Administrator's Guide

Last update 16/02/2026

Table of contents

1 Administrator's Guide. INTRODUCTION 28
2 Software Lifecycle Policy 29
3 General description of the INTELLECT™ software 30
4 Requirements for the software and hardware platform 31
5 Personnel skills requirements 32
6 Installing and removing INTELLECT™ software 33
7 License key 34
8 Configuring system startup and shutdown 35
9 Working with the System settings dialog box 36
10 Intellect configuration and setup 37
11 The Report System 42
12 Administrator's Guide. Conclusion 43
13 Appendices 44
14 Administrator's Guide. INTRODUCTION 45
14.1 Purpose of the INTELLECT™ intelligent video surveillance system 45
14.2 Setting up logical interrelations among objects in the Intellect software system 45
14.3 Purpose and structure of the guide 46
14.4 License method of the INTELLECT™ software 46
15 Software Lifecycle Policy 47
15.1 Software Lifecycle Phases 47
15.2 Software Technical Support 47
15.3 Standard Period for Release of Software Updates 47
15.4 Licensing Policy with Regard to Software Updates 47
16 General description of the INTELLECT™ software 48
16.1 Intellect functionality 48
16.1.1 Video surveillance functionality 48
16.1.2 Audio monitoring functionality 49
16.1.3 Structuring of the protected facilities functionality 49
16.1.4 Event registration and processing functionality 49
16.1.5 Notification functionality 50

16.1.6 Workability control functionality 50
16.1.7 Automatic management functionality 50
16.1.8 Access control functionality 50
16.1.9 Integration of the distributed video surveillance and audio monitoring system functionality 50
16.2 Structure of the digital video surveillance and audio monitoring system based on INTELLECT™ software 50
16.2.1 Basic hardware components of the digital video surveillance system 51
16.2.2 Software 52
16.2.2.1 Operating system 52
16.2.2.2 Software kernels 52
16.2.2.3 Program modules 52
16.2.2.4 Interaction of basic modules with the Intellect kernel 52
16.2.2.5 Interaction of modules of other vendors with Intellect kernel 53
16.2.3 Internal video Server database 54
16.2.4 Communication environment 55
16.3 Intellect software package restrictions 55
16.4 Hashing procedure 57
16.5 Traffic encryption in the Intellect software 57
17 Requirements for the software and hardware platform 58
17.1 Requirements for base PCs 58
17.1.1 General requirements for PCs 58
17.1.2 Operating system requirements 59
17.1.2.1 Specific requirements for working with Intellect 62
17.1.3 Free disk space (video archive size) required 62
17.1.4 Defining disk space (audio archive size) 65
17.1.5 Define required disk space (size of event log database) 66
17.1.6 Define required disk space (VMDA metadata storage) 66
17.1.7 Intellect software working in virtual machines 66
17.2 Requirements for TCP/IP Network 67
17.2.1 Requirements for TCP/IP Network bandwidth for video signal transferring 68
17.2.2 Requirements for TCP/IP network bandwidth for database synchronization functionality 69
17.2.3 Requirements to the TCP/IP network quality 69
17.3 Requirements for PTZ and control panels 70
17.4 Requirements for audio input units 70
17.5 Requirements for IP devices 70

17.6 Requirements for GSM Equipment ... 71
17.7 Requirements for voice modems ... 71
17.8 Requirements for software which is used while integrating ... 71
17.9 Requirements for anti-virus software ... 71
17.10 Requirements for BIOS configuration ... 71
17.11 Hardware requirements for Intellect and vertical solutions detection tools ... 72
18 Personnel skills requirements ... 74
19 Installing and removing INTELLECT™ software ... 75
19.1 Installing Intellect ... 75
19.1.1 Description of INTELLECT™ software distribution package ... 75
19.1.2 Getting ready for Intellect installation ... 76
19.1.2.1 OS language settings ... 76
19.1.2.2 System settings ... 79
19.1.3 Installation of Intellect as a Server/Remote Administrator's workstation ... 79
19.1.4 Installation of INTELLECT™ software to the Client ... 93
19.1.5 Updating Intellect ... 103
19.1.6 Using Product.msi and Redist.exe for Intellect installation ... 109
19.1.7 Separate installation of components for Intellect operation ... 109
19.1.7.1 Updating Drivers Pack separately from the main product ... 110
19.1.7.1.1 Installation without uninstalling the previous version ... 110
19.1.7.1.2 Installation with uninstalling the previous version ... 111
19.1.8 Possible installation problems and their solutions ... 111
19.1.8.1 Error while installing driver for the FX4 card ... 112
19.1.8.2 Error code 26352 ... 112
19.2 Restoring Intellect ... 112
19.3 Removing INTELLECT™ software ... 115
19.3.1 Removing Intellect from the Start menu ... 115
19.3.2 Removing INTELLECT™ software from the OS Windows panel Add or Remove programs ... 119
19.3.3 Removing INTELLECT™ software using the installation kit ... 121
19.3.4 Removing INTELLECT™ software installed as a Service ... 122
19.4 Installing INTELLECT™ software in a silent mode ... 123
19.5 Remote installation, removal and update of Intellect software ... 127
19.5.1 Remote installation of Intellect software ... 128
19.5.2 Remote update of Intellect software ... 128

19.5.3 Remote removal of Intellect software ... 129
19.6 Configuring Cluster Service for Intellect ... 129
19.6.1 Example. Consolidation of two Servers into cluster and Intellect configuration ... 129
19.6.1.1 Preconfiguration of servers ... 129
19.6.1.2 Consolidation of two Servers into cluster and Intellect configuration ... 130
20 License key ... 132
20.1 Binding the license key to computer equipment ... 132
20.2 Match search in the license key ... 133
20.3 Features of the Intellect software operation when the object limit is exceeded ... 133
20.4 Decoding license key ... 134
21 Configuring system startup and shutdown ... 136
21.1 Configuration of Intellect™ software startup ... 136
21.1.1 Possible options for Intellect™ software startup ... 136
21.1.2 Configuring Intellect system automatic startup from Windows OS Startup ... 136
21.1.3 Configuring Intellect system automatic startup bypassing standard Windows OS ... 137
21.2 Configuring Intellect™ system shutdown ... 138
22 Working with the System settings dialog box ... 139
22.1 General information about the System settings dialog box ... 139
22.2 Startup and shutdown of the System settings dialog box ... 139
22.2.1 Startup of the System settings dialog box ... 139
22.2.2 Shutdown of the System settings dialog box ... 140
22.3 Setting procedure for system objects ... 141
22.3.1 Select an object ... 141
22.3.2 Create an object ... 141
22.3.3 Edit an object ... 144
22.3.4 Change the parent object ... 145
22.3.5 Copy objects ... 145
22.3.6 Enable or disable objects ... 146
22.3.7 Delete an object ... 148
22.3.8 Identifiers (numbers) of system objects ... 149
22.3.8.1 The Hardware tab ... 150
22.3.8.2 The Interfaces tab ... 153
22.3.8.3 The Users tab ... 154
22.3.8.4 The Programming tab ... 154

23 Intellect configuration and setup 156
23.1 Configuration procedure for servers, clients and remote workstations 156
23.1.1 Server settings 156
23.1.1.1 Server hardware and software platform 156
23.1.1.2 Setting up a Server 156
23.1.2 Configuring a Remote Admin Workstation 157
23.1.2.1 Remote Admin Workstation hardware and program platform 157
23.1.2.2 Remote Admin Workstation configuration 157
23.1.2.3 Videogate configuration 157
23.1.2.4 Configuring backup archive server 158
23.1.2.5 Configuring remote Web-server 158
23.1.3 OS settings for correct operation of Remote Admin Workstation or Server 158
23.1.4 Configuring Remote Clients (RC) 159
23.1.4.1 Remote Client hardware and software platform 159
23.1.4.2 Configuring Remote Client 159
23.1.4.3 OS settings for correct operation of Remote Client 160
23.2 Configuration of distributed architecture 160
23.2.1 General principles of designing the digital video surveillance system with distributed architecture 160
23.2.2 Configuring procedure for the distributed system 160
23.2.3 Selecting the structure of the distributed system 161
23.2.4 Synchronizing the databases of servers and remote workstations 161
23.2.5 Registration of servers, clients and remote workstations on the administering server 163
23.2.6 Configuring the interaction of distributed system components 165
23.2.7 Configuring time synchronization in the distributed system 168
23.2.8 Role-assignment in distributed system 168
23.2.9 Features of distributed system operation using NAT 169
23.3 Configuration of hardware 170
23.3.1 Configuring of using 64-bits modules 170
23.3.2 Configuring video subsystem 171
23.3.2.1 General information on configuring video subsystem 171
23.3.2.1.1 Video subsystem components description 171
23.3.2.1.2 Configuring video capture cards 171
23.3.2.1.3 Configuring IP-devices 172
23.3.2.1.4 Video signal compression and decompression 172
23.3.2.1.5 How to record digitized video signals 173

23.3.2.1.6 Digital video signal transmission to Remote Workstations 174
23.3.2.1.7 Video signal display 174
23.3.2.2 Registrating Video Capture Devices and cameras in INTELLECT™ software 174
23.3.2.3 Configuring the video signals processing mode while using video capture cards and analog video cameras 175
23.3.2.3.1 Setting up format (PAL or NTSC) for the input analog video signal 175
23.3.2.3.2 Frame rate settings 175
23.3.2.3.2.1 Video capture card resources 176
23.3.2.3.2.2 Operation modes of the video capture cards' ADC 178
23.3.2.3.2.3 Frame rate setup procedure 178
23.3.2.3.2.4 Configuring video subsystem with disabled video channels 178
23.3.2.3.2.5 Actual frame rate 180
23.3.2.3.2.6 Changing frame grooming 181
23.3.2.3.2.7 Allocation of video capture card's resources 182
23.3.2.3.2.8 Video signal processing priorities 184
23.3.2.3.2.9 Setting video processing priority 186
23.3.2.3.2.10 Setting video recording priority 186
23.3.2.3.3 Brightness, contrast, color depth and color rendition format settings 187
23.3.2.3.3.1 Brightness and contrast settings 187
23.3.2.3.3.2 Color depth adjustment 189
23.3.2.3.3.3 Selecting the color rendition format 190
23.3.2.3.4 Configuring video compression 191
23.3.2.3.4.1 Compression rate settings 191
23.3.2.3.4.2 Key frame rate settings 192
23.3.2.3.4.3 Setting delta frame creation criterion 193
23.3.2.4 Creating and configuring a virtual Video Capture Device 194
23.3.2.4.1 General information about the virtual Video Capture Device 194
23.3.2.4.2 Creating and configuring the virtual Video Capture Device 195
23.3.2.4.3 Features of playing black the files in the virtual Video Capture Device 198
23.3.2.5 Configuring video archiving 199
23.3.2.5.1 General information on video archiving 199
23.3.2.5.2 Video archiving procedure 201
23.3.2.5.3 Selecting the disks for video archive storage 201
23.3.2.5.4 Using network disks 202
23.3.2.5.5 Disabling automatic recording upon alarm registration 204
23.3.2.5.6 Configuring video frame rate 204
23.3.2.5.7 Configuring video in the Hot record mode 205

