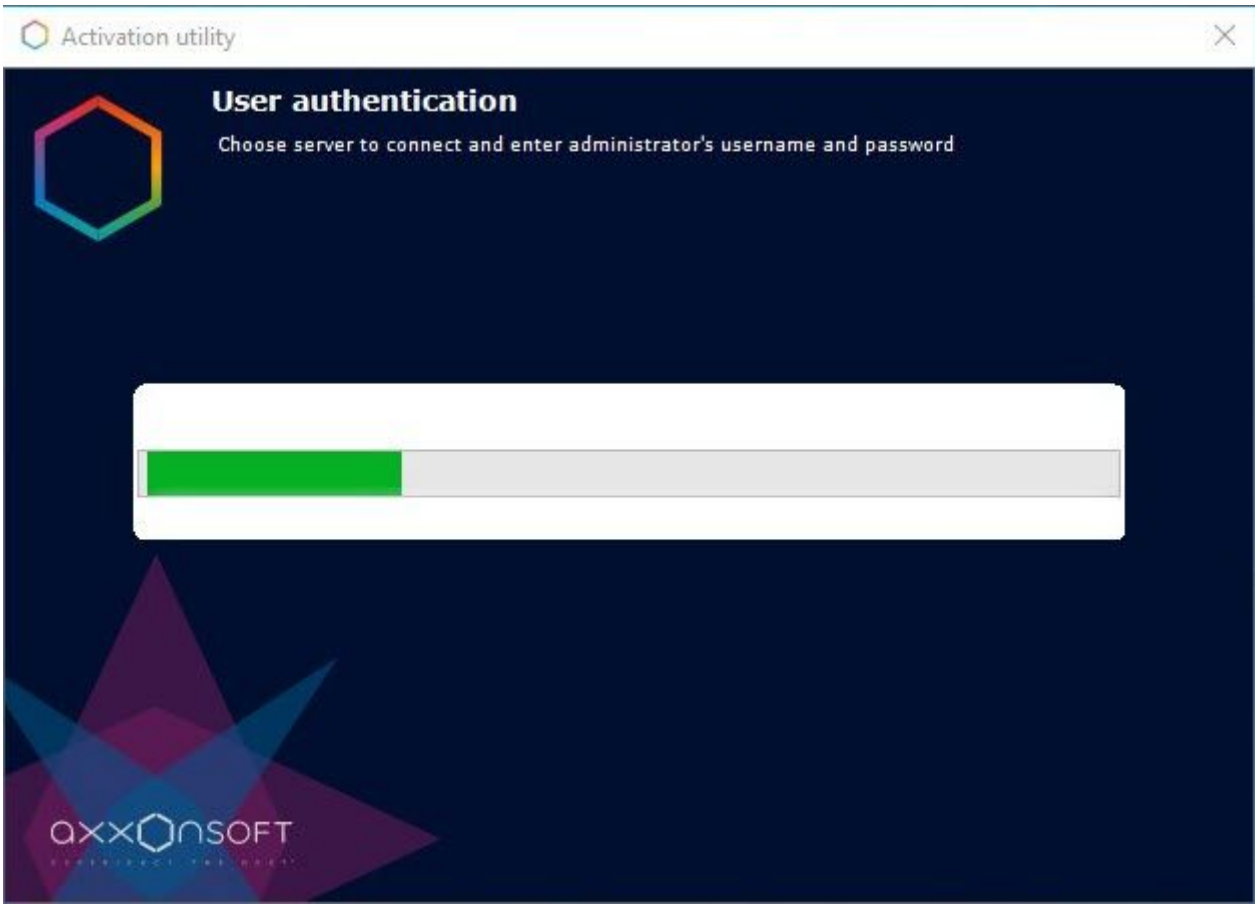
Then you must select the name of one of the Axxon Domain servers to which the license file will be applied (the file is applied to all Axxon Domain servers launched at the moment of activation) and connect to the system, under an administrator's user name and password, to continue the activation process.

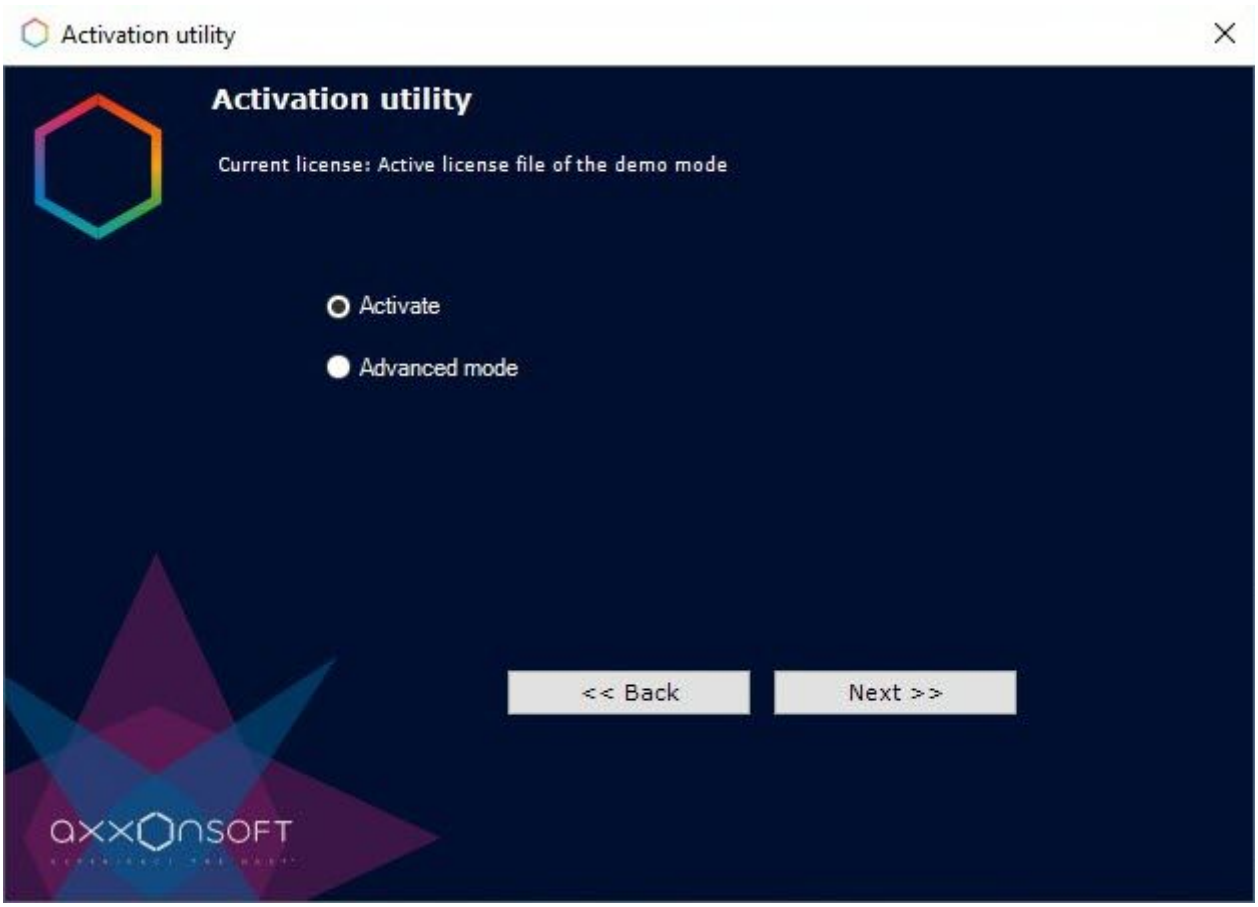


After the download is complete the main window of license utility will be displayed.

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[198], 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.

17.3 Axxon Support Tool

17.3.1 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.

17.3.2 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.

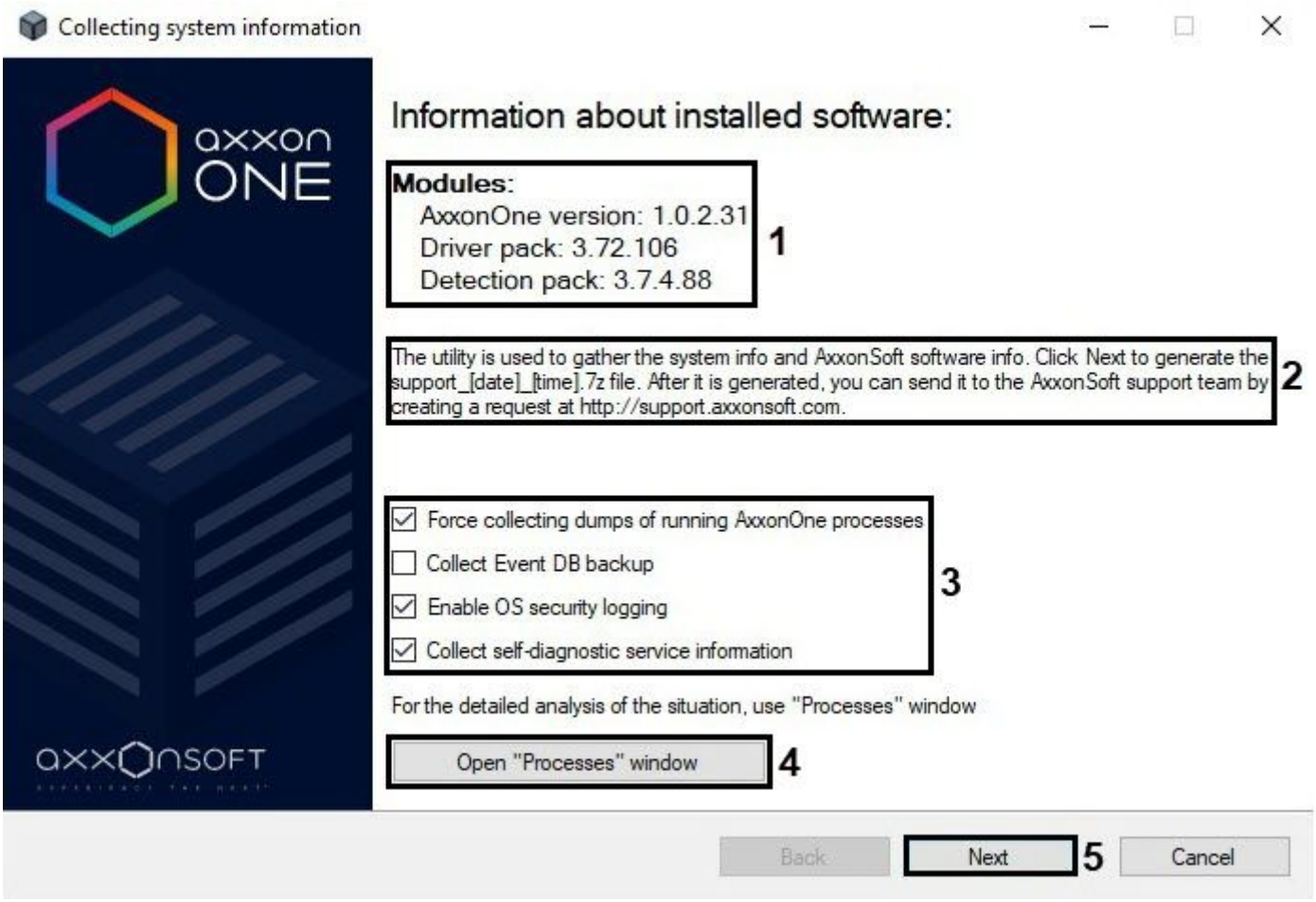
198 https://docs.axxonsoft.com/confluence/display/one20en/Activation+Guide

To close the Support.exe utility, click the **Cancel** button or .

17.3.3 Description of the Support.exe utility interface

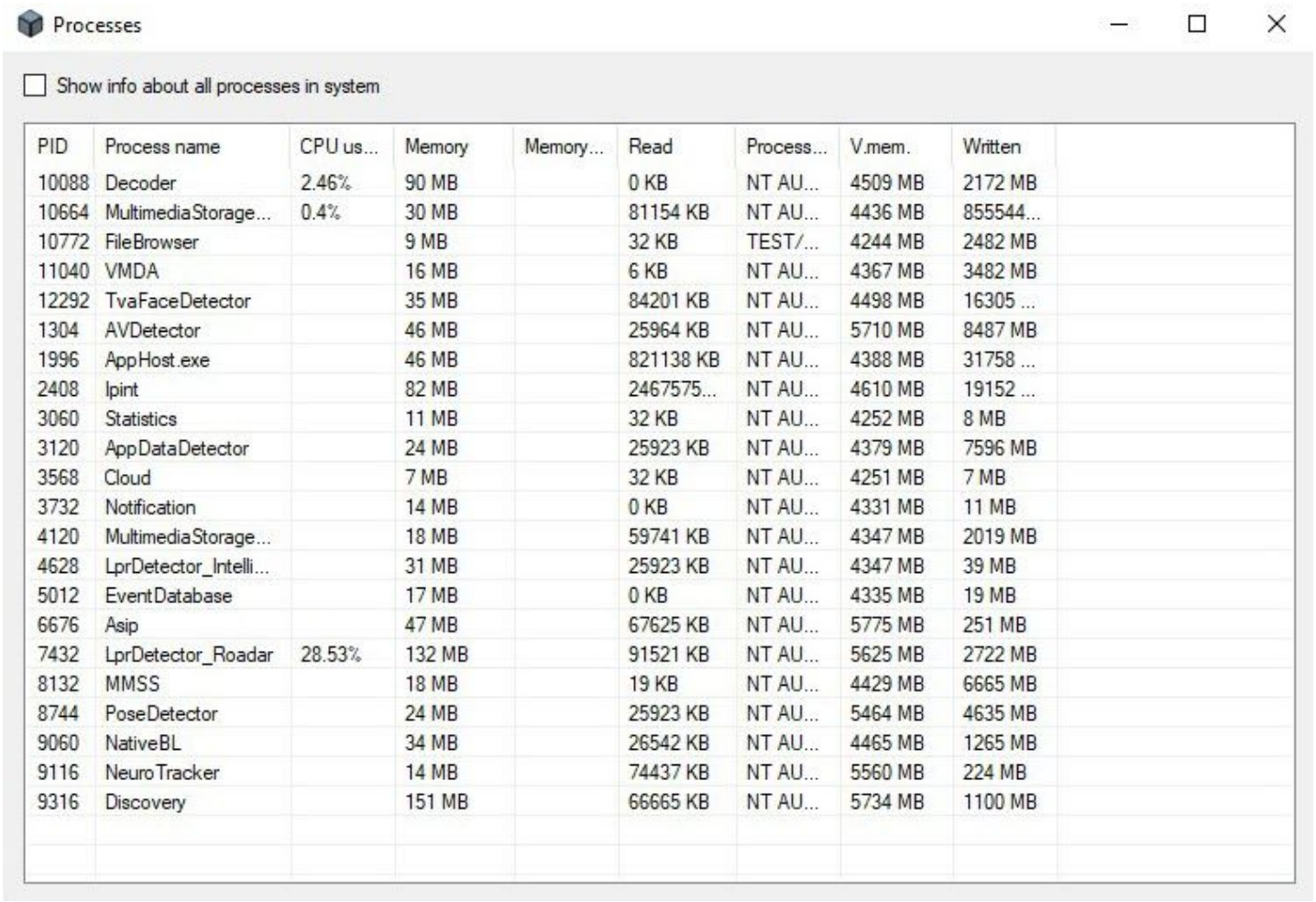
The Support.exe user interface includes the following elements:

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**).



17.3.4 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.



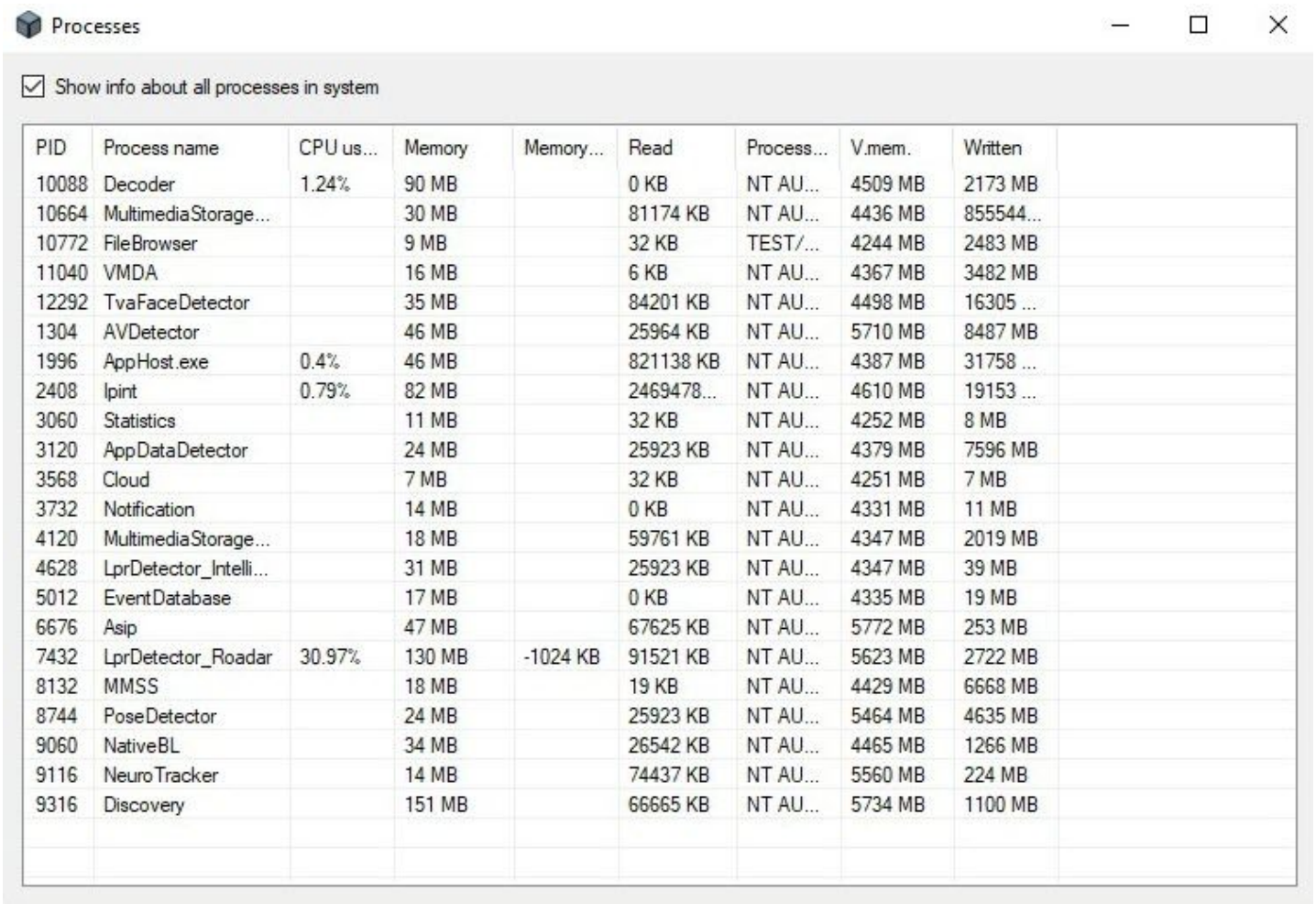
A list of all possible *Axxon One* processes is given in the table.

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.



Click the button to close the **Processes** window.

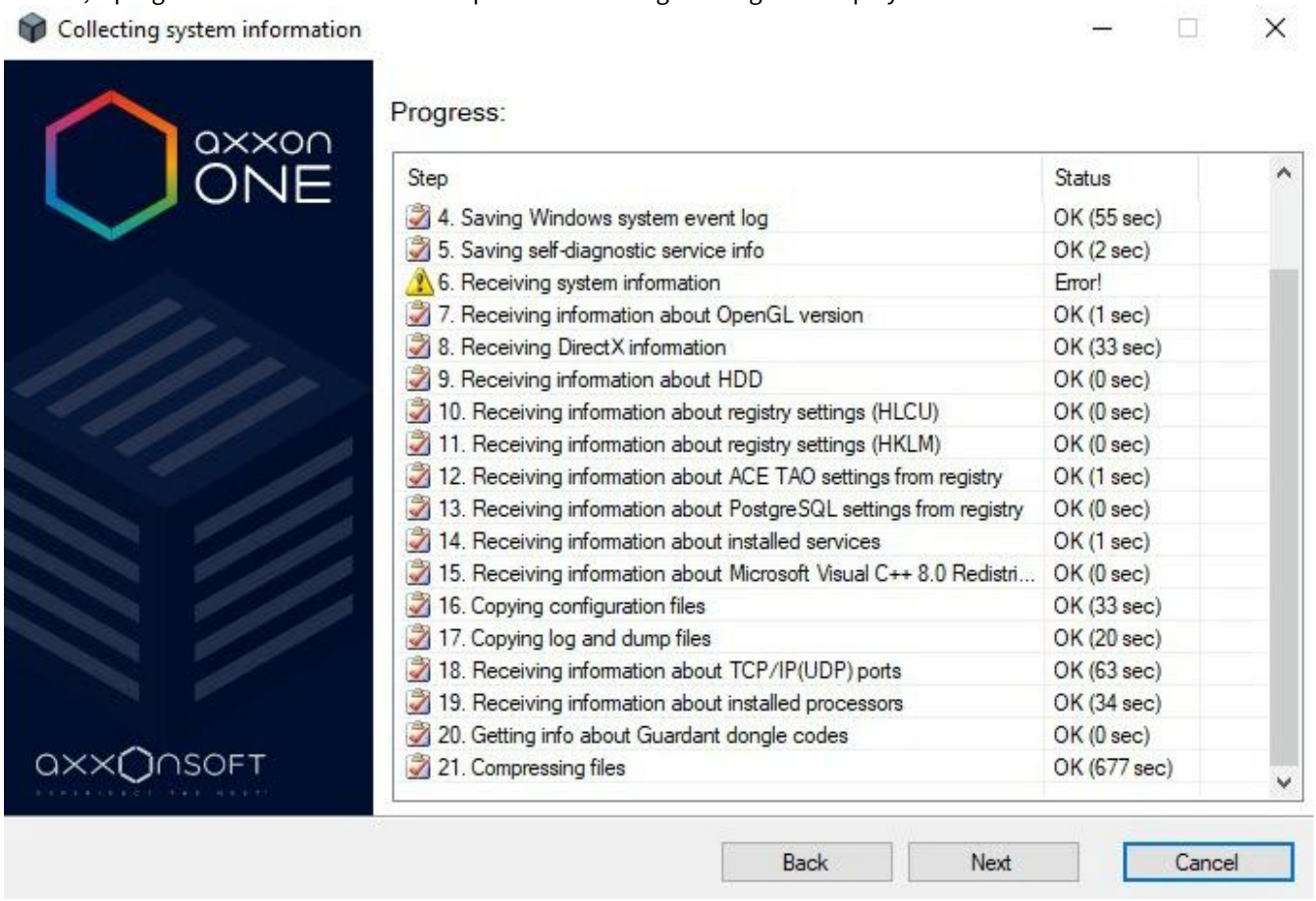
17.3.5 Collecting Data on the Configuration of Servers and Clients Using the Support

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(see page 863)).

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(see page 619)) 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 **Status**. 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.

17.4 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)

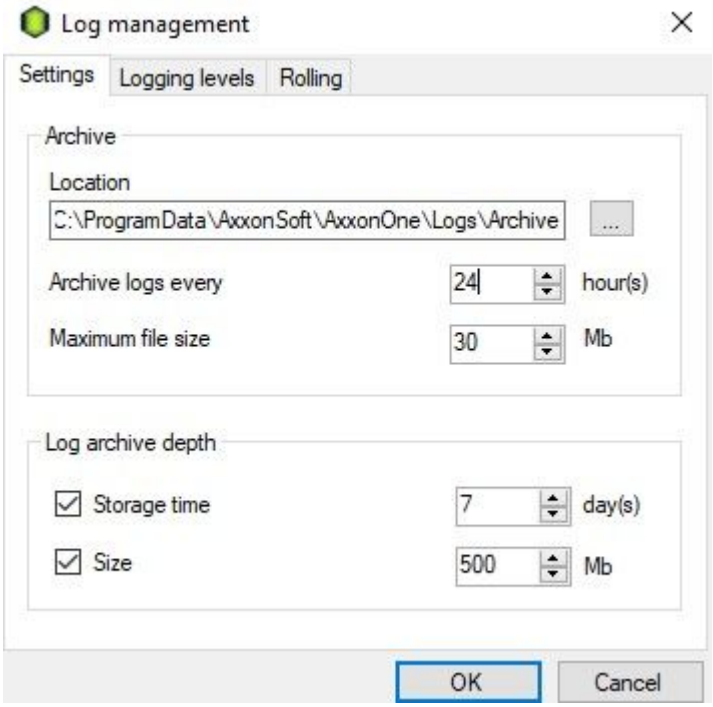
The log management utility is used to configure the following parameters:

1. Parameters for the archive of external logs containing information about system events.
2. Loging levels for the *Axxon One* Client and Server.

17.4.1 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).

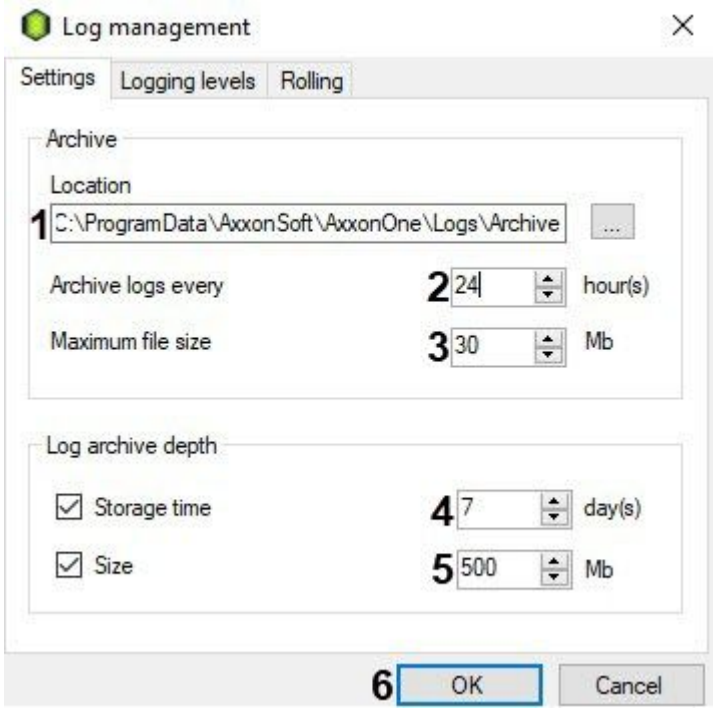
17.4.2 Configuring a Log archive

Configuring a log archive is carried out in the **Settings** tab of the log management utility.