23.3.2.5.8 Configuring video in the Pre-alarm record mode ... 206
23.3.2.5.9 Configuring video in the Post-alarm record mode ... 208
23.3.2.5.10 Configuring audio and video synchro recording ... 209
23.3.2.5.11 Selecting current disk for recording ... 209
23.3.2.5.12 Viewing current disk for recording ... 211
23.3.2.5.13 Configuring video camera archive depth ... 211
23.3.2.5.14 Video Archive Encryption ... 212
23.3.2.5.15 Creating and configuring the MPEG4 Encoder object ... 213
23.3.2.6 Additional information on camera ... 214
23.3.2.7 Configuring video detection tools ... 215
23.3.2.7.1 General description of Intellect software detection tools ... 215
23.3.2.7.2 Enabling, configuring and disabling basic video detection tools ... 216
23.3.2.7.2.1 General information on basic detection tools ... 216
23.3.2.7.2.2 Requirements to video parameters while working with detection tools and Tracker ... 216
23.3.2.7.2.3 Procedure for enabling and configuring basic detection tools ... 217
23.3.2.7.2.4 Connecting basic detection tools ... 217
23.3.2.7.2.5 Configuring basic detection tools ... 218
23.3.2.7.3 Configuring smart video detection tools ... 230
23.3.2.7.3.1 General information on forensic search ... 230
23.3.2.7.3.2 Requirements for video parameters to perform the forensic search in the archive ... 231
23.3.2.7.3.3 Hardware requirements for the Tracker with neural filter operation ... 232
23.3.2.7.3.4 Video requirements to be met for abandoned object detection tool of the Tracker object operation ... 233
23.3.2.7.3.5 Creating and configuring VMDA metadata storage ... 233
23.3.2.7.3.6 Recommendations on configuring smart video detection tools ... 234
23.3.2.7.3.7 Creating and configuring the Tracker object ... 235
23.3.2.7.3.8 Configuring object classification ... 241
23.3.2.7.4 Embedded detectors ... 251
23.3.2.7.4.1 Creating embedded detectors ... 252
23.3.2.7.4.2 Configuring embedded detection ... 252
23.3.2.7.4.3 AxxonSoft Tracker in Axis devices ... 253
23.3.2.7.4.4 Example of setting up and using the embedded detectors on Bosch FLEXIDOME IP dynamic 7000 VR IP camera ... 257
23.3.2.7.5 Face detection tool ... 260
23.3.2.7.5.1 General information on face detection tool ... 260
23.3.2.7.5.2 Requirements to video parameters while using face detection tool ... 261
23.3.2.7.5.3 Configuring Face detection tool ... 261
23.3.2.8 Configuration of multistream video ... 266

23.3.2.9 Video record from computer monitor ... 269
23.3.2.10 Configuring fisheye cameras ... 272
23.3.3 Configuring audio subsystem ... 273
23.3.3.1 General information on configuring audio subsystem ... 273
23.3.3.1.1 Audio digitizing devices ... 274
23.3.3.1.1.1 Video capture cards ... 274
23.3.3.1.1.2 Standard soundcards, microphones, loudspeakers and headphones ... 274
23.3.3.1.1.3 Multichannel audio capture devices ... 275
23.3.3.1.1.4 IP-devices ... 275
23.3.3.1.2 Configuring the digitization devices for audio signals ... 275
23.3.3.1.3 Digitized audio signal recording ... 275
23.3.3.1.4 Digital audio signal transmission to Remote Workstations and servers ... 276
23.3.3.1.5 Audio signal playback ... 276
23.3.3.2 Registration of audio cards and microphones in INTELLECT™ software ... 276
23.3.3.3 Configuring audio signals digitization and processing ... 276
23.3.3.3.1 Audio signals sample rate settings ... 276
23.3.3.3.2 Setting up the audio signal volume amplification ... 276
23.3.3.3.3 Setting up the Automatic Gain Control for sound cards of Olha line ... 277
23.3.3.4 Configuring audio signals recording ... 278
23.3.3.4.1 Audio signals recording modes ... 278
23.3.3.4.2 Selecting the disks for audio archive storage ... 279
23.3.3.4.3 Setting up the sound activated recording ... 280
23.3.3.4.4 Setting up the audio and video synchro recording ... 281
23.3.3.5 Configuring audio playback ... 282
23.3.3.5.1 Creating and configuring the Audio playback card object ... 282
23.3.3.5.2 Creating and configuring the Speaker object ... 283
23.3.3.6 Features of standard sound card use ... 284
23.3.3.6.1 General information on standard sound cards ... 284
23.3.3.6.2 Features of standard sound card setup ... 284
23.3.3.7 Using multi-channel audio capture devices ... 286
23.3.3.7.1 General information on multi-channel audio capture devices ... 286
23.3.3.7.2 Setting up multi-channel audio capture devices ... 286
23.3.3.8 Using IP-devices ... 287
23.3.3.8.1 General information on IP-devices ... 287
23.3.3.8.2 Setting up the transmission of audio signals to IP devices ... 287

23.3.3.8.3 Setting up the transmission of duplex audio signals to IP-devices ... 289
23.3.4 Configuring events logging ... 289
23.3.5 Configuring the Event Viewer databases synchronization ... 291
23.3.5.1 General information on the Event Viewer databases synchronization ... 291
23.3.5.2 Configuring the Event Viewer database synchronization ... 291
23.3.5.3 Example of macro to start the Event Viewer databases synchronization ... 292
23.3.6 Configuring telemetry ... 293
23.3.7 Configuring operation of distributed architecture in the failover mode ... 293
23.3.7.1 General information about Failover mode ... 293
23.3.7.1.1 Purpose and features of the Failover mode ... 294
23.3.7.1.2 Examples of Failover system organization ... 294
23.3.7.1.2.1 1 main Server + standby Server ... 294
23.3.7.1.2.2 N main Servers + standby server ... 295
23.3.7.1.2.3 Two Servers being standby for each other ... 296
23.3.7.1.3 Limitations of the Failover mode ... 296
23.3.7.2 Configuring Failover service ... 298
23.3.7.3 Limiting number of failovers running simultaneously ... 300
23.3.7.4 Configuring archive synchronization of main and backup Servers ... 300
23.3.8 Configuring the SNMP-service ... 302
23.3.8.1 SNMP service setting order ... 302
23.3.8.2 Creating the SNMP trap object ... 302
23.3.8.3 Events selection for transmitting to SNMP manager ... 304
23.3.8.4 Configuring the message conversion into SNMP format ... 305
23.3.8.5 Setting up the trap with SNMP-message ... 307
23.3.8.6 SNMP configuration for traps receiving on remote computer ... 307
23.3.9 Setting up and connecting the special keyboard ... 307
23.3.9.1 Setting up the Keyboard object in INTELLECT™ software ... 308
23.3.9.2 Settings the interpretation rules of the Special keyboard layout by Intellect program complex ... 309
23.3.10 Configuring the System restart service ... 309
23.3.10.1 General information on the System restart service module ... 309
23.3.10.2 Activating the hardware control of workability ... 310
23.3.10.3 Configuring the software control of workability ... 310
23.3.10.4 Getting the information on memory consumption for processes ... 312
23.3.11 Configuring backup archiving ... 312
23.3.11.1 Purpose and implementation of backup archiving in the Intellect software ... 312

23.3.11.2 Configuring the Backup archive module ... 313
23.3.11.2.1 Configuration procedure for the Backup archive object ... 313
23.3.11.2.2 Creating the Backup archive object ... 313
23.3.11.2.3 Selecting and configuring the cameras for the Backup archive ... 314
23.3.11.2.4 Selecting cameras as a group for the Backup archive ... 315
23.3.11.2.5 Setting the parameters of video archive transmission over LAN ... 317
23.3.11.2.6 Selecting disks to store the archive of the Backup archive module ... 318
23.3.11.2.7 Configuring the grooming of the video archive ... 320
23.3.11.2.8 Configuring the schedule of the video archive copying ... 321
23.3.11.2.9 Enabling cooperation of Backup archive with Failover service ... 323
23.3.11.3 Configuring the Backup audio archive module ... 323
23.3.12 Configuring the Videogate module ... 325
23.3.12.1 General information on the videogate ... 325
23.3.12.2 Order of setting up the Videogate object ... 327
23.3.12.3 Creating the Videogate object ... 327
23.3.12.4 Selecting and configuring the cameras for the Videogate module ... 328
23.3.12.5 Selecting video cameras in bulk for the Videogate module ... 330
23.3.12.6 Selecting disks for storing the archive of the Videogate module ... 333
23.3.12.7 Configuring the recording to the Videogate archive ... 335
23.3.13 Notification services ... 336
23.3.13.1 Setting up the Alarm Message window ... 336
23.3.13.1.1 General description and usage details of the Alarm Message window ... 337
23.3.13.1.2 Creating and setting up the Alarm Message Window object ... 337
23.3.13.2 Setting up the Short Message Service (SMS) ... 338
23.3.13.2.1 General description and usage details of the Short Message Service ... 338
23.3.13.2.2 Creating and setting up the Short Message Service object ... 339
23.3.13.2.3 Creating and setting up the short messages ... 339
23.3.13.2.4 Creating and setting up the macro for sending the short message ... 340
23.3.13.3 Setting up the Mail Message Service (E-mail) ... 341
23.3.13.3.1 General description and usage details of the Mail Message Service ... 341
23.3.13.3.2 Creating and setting up the Mail Message Service ... 342
23.3.13.3.3 Creating e-mail messages ... 343
23.3.13.3.4 Creating and setting up a macro for sending the e-mail message ... 344
23.3.13.4 Setting up the Voice Message Service (V-dial) ... 344
23.3.13.4.1 General information and usage details of the Voice Message Service ... 344

23.3.13.4.2 Creating and setting up the Voice Message Service object ... 345
23.3.13.4.3 Creating voice messages ... 345
23.3.13.4.4 Creating and setting up the macro for sending the voice message ... 346
23.3.13.5 Setting up the Voice Notification Service ... 347
23.3.13.5.1 General description and usage details of the Voice Notification Service (VNS) ... 347
23.3.13.5.2 Creating and setting up the Voice Notification Service object ... 347
23.3.13.5.3 Creating a macro for sending and stop playing the voice notification ... 348
23.3.13.6 Sending messages via Telegram bot ... 349
23.3.13.6.1 Configuring message sending from Intellect to Telegram ... 349
23.3.13.6.2 Examples of macros for sending a message to Telegram ... 350
23.3.14 Replicating archive from unconnected servers using the removable storage ... 352
23.3.14.1 Order of archive replication from unconnected servers ... 352
23.3.14.2 Configuring the Data replication service object ... 352
23.3.14.3 Configuring the Target objects tree for data replication ... 353
23.3.14.4 Creating the query file ... 354
23.3.14.5 Copying the archive from the Source ... 354
23.3.14.6 Restoring the archive on the Target ... 356
23.3.15 Configuring the Web-server module ... 357
23.3.15.1 General description of the Web-server module ... 357
23.3.15.2 System requirements ... 357
23.3.15.3 Installing Java Runtime Environment ... 357
23.3.15.4 Authorization on the Web-server home page ... 358
23.3.15.5 Starting and setting up the Web-server module ... 359
23.3.15.6 Configuring the videoserver to connect Clients via the Web-server module ... 359
23.3.15.6.1 Creating the Web-server object ... 359
23.3.15.6.2 Selecting and configuring cameras for the Web-server module ... 361
23.3.15.6.3 Bulk selecting and configuring cameras for Web-server ... 362
23.3.15.6.4 Setting the parameters of connecting Clients to the Web-server ... 364
23.3.15.6.5 Configuring the authorization for the Web-server module. Default user ... 365
23.3.15.6.6 Enabling the processing of SDC (ECHD) requests and selecting the RTSP server ... 366
23.3.15.6.7 Configuring PTZ control priority for Web-server ... 367
23.3.15.7 Configuring the Server to connect the Clients via the Web-server 2.0 module ... 368
23.3.15.7.1 Creating the Web server 2.0 object ... 368
23.3.15.7.2 Configuring the Events filter for the Web-server 2.0 module ... 369
23.3.15.7.3 Using the Web server settings for the Web-server 2.0 module ... 370