To configure a log archive, you must perform the following steps:

1. In the **Location** field (**1**), enter the complete path to the directory to which the event logs should be moved after archiving.

   > **Note**
   >
   > To set the path using standard Windows methods, click ... .



2. In the **Archive logs every...hour(s)** field (**2**), enter the interval for event log archiving, in hours.
3. Set the maximum size of the log archive file in megabytes (**3**). When the specified size is reached, a new log archive file is created.
4. In the **Log archive depth** group, set the following parameters:
    a. In the **Storage time** field (**4**), indicate the maximum retention time in days of a log in the archive, after which the log is deleted.
    b. In the **Size** field (**5**), indicate the maximum size of the archive, above which the oldest logs are deleted from the archive.

> **Note**
>
> Archive disk space restrictions take priority over log retention time restrictions. For example, the oldest logs will be automatically deleted even if their retention time has not expired, if the archive size has exceeded the maximum value.

> **Note**
>
> If it is not necessary to impose any limitations on log retention period and/or size, clear the corresponding check boxes in the **Log archive depth** (**4**-**5**).

5. Click **OK** (**6**) to save changes.

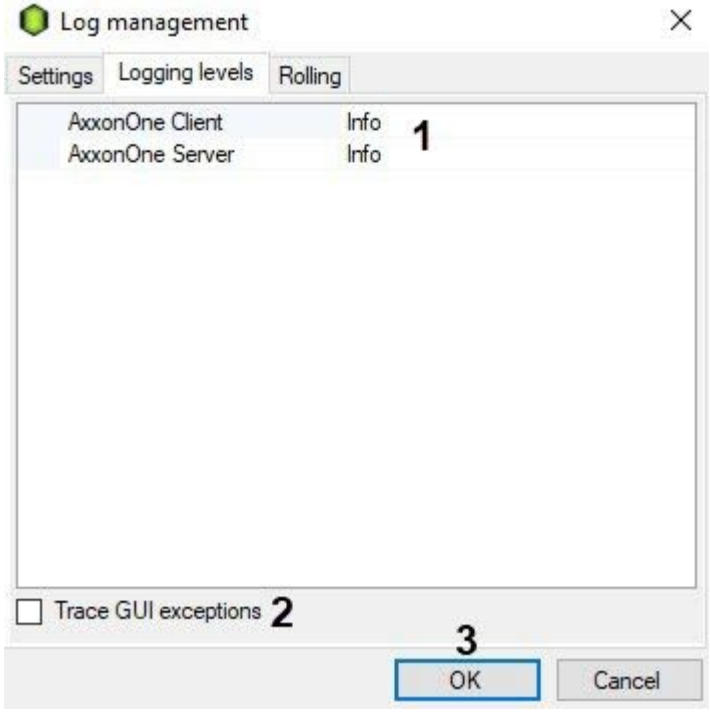
Configuration of the log archive is now complete.

17.4.3 Configuring 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). Configuration of levels is carried out in the **Logging levels** tab of the log management utility.

To configure the logging level, you must perform the following steps:

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.

> **Note**
>
> If the *Axxon One* VMS is installed in the **Failover Server and Client** configuration, you can log in as either a Client or a Supervisor.

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

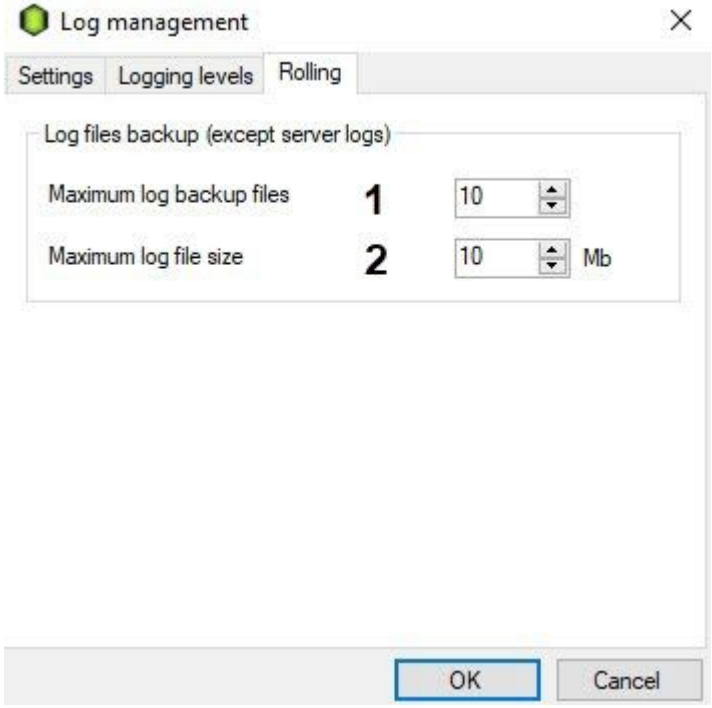
2. If you need to include GUI exceptions into the logs, select the corresponding check box (**2**).
3. Click **OK** (**3**) to save changes.

Configuration of logging levels is complete.

17.4.4 Set the size and maximum number of logs

To adjust the size and maximum number of logs:

1. Switch to the **Rolling** tab.

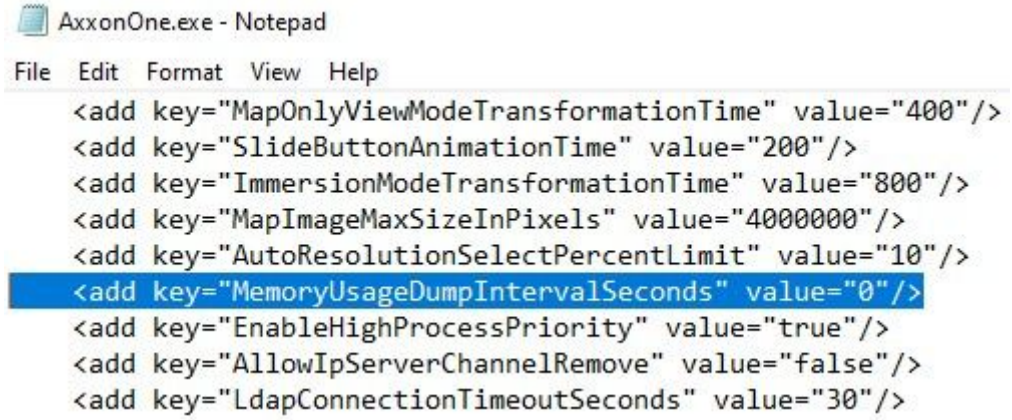


2. Set the maximum number of logs (**1**).
3. Set the maximum size of the log in megabytes (**2**). When the specified size is reached, a new log is created.
4. Click **OK** to save changes.

17.4.5 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(see page 99)).
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 an Axxon One Client(see page 94)).

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.

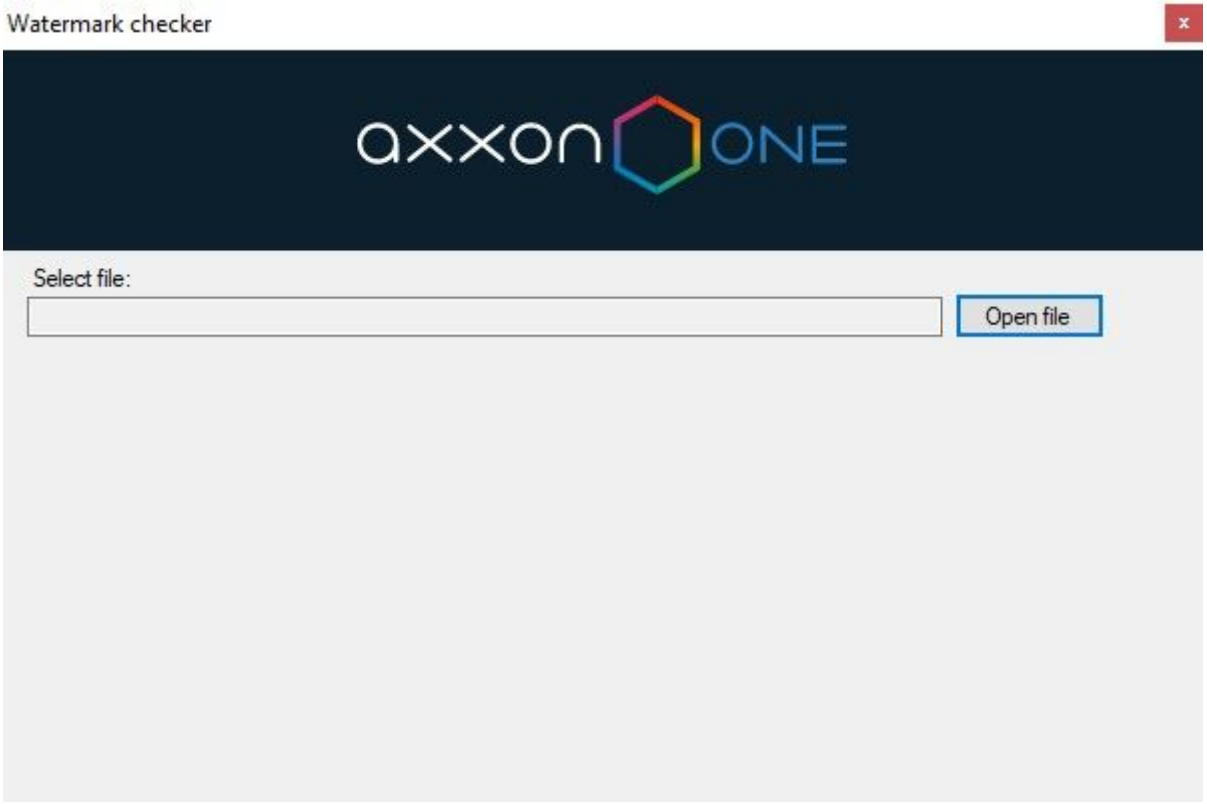
17.5 Digital signature verification utility

This utility verifies the digital signature that is added during export of video and snapshots from *Axxon One*.

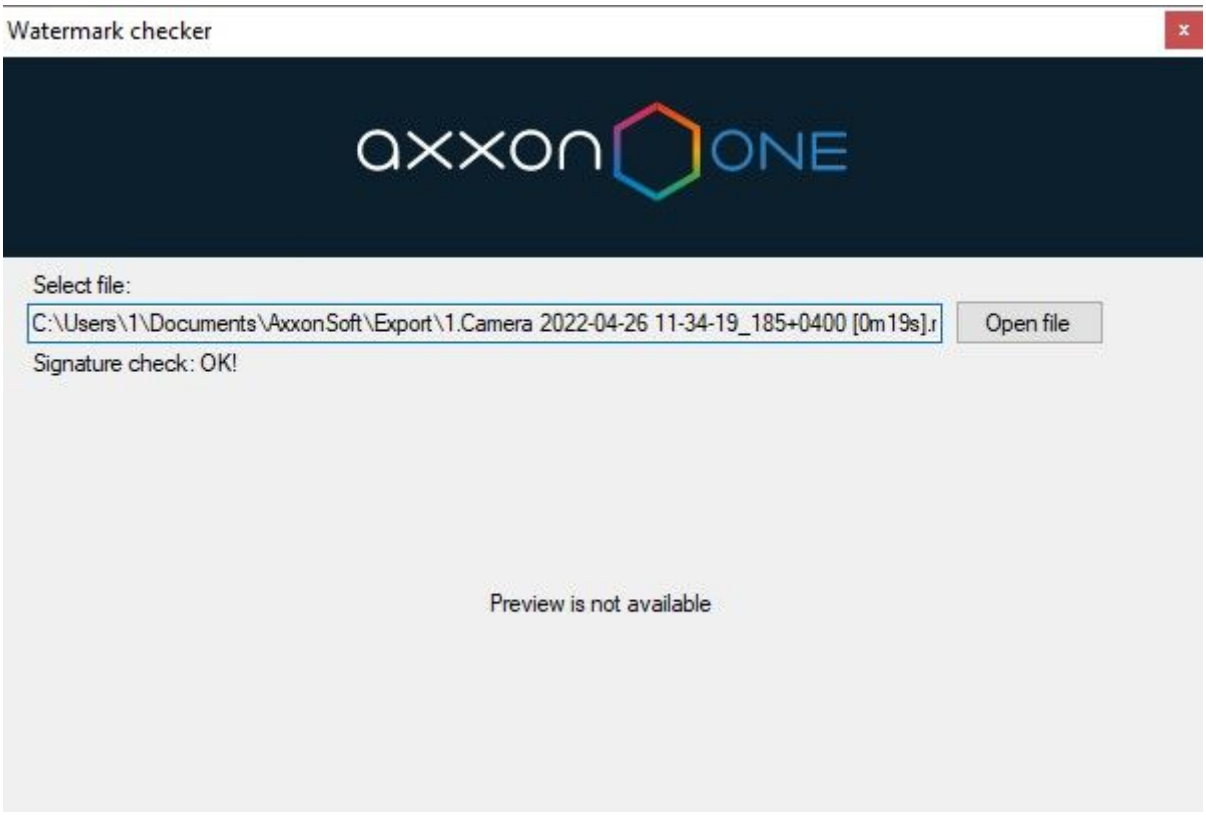
To start the utility, open the standard **Start** menu in Windows: **Start > Programs > Axxon One > Utilities > Watermark checker**.

> **Note**
>
> The utility executable file WatermarkCheck.exe is also located in the folder <System disk>:\Program Files\AxxonSoft\AxxonOne\bin\.

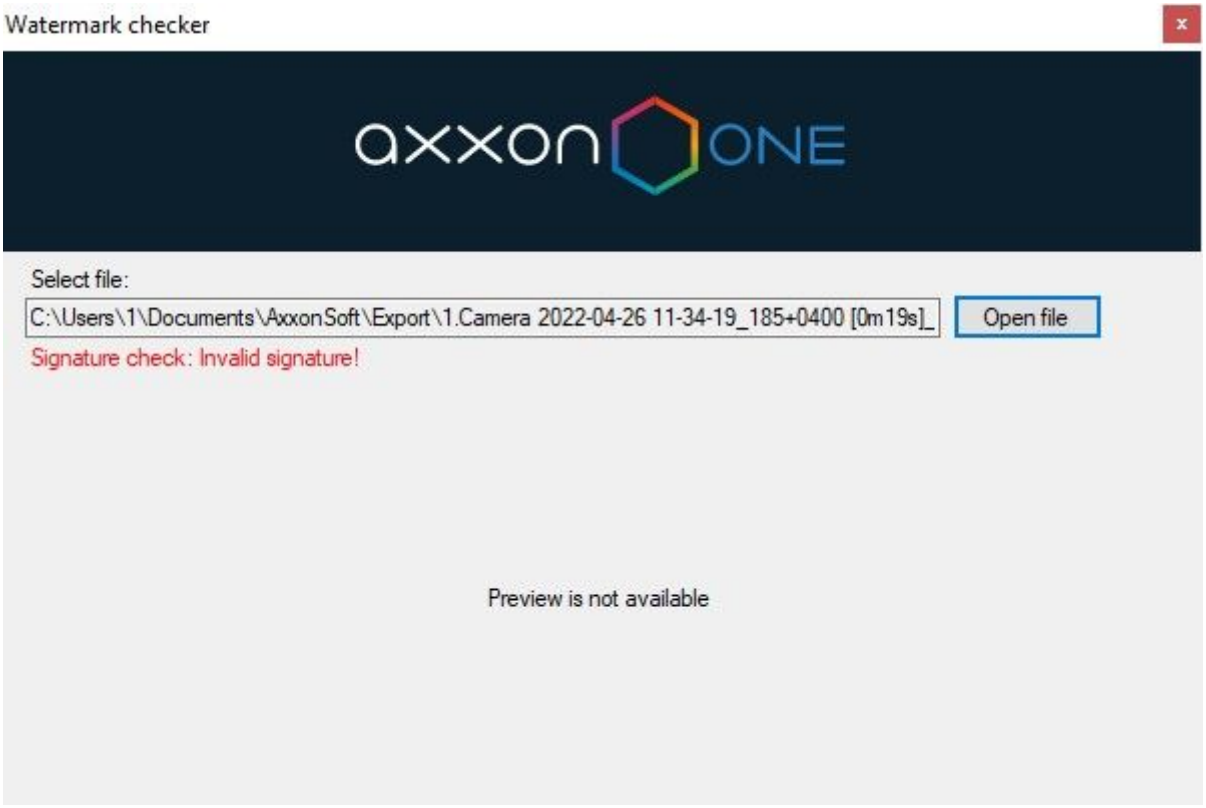
To check a digital signature, click the **Open file** button and select the file of the exported snapshot or video.



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.

17.6 Backup and Restore Utility

17.6.1 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.

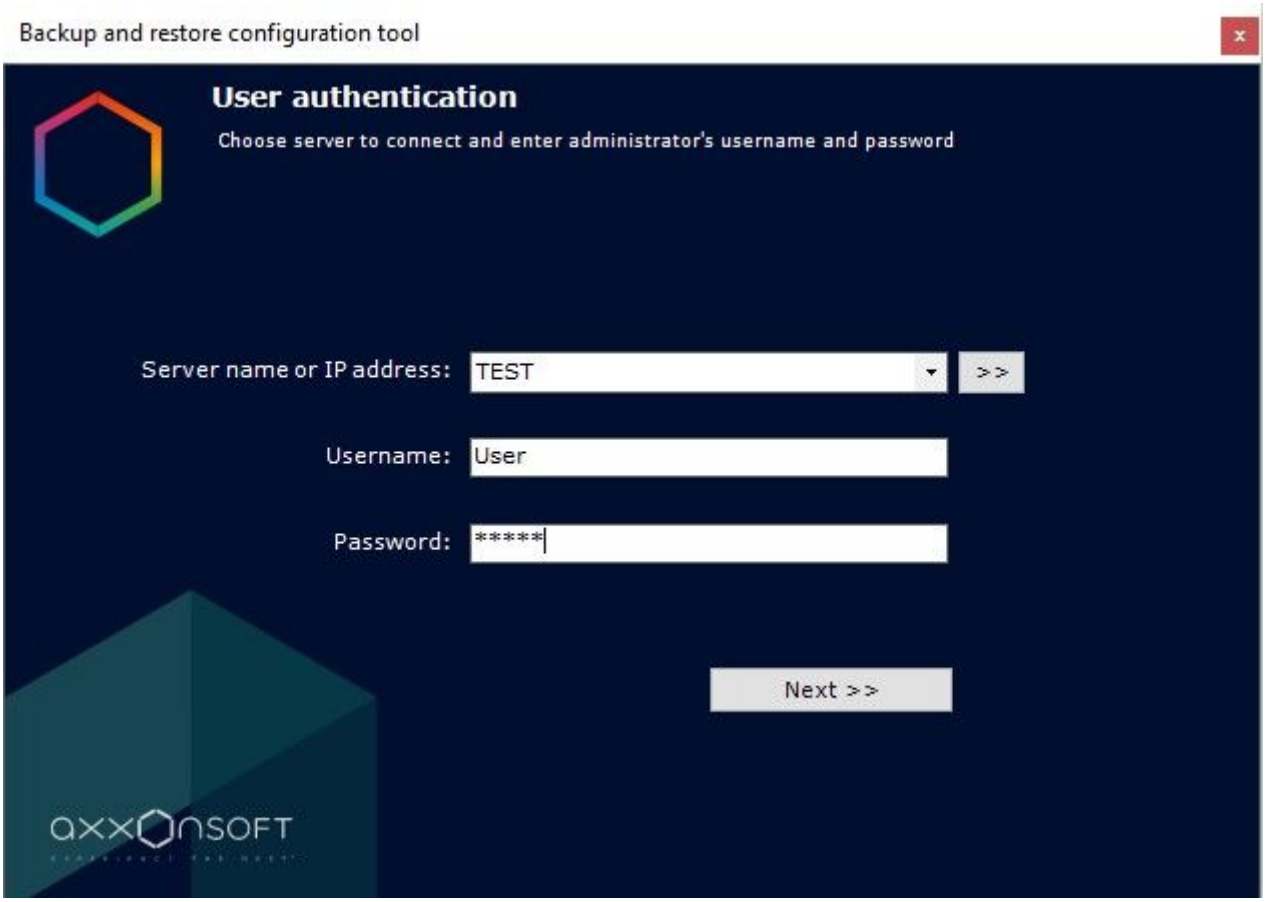
17.6.2 Starting and quitting BackupTool.exe

Start BackupTool.exe from **Start** -> **All Programs** -> **Axxon One** -> **Utilities** -> **Backup and restore**, or from the tray menu (see the Axxon One Tray Tool(see page 860) section).

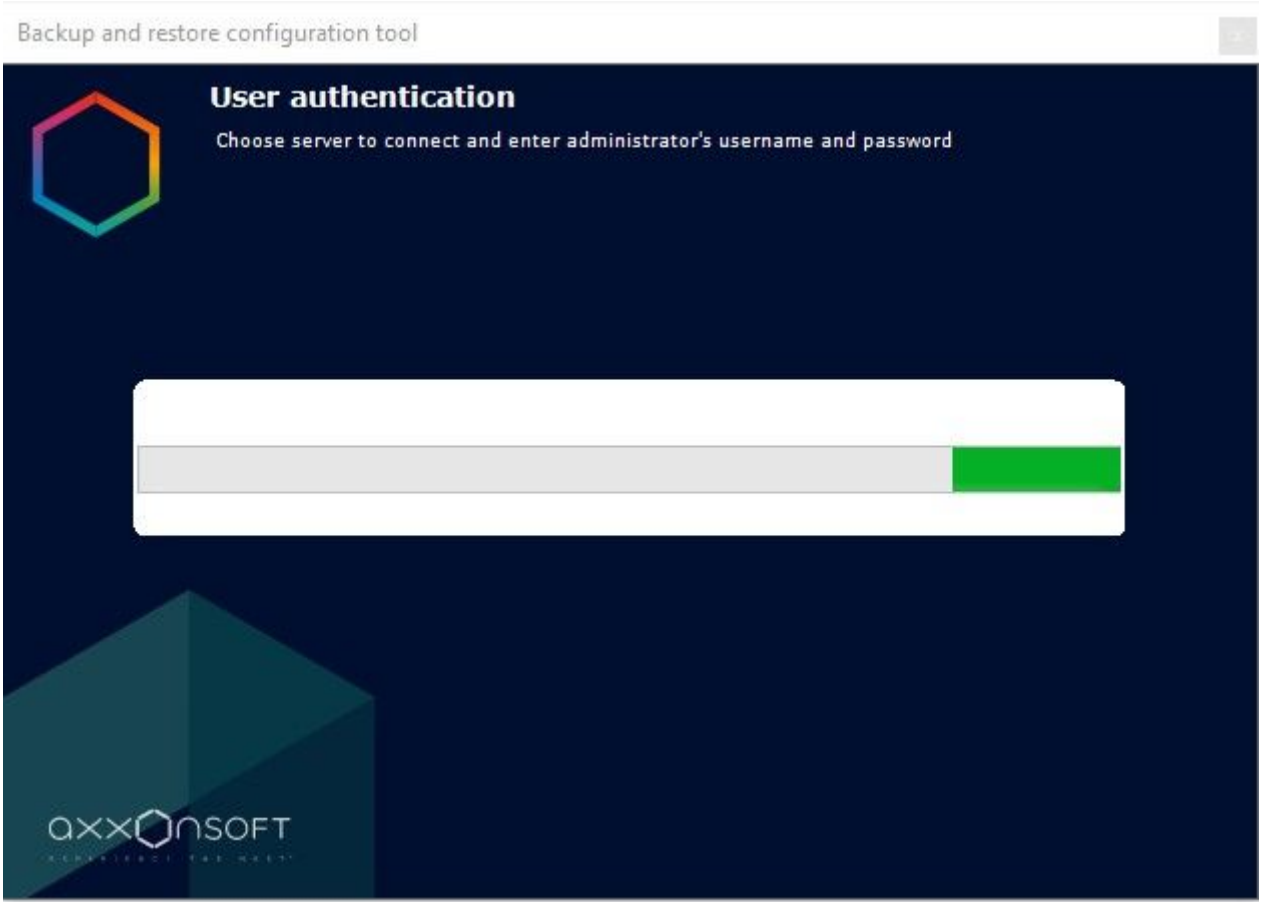
> **Note.**
>
> The BackupTool.exe executable is located at <*Axxon One* installation folder>\Axxon One\bin\.

After you perform this action, BackupTool.exe displays a dialog box.

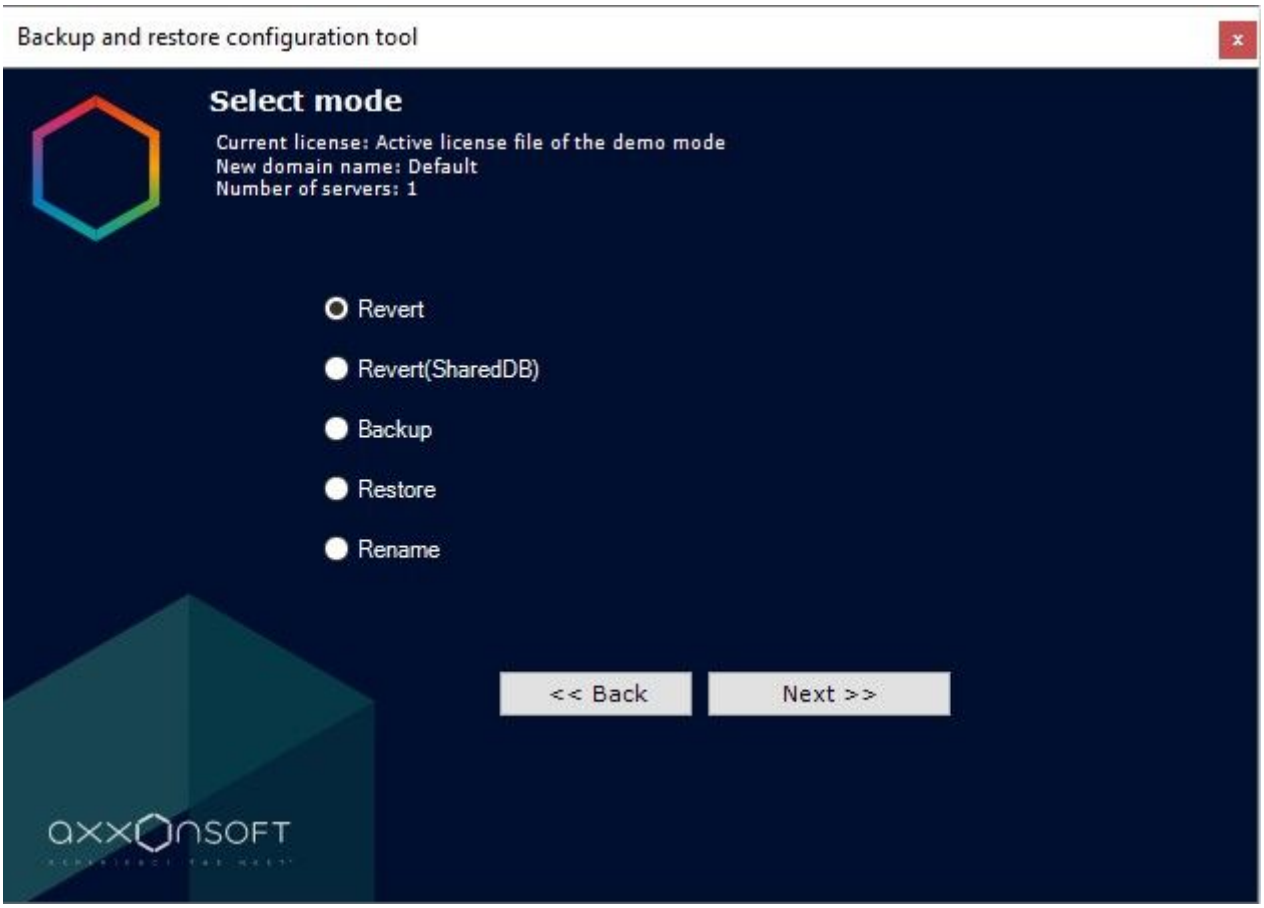
Then select the name of an Axxon-domain Server whose configuration you want to use and log in to it, using the name and password of an *Axxon One* administrator.



A progress indicator is displayed.



After loading is complete, the main page of the Backup and restore utility is shown.

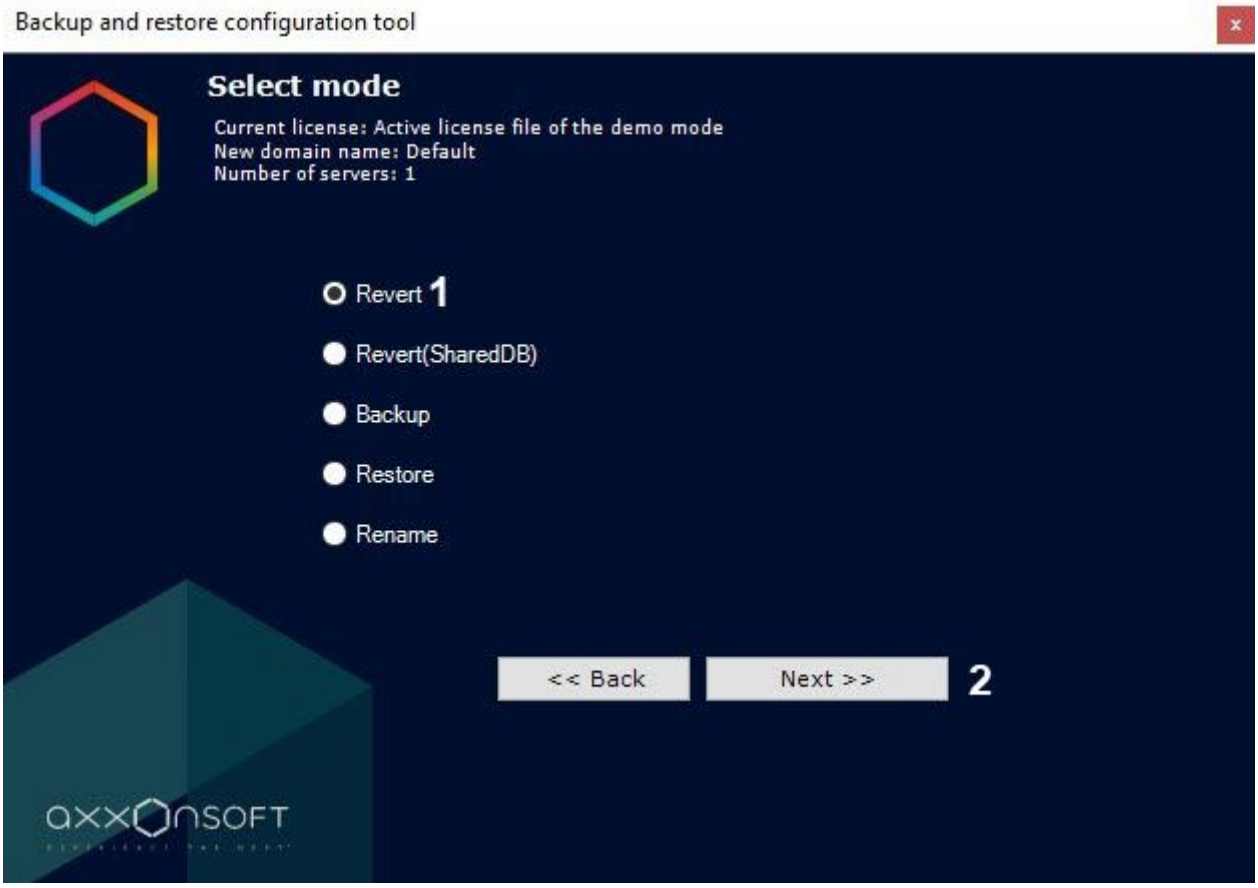


To quit BackupTool.exe, click the button.

17.6.3 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**).

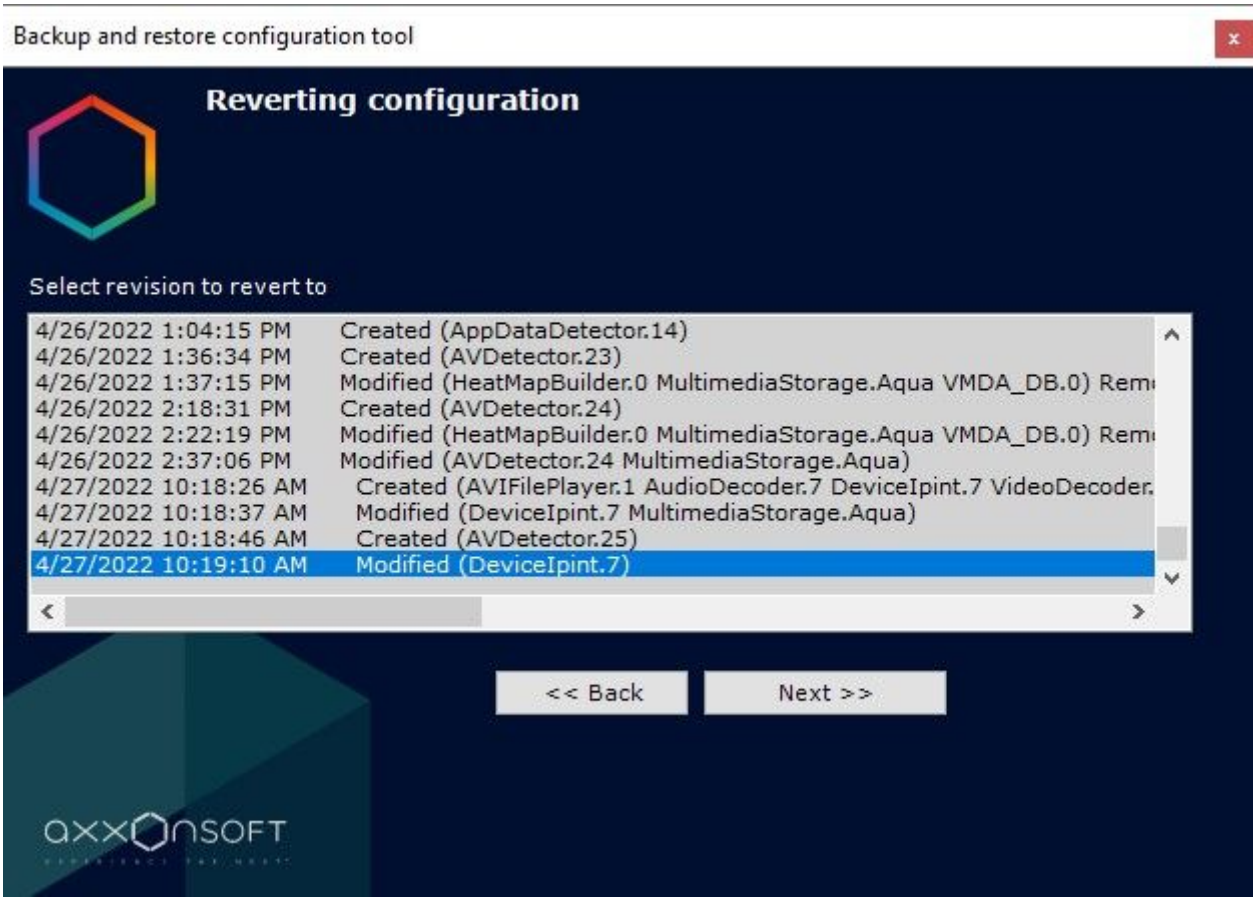


A window then opens, displaying a list of available restore points and their respective creation times, with a description of what was changed.

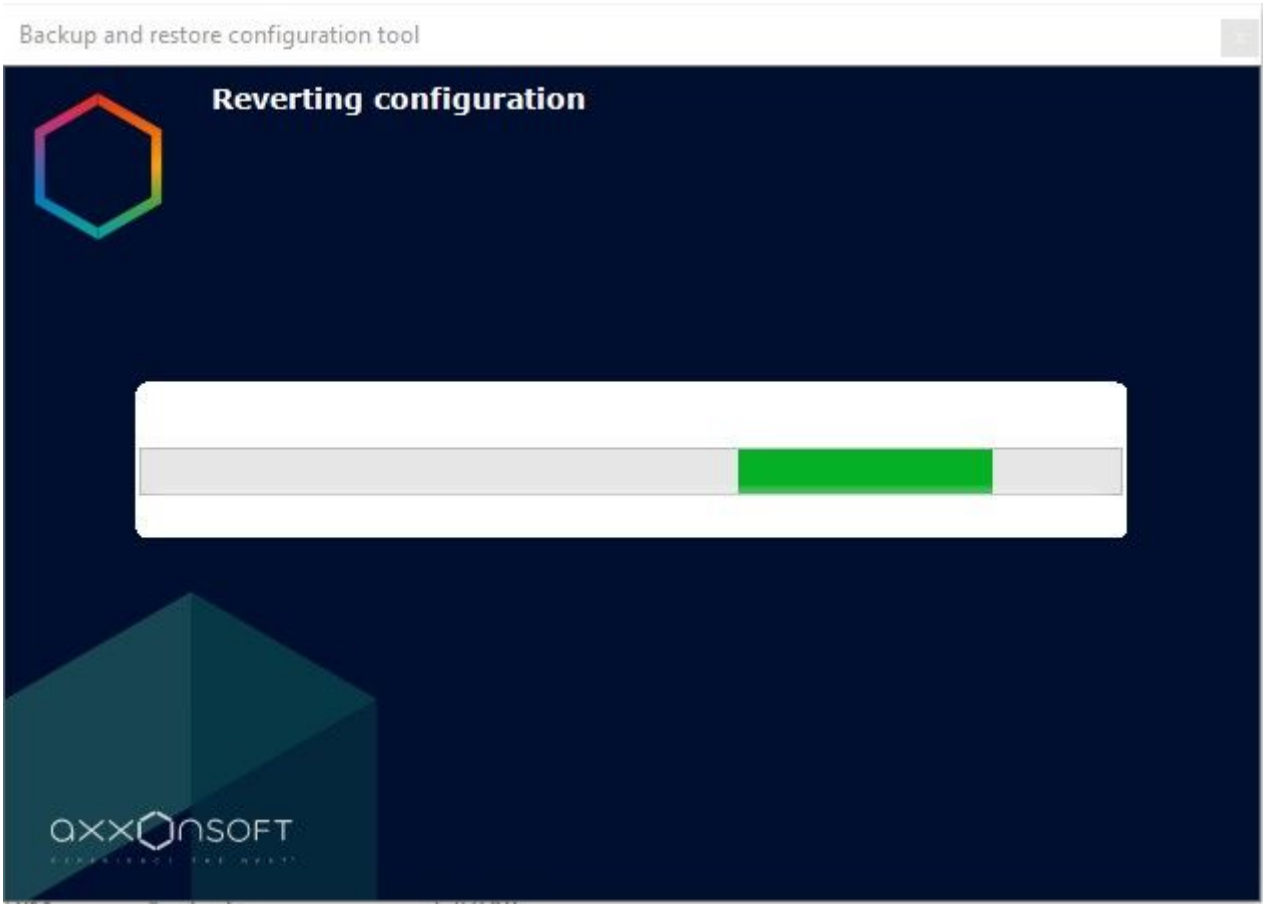
> **Note.**
>
> If multiple changes were made in a configuration but the **Apply** button was clicked only once, only one restore point is created in the list.

In the list, select the restore point to which you want to roll back. To continue, click the **Next** button.

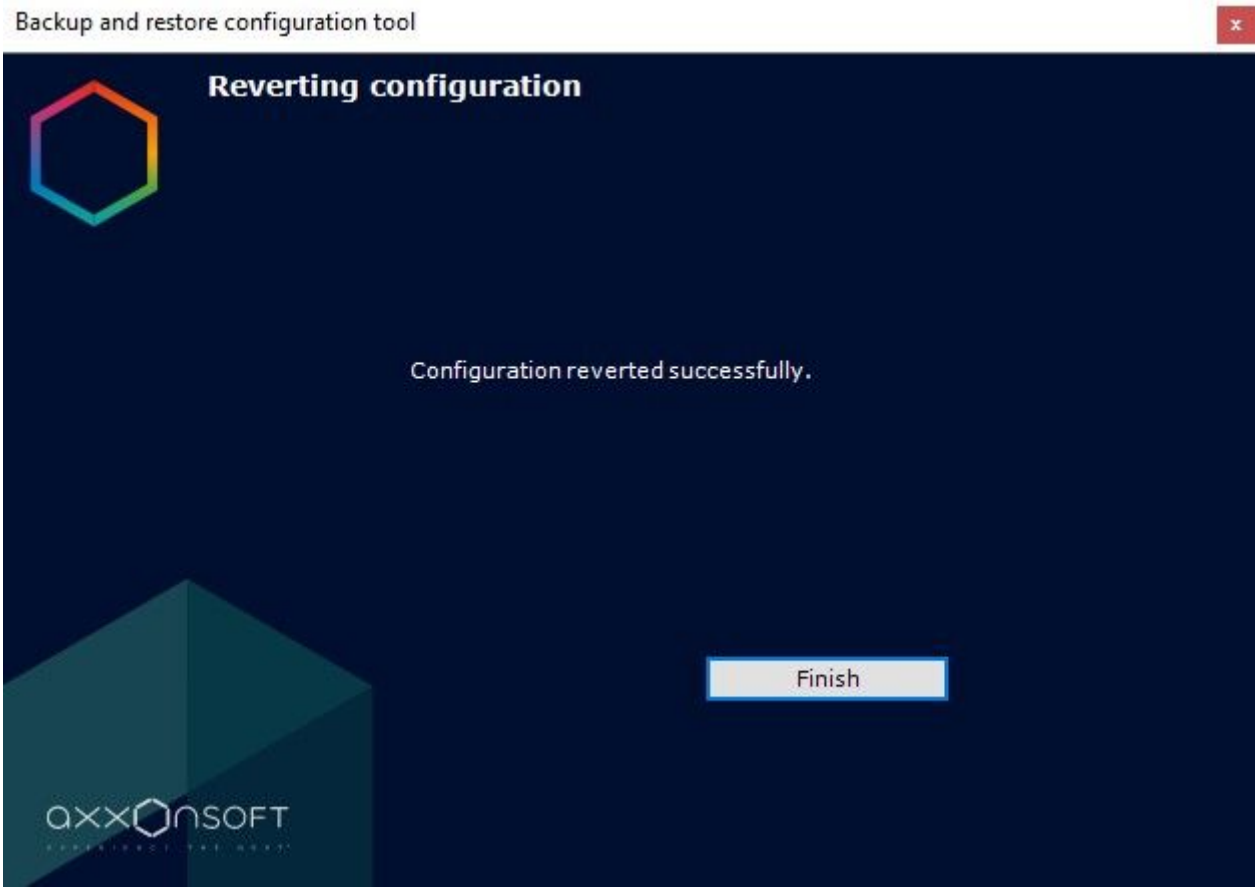
> **Note.**
>
> **Empty configuration** corresponds to when the system was first created.



Rollback of the configuration now begins.



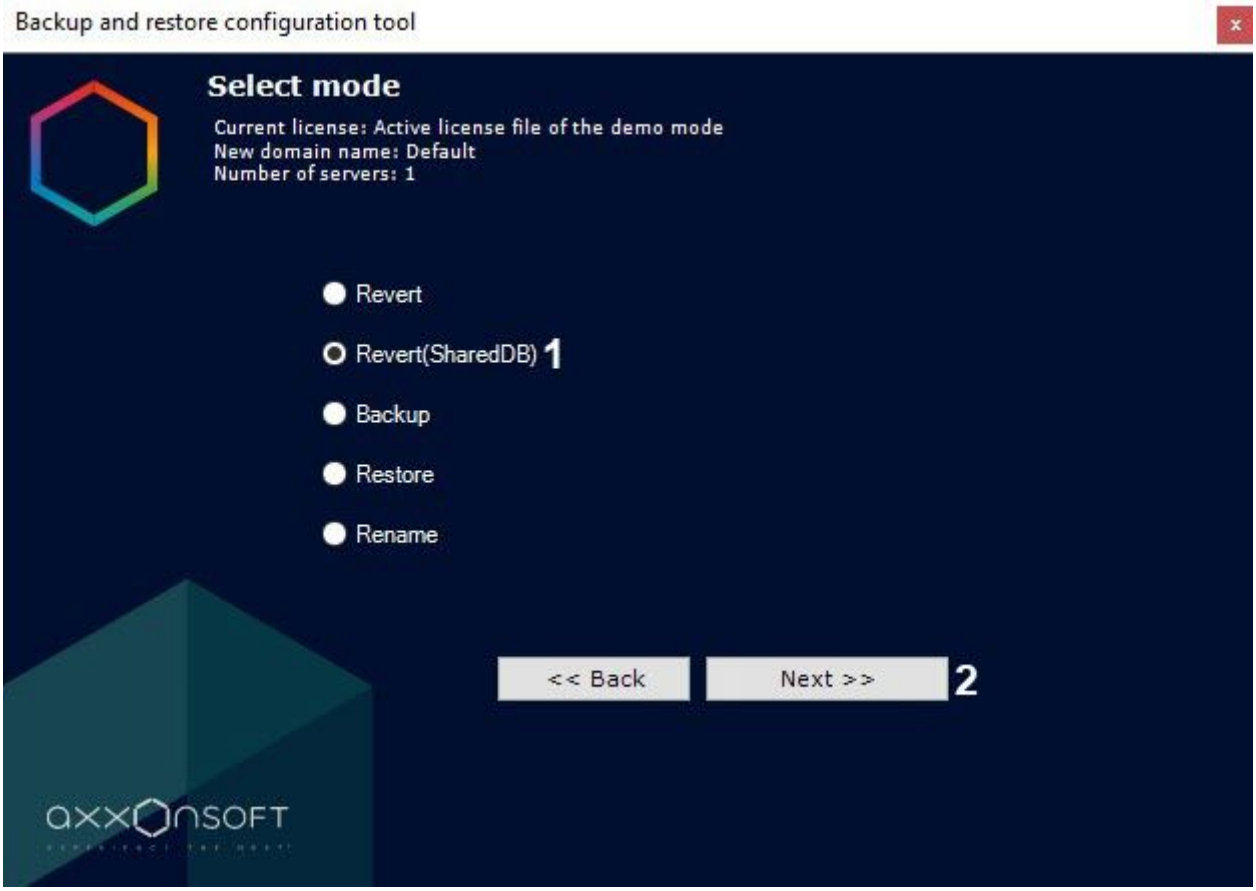
After the operation is completed, a message is shown to notify of successful rollback.



To close the window, click the **Finish** button.

17.6.4 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 >>** (**2**).



Further steps are the same as for rolling back the local configuration (see Roll back the local configuration to a selected restore point(see page 880)).

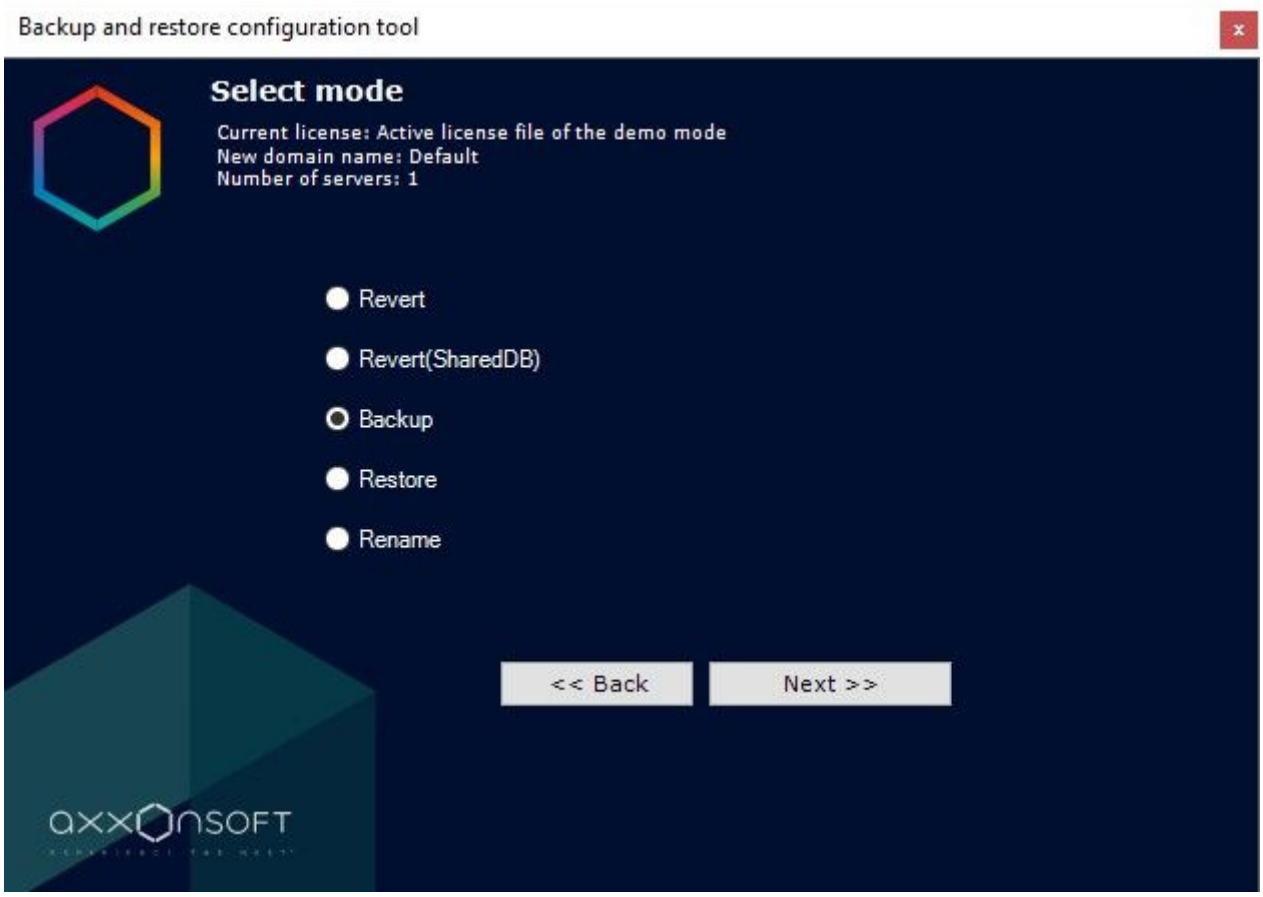
17.6.5 Configuration backup

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.