23.3.15.7.4 Selecting maps ... 371
23.3.15.7.5 Applying changes of the user rights ... 372
23.3.15.7.6 Network settings of the Web Server 2.0 module ... 373
23.3.15.7.6.1 Changing the network interface used by the Web Server 2.0 module ... 373
23.3.15.7.6.2 Changing the port used by the Web Server 2.0 module ... 374
23.3.15.7.7 Configuring default response type for HTTP API requests ... 374
23.3.15.7.8 Registering a server in the cloud for Intellect push notifications ... 375
23.3.15.7.9 HTTPS settings ... 376
23.3.15.8 Web-server home page template and Java applet settings ... 377
23.3.15.9 Setting up the surveillance monitor interface of the Web-server module ... 379
23.3.15.10 Setting up the display of the data for traffic estimation in the Web-server ... 379
23.3.15.11 Setting up the Web-server module to act as a gate on a different HTTP-server ... 380
23.3.15.12 Updating the push notifications certificate for Intellect 4.11.1 and earlier versions ... 380
23.3.16 Configuring RTSP Server module ... 381
23.3.16.1 General info ... 381
23.3.16.2 Creating the RTSP Server object ... 382
23.3.16.3 Configuring the Unicast mode ... 382
23.3.16.4 Configuring the Multicast mode ... 383
23.3.16.5 Additional settings ... 384
23.3.16.6 Bulk settings for cameras ... 386
23.3.16.7 Examples of addresses to receive video from RTSP Server ... 386
23.3.17 Counting the system events ... 388
23.3.17.1 General Information on counting the system events ... 388
23.3.17.2 Configuring the Event counter ... 388
23.3.17.3 Data output and counter control ... 390
23.3.18 Configuring PS-RTP Server ... 391
23.3.19 Configuring ONVIF-Server module ... 393
23.3.19.1 General information about ONVIF-Server module ... 393
23.3.19.2 Configuring ONVIF-Server object ... 394
23.3.19.3 Configuring getting video using ONVIF-Server module ... 396
23.3.19.4 Features of embedded storage operation via ONVIF-Server ... 397
23.3.19.5 Filtering the ONVIF-Server events ... 397
23.3.19.6 Configuring ONVIF-Server module for the Multicast mode ... 402
23.3.20 Configuring integration with third-party systems ... 404
23.3.20.1 Configuring interaction with Manitou software ... 404

23.3.20.2 Configuring the integration with VideoIntellect software ... 406
23.3.20.2.1 Setting up the connection to VideoIntellect ... 407
23.3.20.2.2 Setting up the detector triggering reception from VideoIntellect ... 407
23.3.20.3 Configuring integration with VideoGuard system ... 408
23.3.20.4 Configuring BACnet integration ... 412
23.3.20.5 Configuring integration with YITU face recognition system ... 412
23.3.21 Configuring SIP-terminal ... 413
23.3.21.1 Configuring the Intellect's SIP server ... 414
23.3.21.1.1 Network settings of the Intellect's SIP server ... 414
23.3.21.1.2 Configuring SIP-devices of the Intellect's SIP server ... 415
23.3.21.1.2.1 Configuring the SIP-device ... 415
23.3.21.1.2.2 Configuring the SIP-device connection to Intellect ... 416
23.3.21.1.2.3 Configuring the Video / Audio ... 416
23.3.21.1.2.4 Configuring the tone DTMF commands ... 417
23.3.21.1.3 Configuring SIP-operators of the Intellect's SIP server ... 419
23.3.21.2 Configuring the Intellect's SIP client ... 420
23.3.21.2.1 Network settings of the Intellect's SIP client ... 420
23.3.21.2.2 Configuring SIP-devices of the Intellect's SIP client ... 421
23.3.21.2.3 Configuring SIP-operators of the Intellect's SIP client ... 421
23.3.21.3 Configuring address book of SIP-terminal ... 424
23.3.21.4 Configuring special numbers of SIP-terminal ... 425
23.3.21.5 Configuring numbers of SIP-terminal ... 425
23.3.21.6 Macros for working with SIP-terminal ... 427
23.3.21.7 Selecting speaker, microphone and camera for SIP-operator ... 429
23.3.21.8 Configuring SIP trunk ... 429
23.3.21.9 Configuring a SIP-terminal for Failover service ... 431
23.3.22 Configuring Incident server and Incident handler ... 431
23.3.22.1 Creating the Incident server object ... 432
23.3.22.2 Creating the Incident handler object ... 432
23.3.22.3 Selecting events to display and handle ... 433
23.3.22.3.1 Displaying and handling events in bulk ... 435
23.3.22.3.1.1 Functions used in this window ... 435
23.3.22.3.1.2 Order of adding events to the Incident handler ... 437
23.3.22.4 Setting the events priority ... 440
23.3.22.5 Creating and configuring the logic of event handling ... 440
23.3.22.5.1 Configuring the elements ... 442

23.3.22.5.1.1 Configuring the image 442
23.3.22.5.1.2 Configuring the button 443
23.3.22.5.1.3 Configuring the combobox 444
23.3.22.5.1.4 Configuring the comment 446
23.3.22.5.1.5 Configuring the radio button 447
23.3.22.5.1.6 Configuring the checkbox 448
23.3.22.6 Configuring the display of logic 450
23.3.22.7 Configuring the use of an external database 451
23.3.22.7.1 Configuring the connection to an external database in dialog mode 452
23.4 Configuration of interfaces 455
23.4.1 Intellect Software System's interface language 455
23.4.1.1 Installing the language 455
23.4.1.2 Switching languages in the Intellect Software System 456
23.4.2 Configuring the user interface 457
23.4.2.1 The user interface in the Intellect software 457
23.4.2.2 Setup procedure for the displays 458
23.4.2.3 Creating a Display object 458
23.4.2.4 Placing the interface components on the screen 459
23.4.2.4.1 Window coordinates and size 459
23.4.2.4.2 Moving a window and displaying on top of all windows 460
23.4.2.4.3 Selecting a physical monitor for display 460
23.4.2.4.4 Popup windows 461
23.4.2.5 Assigning the displays to the operator workstations 461
23.4.2.5.1 Assigning displays manually 461
23.4.2.5.2 Assigning displays via Wizard 463
23.4.2.5.3 Assigning displays via display activation 463
23.4.2.6 Examples of the user interface configuration 464
23.4.3 Configuration of video display 465
23.4.3.1 Configuring video display on Video Surveillance Monitor 465
23.4.3.1.1 General information on video signal displaying 465
23.4.3.1.2 Setup procedure for the Monitor object 466
23.4.3.1.3 Creating the Monitor object 466
23.4.3.1.4 Setting the parameters of the Monitor interface box 467
23.4.3.1.5 Selecting and configuring video cameras 471
23.4.3.1.6 Selecting and configuring video cameras in bulk 473

23.4.3.1.7 Configuring an auto select of video stream for displaying ... 475
23.4.3.1.8 Configuring the display mode of camera windows ... 477
23.4.3.1.9 Selecting the display mode ... 479
23.4.3.1.10 Setting the Telemetry control priority using the Monitor object ... 480
23.4.3.1.11 Configuring the captions showing ... 481
23.4.3.1.11.1 Enabling the captions showing ... 481
23.4.3.1.11.2 Configuring captions display on a video image ... 482
23.4.3.1.12 Configuring buttons display on the Video surveillance monitor ... 485
23.4.3.1.12.1 Enable buttons display on the Monitor ... 485
23.4.3.1.12.2 Configuring a button to display on the Monitor ... 485
23.4.3.1.13 Binding Audio player to the Monitor ... 488
23.4.3.1.14 Configuring a rotation angle of video image ... 489
23.4.3.1.15 Configuring Video surveillance windows interface ... 489
23.4.3.2 Configuring object's panoramic view by means of the Scene object ... 490
23.4.3.2.1 Creating the Scene object ... 491
23.4.3.2.2 Setting the parameters of the Scene interface box ... 491
23.4.3.2.3 Selecting and configuring cameras for the Scene object ... 492
23.4.3.3 Configuring video transmission to Remote Workstations ... 494
23.4.4 Configuration of audio ... 495
23.4.4.1 Configuring audio signals playback using the video monitor ... 495
23.4.4.2 Configuring audio signals playback using the Audio player object ... 495
23.4.4.2.1 Audio player setup sequence ... 495
23.4.4.2.2 Creating the Audio player object ... 496
23.4.4.2.3 Setting the parameters of the Audio player interface box ... 497
23.4.4.2.4 Setting up the recording and audio signals' playback ... 499
23.4.4.3 Features of audio signals export using the video monitor ... 500
23.4.4.4 Setting up the audio signal transmission to Remote Workstations and servers ... 501
23.4.5 Configuring the interactive map for object state indication and controlling the objects ... 501
23.4.5.1 General information on the structure of the interactive map of the protected facility ... 501
23.4.5.2 Configuring the interactive map ... 502
23.4.5.2.1 Setup procedure for the interactive map ... 502
23.4.5.2.2 Setting up the position of the Map on the screen ... 502
23.4.5.2.3 Creating the layers of the interactive map ... 504
23.4.5.2.3.1 Configuring the external Map server ... 508
23.4.5.2.4 Attaching objects to the layers of interactive map ... 509

23.4.5.2.5 Operations with objects in the Map editor utility ... 513
23.4.5.2.5.1 Operations with the objects, added to the layer ... 513
23.4.5.2.5.2 Editing the additional data and type of icon display ... 514
23.4.5.2.5.3 Editing the font, color, background or frame size of object name ... 516
23.4.5.2.5.4 Editing the object size ... 517
23.4.5.2.5.5 Editing the position of object ... 517
23.4.5.2.5.6 Changing the camera angle display ... 519
23.4.5.2.5.7 Editing color and transparency (polygon and ellipsis) ... 520
23.4.5.2.5.8 Editing the line thickness ... 520
23.4.5.2.5.9 Adding or removing apexes of polygon or polyline ... 521
23.4.5.2.5.10 Setting the order of displaying objects on map ... 522
23.4.5.2.5.11 Configuring the objects states display (polygon and ellipsis) ... 522
23.4.5.2.6 Linking the layers of the interactive map ... 523
23.4.5.2.7 Cancelling the last action in Map editor ... 526
23.4.5.2.8 Configuring object ID is displaying ... 526
23.4.5.2.9 Editing object properties using the Properties panel ... 527
23.4.5.2.10 Configuring viewing Map editor utility ... 528
23.4.5.2.11 Searching object in the Map editor utility by its name and ID ... 529
23.4.5.3 Configuring the mechanism for searching and processing alarm signals on multilayer maps ... 529
23.4.5.3.1 Displaying the Map over all windows ... 530
23.4.5.3.2 Autoswitch to a layer with an alarm signal ... 530
23.4.5.3.3 Recursive search for a layer with an alarm signal ... 531
23.4.5.4 Configuring the smoothing method of the Map when scaling ... 531
23.4.5.5 Configuring the number of events displayed in the Map window ... 532
23.4.5.6 Configuring the event tooltips ... 533
23.4.5.7 Configuring the order of reactions in the object menu ... 534
23.4.5.8 Enabling the frame or video request function ... 535
23.4.5.9 Selecting a Video Gate to display video on the map ... 536
23.4.6 Configuring the Backup archive panel object ... 536
23.4.7 Configuring the Operator protocol interface object ... 537
23.4.7.1 Creating the Operator protocol object ... 537
23.4.7.2 Configuring the position of the Operator protocol object ... 538
23.4.7.3 Setting up the event filter for the Operator protocol ... 539
23.4.7.4 Setting the options for handling events in the Operator protocol ... 541
23.4.7.5 Configuring the checklist ... 543
23.4.7.6 Configuring the Operator protocol interface ... 543