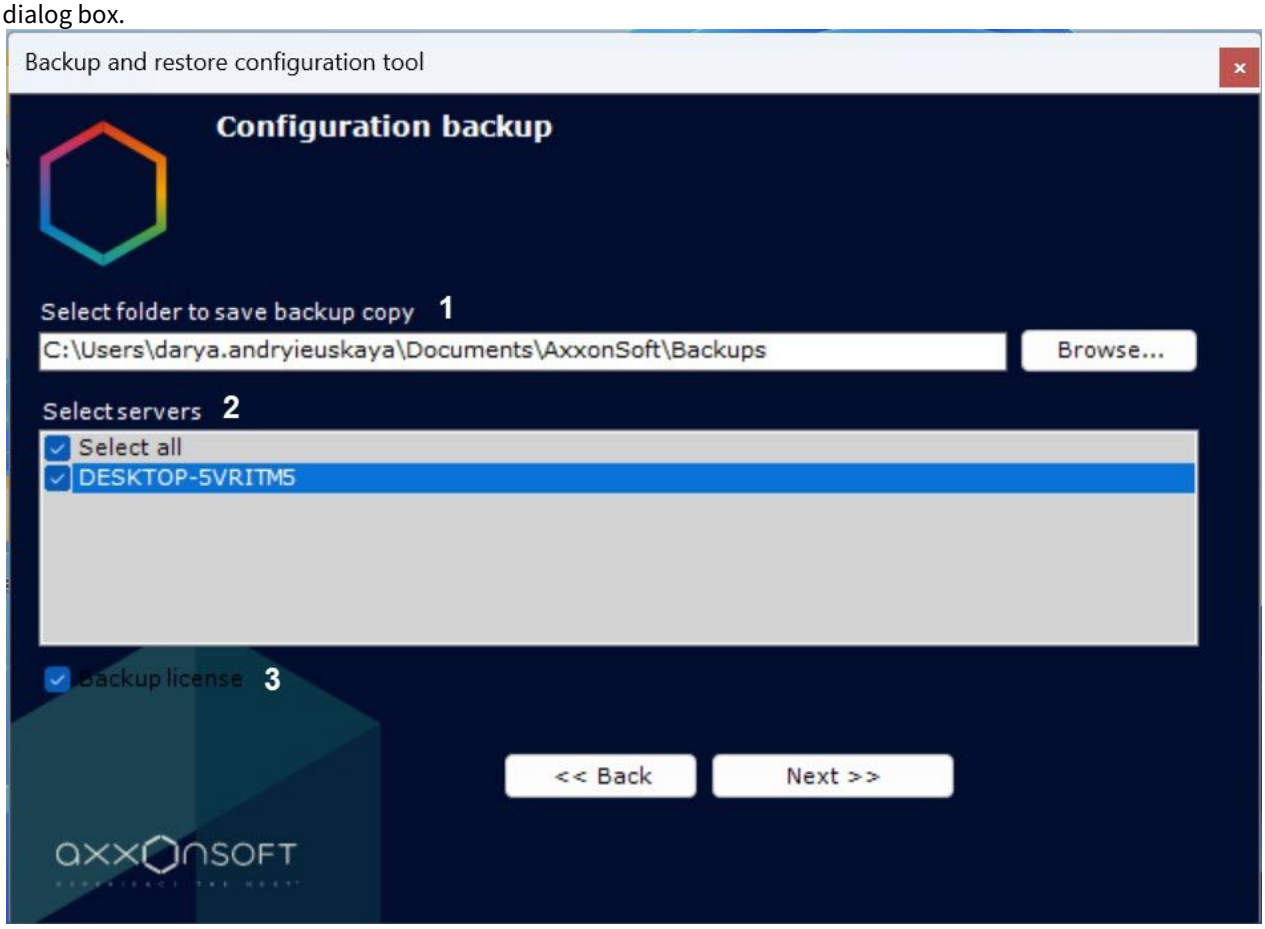
To create a backup of the system configuration:

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

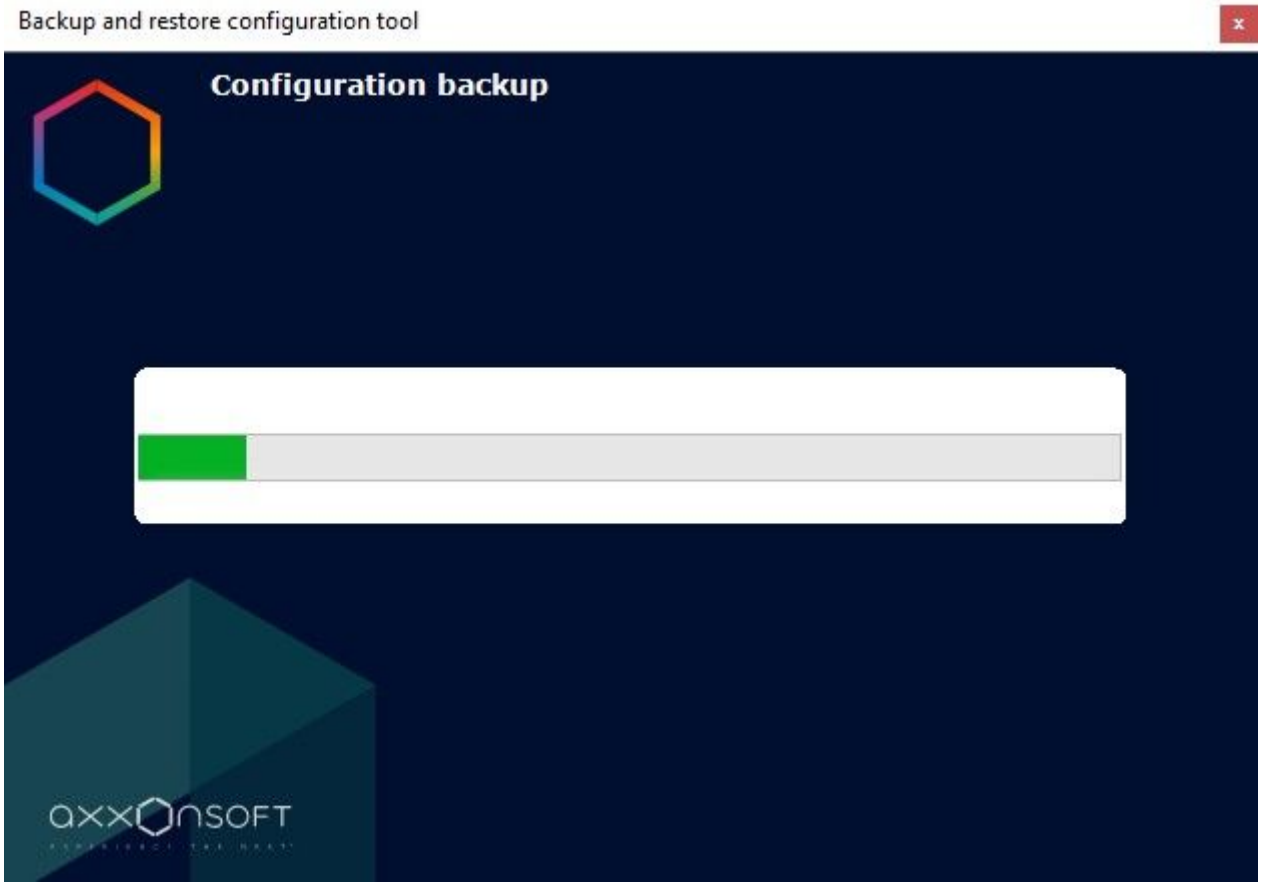
dialog box.



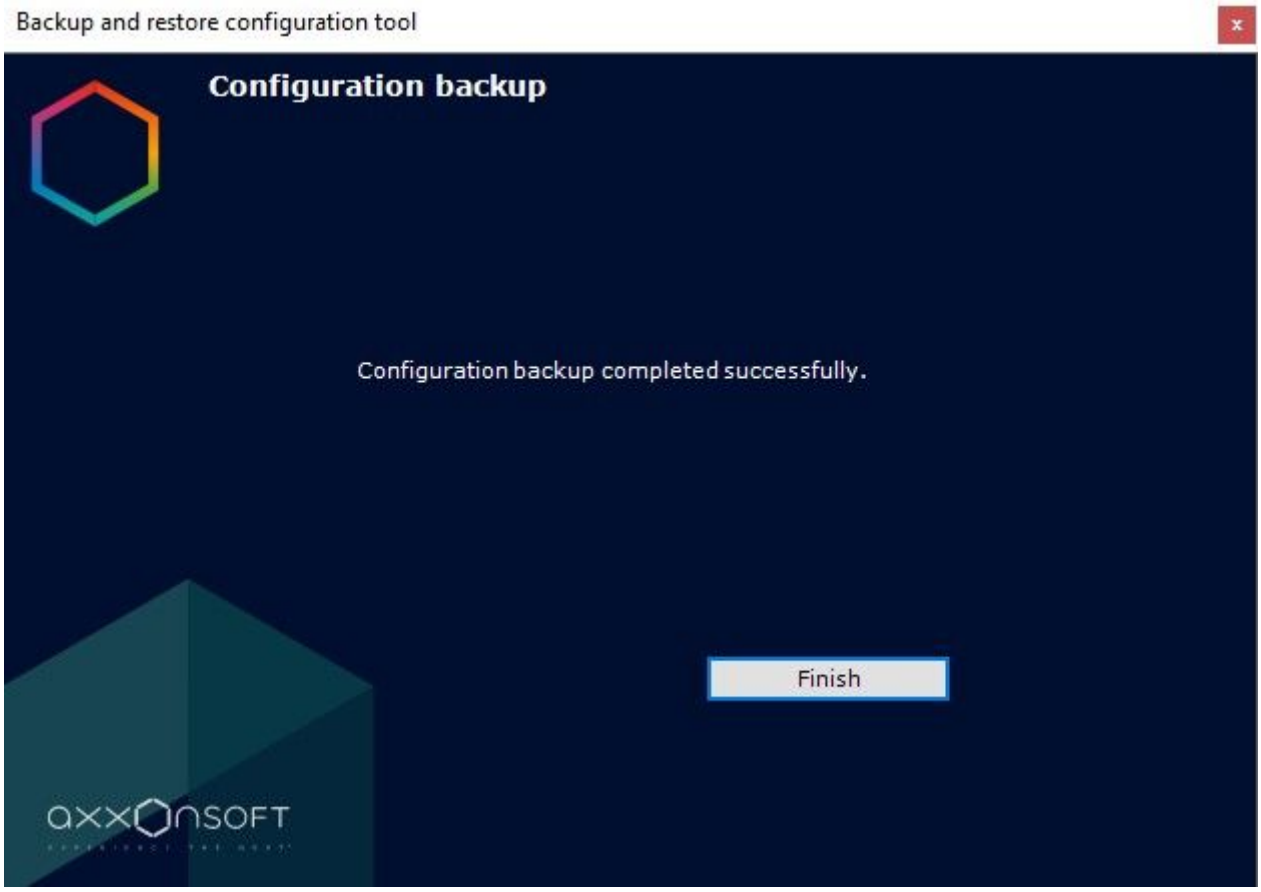
> **Note**
>
> For each copy of the backup configuration, a separate folder is created. The folder name contains the date and time of the backup copy and has the following format: YYYYMMDDHHMMSS. The default time zone is UTC + 0

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.

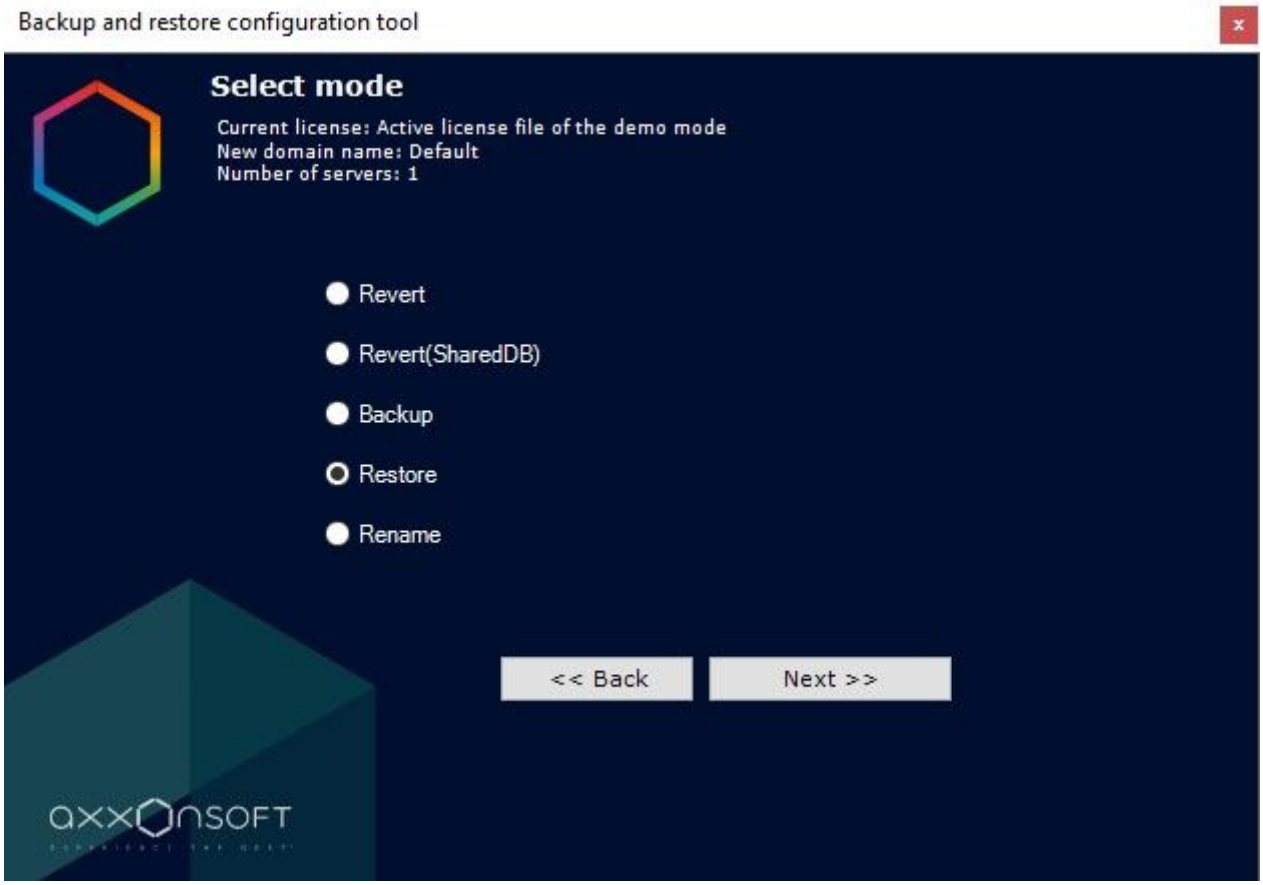
17.6.6 Configuration restore

> **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 (for licensing without the Guardant key).
>
> The information about the product version and the PC's HID can be found in a JSON file in the saved configuration folder.

> **Attention!**
>
> To successfully restore a configuration, please ensure that the current Server name is exactly the same as the Server name in the backup configuration.

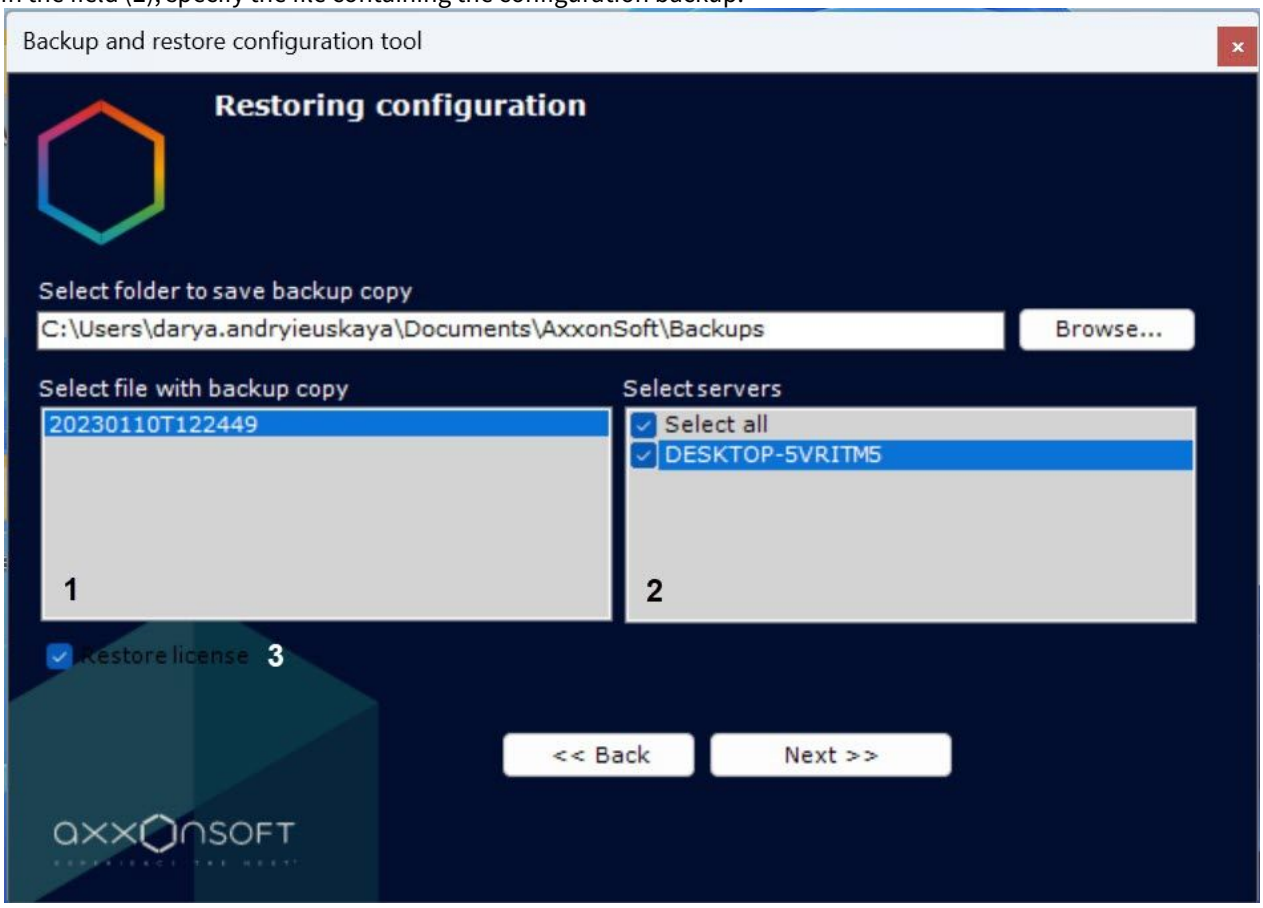
To restore a configuration:

1. On the main page of the Backup and restore utility, set the switch to the **Restore** position.



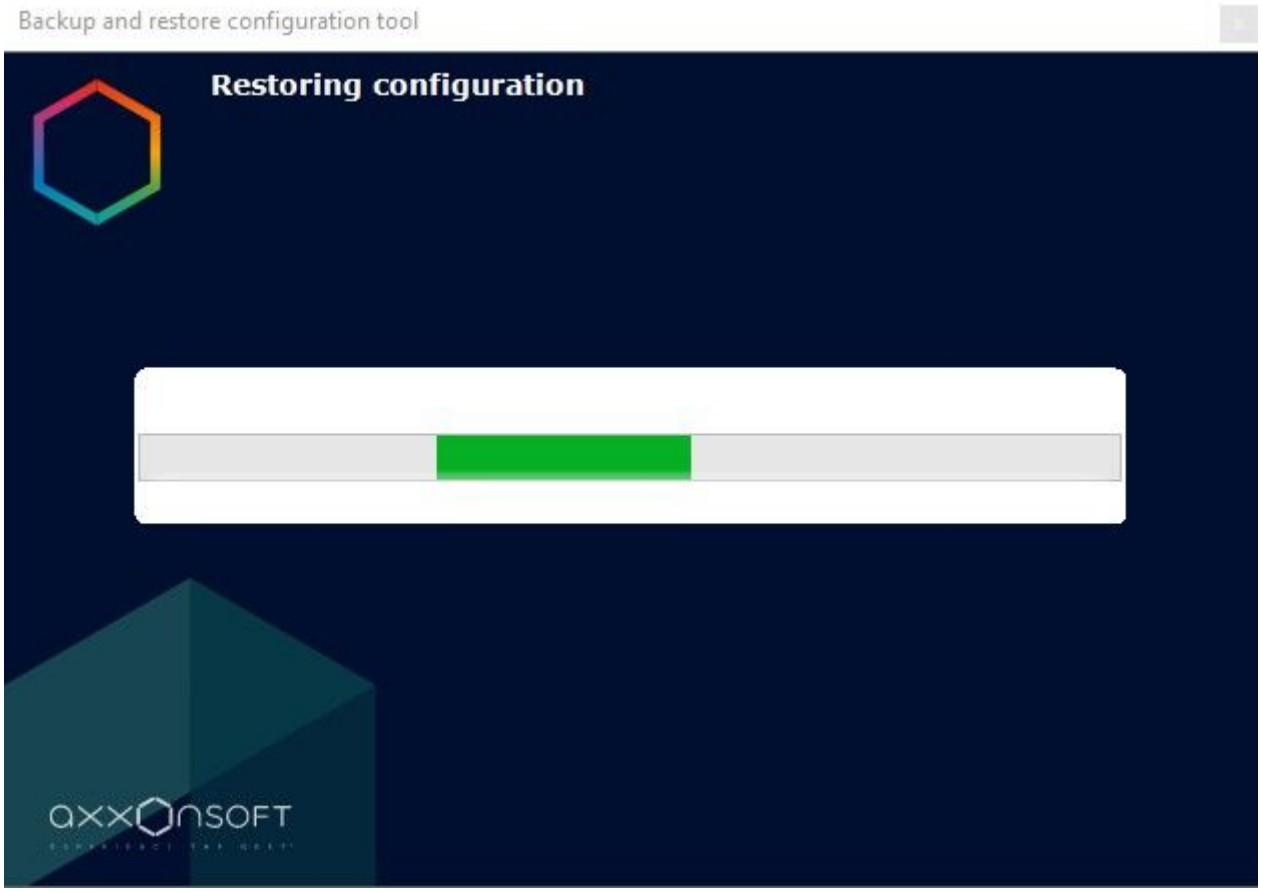
A window then opens for configuring restoration of the configuration.

2. In the field (**1**), specify the file containing the configuration backup.

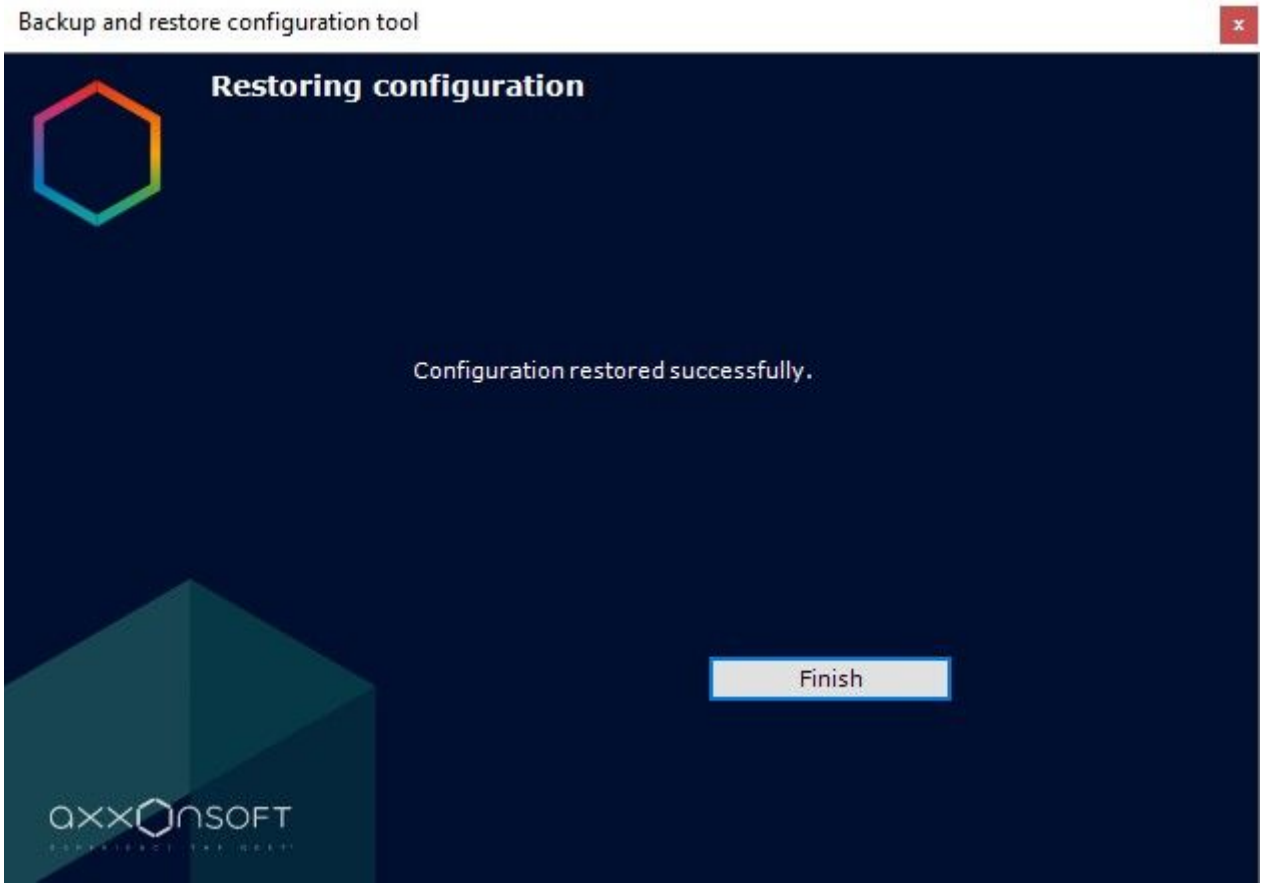


3. After the file is opened, the servers on the current domain are displayed in the other field (**2**). You can select a server in the list only if it is on the domain and the open file contains the corresponding backup.
4. Set the **Restore license** checkbox (**3**) to restore the license key that was saved at the configuration backup stage (see Configuration backup(see page 885)). 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.