23.4.7.7 Connecting external DBs ... 544
23.4.7.7.1 Connecting an external configuration database ... 544
23.4.7.7.2 Connecting an external Event protocol database ... 545
23.4.7.7.3 Configuring the database server connection in a dialog mode ... 546
23.4.8 Configuring the Event Viewer interface object ... 548
23.4.8.1 Order of configuring the Event Viewer interface object ... 548
23.4.8.2 Configuring event filters for displaying in the Event viewer ... 548
23.4.8.3 Event viewer parameters ... 551
23.4.8.4 Parameters of displaying the Event Viewer interface box ... 552
23.4.9 Configuring the Incident manager interface object ... 554
23.4.9.1 Creating the Incident manager object ... 555
23.4.9.2 Configuring the Incident manager position on the screen ... 556
23.4.9.3 Configuring the main parameters of the Incident manager ... 557
23.4.9.4 Configuring the events grouping in Incident manager ... 558
23.4.9.5 Configuring user rights in Incident manager ... 559
23.4.10 Setting up the sound switch ... 560
23.4.10.1 Creating and configuring the Live sound switch object ... 560
23.4.10.2 Using the Live sound switch object ... 563
23.4.10.2.1 Template configuration ... 565
23.4.10.2.2 Managing templates ... 565
23.4.10.2.3 Playing audio by template ... 566
23.4.10.2.4 Adding audio files as sound sources ... 566
23.4.11 Setting up the Captions search window ... 568
23.4.11.1 The Captions search interface object setup procedure ... 568
23.4.11.2 Selecting the captioners ... 568
23.4.11.3 Specifying the captions search parameters ... 569
23.4.11.4 Setting up the Captions search interface window displaying ... 570
23.4.12 Configuring HTML interface ... 573
23.4.12.1 General description of HTML interface in Intellect software ... 573
23.4.12.2 Procedure of HTML interface configuring ... 573
23.4.12.3 Creating HTML interface object and setting its position ... 573
23.4.12.4 Creating and configuring the HTML page object ... 574
23.4.12.4.1 Creating the HTML page object ... 574
23.4.12.4.2 Open web-page by URL ... 575
23.4.12.4.3 Loading file from disk and saving to disk ... 576

23.4.12.4.4 Link to the HTML page object ... 577
23.4.12.5 Selecting start page for displaying in HTML interface ... 578
23.4.12.6 Selecting objects to track their states ... 578
23.4.12.7 Changing the displayed version of Internet Explorer ... 579
23.4.13 Setting up the voice notification ... 580
23.4.13.1 Setting up the voice notification using Audio player object ... 581
23.4.13.2 Setting up the voice notification using Sound notification object ... 582
23.4.14 Configuring the Display manager ... 583
23.4.15 Configuring the State statistics display ... 584
23.4.15.1 Configuring the State statistics window position on the screen ... 585
23.4.15.2 Selecting the objects to be included in State statistics and configuring the pixels number ... 585
23.4.15.3 Configuring the database connection ... 586
23.4.15.4 Configuring the interface parameters of the State statistics window ... 587
23.4.16 Configuring the Charts to display analog sensor readings ... 588
23.4.16.1 Setting the Charts window position on the screen ... 589
23.4.16.2 Configuring the chart display ... 590
23.4.17 Configuring the SIP-panel interface object ... 591
23.4.17.1 Basic settings of the SIP-panel interface object ... 591
23.4.17.2 Advanced settings of the SIP-panel interface object ... 593
23.4.17.3 Operator settings of the SIP-panel interface object ... 594
23.5 Configuration of users and permissions ... 595
23.5.1 Rights administration ... 595
23.5.1.1 The users' rights ... 595
23.5.1.2 User registration and removal ... 596
23.5.1.2.1 General information about user registration in Intellect software ... 596
23.5.1.2.2 User registration procedure ... 596
23.5.1.2.3 Administrator password registration ... 596
23.5.1.2.4 Department registration ... 598
23.5.1.2.5 Registration of Operator accounts ... 598
23.5.1.2.6 Removing user accounts ... 599
23.5.1.3 Registration of users' rights ... 600
23.5.1.3.1 Registration of operator rights ... 600
23.5.1.3.2 General information on the limits to the administrative functions ... 600
23.5.1.3.3 Limiting access to the tabs of the System Settings window ... 601
23.5.1.3.4 Limiting access to the system objects administration, control and viewing functions ... 601

23.5.1.3.5 Limiting access to shutting the system down ... 603
23.5.1.3.6 Limiting the rights to hide the interface components ... 604
23.5.1.3.7 Permissions for working with archives ... 605
23.5.1.3.7.1 Limiting access to archive playback ... 605
23.5.1.3.7.2 Limiting access to Backup archive playback ... 606
23.5.1.3.7.3 Permission to remove archive video files ... 607
23.5.1.3.7.4 Permissions to protect archive files from rewriting ... 608
23.5.1.3.7.5 Permissions for export and printout ... 609
23.5.1.3.7.6 Permissions to the hidden archive ... 610
23.5.1.3.7.7 Permissions to view video before and after inverted mask ... 610
23.5.1.3.7.8 Permissions to use VMDA filters ... 611
23.5.1.3.8 Configuring session auto termination when user is inactive ... 612
23.5.1.3.9 Configuring rights to use ONVIF Server ... 613
23.5.1.3.10 Combining (importing) permissions ... 614
23.5.1.3.11 Limiting access to sending commands (reactions) ... 615
23.5.1.4 Assigning the rights and password to operators for authorization in the Intellect ... 616
23.5.1.5 Setting up the default user ... 618
23.5.1.6 Changing permissions assigned to Operator ... 619
23.5.2 Configuration of the LDAP Service ... 620
23.5.2.1 General information about the LDAP Service module ... 620
23.5.2.2 Configuring the connection to the LDAP address book ... 621
23.5.2.3 Configuration of correspondence between address attributes and Intellect DB fields ... 623
23.5.2.4 Examples of LDAP Service configuration ... 624
23.5.2.5 Example macro for user import from LDAP address book ... 626
23.5.3 Active Directory configuration ... 627
23.5.3.1 General information about Active Directory and Intellect operation ... 627
23.5.3.2 Connecting the Intellect and Active Directory users ... 627
23.5.3.3 Connecting the Intellect user permissions to Active Directory groups ... 628
23.5.3.4 Starting the Active Directory synchronization ... 629
23.5.4 Configuring two-factor authentication ... 630
23.6 System settings (the Programming tab) ... 631
23.6.1 Configuring internal synchronization ... 631
23.6.2 Connection of objects with cameras ... 632
23.6.3 Creating and configuring Macro events ... 633
23.6.3.1 Configuring the macro events ... 634
23.6.3.2 Example of macro event ... 636

23.6.4 Creating and using macros ... 637
23.6.4.1 Creating macros ... 637
23.6.4.2 Examples of macros ... 641
23.6.5 Creating and using the Timer object ... 643
23.6.5.1 Creating and configuring the Timer object ... 643
23.6.5.2 Using the Timer object ... 645
23.6.6 Creating and using time schedules ... 647
23.6.6.1 Creating and configuring Time schedules ... 647
23.6.6.2 Viewing time schedules states ... 652
23.6.6.3 Examples of time schedules usage ... 653
23.6.7 Subdivision of the protected facility into areas and regions ... 655
23.6.7.1 About areas and regions ... 655
23.6.7.2 Creating areas ... 655
23.6.7.3 Creating Regions ... 656
23.6.7.4 Creating the rule of states transition ... 658
23.6.7.5 Examples of using areas and regions ... 660
23.6.7.5.1 Example 1. ... 661
23.6.7.5.2 Example 2. ... 661
23.6.7.5.3 Example 3. ... 662
23.7 Disabling Windows OS sleep mode when Intellect is running ... 663
24 The Report System ... 665
24.1 General information on the Report System ... 665
24.2 Starting and shutting-down the Report system ... 665
24.2.1 Starting the Report system ... 665
24.2.2 Shutting-down the Report system ... 666
24.3 The Report window ... 667
24.3.1 The OptionsForm window ... 669
24.4 Connecting to databases ... 671
24.4.1 Connecting to the main database of the Intellect system ... 671
24.4.1.1 Selecting an Access database and setting up the connection ... 671
24.4.1.2 Selecting an SQL database and setting up its parameters ... 675
24.4.2 Connecting to the Events Log (PROTOCOL table) ... 681
24.5 Manual loading of the configuration and registered events from the database ... 682
24.6 Viewing the general information on the events in the database ... 683

24.7 Creating the log of changes made to the system configuration ... 684
24.8 Using the report templates in the Report system ... 686
24.8.1 Recommendations for template creation ... 686
24.8.2 Creating a report template ... 686
24.8.3 Deleting the report templates ... 688
24.9 Using screen and printed reports ... 688
24.9.1 Creating a screen report ... 688
24.9.1.1 Creating a screen report from the report template ... 690
24.9.2 Creating a printed report ... 691
24.9.2.1 Creating a printed report from a report template ... 693
24.9.3 Printing the report ... 695
24.9.4 Exporting the report to a file ... 696
24.10 Video recording playback from the Report system ... 698
24.10.1 Playback of the video recordings from the Report system ... 698
24.10.2 Selecting the playback mode of video recordings ... 700
24.11 Filtering the events in the screen report according to the additional information ... 701
24.12 The keyboard shortcuts list ... 701
25 Administrator's Guide. Conclusion ... 703
26 Appendices ... 704
26.1 Appendix 1. Interface ... 704
26.1.1 Description of the Main control panel Interface ... 704
26.1.2 Description of the System settings dialog box ... 704
26.1.3 Information about program ... 706
26.1.4 Description of the Main control panel Interface ... 706
26.1.5 Description of the System settings dialog box ... 706
26.1.5.1 Tabs panel ... 706
26.1.5.2 Objects tree ... 707
26.1.5.3 Context menu of the system object ... 708
26.1.5.3.1 The Create object function ... 708
26.1.5.3.2 The Change parameter function ... 709
26.1.5.3.3 The Camera discovery tool function ... 710
26.1.5.3.4 The Delete object function ... 710
26.1.5.3.5 The Create folder function ... 710
26.1.5.3.6 The Move to folder function ... 712

26.1.5.3.7 The Save function ... 713
26.1.5.3.8 The Find function ... 715
26.1.5.3.9 The Reconnect function ... 716
26.1.5.3.10 The Send key to all function ... 717
26.1.5.3.11 The Send key function ... 718
26.1.5.3.12 The Save configuration function ... 719
26.1.5.3.13 The Load configuration function ... 720
26.1.5.3.14 The Collapse tree function ... 721
26.1.5.3.15 The Expand tree function ... 722
26.1.5.4 The object settings panel ... 723
26.1.5.5 The Apply and Cancel buttons ... 726
26.1.5.6 The elements of the System settings dialog box ... 727
26.1.5.7 The Architecture tab ... 728
26.1.5.7.1 Connection settings table ... 728
26.1.5.8 The Hardware tab ... 729
26.1.5.8.1 The Hardware tab components ... 729
26.1.5.8.2 The Settings panel of the Computer object ... 729
26.1.5.8.3 The Settings panel of the Video capture device object ... 735
26.1.5.8.4 The Settings panel of the Camera object ... 738
26.1.5.8.5 The Settings panel of the Detection zone object ... 750
26.1.5.8.6 The Settings panel of the Audio card object ... 755
26.1.5.8.7 The Settings panel of the Microphone object ... 756
26.1.5.8.8 The Settings panel of the Telemetry Controller object ... 759
26.1.5.8.9 The Settings panel of the PTZ device object ... 761
26.1.5.8.10 The Settings panel of the Control panel object ... 765
26.1.5.8.11 The Settings panel of the Backup archive object ... 767
26.1.5.8.12 The Settings panel of the Keyboard object ... 771
26.1.5.8.13 The Settings panel of the System restart service object ... 772
26.1.5.8.14 The Settings panel of the Voice notification service object ... 775
26.1.5.8.15 The Settings panel of the Voice Message Service object ... 777
26.1.5.8.16 The Settings panel of the Voice message object ... 778
26.1.5.8.17 The Settings panel of the Short Message Service object ... 780
26.1.5.8.18 The Settings panel of the Short Message object ... 781
26.1.5.8.19 The Settings panel of the Mail Message Service object ... 783
26.1.5.8.20 The Settings panel of the Mail message object ... 785