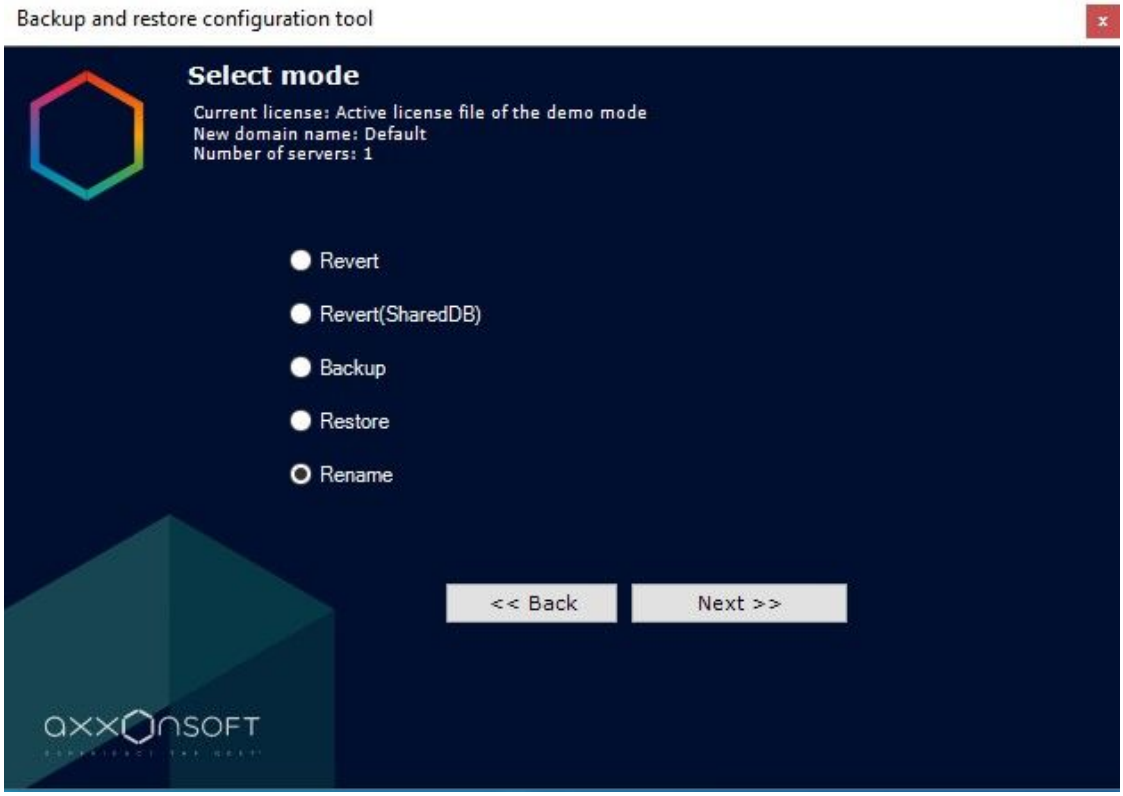
17.6.7 Changing the Server name

To change the local Server name using the Backup and Restore Utility, do the following:

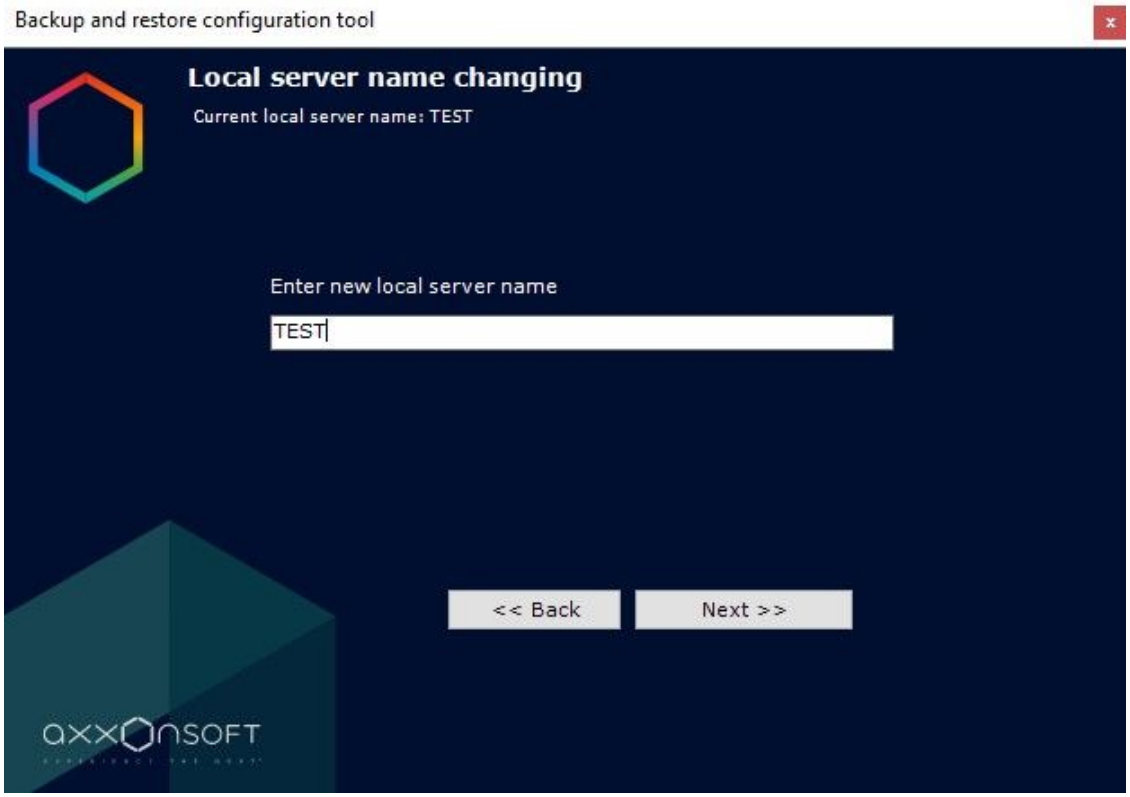
> **Attention!**
>
> After this command is completed, the Server is excluded from Axxon-domain. You will not be able to access the archive. All maps, automatic rules and macros will be deleted. The cameras of the renamed Server will be deleted from the layouts.

1. Connect to the Server that requires a name change (see Starting and quitting BackupTool.exe(see page 877)).

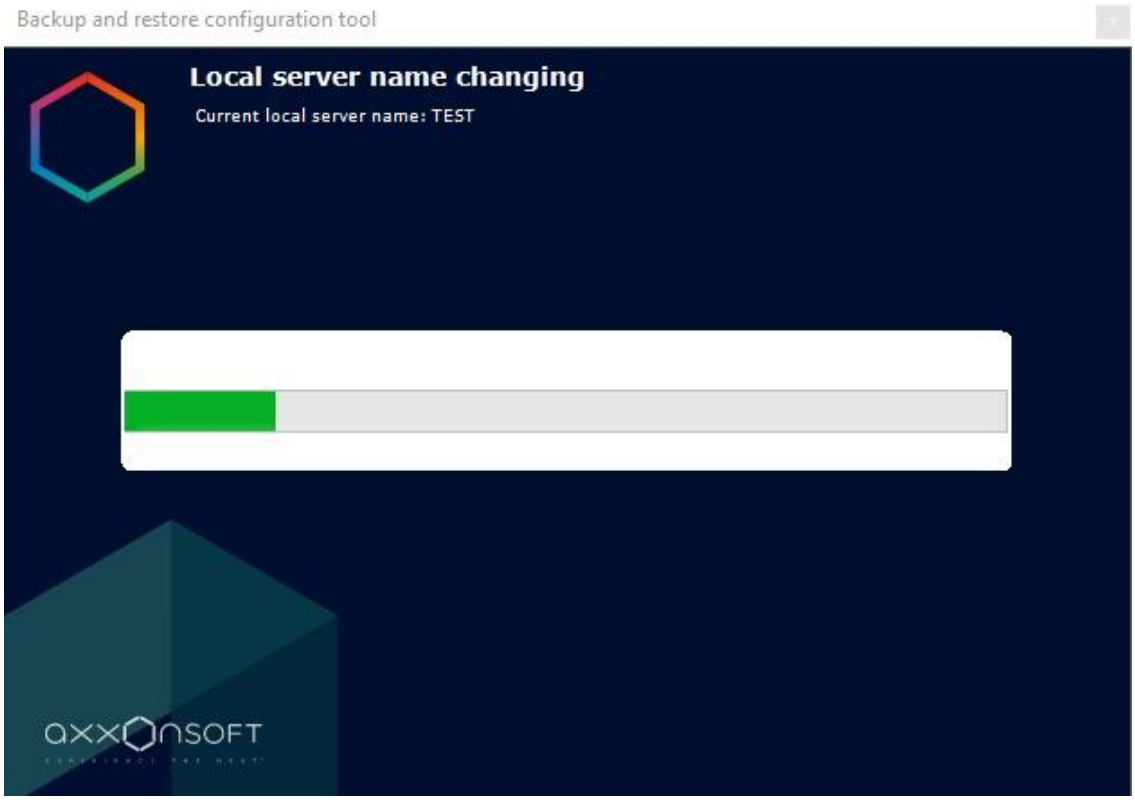
2. Select **Rename** and click the **Next** button on the Utility main page.



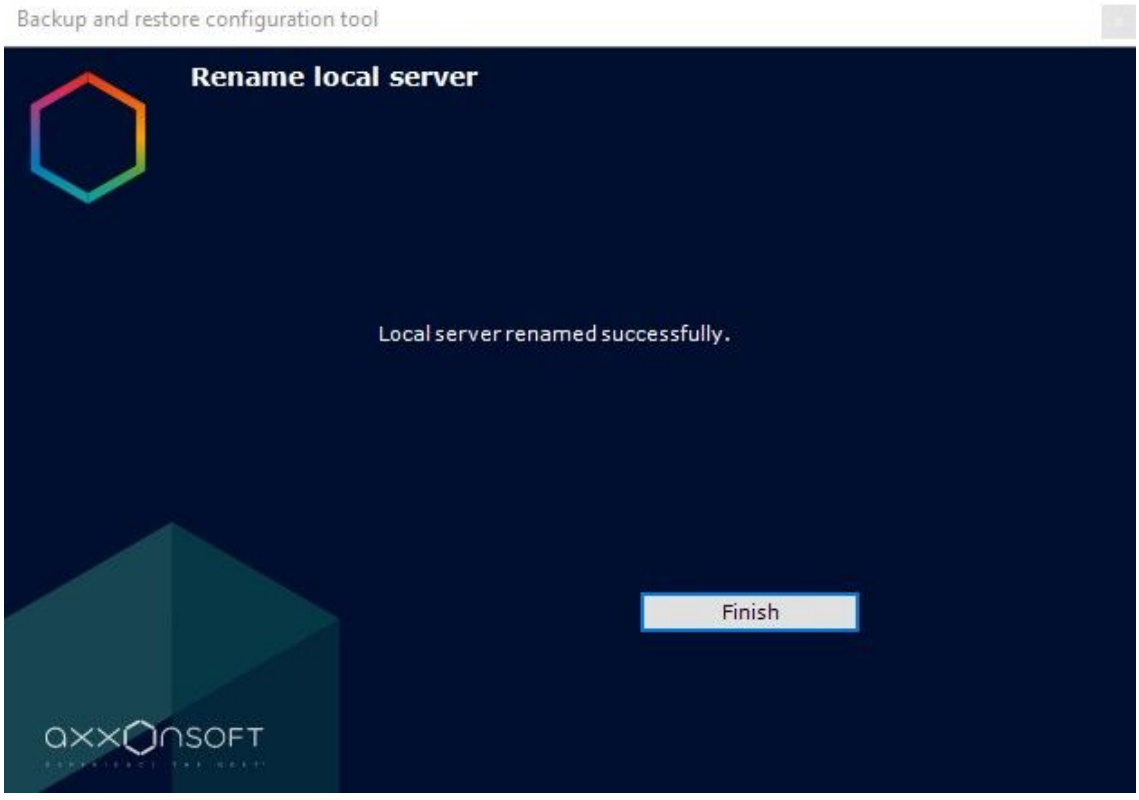
3. Enter the new Server name and click the **Next** button.



The Server name change process will start.



If the operation completes successfully, a notification message will appear.

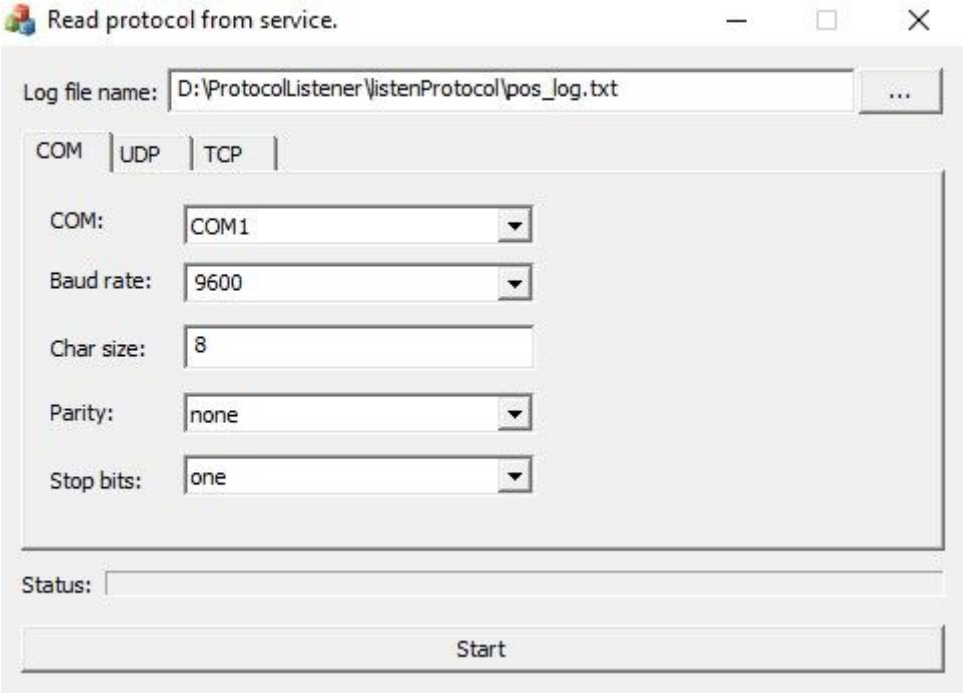


Server name change is complete.

17.7 POS-terminal log collection utilit

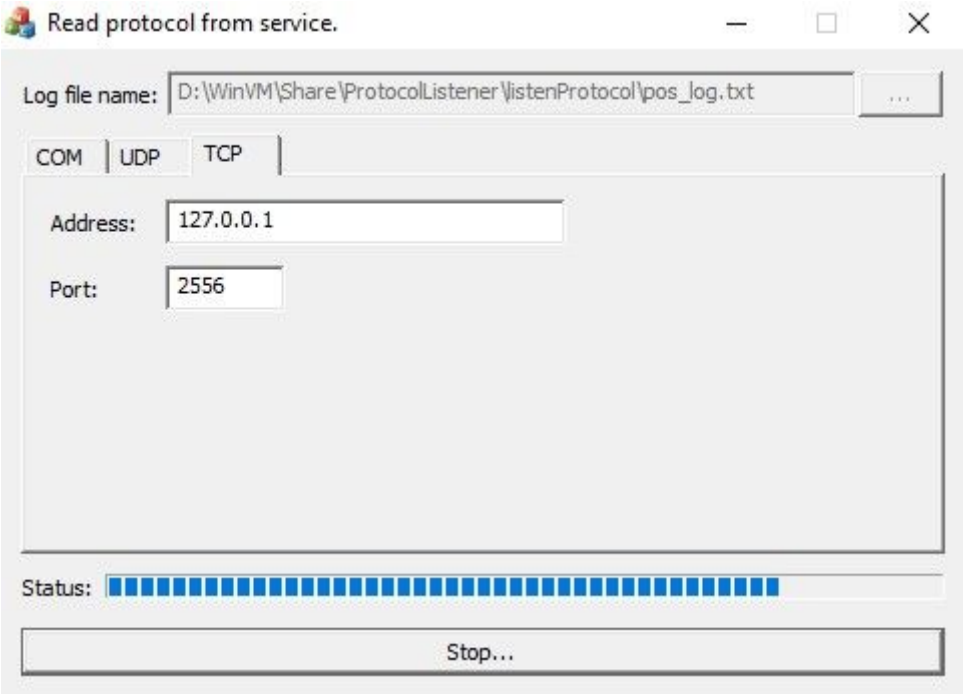
To collect information from the POS-terminal using a special utility, do the following:

1. Disable the Event Source object (see Configuring POS devices(see page 193)) and shutdown the Server (see Shutting down a Server(see page 100)).
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[199].
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.

199 https://www.axxonsoft.com/support/downloads/utilities



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.

17.8 Console utility for working with archives

vfs_format.exe is a console utility for working with *Axxon One* archives.

Attention!

For the correct operation of the utility, you have to remove the corresponding archive volume in *Axxon One* without removing the archive files (see Removing archive volumes(see page 231)).

The utility is located in <*Axxon One* installation folder>\bin>.

Attention!

Run the command line as Administrator.

Note

To launch 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.

The utility contains the following parameters:

Parameter	Description
--help	Help window

Parameter	Description
--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	Populate an archive with multiple copies of video footage from another archive. The system fills up a destination archive with multiple copies of a source archive. For easier timeline handling, each new copy is written with 1 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
--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 re-indexing 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.

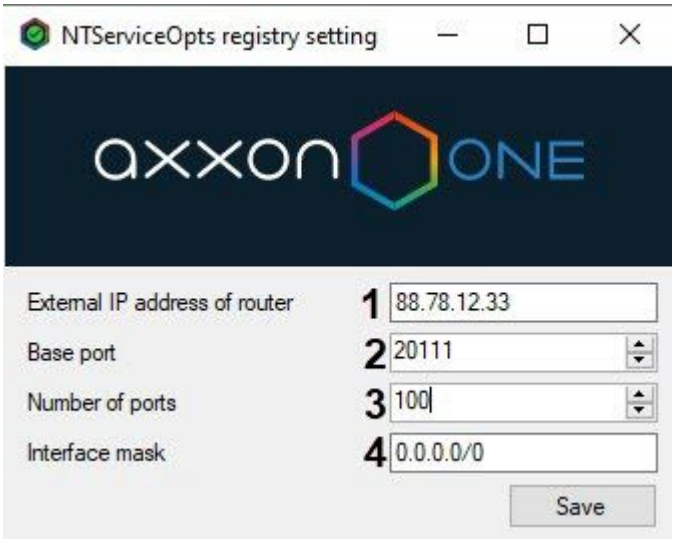
Parameter	Description
--clear-meta	Delete metadata of the archive volume. For example: vfs-format.exe --volume D:\ --clear-meta
--clear-data	Delete the archive volume service information (does not operate without the **from** and **to** arguments). For example: vfs_format.exe --volume C:\archiveAliceBlue.afs --clear-data --from 20220210T110000 --to 20220210T114000. --from and --to are used to set the UTC time intervals in the ISO YYYYMMDDThhmmss format. Then you should confirm the deletion.
--log-level	Set the logging level for this action. Available values: • 0 – OFF • 10 – ERROR • 20 – WARN • 40 – INFO • 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.

To log error messages, you should add a 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.

17.9 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[200] (**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.

200 https://en.wikipedia.org/wiki/Network_address_translation

18 Appendices

18.1 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.

18.2 Appendix 2. Known issues in the Axxon One Software Package

18.2.1 Possible errors during installation

On the page:

- Error connecting to the Postgres Database(see page 904)
- Error installing Drivers Pack(see page 904)
- Window 10 OS installation error(see page 904)
- Server error on Windows 11 OS and Windows Server 2019 OS(see page 904)
- An error occurred when installing on Windows with the language pack Norsk (bokmål)(see page 905)
- Error uninstalling Axxon One on systems with Videoinspector installed(see page 905)

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.

18.2.1.1 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(see page 905).

18.2.1.2 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'.
```

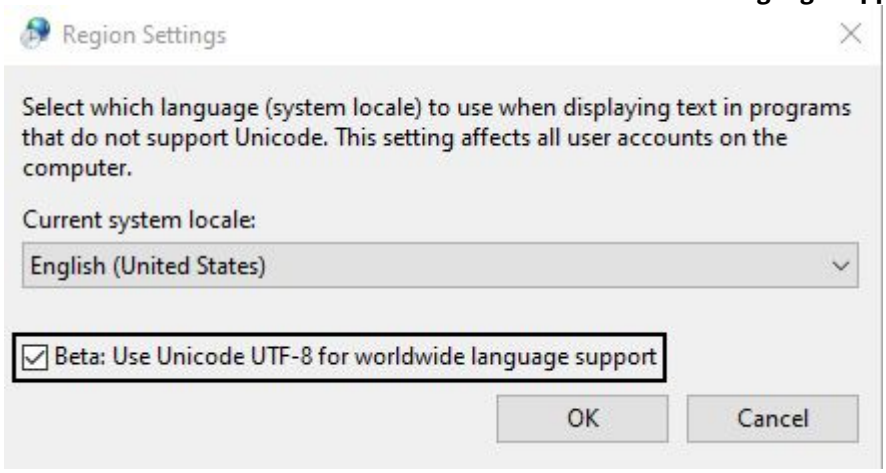
This can be solved by installing the Windows update KB2999226[201].

18.2.1.3 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*.

18.2.1.4 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.

201 https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows

18.2.1.5 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).

18.2.1.6 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.*

18.2.2 Possible Errors During Start-Up

18.2.2.1 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.

18.2.3 Possible Errors During Operation

On page:

- All video channels or archives stop working once the license maximum is reached(see page 906)
- No signal from video cameras and failure to connect to other Servers(see page 906)
- Incorrect display of Client interface elements(see page 906)
- Server error on Windows Server 2012(see page 906)
- Emergency shutdown of the Client on Windows 8.1(see page 906)
- Error creating new archives even when license restriction on total capacity is observed(see page 906)
- Axxon One VMS operation with Windows Defender software(see page 907)
- Upper panel display problem(see page 907)
- High CPU load during OpenGL software emulation(see page 907)
- Axxon One operation with NetLimiter 2(see page 907)
- Exported videos' playback in Movies and TV application(see page 907)
- Axxon One operation on Windows N and KN editions(see page 907)

18.2.3.1 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.

18.2.3.2 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.

18.2.3.3 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.

18.2.3.4 Server error on Windows Server 2012

You may experience errors when running the Server on Windows Server 2012. To fix the errors:

1. Go to the registry branch HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems\.
2. Find the **Windows** parameter and change its value as follows: in the string "SharedSection = 1024,20480, **768** ", replace **768** with **4096**.
3. Save the changes and restart the computer.

18.2.3.5 Emergency shutdown of the Client on Windows 8.1

You may see the Client shutting down on Windows 8.1 with an error: " The name of the failed module: KERNELBASE.dll Exception code: 0xe0434352 ".

In this case, please contact Microsoft support.

18.2.3.6 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.

18.2.3.7 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.

18.2.3.8 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[202] drivers.

18.2.3.9 High CPU load during OpenGL software emulation

If your computer's graphics card does not meet OpenGL requirements (see Limitations of Axxon One(see page 46)), OpenGL can be emulated in software.

But in this case the CPU load may be high.

18.2.3.10 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.*

18.2.3.11 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.

18.2.3.12 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[203].

18.3 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(see page 62)).

202 https://www.intel.com/content/www/us/en/support/products/80939/graphics.html
203 https://support.microsoft.com/en-us/topic/media-feature-pack-list-for-windows-n-editions-c1c6fffa-d052-8338-7a79-a4bb980a700a

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.

18.4 Appendix 4. Using Axxon One with antivirus software

On the page:

- ESET NOD32(see page 909)
- ESET NOD32 Internet Security(see page 909)
- ESET Smart Security(see page 909)
- AVG(see page 909)
- DrWeb(see page 909)

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.

18.4.1 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(see page 905).

18.4.2 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.

18.4.3 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).

18.4.4 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.

18.4.5 DrWeb

If you use DrWeb antivirus, do the following before installing *Axxon One*:

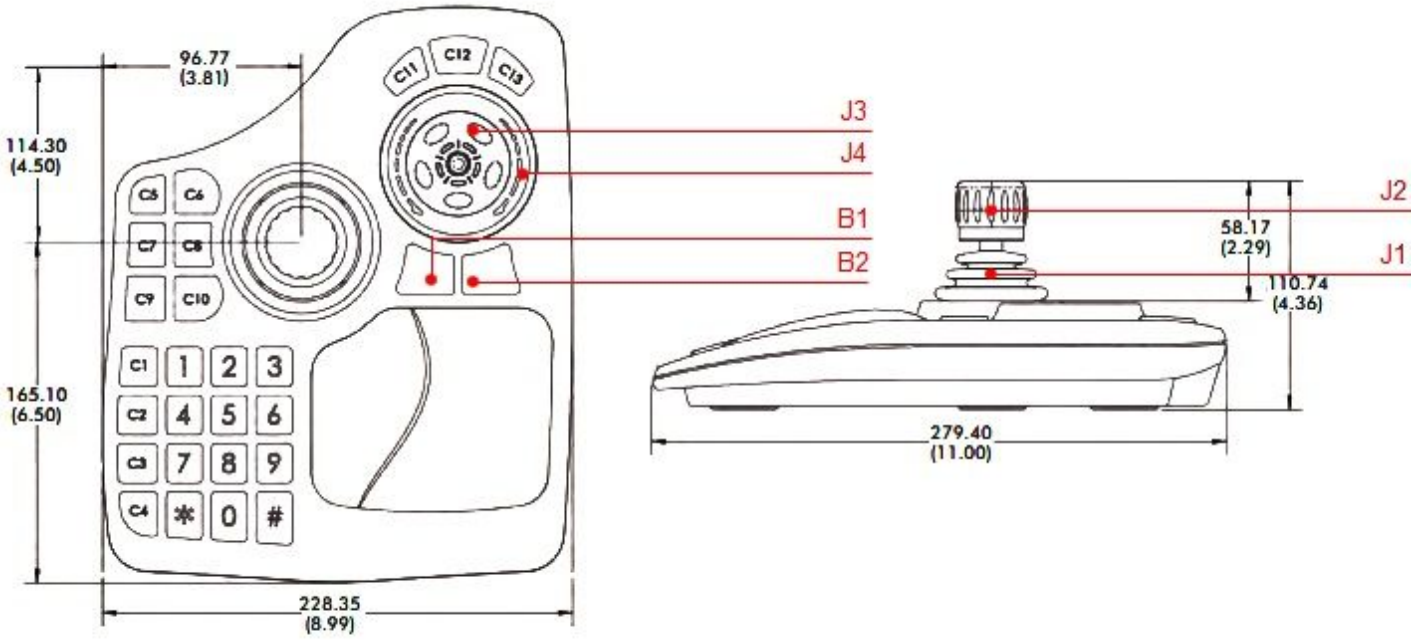
1. Disable the automatic start of the DrWeb firewall.
2. In the proactive protection settings, select the option to use custom settings and enable the following options:
    a. Allow low-level disk access
    b. Allow system services
    c. Allow loading drivers
    d. Allow User drivers
    e. Allow 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.

18.5 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(see page 790)).
> 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.

18.6 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 ID**	
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

18.7 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
```

18.8 Appendix 8. Configuring and operating Axxon One in Linux OS

18.8.1 Linux OS supported versions

Axxon One supports all 64-bit distribution packages:

- **Debian**: 11, 10, 9;
- **Ubuntu**: 22, 20, 19, 18;

Axxon One supports PostgreSQL versions from 9.5 to 12. For the current versions of distribution packages, the necessary versions of PostgreSQL are located in the regular repositories. If the versions are not available in the regular repositories of the distribution packages, you can find the installation repositories with the necessary versions in the official documentation: https://www.postgresql.org/docs/.

Attention!

- For *Axxon One* to operate correctly with Linux GUI, you should use one of the following graphical shells: GNOME, XFCE, CINNAMON, MATE.
- For the FailOver cluster to operate correctly, you must use the same versions of PostgreSQL on the cluster Servers.
- The stable operation of the Client is not guaranteed on Ubuntu 18 and 19. It is recommended to install only *Axxon One* Server. Both the Client and *Axxon One* Server are supported on Ubuntu 20 and newer versions.
- The basic Face detection cannot work in Debian 9 (see Configuring Face detection(see page 280)).

The Client can be installed only after installing the Server of the same version.

Updating the OS will not affect *Axxon One* performance. Still, it is recommended to make a backup copy of the configuration before updating the OS (see Configuration backup(see page 885)).

Installing the Axxon One Server in Linux OS(see page 918)
Installing the Axxon One Client in Linux OS(see page 922)

18.8.2 Axxon One limitations in Linux OS

Attention!

To install, upgrade or modify *Axxon One* in Linux OS, it is necessary to use the programs and commands described in this document. If you use third-party programs, *Axxon One* may not work correctly. For more information, see Features and potential problems with Linux OS(see page 917).

The following features are currently not available in *Axxon One* operating on Linux OS:

1. POS devices (see Configuring POS devices(see page 193)).
2. Web Boards (see Working with Web Boards(see page 781)).
3. Upgrading Servers within a cluster via the supervisor Web-interface (see Updating Servers within a cluster(see page 614)).
4. *Axxon One* Tray Tool(see page 860).
5. The basic Face detection cannot work in Debian 9 (see Configuring Face detection(see page 280)).

Attention!

Upgrade from *Axxon Next* to *Axxon One* in Linux OS is not possible.

18.8.3 Features and potential problems with Linux OS

On the page:

- Problem with displaying a dialog box or a drop-down list(see page 917)
- Peculiarities of detection tools operation on NVIDIA GPUs in Linux OS(see page 917)
- Problem with incorrect CPU load when decoding on Intel GPU in detection tool configuration(see page 918)
- Peculiarities of database operation when the PostgreSQL service is stopped(see page 918)

18.8.3.1 Problem with displaying a dialog box or a drop-down list

In some cases, when you change the configuration of objects for which you need to set a location or select a value from the drop-down list, when you click on the button to select a location or list value, they do not open.

Note

In fact, the location selection window or a drop-down list are opened outside the interface shell, and therefore are not visible to the user.

To resolve this problem, select a different desktop environment and restart *Axxon One*. For example, use Gnome Classic instead of Gnome for Debian 11.

18.8.3.2 Peculiarities of detection tools operation on NVIDIA GPUs in Linux OS

By default, the Nouveau driver can be installed in Linux OS. This driver does not guarantee stable operation when using NVIDIA graphics cards for decoding *Axxon One* detection tools (see Configuring detection tools(see page 234)).

To resolve the problem, you need to install the current graphics card driver from the official NVIDIA website and run the command in the terminal:

```
nvidia-smi
```

If the operating system uses the installed driver to work, the driver version will be displayed. Otherwise, if the current driver is installed, but the operating system uses the Nouveau driver, you need to add it to the exclusions list and restart the computer. Below is an example of Ubuntu commands to add the Nouveau driver to the exclusion list:

```
sudo bash -c "echo blacklist nouveau > /etc/modprobe.d/blacklist-nvidia-nouveau.conf"
sudo bash -c "echo options nouveau modeset=0 >> /etc/modprobe.d/blacklist-nvidia-nouveau.conf"
```

After restarting, the operating system will use the installed NVIDIA driver.

18.8.3.3 Problem with incorrect CPU load when decoding on Intel GPU in detection tool configuration

When enabling decoding on Intel GPU in detection tool configuration, the AVDetector and Decoder processes may cause incorrect CPU load. To solve this problem, do the following:

1. Change the package configuration using the command:

```
sudo dpkg-reconfigure axxon-one-core
```

2. In the groups selection dialog box, set the checkbox next to the **render** group.

18.8.3.4 Peculiarities of database operation when the PostgreSQL service is stopped

If you stop the PostgreSQL service and then start it, the EventDatabase won't connect to PostgreSQL until the service is restarted manually.

To restore the database operation when manually stopping the PostgreSQL service, you must manually restart the EventDatabase service using the command:

- via service:

```
service axxon-one-db restart
```

- via systemctl:

```
systemctl restart axxon-one-db.service
```

You can also restart the device to restore the database operation.

18.8.4 Installing Axxon One in Linux OS

> **Attention!**
>
> All *Axxon One* installation steps must be performed in the terminal using the root user, who has administrative access to the system.
> The sudo software is used for installing *Axxon One*. Sudo commands are described in this guide. If you use third-party programs, such as the Discover Update Center, this may result in you having to reinstall *Axxon One*.

18.8.4.1 Installing the Axxon One Server in Linux OS

18.8.4.1.1 Installing from repository

Installation from the repository is performed automatically, including all the system components.

To install from the repository, do the following:

1. Sequentially run the commands:

```
echo 'deb http://download.axxonsoft.com/debian-repository stretch backports/main' | sudo
tee -a /etc/apt/sources.list.d/axxonsoft.list
```

```
echo 'deb http://download.axxonsoft.com/debian-repository weekly main backports/main' |
sudo tee -a /etc/apt/sources.list.d/axxonsoft.list
wget --quiet -O - "http://download.axxonsoft.com/debian-repository/
info@axxonsoft.com.gpg.key" | sudo apt-key --keyring /etc/apt/trusted.gpg.d/axxonsoft.gpg
add - && sudo apt-get update
```

Note

If the distribution packages based on Debian 10 are used, it may be necessary to install additional packages:

```
sudo apt-get install wget
sudo apt-get install gnupg
```

2. To install *Axxon One* Server, run the following command:

```
sudo apt install axxon-one
```

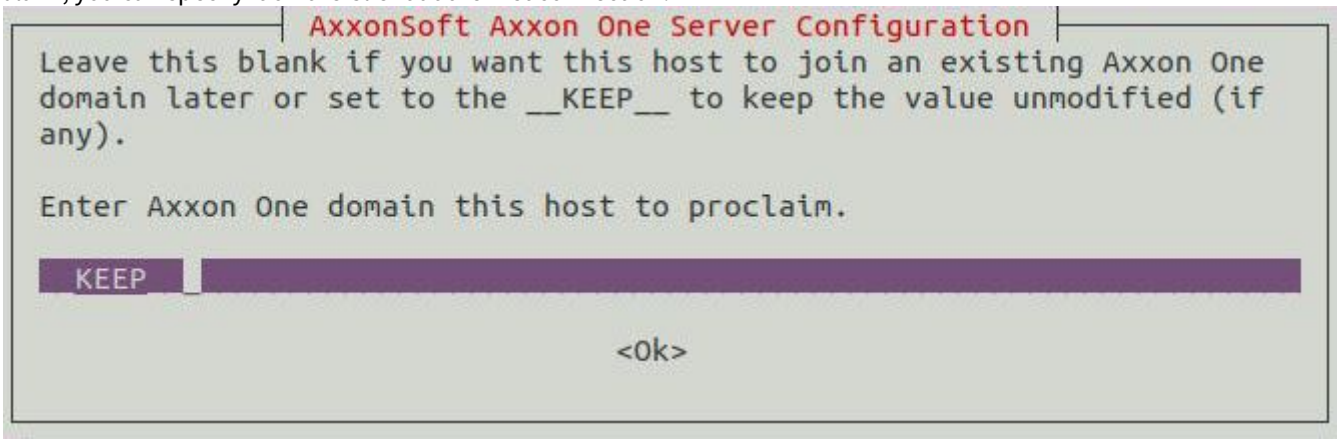
To install the FailOver Server, run the following command:

```
sudo apt install axxon-one-raft
```

Attention!

It is not allowed to simultaneously install the regular Server and the FailOver Server.

During the installation, the installer will request the name of the domain for the *Axxon One* Server. If you leave this field blank, you can specify it on the Client at the first connection.



18.8.4.1.2 Manual installation

Attention!

Before installing *Axxon One* in Linux OS, you need to read about the supported versions and operating system requirements (see Linux OS supported versions(see page 916)).

The following packages are required to install *Axxon One*:

Package examples
Minimum number of packages for *Axxon One* installation of the **Server** type:

```
axxon-drivers-pack_3.73_amd64.deb
axxon-detector-pack_3.8_amd64.deb
axxon-one-core_1.9.0_amd64.deb
axxon-one_1.9.0_all.deb
```

Minimum number of packages for *Axxon One* installation of the **Server in the Failover mode** type:

```
axxon-drivers-pack_3.73_amd64.deb
axxon-detector-pack_3.8_amd64.deb
axxon-one-core_1.9.0_amd64.deb
axxon-one-raft_1.9.0_amd64.deb
```

To install the *Axxon One* Server manually, do the following:

1. Add the repositories by sequentially running the following commands:

```
echo 'deb http://download.axxonsoft.com/debian-repository stretch backports/main' | sudo
tee -a /etc/apt/sources.list.d/axxonsoft.list
echo 'deb http://download.axxonsoft.com/debian-repository weekly main backports/main' |
sudo tee -a /etc/apt/sources.list.d/axxonsoft.list
wget --quiet -O - "http://download.axxonsoft.com/debian-repository/
info@axxonsoft.com.gpg.key" | sudo apt-key --keyring /etc/apt/trusted.gpg.d/axxonsoft.gpg
add - && sudo apt-get update
```

> **Note**
>
> If you install *Axxon One* on Ubuntu 22, then after running the commands from the step 1, you should sequentially run the following commands to install PostgreSQL version 10 compatible with Ubuntu 22:
>
> ```
> sudo sh -c 'echo "deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-
> pgdg main" > /etc/apt/sources.list.d/pgdg.list'
> wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key
> add -
> sudo apt-get update
> sudo apt-get -y install postgresql-10
> ```

2. To install *Axxon One*, *DetectorPack*, *DriverPack,* and *DetectorPack* add-ons, contact AxxonSoft and get the necessary packages from the manager.
3. Copy the received packages to the Downloads folder.
4. To install the packages, run the command:

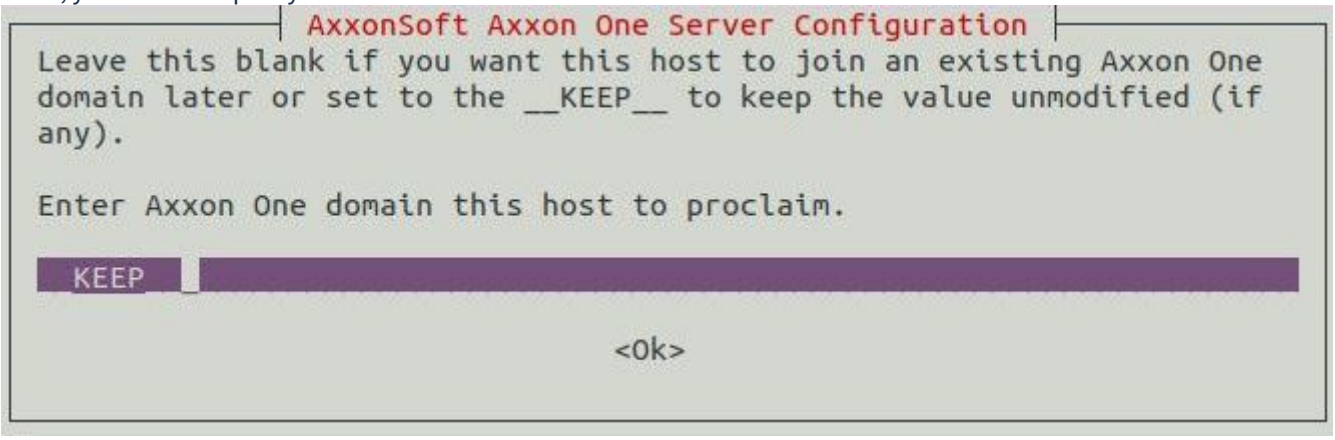
```
sudo dpkg -i /home/user/Downloads/axxon-d*.deb || sudo apt-get install -f -y
```

where
user—user name;
Downloads—folder with downloaded packages.

> **Attention!**
>
> - You must install *DetectorPack* with add-ons and *DriverPack* before installing the main part of *Axxon One*.

- The folder must not contain other packages.
- It is not allowed to simultaneously install the regular Server and the Failover Server.

During the installation, the installer will request the name of the domain for the *Axxon One* Server. If you leave this field blank, you can later specify it on the Client at the first connection.



5. If necessary, you can change the Server configuration after installation (see Axxon One Server configuration change on Linux OS(see page 928)).

Installation is complete.

18.8.4.1.3 Installing add-ons to the basic DetectorPack in Linux OS

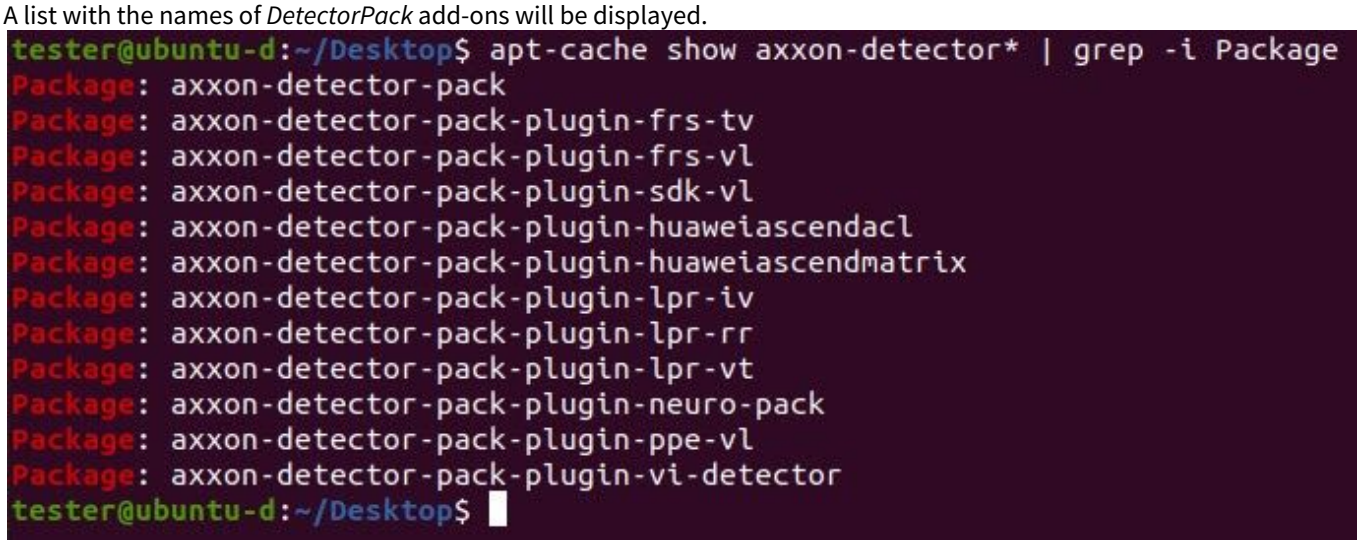
By default, *Axxon One* distribution package comes with only the basic *DetectorPack* (see Installing DetectorPack add-ons(see page 74)).

To install the add-ons to the basic *DetectorPack* in Linux OS, do the following:

1. Run the command to get a list of *DetectorPack* add-ons:

```
apt-cache show axxon-detector* | grep -i Package
```

A list with the names of *DetectorPack* add-ons will be displayed.



2. Run the following command to install the necessary add-ons:

```
apt-get install %add-on name%
```

For example, to install the Neuro Pack add-on, run the command:

```
apt-get install axxon-detector-pack-plugin-neuro-pack
```

3. After installing the necessary add-ons, restart the Server:

```
service axxon-one restart
```

Attention!

It is required that the versions of the basic *DetectorPack* and the *DetectorPack* add-ons are the same. If the versions differ, it is necessary to update the version of the basic *DetectorPack* so it matches the version of the *DetectorPack* add-on.

18.8.4.2 Installing the Axxon One Client in Linux OS

Attention!

- The stable operation of the Client is not guaranteed on Ubuntu 18 and 19. It is recommended to install only *Axxon One* Server (see Installing the Axxon One Server in Linux OS(see page 918)). Both the Client and *Axxon One* Server are supported on Ubuntu 20 and newer versions.
- The Client can be installed only after installing the Server of the same version (see Installing the Axxon One Server in Linux OS(see page 918)).

To install the *Axxon One* Client in Linux OS, do the following:

1. Add the repositories by sequentially running the following commands:

```
echo 'deb http://download.axxonsoft.com/debian-repository stretch backports/main' | sudo
tee -a /etc/apt/sources.list.d/axxonsoft.list
echo 'deb http://download.axxonsoft.com/debian-repository weekly main backports/main' |
sudo tee -a /etc/apt/sources.list.d/axxonsoft.list
wget --quiet -O - "http://download.axxonsoft.com/debian-repository/
info@axxonsoft.com.gpg.key" | sudo apt-key --keyring /etc/apt/trusted.gpg.d/axxonsoft.gpg
add - && sudo apt-get update
```

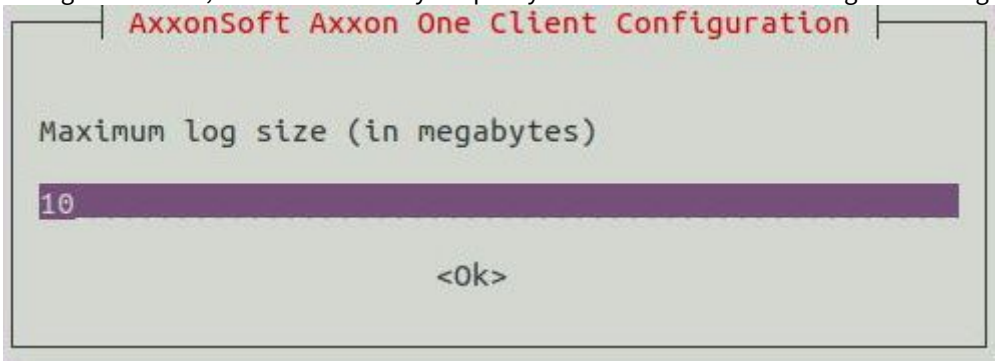
2. If you use Ubuntu 20.04 or Debian 11, then install the mono-complete from the stretch repository:

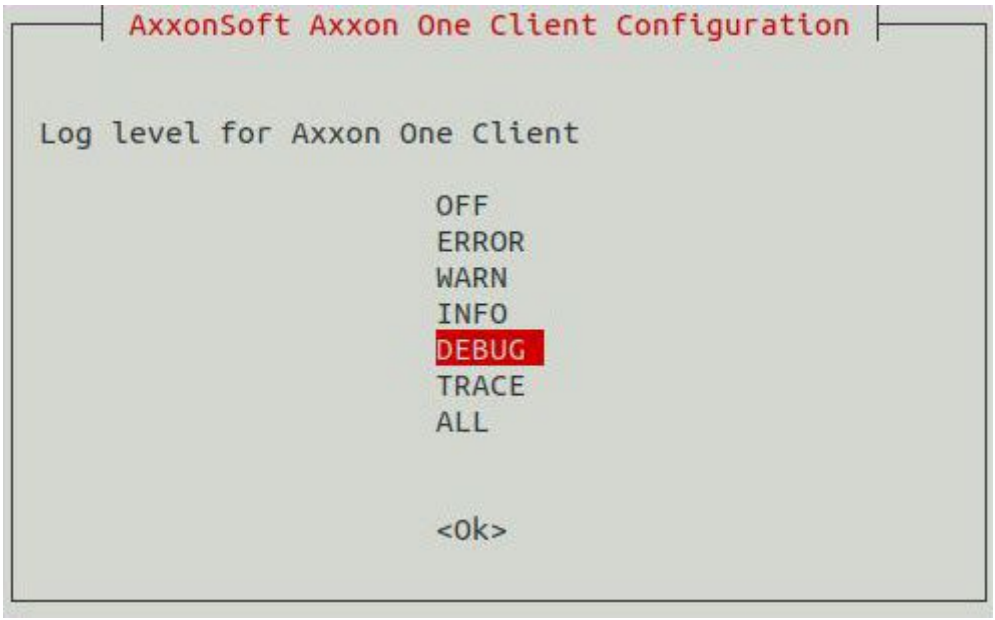
```
sudo apt-get install mono-complete -t stretch
```

3. Contact AxxonSoft and get the necessary packages for installing the Client from the AxxonSoft manager.
4. Go to the folder with the downloaded deb packages.
5. Run the commands:

```
sudo dpkg -i axxon-one-client-bin*.deb || sudo apt-get install -f -y
sudo dpkg -i axxon-one-client_*all.deb || sudo apt-get install -f -y
```

6. During installation, it will be necessary to specify the maximum size of the log files in megabytes and the log level.





> **Note**
>
> The specified value can be changed (see Configuring the Axxon One Client logging parameters on Linux OS(see page 926)). To do this, run the command:
> sudo dpkg-reconfigure axxon-one-client

When the installation is complete, the Client icon will be displayed in the application menu.

> **Attention!**
>
> - It is not allowed to run the *Axxon One* Client as a Linux user with the root rights.
> - Authorization in the Client is allowed as any *Axxon One* user.

By default, at the first Client start, the OS interface language will be used. To change the language of the Client interface at the first start, do the following:

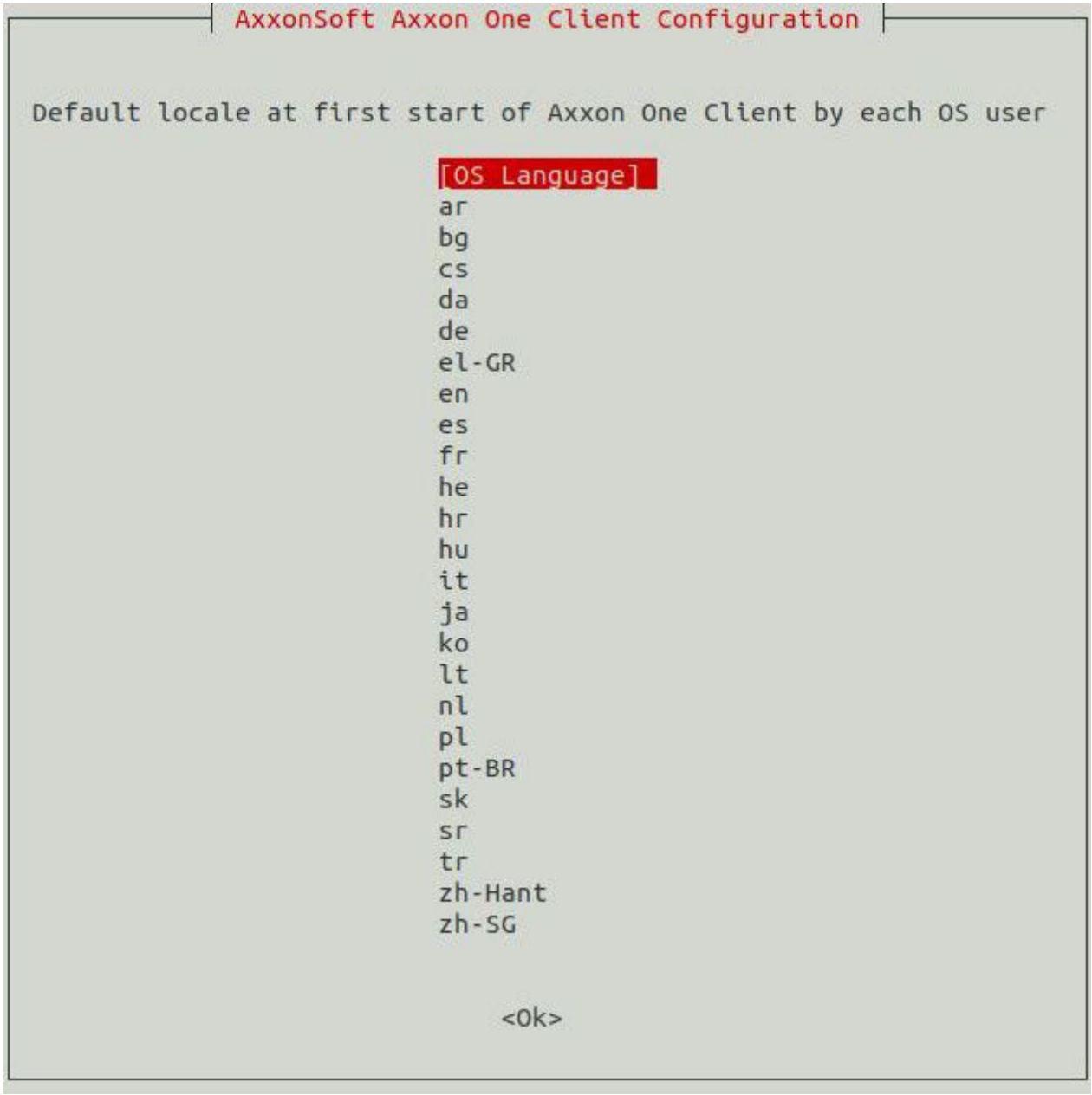
1. Run the command:

```
sudo dpkg-reconfigure axxon-one-client
```

2. Select the required language:

> **Attention!**
>
> - This setting should be configured for each OS user separately.

- For the next launches the interface language can be changed in the Client settings (see Selecting the interface language(see page 551)).



18.8.5 Starting and stopping the Axxon One Server in Linux OS

Note

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

Server start:

```
sudo service axxon-one start
```

Server stop:

```
sudo service axxon-one stop
```

Server restart:

```
sudo service axxon-one restart
```

Server status check:

```
sudo service axxon-one status
```

18.8.6 Updating Axxon One on Linux OS

There are two options to update *Axxon One* on Linux OS: from the repository and from the folder.

1. To update *Axxon One* from the repository, sequentially execute the commands as a **root**:

   ```
   sudo apt-get update
   sudo apt-get upgrade
   ```

2. To update *Axxon One* from the folder, do the following:
   a. Go to the folder with the downloaded packages.
   b. Execute the following command:

      ```
      sudo dpkg -i *
      ```

Package examples

Example of packages required to update the Server side:

```
axxon-drivers-pack_3.73_amd64.deb
axxon-detector-pack_3.8_amd64.deb
axxon-one-core_1.9.0_amd64.deb
axxon-one_1.9.0_all.deb
```

Example of packages required to update the Server in the Failover mode:

```
axxon-drivers-pack_3.73_amd64.deb
axxon-detector-pack_3.8_amd64.deb
axxon-one-core_1.9.0_amd64.deb
axxon-one-raft_1.9.0_amd64.deb
```

Example of packages required for the Server and Client updating type:

```
axxon-drivers-pack_3.73_amd64.deb
axxon-detector-pack_3.8_amd64.deb
axxon-one_1.9.0_all.deb
axxon-one-core_1.9.0_amd64.deb
```

```
axxon-one-client-bin_1.9.0_amd64.deb
axxon-one-client_1.9.0_all.deb
```

These options describe an update within one version of *Axxon One* (for example, from 1.0 to 1.9). If you want to update from *Axxon One* 1.0 to *Axxon One* 2.0, you should first update the repositories. The repositories and the commands are specified in the item 1 on the page Installing from repository(see page 918).