26.1.5.8.21 The Settings panel of the Web-server object ... 787
26.1.5.8.22 The Settings panel of the RTSP Server object ... 792
26.1.5.8.23 The Settings panel of the Operator query panel object ... 794
26.1.5.8.24 The Settings panel of the Alarm Message Window object ... 796
26.1.5.8.25 The Settings panel of the Videogate object ... 797
26.1.5.8.26 The Settings panel of the Event counter object ... 800
26.1.5.8.27 The Settings panel of the Data replication service object ... 804
26.1.5.8.28 The Settings panel of the Failover service object ... 804
26.1.5.8.29 The Settings panel of the Backup audio archive object ... 806
26.1.5.8.30 The Settings panel of the Web-server 2.0 object ... 807
26.1.5.8.31 The Settings panel of the Edge storage object ... 810
26.1.5.8.32 The Settings panel of the PS-RTP server object ... 811
26.1.5.8.33 The Settings panel of the Manager of failover services object ... 815
26.1.5.8.34 The Settings panel of the ONVIF-Server object ... 816
26.1.5.8.35 The Settings panel of the ONVIF-Server Profile object ... 819
26.1.5.8.36 The Settings panel of the Telegram bot object ... 821
26.1.5.8.37 The Settings panel of the SIP-terminal object ... 822
26.1.5.8.38 The Settings panel of the SIP-device object ... 827
26.1.5.8.39 The Settings panel of the SIP-operator object ... 831
26.1.5.8.40 The Settings panel of the Address book object ... 835
26.1.5.8.41 The Settings panel of the Incident handler object ... 836
26.1.5.8.41.1 Object general settings and the Filters tab ... 837
26.1.5.8.41.2 The Logic tab ... 839
26.1.5.8.41.3 The Main tab ... 840
26.1.5.9 The Interfaces tab ... 841
26.1.5.9.1 Interfaces tab components ... 841
26.1.5.9.2 The Settings panel of the Display object ... 841
26.1.5.9.3 The Settings panel of the Monitor object ... 843
26.1.5.9.4 The Settings panel of the Audio player object ... 855
26.1.5.9.5 The Settings panel of the Telemetry control panel object ... 857
26.1.5.9.6 The Settings panel of the Backup archive panel object ... 861
26.1.5.9.7 The Settings panel of the Map object ... 862
26.1.5.9.8 The Settings panel of the Layer object ... 867
26.1.5.9.9 The Settings panel of the Event viewer object ... 869
26.1.5.9.9.1 The Main tab ... 870

26.1.5.9.9.2 The Filters tab ... 874
26.1.5.9.10 The Settings panel of the Operator protocol object ... 875
26.1.5.9.10.1 The Filters tab ... 876
26.1.5.9.10.2 The DB tab ... 881
26.1.5.9.10.3 The DB protocol tab ... 882
26.1.5.9.10.4 The Interface tab ... 883
26.1.5.9.11 The Settings panel of the External window object ... 884
26.1.5.9.12 The Settings panel of the Scene object ... 885
26.1.5.9.13 The settings panel of the HTML Interface object ... 886
26.1.5.9.14 The settings panel of the HTML page object ... 888
26.1.5.9.15 The Settings panel of the Display manager object ... 889
26.1.5.9.16 The Settings panel of the State statistics object ... 891
26.1.5.9.17 The Settings panel of the Charts object ... 895
26.1.5.9.18 The Settings panel of the SIP-panel object ... 897
26.1.5.9.19 The Settings panel of the Incident manager object ... 902
26.1.5.9.19.1 General object settings and the Main tab ... 902
26.1.5.9.19.2 The Group by tab ... 905
26.1.5.9.19.3 The Rights tab ... 906
26.1.5.10 The Programming tab ... 907
26.1.5.10.1 The Settings panel of the Security zone object ... 907
26.1.5.10.2 The Settings panel of the Macro object ... 912
26.1.5.10.3 The Settings panel of the Program object ... 916
26.1.5.10.4 The Settings panel of the Time schedule object ... 917
26.1.5.10.5 The Settings panel of the Script object ... 918
26.1.5.10.6 The Settings panel of the Region object ... 919
26.1.5.10.7 The Settings panel of the Rule of states transition object ... 920
26.1.5.10.8 The Settings panel of the Macro event object ... 921
26.1.5.11 The Users tab ... 923
26.1.5.11.1 The Users tab components ... 923
26.1.5.11.2 The Settings panel of the Department object ... 923
26.1.5.11.3 The Settings panel of the User object ... 924
26.1.5.11.4 The Settings panel of the User permissions object ... 926
26.1.6 Information about program ... 931
26.2 Appendix 2. Relevant information on using Windows operating system ... 933
26.2.1 Working with Windows OS registry ... 933
26.2.1.1 General information about Windows OS registry ... 933

26.2.1.2 Using the registry editor ... 935
26.2.1.2.1 Starting and shutting-down the editor ... 935
26.2.1.2.2 Interface elements of the registry editor ... 936
26.2.1.2.3 Navigating the registry tree ... 937
26.2.1.3 Adding string parameters to the registry ... 937
26.2.1.4 Modifying the value of string parameters in Windows OS registry ... 940
26.2.1.5 Deleting parameters from the Windows OS registry ... 942
26.2.1.6 Configuring network drives visibility when UAC is enabled in Windows OS ... 944
26.2.2 Connecting network disks in Windows Vista and Windows 7 OS ... 946
26.2.3 Setting up serial (COM) ports in Windows ... 946
26.2.4 Working with Windows OS services for operating Intellect™ installed as a Service ... 947
26.2.4.1 General information on Intellect operation as a Service ... 947
26.2.4.1.1 Starting the Service ... 947
26.2.4.1.2 Users ... 947
26.2.4.1.3 Access to the database ... 948
26.2.4.2 Configuring the restart of the Intellect Core Server service ... 948
26.2.4.3 Using network disks of INTELLECT™ installed as a Service ... 949
26.2.4.4 Starting Intellect as a Service ... 950
26.2.4.5 Disabling Intellect as a Service startup ... 950
26.2.4.6 Configuring INTELLECT™ as a Service to work with Active Directory (AD) ... 951
26.2.4.7 Updating Intellect installed as a Service ... 951
26.2.5 The list of TCP ports used in INTELLECT™ ... 951
26.2.5.1 ACFA subsystem ... 958
26.2.6 Configuring Windows Firewall ... 965
26.2.7 Disable the Data execution prevention (DEP) function for Intellect software package ... 965
26.2.8 Configuring the best performance mode ... 967
26.2.9 Features of ElasticSearch service operation ... 968
26.2.9.1 Limiting RAM for Elasticsearch service ... 968
26.2.9.2 Running titles database update for restoration of ElasticSearch ... 969
26.3 Appendix 3. INTELLECT™ software database management ... 969
26.3.1 INTELLECT™ software database functions ... 969
26.3.2 Guidelines on Intellect system database use ... 970
26.3.3 Converting the database from MS Access to MS SQL format ... 971
26.3.4 INTELLECT™ software database connection ... 976
26.3.5 Viewing the Intellect database ... 981

26.3.6 Moving Intellect configuration database to the latest version of MS SQL Server ... 986
26.3.7 Database synchronization setup ... 988
26.3.8 Stored procedures for adding or deleting a large number of objects ... 992
26.3.8.1 Running stored procedures ... 992
26.3.8.2 Examples of stored procedures use for adding or deleting Camera objects ... 993
26.3.8.3 Example of stored procedure use for adding Tracker objects ... 993
26.3.8.4 Example of stored procedure use for adding VMDA Detection objects ... 994
26.3.9 Removing the events from the PROTOCOL table using SQL queries ... 994
26.3.10 Removing the event table from the Intellect database ... 995
26.3.11 Compressing the database size ... 995
26.3.12 Restoring the Intellect database from the Suspect mode ... 996
26.4 Appendix 4. Updating Java time zones for proper operation with archive in iOS client ... 998

1 Administrator's Guide. INTRODUCTION

2 Software Lifecycle Policy

3 General description of the INTELLECT™ software

- Intellect functionality
- Structure of the digital video surveillance and audio monitoring system based on INTELLECT™ software
    - Basic hardware components of the digital video surveillance system
    - Software
        - Operating system
        - Software kernels
        - Program modules
        - Interaction of basic modules with the Intellect kernel
        - Interaction of modules of other vendors with Intellect kernel
    - Internal video Server database
    - Communication environment
- Intellect software package restrictions
- Hashing procedure
- Traffic encryption in the Intellect software

4 Requirements for the software and hardware platform

- Requirements for base PCs
  - General requirements for PCs
  - Operating system requirements
  - Free disk space (video archive size) required
  - Defining disk space (audio archive size)
  - Define required disk space (size of event log database)
  - Define required disk space (VMDA metadata storage)
  - Intellect software working in virtual machines
- Requirements for TCP/IP Network
- Requirements for PTZ and control panels
- Requirements for audio input units
- Requirements for IP devices
- Requirements for GSM Equipment
- Requirements for voice modems
- Requirements for software which is used while integrating
- Requirements for anti-virus software
- Requirements for BIOS configuration
- Hardware requirements for Intellect and vertical solutions detection tools

5 Personnel skills requirements

6 Installing and removing INTELLECT™ software

- Installing Intellect
  - Description of INTELLECT™ software distribution package
  - Getting ready for Intellect installation
  - Installation of Intellect as a Server/Remote Administrator's workstation
  - Installation of INTELLECT™ software to the Client
  - Updating Intellect
  - Using Product.msi and Redist.exe for Intellect installation
  - Separate installation of components for Intellect operation
    - Updating Drivers Pack separately from the main product
  - Possible installation problems and their solutions
- Restoring Intellect
- Removing INTELLECT™ software
  - Removing Intellect from the Start menu
  - Removing INTELLECT™ software from the OS Windows panel Add or Remove programs
  - Removing INTELLECT™ software using the installation kit
  - Removing INTELLECT™ software installed as a Service
- Installing INTELLECT™ software in a silent mode
- Remote installation, removal and update of Intellect software
  - Remote installation of Intellect software
  - Remote update of Intellect software
  - Remote removal of Intellect software
- Configuring Cluster Service for Intellect
  - Example. Consolidation of two Servers into cluster and Intellect configuration

7 License key

- Binding the license key to computer equipment
- Match search in the license key
- Features of the Intellect software operation when the object limit is exceeded
- Decoding license key

8 Configuring system startup and shutdown

- Configuration of Intellect™ software startup
  - Possible options for Intellect™ software startup
  - Configuring Intellect system automatic startup from Windows OS Startup
  - Configuring Intellect system automatic startup bypassing standard Windows OS
- Configuring Intellect™ system shutdown

9 Working with the System settings dialog box

- General information about the System settings dialog box
- Startup and shutdown of the System settings dialog box
  - Startup of the System settings dialog box
  - Shutdown of the System settings dialog box
- Setting procedure for system objects
  - Identifiers (numbers) of system objects

10 Intellect configuration and setup

- Configuration procedure for servers, clients and remote workstations
  - Server settings
    - Server hardware and software platform
    - Setting up a Server
  - Configuring a Remote Admin Workstation
    - Remote Admin Workstation hardware and program platform
    - Remote Admin Workstation configuration
    - Videogate configuration
    - Configuring backup archive server
    - Configuring remote Web-server
  - OS settings for correct operation of Remote Admin Workstation or Server
  - Configuring Remote Clients (RC)
    - Remote Client hardware and software platform
    - Configuring Remote Client
    - OS settings for correct operation of Remote Client
- Configuration of distributed architecture
  - General principles of designing the digital video surveillance system with distributed architecture
  - Configuring procedure for the distributed system
  - Selecting the structure of the distributed system
  - Synchronizing the databases of servers and remote workstations
  - Registration of servers, clients and remote workstations on the administering server
  - Configuring the interaction of distributed system components
  - Configuring time synchronization in the distributed system
  - Role-assignment in distributed system
  - Features of distributed system operation using NAT
- Configuration of hardware
  - Configuring of using 64-bits modules
  - Configuring video subsystem
    - General information on configuring video subsystem
    - Registrating Video Capture Devices and cameras in INTELLECT™ software
    - Configuring the video signals processing mode while using video capture cards and analog video cameras
    - Creating and configuring a virtual Video Capture Device
    - Configuring video archiving
    - Additional information on camera
    - Configuring video detection tools
    - Configuration of multistream video
    - Video record from computer monitor
    - Configuring fisheye cameras
  - Configuring audio subsystem
    - General information on configuring audio subsystem
    - Registration of audio cards and microphones in INTELLECT™ software
    - Configuring audio signals digitization and processing
    - Configuring audio signals recording
    - Configuring audio playback
    - Features of standard sound card use
    - Using multi-channel audio capture devices
    - Using IP-devices
  - Configuring events logging
  - Configuring the Event Viewer databases synchronization
    - General information on the Event Viewer databases synchronization
    - Configuring the Event Viewer database synchronization
    - Example of macro to start the Event Viewer databases synchronization
  - Configuring telemetry
  - Configuring operation of distributed architecture in the failover mode
    - General information about Failover mode
    - Configuring Failover service

    - Limiting number of failovers running simultaneously
    - Configuring archive synchronization of main and backup Servers
- Configuring the SNMP-service
    - SNMP service setting order
    - Creating the SNMP trap object
    - Events selection for transmitting to SNMP manager
    - Configuring the message conversion into SNMP format
    - Setting up the trap with SNMP-message
    - SNMP configuration for traps receiving on remote computer
- Setting up and connecting the special keyboard
    - Setting up the Keyboard object in INTELLECT™ software
    - Settings the interpretation rules of the Special keyboard layout by Intellect program complex
- Configuring the System restart service
    - General information on the System restart service module
    - Activating the hardware control of workability
    - Configuring the software control of workability
    - Getting the information on memory consumption for processes
- Configuring backup archiving
    - Purpose and implementation of backup archiving in the Intellect software
    - Configuring the Backup archive module
    - Configuring the Backup audio archive module
- Configuring the Videogate module
    - General information on the videogate
    - Order of setting up the Videogate object
    - Creating the Videogate object
    - Selecting and configuring the cameras for the Videogate module
    - Selecting video cameras in bulk for the Videogate module
    - Selecting disks for storing the archive of the Videogate module
    - Configuring the recording to the Videogate archive
- Notification services
    - Setting up the Alarm Message window
    - Setting up the Short Message Service (SMS)
    - Setting up the Mail Message Service (E-mail)
    - Setting up the Voice Message Service (V-dial)
    - Setting up the Voice Notification Service
    - Sending messages via Telegram bot
- Replicating archive from unconnected servers using the removable storage
    - Order of archive replication from unconnected servers
    - Configuring the Data replication service object
    - Configuring the Target objects tree for data replication
    - Creating the query file
    - Copying the archive from the Source
    - Restoring the archive on the Target
- Configuring the Web-server module
    - General description of the Web-server module
    - System requirements
    - Installing Java Runtime Environment
    - Authorization on the Web-server home page
    - Starting and setting up the Web-server module
    - Configuring the videoserver to connect Clients via the Web-server module
    - Configuring the Server to connect the Clients via the Web-server 2.0 module
    - Web-server home page template and Java applet settings
    - Setting up the surveillance monitor interface of the Web-server module
    - Setting up the display of the data for traffic estimation in the Web-server
    - Setting up the Web-server module to act as a gate on a different HTTP-server
    - Updating the push notifications certificate for Intellect 4.11.1 and earlier versions
- Configuring RTSP Server module
- Counting the system events

        - General Information on counting the system events
        - Configuring the Event counter
        - Data output and counter control
    - Configuring PS-RTP Server
    - Configuring ONVIF-Server module
        - General information about ONVIF-Server module
        - Configuring ONVIF-Server object
        - Configuring getting video using ONVIF-Server module
        - Features of embedded storage operation via ONVIF-Server
        - Filtering the ONVIF-Server events
        - Configuring ONVIF-Server module for the Multicast mode
    - Configuring integration with third-party systems
        - Configuring interaction with Manitou software
        - Configuring the integration with VideoIntellect software
        - Configuring integration with VideoGuard system
        - Configuring BACnet integration
        - Configuring integration with YITU face recognition system
    - Configuring SIP-terminal
        - Configuring the Intellect's SIP server
        - Configuring the Intellect's SIP client
        - Configuring address book of SIP-terminal
        - Configuring special numbers of SIP-terminal
        - Configuring numbers of SIP-terminal
        - Macros for working with SIP-terminal
        - Selecting speaker, microphone and camera for SIP-operator
        - Configuring SIP trunk
        - Configuring a SIP-terminal for Failover service
    - Configuring Incident server and Incident handler
        - Creating the Incident server object
        - Creating the Incident handler object
        - Selecting events to display and handle
        - Setting the events priority
        - Creating and configuring the logic of event handling
        - Configuring the display of logic
        - Configuring the use of an external database
- Configuration of interfaces
    - Intellect Software System's interface language
        - Installing the language
        - Switching languages in the Intellect Software System
    - Configuring the user interface
        - The user interface in the Intellect software
        - Setup procedure for the displays
        - Creating a Display object
        - Placing the interface components on the screen
        - Assigning the displays to the operator workstations
        - Examples of the user interface configuration
    - Configuration of video display
        - Configuring video display on Video Surveillance Monitor
        - Configuring object's panoramic view by means of the Scene object
        - Configuring video transmission to Remote Workstations
    - Configuration of audio
        - Configuring audio signals playback using the video monitor
        - Configuring audio signals playback using the Audio player object
        - Features of audio signals export using the video monitor
        - Setting up the audio signal transmission to Remote Workstations and servers
    - Configuring the interactive map for object state indication and controlling the objects
        - General information on the structure of the interactive map of the protected facility
        - Configuring the interactive map

    - Configuring the mechanism for searching and processing alarm signals on multilayer maps
    - Configuring the smoothing method of the Map when scaling
    - Configuring the number of events displayed in the Map window
    - Configuring the event tooltips
    - Configuring the order of reactions in the object menu
    - Enabling the frame or video request function
    - Selecting a Video Gate to display video on the map
- Configuring the Backup archive panel object
- Configuring the Operator protocol interface object
    - Creating the Operator protocol object
    - Configuring the position of the Operator protocol object
    - Setting up the event filter for the Operator protocol
    - Setting the options for handling events in the Operator protocol
    - Configuring the checklist
    - Configuring the Operator protocol interface
    - Connecting external DBs
- Configuring the Event Viewer interface object
    - Order of configuring the Event Viewer interface object
    - Configuring event filters for displaying in the Event viewer
    - Event viewer parameters
    - Parameters of displaying the Event Viewer interface box
- Configuring the Incident manager interface object
    - Creating the Incident manager object
    - Configuring the Incident manager position on the screen
    - Configuring the main parameters of the Incident manager
    - Configuring the events grouping in Incident manager
    - Configuring user rights in Incident manager
- Setting up the sound switch
    - Creating and configuring the Live sound switch object
    - Using the Live sound switch object
- Setting up the Captions search window
    - The Captions search interface object setup procedure
    - Selecting the captioners
    - Specifying the captions search parameters
    - Setting up the Captions search interface window displaying
- Configuring HTML interface
    - General description of HTML interface in Intellect software
    - Procedure of HTML interface configuring
    - Creating HTML interface object and setting its position
    - Creating and configuring the HTML page object
    - Selecting start page for displaying in HTML interface
    - Selecting objects to track their states
    - Changing the displayed version of Internet Explorer
- Setting up the voice notification
    - Setting up the voice notification using Audio player object
    - Setting up the voice notification using Sound notification object
- Configuring the Display manager
- Configuring the State statistics display
    - Configuring the State statistics window position on the screen
    - Selecting the objects to be included in State statistics and configuring the pixels number
    - Configuring the database connection
    - Configuring the interface parameters of the State statistics window
- Configuring the Charts to display analog sensor readings
    - Setting the Charts window position on the screen
    - Configuring the chart display
- Configuring the SIP-panel interface object
    - Basic settings of the SIP-panel interface object
    - Advanced settings of the SIP-panel interface object

        - Operator settings of the SIP-panel interface object
- Configuration of users and permissions
    - Rights administration
        - The users' rights
        - User registration and removal
        - Registration of users' rights
        - Assigning the rights and password to operators for authorization in the Intellect
        - Setting up the default user
        - Changing permissions assigned to Operator
    - Configuration of the LDAP Service
        - General information about the LDAP Service module
        - Configuring the connection to the LDAP address book
        - Configuration of correspondence between address attributes and Intellect DB fields
        - Examples of LDAP Service configuration
        - Example macro for user import from LDAP address book
    - Active Directory configuration
        - General information about Active Directory and Intellect operation
        - Connecting the Intellect and Active Directory users
        - Connecting the Intellect user permissions to Active Directory groups
        - Starting the Active Directory synchronization
    - Configuring two-factor authentication
- System settings (the Programming tab)
    - Configuring internal synchronization
    - Connection of objects with cameras
    - Creating and configuring Macro events
        - Configuring the macro events
        - Example of macro event
    - Creating and using macros
        - Creating macros
        - Examples of macros
    - Creating and using the Timer object
        - Creating and configuring the Timer object
        - Using the Timer object
    - Creating and using time schedules
        - Creating and configuring Time schedules
        - Viewing time schedules states
        - Examples of time schedules usage
    - Subdivision of the protected facility into areas and regions
        - About areas and regions
        - Creating areas
        - Creating Regions
        - Creating the rule of states transition
        - Examples of using areas and regions
- Disabling Windows OS sleep mode when Intellect is running

11 The Report System

- General information on the Report System
- Starting and shutting-down the Report system
  - Starting the Report system
  - Shutting-down the Report system
- The Report window
  - The OptionsForm window
- Connecting to databases
  - Connecting to the main database of the Intellect system
    - Selecting an Access database and setting up the connection
    - Selecting an SQL database and setting up its parameters
  - Connecting to the Events Log (PROTOCOL table)
- Manual loading of the configuration and registered events from the database
- Viewing the general information on the events in the database
- Creating the log of changes made to the system configuration
- Using the report templates in the Report system
  - Recommendations for template creation
  - Creating a report template
  - Deleting the report templates
- Using screen and printed reports
  - Creating a screen report
    - Creating a screen report from the report template
  - Creating a printed report
    - Creating a printed report from a report template
  - Printing the report
  - Exporting the report to a file
- Video recording playback from the Report system
  - Playback of the video recordings from the Report system
  - Selecting the playback mode of video recordings
- Filtering the events in the screen report according to the additional information
- The keyboard shortcuts list

12 Administrator's Guide. Conclusion

13 Appendices

- Appendix 1. Interface
  - Description of the Main control panel Interface
  - Description of the System settings dialog box
    - Tabs panel
    - Objects tree
    - Context menu of the system object
    - The object settings panel
    - The Apply and Cancel buttons
    - The elements of the System settings dialog box
    - The Architecture tab
    - The Hardware tab
    - The Interfaces tab
    - The Programming tab
    - The Users tab
  - Information about program
- Appendix 2. Relevant information on using Windows operating system
  - Working with Windows OS registry
    - General information about Windows OS registry
    - Using the registry editor
    - Adding string parameters to the registry
    - Modifying the value of string parameters in Windows OS registry
    - Deleting parameters from the Windows OS registry
    - Configuring network drives visibility when UAC is enabled in Windows OS
  - Connecting network disks in Windows Vista and Windows 7 OS
  - Setting up serial (COM) ports in Windows
  - Working with Windows OS services for operating Intellect™ installed as a Service
    - General information on Intellect operation as a Service
    - Configuring the restart of the Intellect Core Server service
    - Using network disks of INTELLECT™ installed as a Service
    - Starting Intellect as a Service
    - Disabling Intellect as a Service startup
    - Configuring INTELLECT™ as a Service to work with Active Directory (AD)
    - Updating Intellect installed as a Service
  - The list of TCP ports used in INTELLECT™
  - Configuring Windows Firewall
  - Disable the Data execution prevention (DEP) function for Intellect software package
  - Configuring the best performance mode
  - Features of ElasticSearch service operation
    - Limiting RAM for Elasticsearch service
    - Running titles database update for restoration of ElasticSearch
- Appendix 3. INTELLECT™ software database management
  - INTELLECT™ software database functions
  - Guidelines on Intellect system database use
  - Converting the database from MS Access to MS SQL format
  - INTELLECT™ software database connection
  - Viewing the Intellect database
  - Moving Intellect configuration database to the latest version of MS SQL Server
  - Database synchronization setup
  - Stored procedures for adding or deleting a large number of objects
  - Removing the events from the PROTOCOL table using SQL queries
  - Removing the event table from the Intellect database
  - Compressing the database size
  - Restoring the Intellect database from the Suspect mode
- Appendix 4. Updating Java time zones for proper operation with archive in iOS client

14 Administrator's Guide. INTRODUCTION

On the page:

- Purpose of the INTELLECT™ intelligent video surveillance system
- Setting up logical interrelations among objects in the Intellect software system
- Purpose and structure of the guide
- License method of the INTELLECT™ software

14.1 Purpose of the INTELLECT™ intelligent video surveillance system

INTELLECT™ software is designed for the deployment of industrial scalable, flexible (adjustable) integrated security systems, based on the digital video surveillance and audio monitoring systems.