Attention!

After the update is completed, it is necessary to check the access rights of the archive file and the folder where it is stored.
The **ngp** user should be specified as the owner of both the file and the folder.

18.8.7 Uninstalling the Axxon One software in Linux OS

To uninstall the *Axxon One* but save the configuration, run the following command:

```
sudo apt remove axxon-*
```

To completely remove the *Axxon One*, run the following commands in sequence:

```
sudo apt --purge remove axxon-* -y
```

```
sudo apt autoremove -y
```

```
sudo rm -r /opt/AxxonSoft/
```

18.8.8 Configuration and log folders

The following folders are being used by default:

1. Logs and Client configuration:

   ```
   /home/USER/.local/share/AxxonSoft/
   ```

2. Server configuration:

   ```
   /opt/AxxonSoft/AxxonOne/
   ```

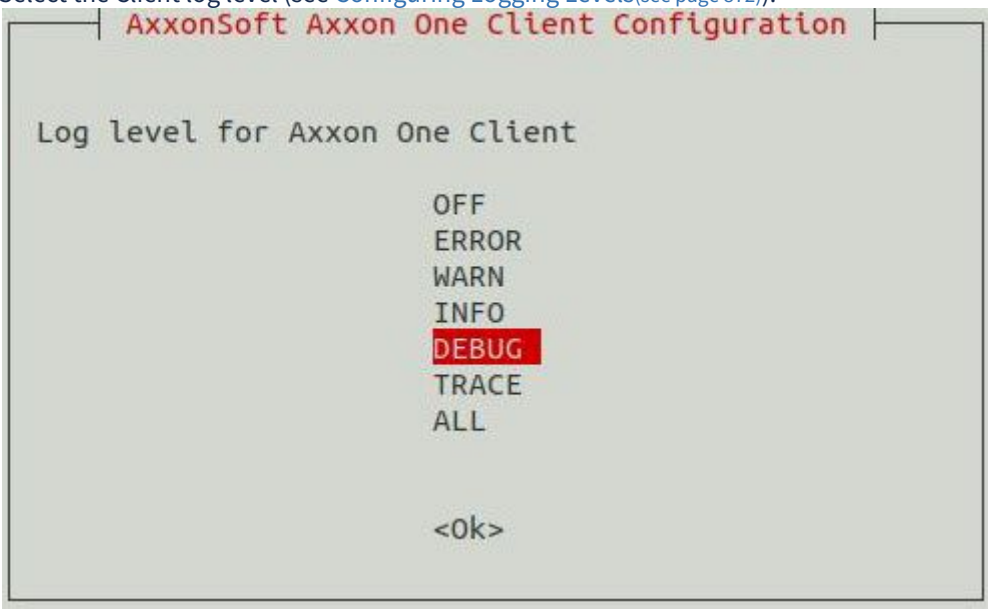
18.8.9 Configuring the Axxon One Client logging parameters on Linux OS

To change the *Axxon One* Client logging parameters, do the following:

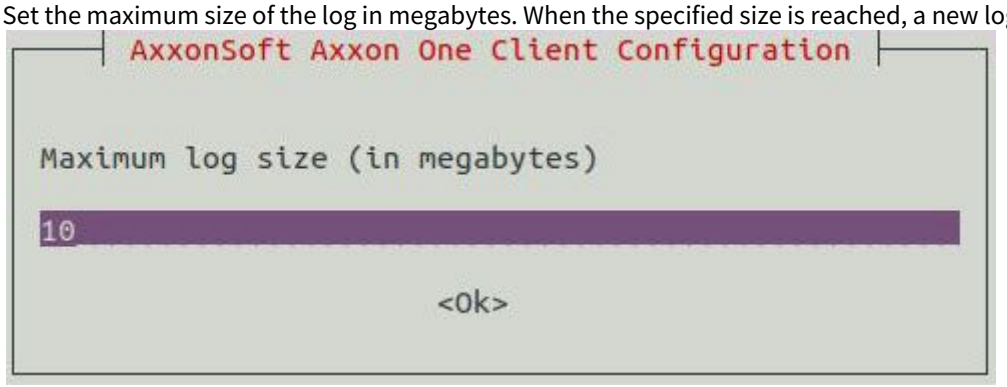
1. Execute the following command.

   ```
   sudo dpkg-reconfigure axxon-one-client
   ```

2. Select the Client log level (see Configuring Logging Levels(see page 872)).



3. Set the maximum size of the log in megabytes. When the specified size is reached, a new log is created.



18.8.10 System data collection in Linux OS

To collect the system data in Linux OS, execute the following command:

```
sudo /opt/AxxonSoft/AxxonOne/bin/support /home/user
```

where

- /opt/AxxonSoft/AxxonOne/bin/support—the utility location directory;
- /home/user—the user's home directory.

By default, the system data report includes information from Linux OS log. To exclude this information from the report, execute the command:

```
--skip-journalctl
```

If you want the report not to include the information on the self-diagnostics service (see Self-diagnostics service(see page 619)), execute the following command:

```
--skip-prometheus
```

18.8.11 Configuring the metadata storage in NAS on Linux OS

To store the metadata in a network attached storage (NAS), do the following:

1. Create a shared network folder.
2. On the Server in Linux OS, create the **netdir** folder. For example, in the **/media** folder:

```
sudo mkdir /media/netdir
```

3. Install the **cifs-utils** utility.

```
sudo apt-get install cifs-utils
```

4. Attach the shared network folder to the created **netdir** folder.

```
sudo mount -t cifs //IP-address/common /media/netdir -o
user=User,password=123,uid=1001,gid=1002,vers=2.0
```

where,

a. IP-address – NAS address,
b. common – shared network folder,
c. user, password – NAS access credentials,
d. uid, gid – id of the user and ngp group; they can be obtained using the following command:

```
id ngp
```

5. In the *Axxon One* metadata storage settings, specify the /media/netdir path (see Configuring storage of the system log and metadata(see page 539)).

After you restart Linux OS, the attached folder will be deleted. To configure the network folder to be attached on the OS loading, do the following:

1. Open the /etc/fstab file.

```
sudo nano /etc/fstab
```

2. Add the following string to the file:

```
//IP-address/common /media/netdir cifs user=User,password=123,uid=1001,gid=1002,vers=2.0 0
0
```

3. Save file.

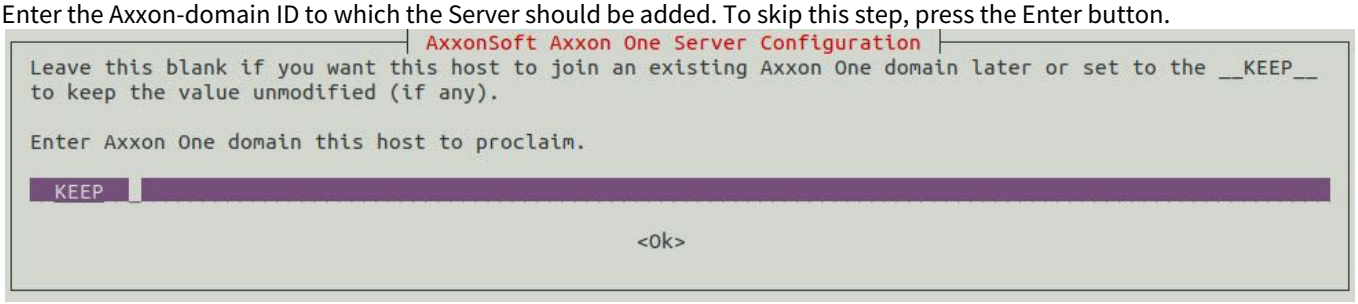
18.8.12 Axxon One Server configuration change on Linux OS

To change the Server configuration, do the following:

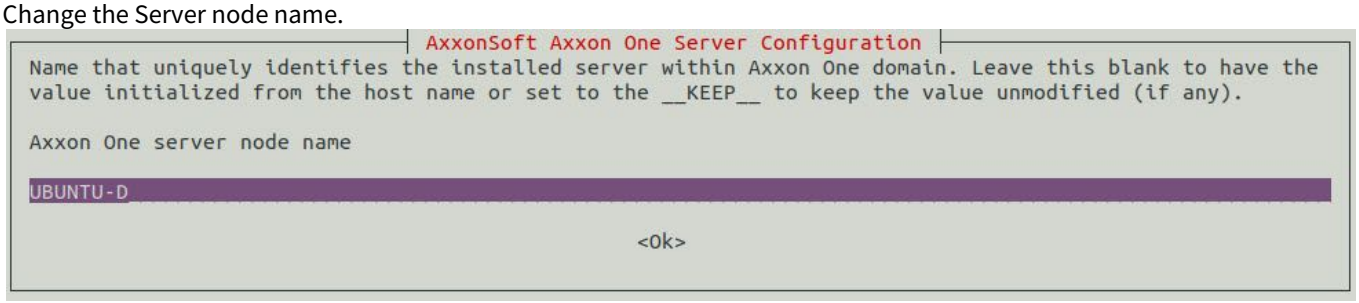
1. Run the following command.

```
sudo dpkg-reconfigure axxon-one
```

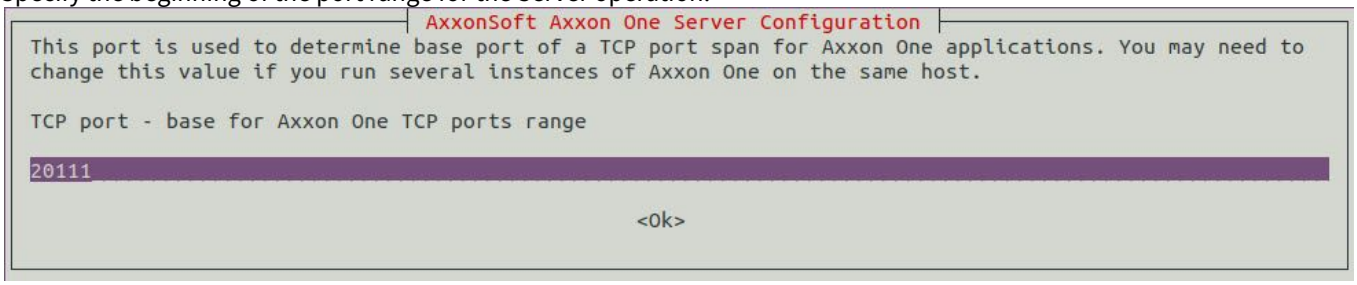
2. Enter the Axxon-domain ID to which the Server should be added. To skip this step, press the Enter button.



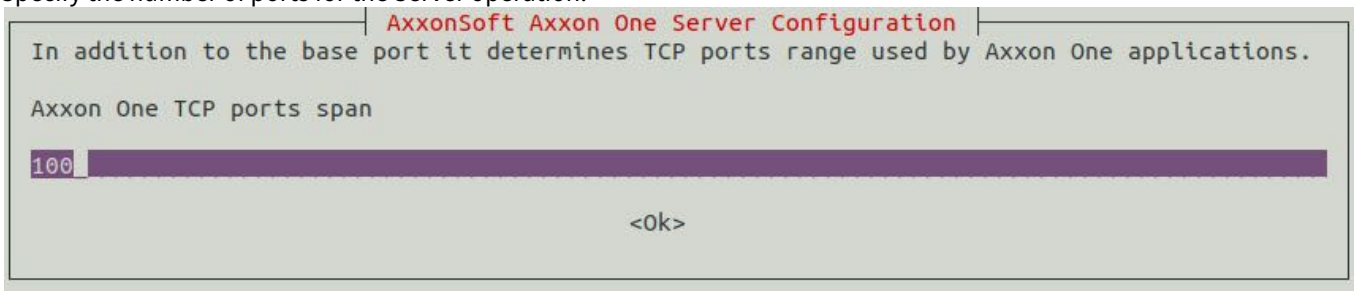
3. Change the Server node name.



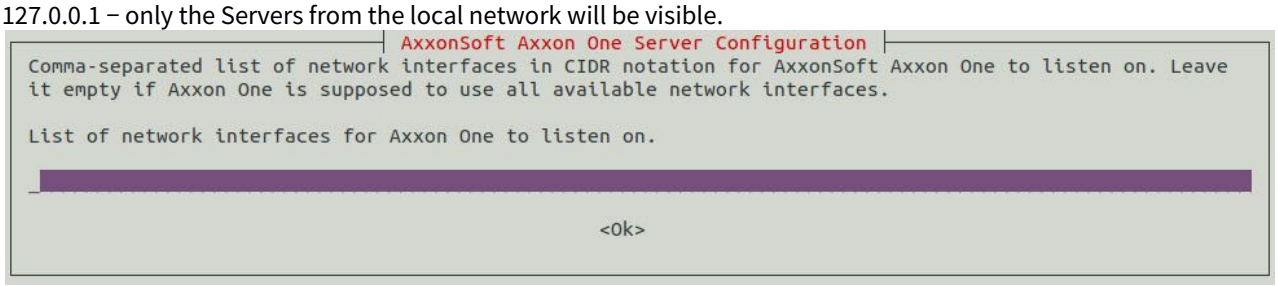
4. Specify the beginning of the port range for the Server operation.



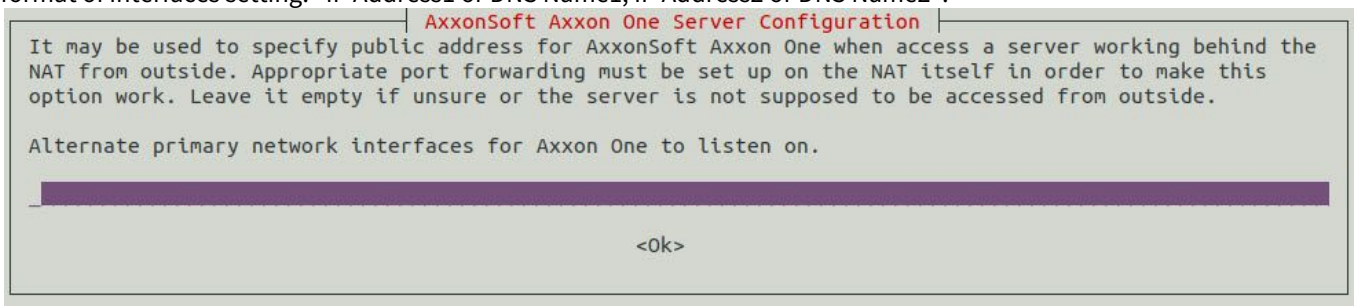
5. Specify the number of ports for the Server operation.



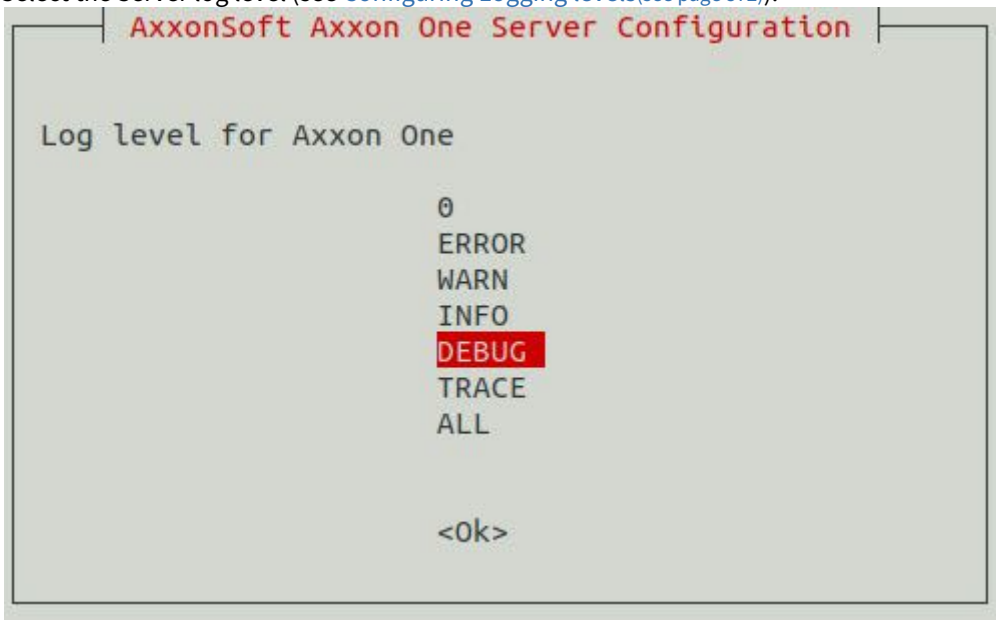
6. Restrict the visibility of Servers from various networks in the Servers list during *Axxon One* setup. Possible values:
   a. 0.0.0.0/0 – Servers from all networks will be visible.
   b. 10.0.1.23/32,192.168.0.7/32 – only the Servers from the specified networks will be visible.
   c. 127.0.0.1 – only the Servers from the local network will be visible.



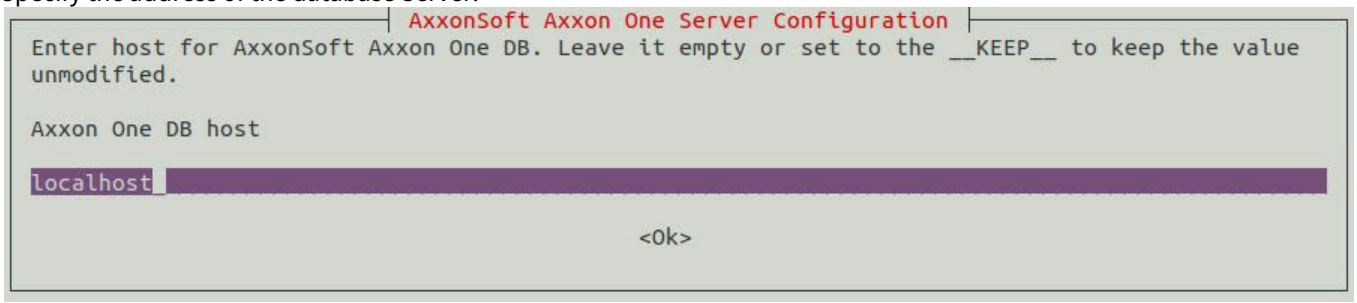
7. Specify the alternative Server address – the external address of the switch if the Server is located behind the NAT[204]. The format of interfaces setting: "IP Address1 or DNS Name1, IP Address2 or DNS Name2".



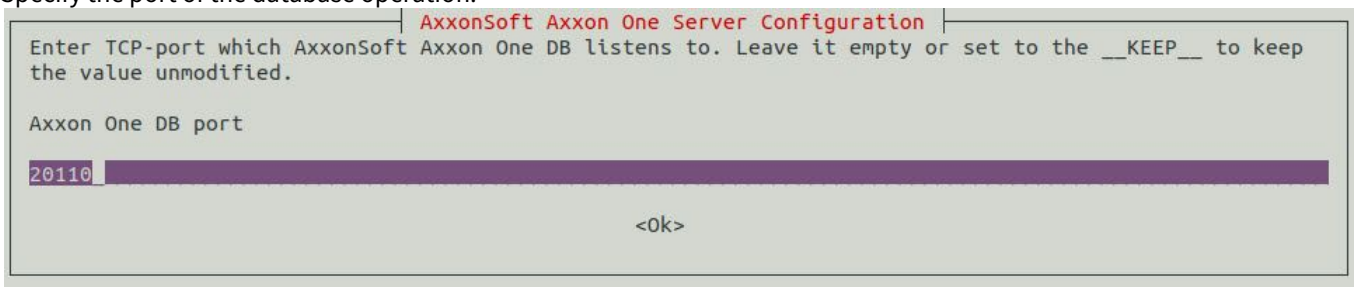
8. Select the Server log level (see Configuring Logging levels(see page 872)).



9. Specify the address of the database Server.

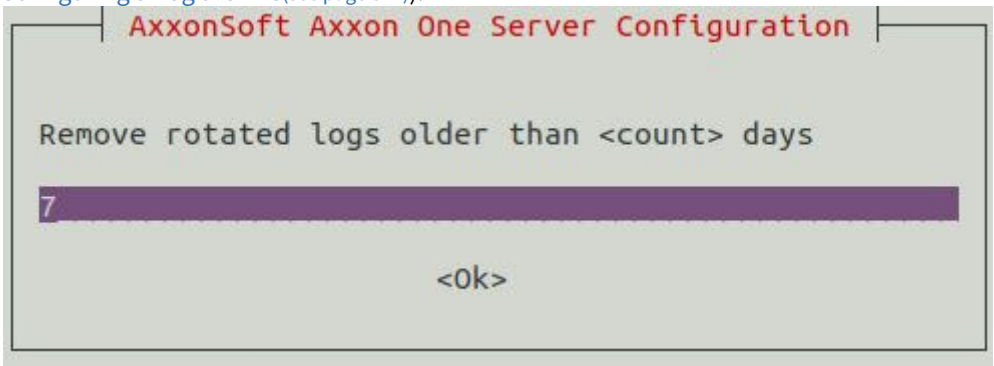


10. Specify the port of the database operation.

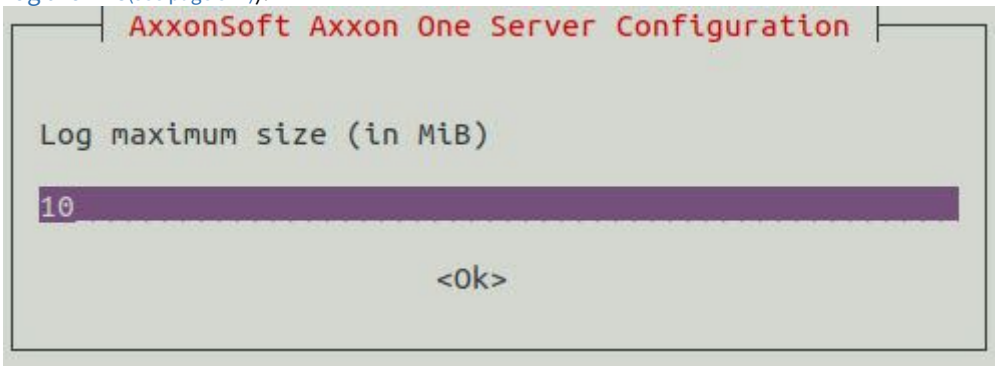


204 https://en.wikipedia.org/wiki/Network_address_translation

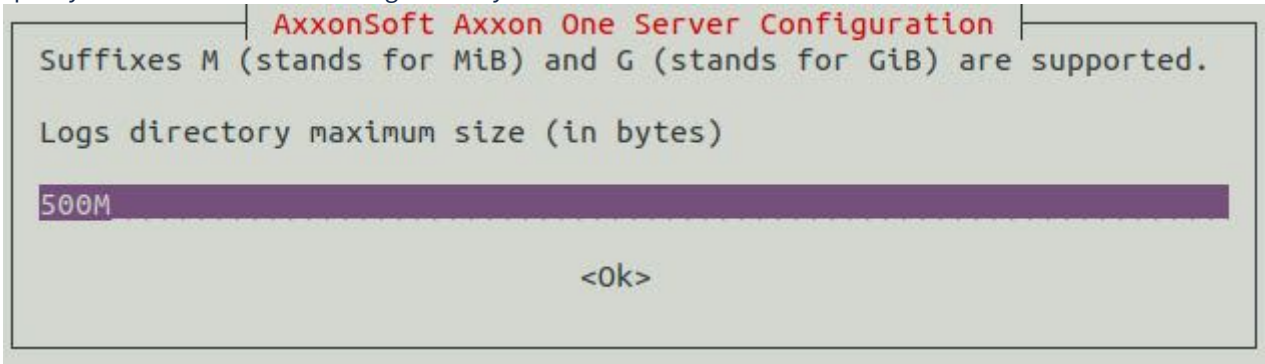
11. Specify the maximum time in days the log will be stored in the archive. After that time, the log will be deleted (see Configuring a Log archive(see page 871)).



12. Specify the maximum size of the archive, above which the earliest logs will be deleted from the archive (see Configuring a Log archive(see page 871)).



13. Specify the maximum size of the log directory.



Server configuration change is complete.

18.8.13 Moving the Axxon One configuration from Windows OS to Linux OS

To transfer *Axxon One* configuration from Windows OS to Linux OS, do the following:

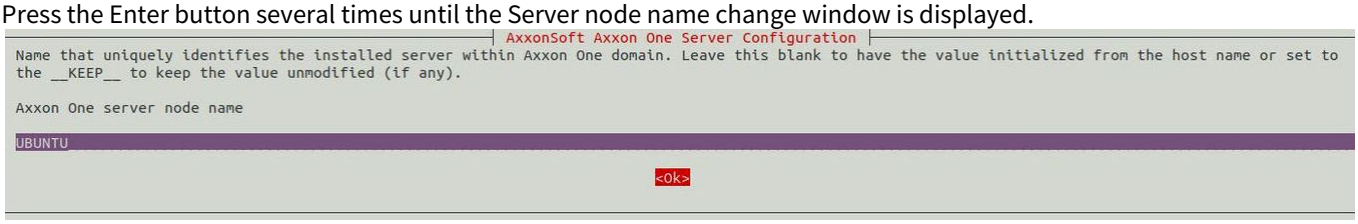
1. Create the backup configuration in Windows OS (see Configuration backup(see page 885)).
2. Execute the following command in Linux OS:

```
sudo dpkg-reconfigure axxon-one
```

> **Attention!**
>
> The Server in Linux OS must belong to some Axxon-domain.

The following window will be displayed.

3. Press the Enter button several times until the Server node name change window is displayed.



4. Enter the Server node name which is used in Windows OS.
5. Run the backup and configuration recovery utility (see Backup and Restore Utility(see page 877)) and select the specified Server on its launch.
6. Restore the configuration by selecting the saved backup.
7. Deactivate the license (see Deactivating a license[205]) and distribute the license file again (see Activation by applying license file[206]).

18.8.14 Starting and stopping the Axxon One self-diagnostics service in Linux OS

> **Note**
>
> The *Axxon One* self-diagnostics service is running by default.