INTELLECT™ software possesses the following basic features:

1. Integration of digital video surveillance and audio monitoring systems with the existing data systems, various security equipment, auxiliary software of other developers, using integrated open interfaces of the data exchange.
2. Compatibility with diverse security devices and data systems, in particular, with the fire and security alarm and access control systems, video surveillance cameras, data analysis systems and systems for recognition of objects (events) and identification by their images.
3. Single-source registration and processing of events, generation of notifications and controlling response in compliance with the flexibly modified logics.
4. Ultimately unlimited capabilities for scaling, solution—specific adjustments, re-distribution of resources with changes in the number or quality of tasks in monitoring protected facilities and operating various equipment.

14.2 Setting up logical interrelations among objects in the Intellect software system

Functional facilities of Intellect software complex are based on logical cooperation of objects. Common data about ways of setting up the logical interrelation is given in the table.

Ways of setting up the logical interrelation	**Description**	**Realization**	**Example**
Objects settings panels	Base setting of system objects interrelation	Is realized with the use of system objects functionality-see. Administrator's Guide.	Setting up the video signal displaying in Monitor interface window
Macros	Setting up simple interrelations among objects which functionalities do not allow to carry out the required operations	Is realized with the use of Macros object functionality-see. Administrator's Guide.	Setting of enabling the additional executive relay with ray closed
Program	Setting up complex interactions among objects, when **Macro** object functionality does not allow to carry out the required operations	Is realized on the basis of Program object as a code on the embedded Intellect program language-see. this guide	It is necessary to return the cameras to the reference position and make a frame

Ways of setting up the logical interrelation	Description	Realization	Example
Script		Is realized on the basis of Script object as a code on embedded JScript language –see. The Script object. Programming using the JScript language.	

14.3 Purpose and structure of the guide

Documentation for the INTELLECT™ intelligent video surveillance system, Video surveillance and audio monitoring Administrator Guide is a reference and information handbook on programming on embedded Intellect software language, which is designed for system administrators, installation and configuration technicians, users with administrator rights to the digital video surveillance and audio monitoring systems, developed on the basis of INTELLECT™ software.

Programming in the INTELLECT™ enables system control by setting up complex logical interactions among objects. This guide contains the following materials:

1. Software programming;
2. Description of embedded program language syntax;
3. Examples of program on the embedded language.

14.4 License method of the INTELLECT™ software

Licensing of the INTELLECT™ software is performed by means of software and program protection.

The INTELLECT™ software protection is built on one of the following components:

1. dallas-codes of video capture cards' cryptochips (FS-5B, FS-6C, FS-8, FS-16(Exp), WS-7, WS-17);
2. dallas-codes of the electronic hardware security key «Guardant»;
3. codes of HID devices (hardware id).

The key file, connecting the software protection with program modules, belongs to the program protection part. A list of available for using functional program modules depends on the configuration of security system's delivery and is registered in the key file.

While extending the system configuration (for example while installing a new functional subsystem) for activating the program module functionality, corresponding to the installed subsystem, in the previous key file has to be changed by a new one, which the updated system functionality will be regulated with.

While using the distributed architecture a single key file is used for all the computers of the system.

Attention!

If the video capture card is changed, its dallas-codes are changed too, so the previous key file should be respectively changed by a new one. While using the distributed architecture the key file should be changed on all the computers of the system.

15 Software Lifecycle Policy

On page:

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

15.1 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.

15.2 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.

15.3 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. Releases with bug and security fixes can be requested from technical support.

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

15.4 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.
- New software features that are subject to licensing will not be available until the license key is updated.

16 General description of the INTELLECT™ software

16.1 Intellect functionality

On the page:

- Video surveillance functionality
- Audio monitoring functionality
- Structuring of the protected facilities functionality
- Event registration and processing functionality
- Notification functionality
- Workability control functionality
- Automatic management functionality
- Access control functionality
- Integration of the distributed video surveillance and audio monitoring system functionality

This section provides information on the basic administered user functions of the distributed digital video and audio surveillance system based on *Intellect*.
Intellect provides the following basic user functions:

16.1.1 Video surveillance functionality

1. Simultaneous display of the images from several cameras (belonging to one or several Servers) on the **Video surveillance monitor** on a single computer screen (display).
2. Priority-oriented automatic selection of the displayed video images from alarm or active cameras (using a special **Video surveillance monitor** with video images from the cameras according to the set parameters).
3. Change the number of the **Surveillance windows** and their layout on the **Video surveillance monitor**.
4. Display of the zoomed in image from the selected camera (**Surveillance window**) displayed on the **Video surveillance monitor**, **Surveillance windows** slideshow option for the selected camera.
5. Color coding of the **Surveillance window** (camera) state: **Armed**, **Alarm**, **Recording**, etc.
6. Remote access to audiovisual streams from any workstation with both local and remote archive recording option.
7. Video recording can be performed:
    a. continuously;
    b. in real-time according to the set events;
    c. on alarm with a pre-event recording option or by Operator's command.
8. Pre-event video recording.
9. Display of the freeze frame by Operator's command without interruption of the recording.
10. Display of the service information on the **Video surveillance monitor**:
    a. current time;
    b. current date;
    c. camera No, ID.
11. Recording by Operator's command.
12. Viewing of the video images from the cameras.

13. Priority viewing of the video images from the cameras based on events (alarms) detection.
14. Video surveillance using the Web interface and mobile apps.
15. Audio and video archive management.
16. Viewing of the recorded videos with the possibility to search the archive by time, event and camera.
17. Synchro playback of the recorded videos on several cameras.
18. Timing of the archived video recordings.
19. Timestamp based video recordings search.
20. Video image processing:
    a. digital zooming;
    b. contrasting;
    c. focusing;
    d. masking;
    e. dynamic outlining.
21. Management of the actuating devices using:
    a. the 3rd party program interface panel;
    b. the universal control panel for the actuating devices management;
    c. a mouse;
    d. a joystick.
22. Viewing video information from all Servers included in the system on any workstation using the TCP/IP communication environment.
23. Storage and export of video frames and video recordings.
24. Integrated use of multi-zone detectors of various types:
    a. Main motion detector;
    b. Motion;
    c. Focusing;
    d. Video signal stability;
    e. Changes in the video image background;
    f. Light-struck camera lens;
    g. Closing camera lens;
    h. Infra-red
25. Detector area(s) masking.
26. Image deinterlacing.
27. Analog video signal output.

16.1.2 Audio monitoring functionality

1. Audio surveillance.
2. Audio and video synchro recording.
3. Sound activated audio recording.
4. Audio recording by Operator's command.
5. Audio recordings export.

16.1.3 Structuring of the protected facilities functionality

1. Conditional subdivision of the protected facility into areas and sections.
2. Using the multilevel (multilayered) interactive **Map** of the protected facility which implements the following functions:
    a. Auto switching and recursive search for links on the map (layers).
    b. Using the active device symbols on the map (layers) with the possibility to manage the devices from the function menu.

16.1.4 Event registration and processing functionality

1. Maintenance of the **Event log**, which displays all registered events or events of certain types according to the preconfigured filters. It is possible to display the corresponding video or a map with the object for each event.
2. Auto notification about different alarm and information events in the **Alarm notification window**.
3. Event management and processing according to the configurable scripts using the **Operator protocol** and **Incidents manager**.

16.1.5 Notification functionality

Auto notification using:

1. SMS (Short Message Service).
2. Emails.
3. V-dial auto redial service.
4. Sound (voice) notification.
5. Telegram bot.

16.1.6 Workability control functionality

1. Software control of workability — the **System restart service** object.
2. Hardware control of workability — *Watchdog.*
3. **Failover**: in case of the connection loss to one of the servers of the distributed system, the configuration is automatically moved to the backup server.

16.1.7 Automatic management functionality

Implementation of the user specific functions (performed according to the individual algorithms) using macros.

16.1.8 Access control functionality

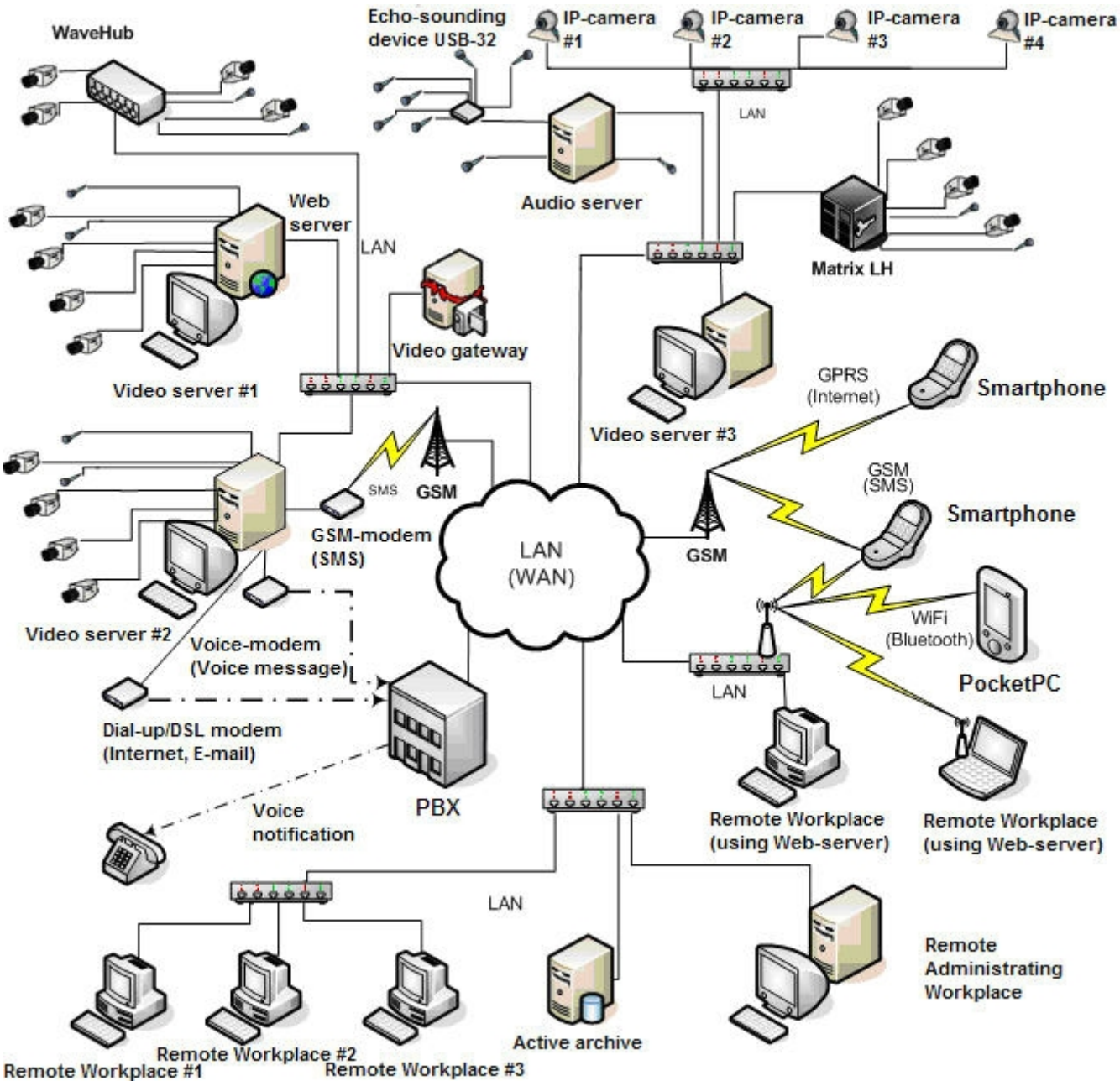
Flexible configuration of the access levels to the system components and the possibility to manage administrator rights.