Controlling the self-diagnostics service via service

Start the service:

```
service axxon-one-selfdiag start
```

Stop the service:

```
service axxon-one-selfdiag stop
```

Restart the service:

```
service axxon-one-selfdiag restart
```

Controlling the self-diagnostics service via systemctl

Start the service:

```
systemctl start axxon-one-selfdiag.service
```

Stop the service:

```
systemctl stop axxon-one-selfdiag.service
```

Restart the service:

```
systemctl restart axxon-one-selfdiag.service
```

Enable the automatic start of the service:

205 https://docs.axxonsoft.com/confluence/display/one20en/Deactivating+a+license
206 https://docs.axxonsoft.com/confluence/display/one20en/Activation+by+applying+license+file

```
systemctl enable axxon-one-selfdiag.service
```

Disable the automatic start of the service:

```
systemctl disable axxon-one-selfdiag.service
```

18.8.15 Archive creation features in Linux OS

18.8.15.1 Archive as a disk creation features in Linux OS

To allocate the disk for recording, execute the command in the root mode.

```
sudo su
```

```
fdisk -l
```

where

- /dev/sd**a** – the first physical disk;
- /dev/sda**1** – the first section of the first physical disk;
- /dev/sda**2** – the second section of the first physical disk;
- dev/sd**b** – the second physical disk.

To delete the disk section, do the following:

1. Go to the disk where it is necessary to delete a section.

   ```
   fdisk /dev/sdb
   ```

2. Delete the section.

   ```
   d
   ```

3. Specify the section number.

   ```
   2
   ```

4. Save the changes.

   ```
   w
   ```

To create a section, do the following:

1. Go to the disk where it is necessary to create a section.

   ```
   fdisk /dev/sdb
   ```

2. Create the section.

```
n
```

3. Specify the section: primary (p) or extended (e).

```
p
```

4. Specify the section number.

```
1
```

5. Specify the section size. G – gigabytes, M – megabytes, K – kilobytes.

```
+5G
```

6. Save the changes.

```
w
```

To create the archive as a disk, do the following:

1. Create a new archive in the *Axxon One* Client (see Creating a local archive(see page 209)).
2. Select the archive volume.
3. Specify the path to section in the address window. For example: /dev/sdb1. If it is required to use the whole disk as an archive, specify the /dev/sdc, /dev/sdd and so on.
4. Set the **Format** checkbox and click the **Apply** button.

> **Attention!**
>
> At this point you cannot change the archive size.

18.8.15.2 Archive as a file creation features in Linux OS

By default, in Linux OS the **ngp** user has rights to record only in the /opt/AxxonSoft/AxxonOne/ directory.

To create an archive in another directory, do the following:

1. Create a folder with write permissions.

```
sudo mkdir -m755 /home/archive
```

2. Change the folder owner to **npg** user.

```
sudo chown -R ngp:ngp /home/archive/
```

3. Check the permissions on created folder.

```
ls -lt /home/
```

If there is a string with the ngp user permissions in the result, it is now possible to create an archive as a file in this directory.

```
drw-r--r--  2 ngp    ngp    4096 aug.   8 15:18 archive
```

18.8.15.3 Features of archives with ext and xfs file systems

When you work with archives (both local and network) on ext and xfs file systems, take into account the following features:

1. When you create an archive (see Creating archive[207]), the displayed free disk space is calculated based on the actual used space.

   Note

   For example, the disk size is 60 GB, and a 10 GB archive is created on it, but it is only 1 GB full.
   When you try to create a second archive on this disk, 59 GB of free space will be displayed, not 50 GB.

2. Availability of the entire archive file size is not guaranteed in cases when other files run out of available space.

   Note

   Due to the ext and xfs file systems features, it is possible to create archives whose total size exceeds the free disk space.

   Attention!

   In such cases, it is necessary for the system administrator to control the free disk space.

18.8.15.4 Features of NAS archives

For connecting to the NAS server, use the following versions of protocols:

- SMB2/SMB3 (2.02, 2.10, 3.00, 3.02, 3.1.1);
- NFSv3, NFSv4.

It is also possible to use the CIFS and iSCSI protocols.

18.8.16 Axxon One Server launch using Docker

To launch the *Axxon One* Server using Docker, do the following:

1. Install Docker:
   - **Ubuntu/Debian...**
     i. Prepare the environment:
        1. Install the packages to use the repository via HTTPS.

           ```
           sudo apt-get install apt-transport-https ca-certificates curl gnupg2
           software-properties-common
           ```

        2. Add official Docker GPG key.

           ```
           curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key
           add -
           ```

           ```
           sudo apt-key fingerprint 0EBFCD88
           ```

207 https://docs.axxonsoft.com/confluence/display/one20en/Creating+archive

3. Configure the repository:
   a. for the x86_64 / amd64 architecture:
      - Debian:

```
sudo add-apt-repository "deb [arch=amd64] https://
download.docker.com/linux/debian $(lsb_release -cs) stable"
```

      - Ubuntu:

```
sudo add-apt-repository "deb [arch=amd64] https://
download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

   b. for the armhf architecture:
      - Debian:

```
sudo add-apt-repository "deb [arch=armhf] https://
download.docker.com/linux/debian $(lsb_release -cs) stable"
```

      - Ubuntu:

```
sudo add-apt-repository "deb [arch=armhf] https://
download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
```

4. Update the lists of packages:

```
sudo apt-get update
```

ii. Install and configure the Docker:
   1. Install docker-ce.

```
sudo apt-get install docker-ce docker-compose
```

   2. Add a user to the Docker.

```
sudo adduser docker
```

   3. Install git and the envsubst utility using the command:

```
sudo apt-get install git gettext binutils
```

> **Note**
>
> Minimum requirements to launch *Axxon One* using Docker on Ubuntu:
> - Dual core processor;
> - 4 GB RAM;
> - 200 GB HDD.

- **Fedora...**
   i. Prepare the environment:
      1. Install the packages and set up the repository:

```
sudo dnf -y install dnf-plugins-core
sudo dnf config-manager --add-repo https://download.docker.com/linux/
fedora/docker-ce.repo
```

2. Refresh metadata cache:

```
dnf makecache
```

ii. Install and configure the Docker:

1. Install Docker with additional packages:

```
dnf -y install docker-ce docker-ce-cli containerd.io docker-buildx-
plugin docker-compose-plugin docker-compose
```

2. Install git and the envsubst utility using the command:

```
dnf install git gettext binutils
```

- other distribution packages: https://docs.docker.com/engine/install/.

2. Connect the *Axxon One* repository. To do this, do the following:
   a. Go to the directory where the container will be located.

```
cd /home/%username
```

   where %username is a username under which the container will be located.
   b. Clone the axxonnext.docker repository.

```
git clone https://src.axxonsoft.dev/bitbucket/scm/one/axxonnext.docker.git
```

> **Attention!**
>
> If the "server certificate verification failed" error occurs, execute the following command in the terminal:
>
> ```
> export GIT_SSL_NO_VERIFY=1
> ```

   c. Update the cloned repository files:
      i. Go to the axxonnext.docker folder:

```
cd /home/%username/axxonnext.docker/
```

      where %username is a username under which the container will be created.
      ii. Download the contents of the git repository:

```
git pull
```

3. Create the *Axxon One* container. To create the *Axxon One* container, do the following:

a. Copy the deb packages of *Axxon One*, Detector Pack and Driver pack to the /home/%username/axxonnext.docker/server/build/ folder.

```
mv /home/user/Downloads/axxon-* /home/axxonnext.docker/server/build/
```

b. Go to the axxonnext.docker/server folder.

```
cd /home/%username/axxonnext.docker/server
```

c. Execute the command:

```
./axxon-one.sh build
```

The assembly of the *Axxon One* container will begin.

d. To view the list of the assembled containers after the operation is complete, execute the command:

```
./axxon-one.sh list
```

The *Axxon One* Server launch using Docker is complete.

Working with the Axxon One container(see page 938)

18.8.16.1 Working with the Axxon One container

- The list of containers.

```
./axxon-one.sh list
```

- Launching the container.

```
./axxon-one.sh start 1.0.2.25
```

- Viewing the container status.

```
./axxon-one.sh status
```

- Stopping the container.

```
./axxon-one.sh stop
```

- Collecting the system data.

```
./axxon-one.sh support
```

The file will be saved in the '~/axxonone.docker/one/data/' directory.

- Viewing the installed packages version.

```
./axxon-one.sh versions
```

18.8.17 Licensing of the software module for License plate recognition (VT) on Linux OS

On this page:

- General information(see page 939)
- Installing the Sentinel LDK Run-time environment(see page 939)
- Installing a hardware key(see page 940)
- Installing a software key(see page 940)
- Updating the license(see page 941)
- Removing a license(see page 942)
- Checking a license(see page 943)

18.8.17.1 General information

The software module for License plate recognition (VT) in *Axxon One* is licensed by the processed video channels and by countries (see License plate recognition (VT)(see page 308)).

Attention!

It is necessary to run the commands as the root user.

18.8.17.2 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(see page 768)).

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.

18.8.17.3 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 *Axxon One* and it is ready to use.

> **Note**
>
> Information about the installed hardware key is displayed in the Sentinel Admin Control Center[208] web application, on the **Sentinel Keys** tab.

The installation of the hardware key is now complete.

18.8.17.4 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
```

208 http://127.0.0.1:1947/

```
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[209] web application, on the **Sentinel Keys** tab.

The installation of the software key is now complete.

18.8.17.5 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>

209 http://127.0.0.1:1947/

```
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[210] web application, on the **Sentinel Keys** tab.

The update of the license is now complete.

18.8.17.6 Removing a license

To delete 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.

210 http://127.0.0.1:1947/

```
haspmld -s
aksusbd
```

5. After you delete 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.

18.8.17.7 Checking a license

You can check the current license status on the Server. To do this, open the Sentinel Admin Control Center[211] 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
```

18.8.18 License activation of License plate recognition IV on 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
```

211 http://127.0.0.1:1947/

License activation of License plate recognition IV is complete.

18.9 Appendix 9. Using Axxon One with NAT

18.9.1 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(see page 899)).

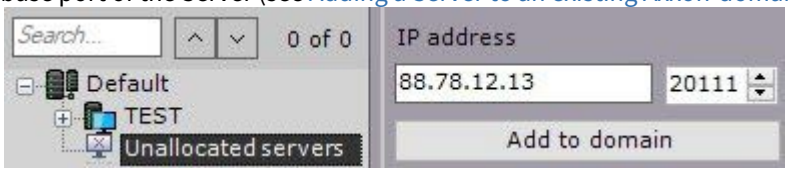
   Attention!

   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(see page 57)).

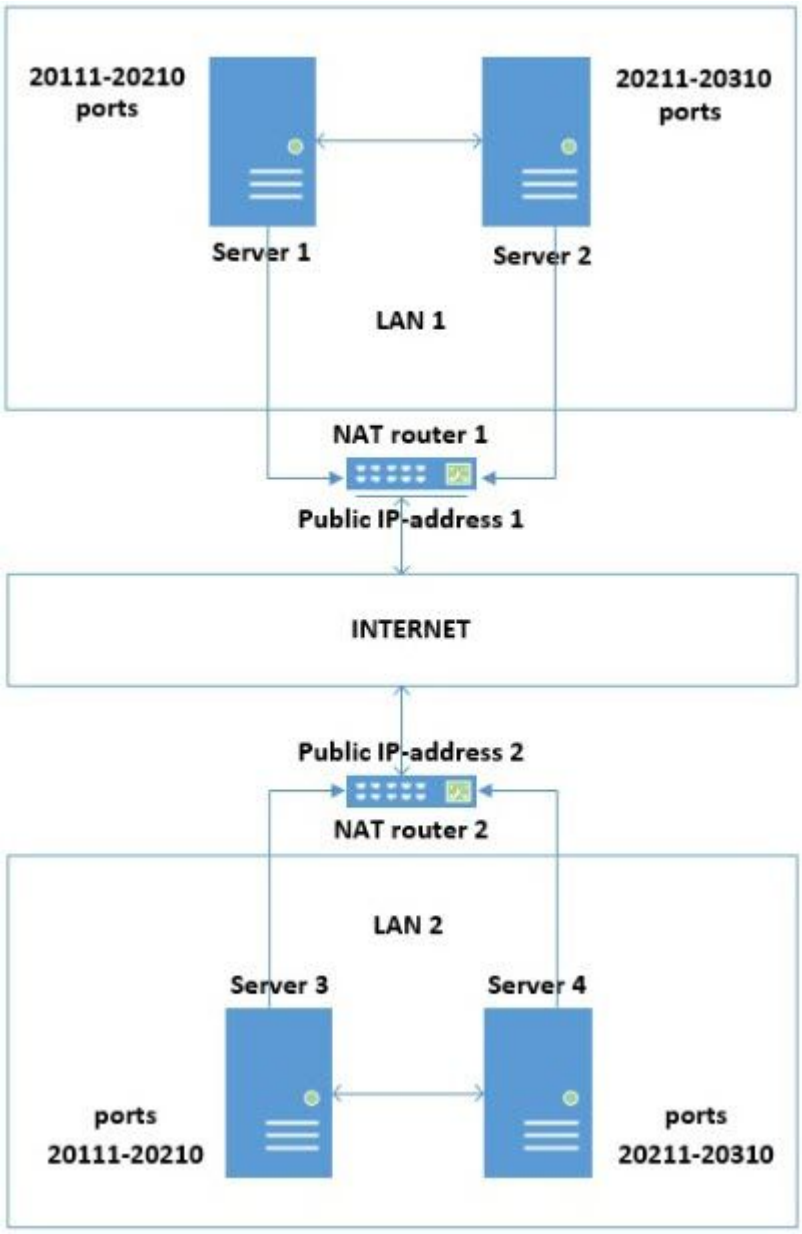
   Attention!

   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 an Axxon One Client(see page 94), Connecting the Client to the Server behind NAT(see page 946)).
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 Axxon-domain(see page 109)).

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.

18.9.2 Connecting the Client to the Server behind NAT

To connect the Client to the Server behind NAT, do the following:

1. On the Server, set the port range for operation. By default, the base port is 20111, and the port range is 20111-20210 (see Ports used by the Axxon One Software Package(see page 57)).
2. Open the port range 27000–35000 on the Server (see Ports used by the Axxon One Software Package(see page 57)).

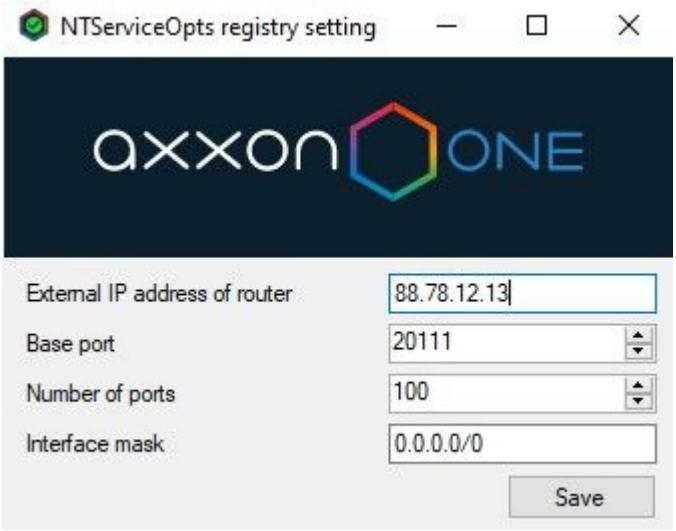
   Attention!

   If you do not open the port range 27000–35000 on the Server, there will be a problem with receiving the events to the Client from the Server. To solve the problem, create the NGP_POLL_EVENTS system variable on the Client and set its value to 1 (see Appendix 10. Creating system variable(see page 951)).

3. Set the router public IP address (see Network settings utility(see page 899)).

   Attention!

   The router public IP address should be static.



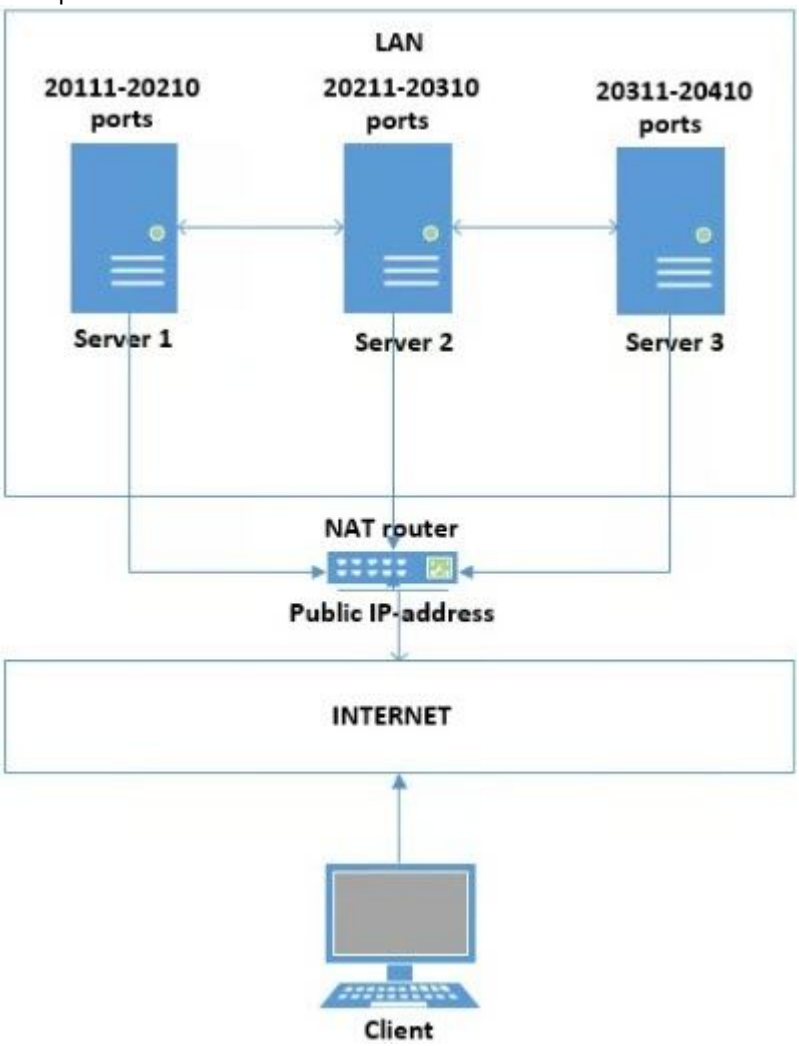
4. On the router, forward the specified Server ports and the gRPC API 20109 port.

5. Launch the Client and specify the router external IP address and the Server external base port in the connection settings (see Starting an Axxon One Client(see page 94)).

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(see page 944)).

Example.



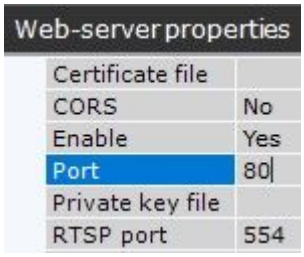
To connect the Client to the Servers behind NAT, do the following:

1. On the Server 1, set the port range 20111-20210 and the router public IP address.
2. On the Server 2, set the port range 20211-20310 and the router public IP address.
3. On the Server 3, set the port range 20311-20410 and the router public IP address.
4. On the Server 1, 2 and 3, open the port range 27000–35000 and create the NGP_POLL_EVENTS system variable on the Client.
5. On the router, configure the forwarding of:
    a. The router ports 20111-20210 to the internal IP address of the Server 1 and ports 20111-20210.
    b. The router ports 20211-20310 to the internal IP address of the Server 2 and ports 20211-20310.
    c. The router ports 20311-20410 to the internal IP address of the Server 3 and ports 20311-20410.
    d. The gRPC API 20109 port (always static) to the internal IP addresses of the Server 1, 2 and 3.
6. When connecting the Client, enter the router public IP address and port:
    a. port 20111 to connect to the Server 1.
    b. port 20211 to connect to the Server 2.
    c. port 20311 to connect to the Server 3.

18.9.3 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:

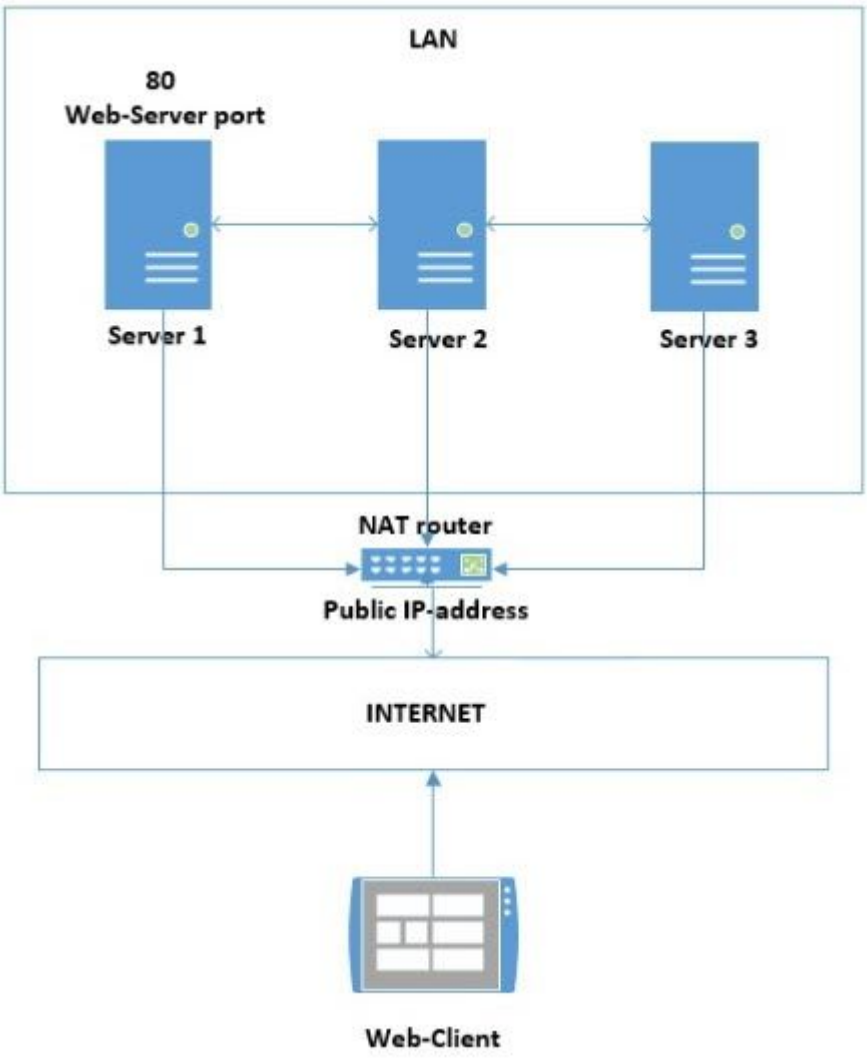
1. On the router, forward the specified port of the Web server (see Configuring the Web-Server(see page 119)). The default port is 80.



> **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(see page 823)).

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.

18.9.4 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(see page 794)

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 10. Creating system variable(see page 951)).
   b. Add an NGP_CLIENT_PORT_SPAN environmental variable and set its value to the number of ports in the range.

      Attention!

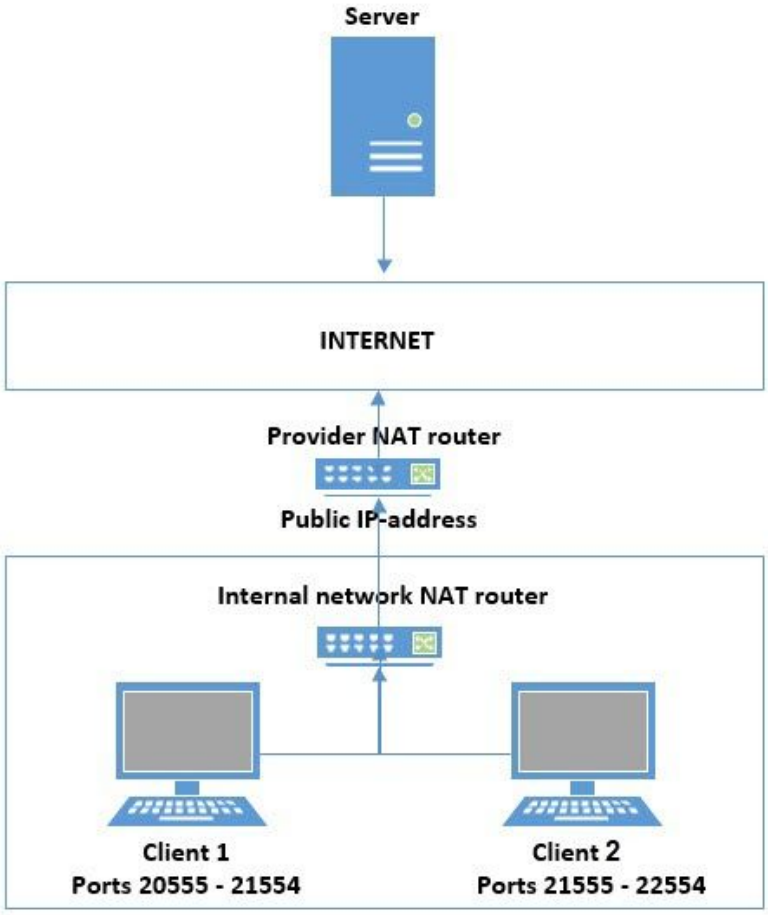
      We recommend you to use no less than 100 ports.

      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:

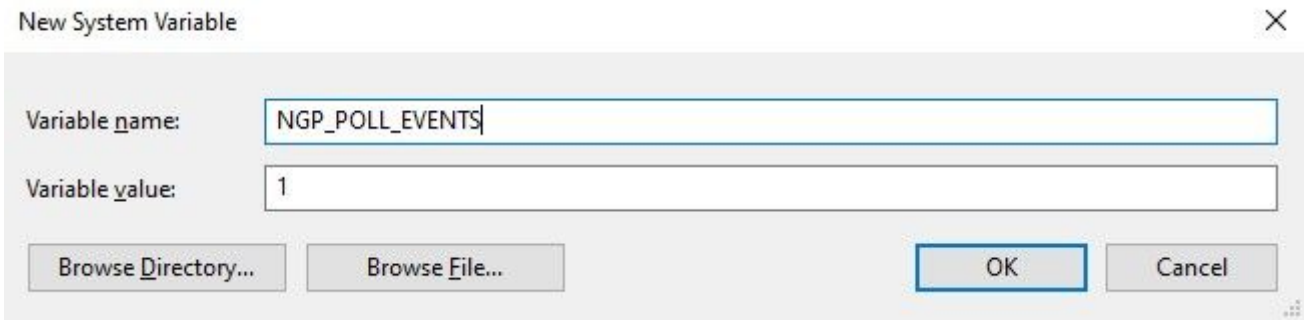
1. On Client 1, set port range to 20555-21554, and the public IP address of your Internet provider's router.
2. On Client 2, set port range to 21555-22554, and the public IP address of your Internet provider's router.

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.

18.10 Appendix 10. 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.