16.1.9 Integration of the distributed video surveillance and audio monitoring system functionality

1. Remote interaction of the software cores and automated replication of the internal databases (containing the system setup parameters and the data on the events registered in the system) between Servers and Remote workstations that are the components of the distributed digital video surveillance system.
2. Creating the integrated database of the system setup parameters and the registered events, followed by their processing in compliance with the standards and the specialized adjustable algorithms, including generation of notifications and system responses.
3. Software-programmable optimization of the video data flows within the distributed digital video surveillance system when there is a lack of communication channel capacity (optional videogate functionality).

16.2 Structure of the digital video surveillance and audio monitoring system based on INTELLECT™ software

The versatile structure of the digital video surveillance and audio monitoring system based on INTELLECT™ software and standard hardware and software is shown in the figure below.



16.2.1 Basic hardware components of the digital video surveillance system

The distributed video surveillance and audio monitoring system based on the INTELLECT™ system may be deployed using the following basic hardware and software components:

1. Servers and Remote workstations based on PCs (IBM PC–based).
2. Network video hubs (WaveHub, Linux Hub, etc.).
3. Network video servers (Matrix, etc.).
4. Analog and IP video cameras.
5. Audio input devices.
6. TCP/IP communication.

16.2.2 Software

16.2.2.1 Operating system

Intellect software operates in Microsoft Windows family.(see Operating system requirements).

16.2.2.2 Software kernels

The Intellect™ system can be implemented in the following options (installation options):

1. Based on the full-featured INTELECT software kernel (this option corresponds to the intellect.exe software module) The full-featured software kernel ensures operation the video server, Administrator and Operator workstation.
2. Software kernel with minimized functionality supporting the Remote Operator Workstation functions (this option corresponds to the slave.exe software module).

Software of the Remote Operator Workstation does not support system administration (create, delete, set system objects, register users, user rights administration), as well as local database maintenance (operations with ROW use a remote database operated by the intellect.exe kernel and belonging to the video server or Remote Administrator Workstation).

Intellect.exe, the fully software kernel, is the central software component of the system. The system kernel interacts with the program modules, which form the software basis for the subsystems.

Integration of the distributed digital video surveillance and audio monitoring system is provided by the data exchange between software kernels.

16.2.2.3 Program modules

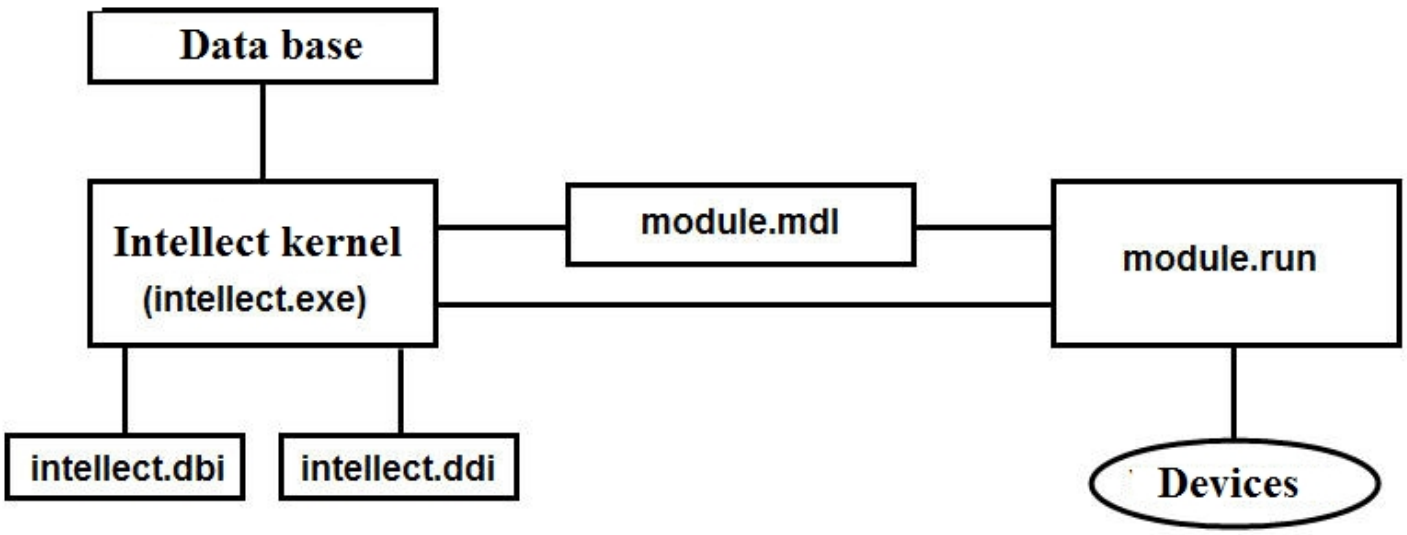
Program modules support direct interworking of the hardware, and also serve as a source of data about protected facilities. The software kernel of the system processes the incoming data from various program modules, providing their integration. The kernel sends ICMP packages to program modules every 5 seconds to check their availability.

The list of the program modules available for the operations depends on the configuration option of the system. Executive files, corresponding to the subsystems are automatically launched by the kernel as the system is configured

For instance, if the **Camera** object is created and as soon as the relevant settings are confirmed, the video sub-system executive module (video.run executable file) will be launched.

16.2.2.4 Interaction of basic modules with the Intellect kernel

Basic modules interact with the Intellect kernel via the data exchange interface of the Intellect kernel, using module.mdl, a dynamic library.The program modules and Intellect kernel interaction scheme are shown in the figure.



Intellect.dbi and intellect.ddi object setting files contain the information about integrated modules (objects) required to support operation of the Intellect kernel. System setting files are edited using ddi.exe, a specialized utility. At the object integration stage, the names and parameters of the integrated object and related system events and responses, used for this object, and the values thereof are recorded in the system setting files.

The module.mdl file supports operation with objects of the same type: creation, modification, deletion, changing object parameters at the configuration stage or during operation and saving updated parameters in the database, as well as certain special operations with the object. Apart from that, the module.mdl transmits parameters of the created or modified objects to the executive module.

The module.mdl file stores the configuration of the object setting panels.

The module.run execution file supports interworking with the units, transmits information about events to the kernel and also supports unit control.

Consequently, module.mdl supports two-way data exchange between the Intellect kernel and module. The responses and events, which are used, will be described in the system manuals of the appropriate object (in intellect.ddi file).

To simplify integration with the joint data systems, auxiliary software or extension modules, Intellect™ system offers an alternative interface for data exchange between modules and the Intellect kernel – IIDK.

16.2.2.5 Interaction of modules of other vendors with Intellect kernel

INTELLECT™ software architecture is designed for intertask communication between the *Intellect* kernel and modules (joint information systems) using the TCP/IP communication environment, requiring the following parameters to support connection:

1. port number;
2. IP address of the PC using the *Intellect* kernel;
3. ID, an identifier of the connectable object;

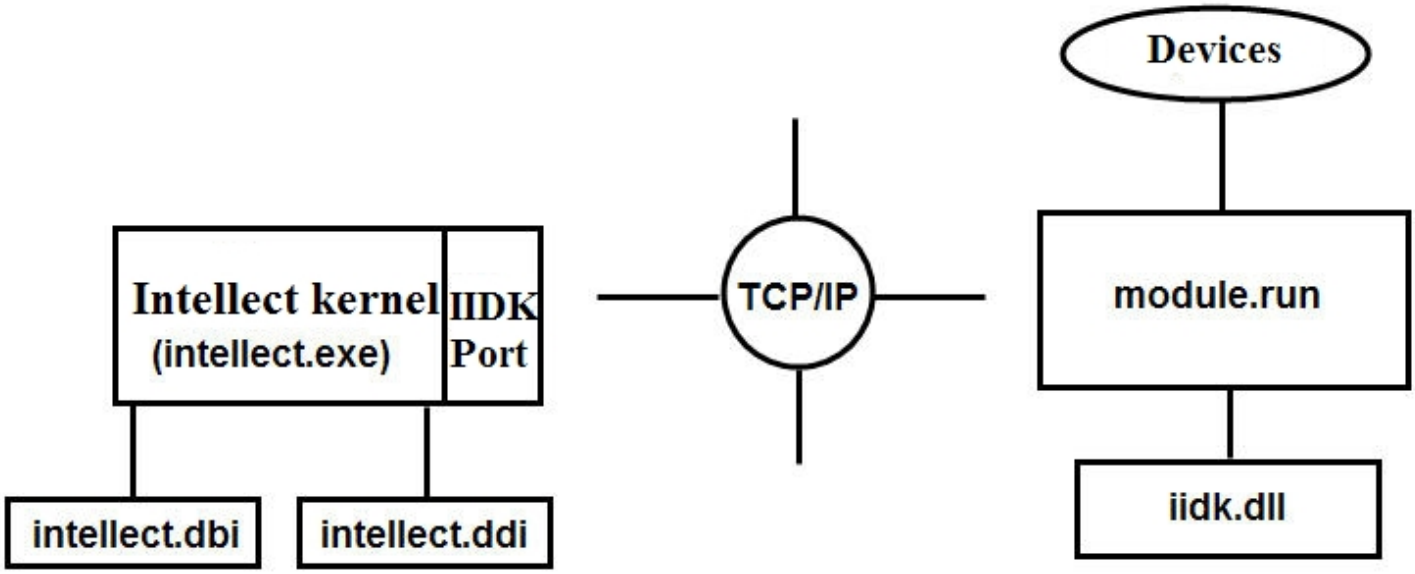
To enable the above mechanism, the **IIDK interface** object should be created in the Intellect software tree based on the **Computer** object at the stage of *Intellect* software configuration.

Where the **IIDK interface** is used, setting panels for the integrated modules (of already existing software) are not created.

To enable interworking between modules and the *Intellect* kernel, one of the following prerequisites should be complied with:

1. Integrated software should be adjusted for TCP/IP data exchange in the *Intellect* kernel format.
2. An interface program module should be developed to support transmission of events and responses of the integrated software in the *Intellect* kernel format and interoperate with the kernel through TCP/IP. This option is used in cases where integrity of the integrated software (for instance, integration of ATM software) is especially important.

The *Intellect* kernel adjusts to the data exchange over the specified port, as soon as the **IIDK interface** is created in the program.



Being a module and hierarchy object-based structure, INTELLECT™ software ensures efficient extension of functionalities through the integration of modules supporting new equipment or new service functions. INTELLECT™ software offers IIDK (Intellect Integration Developer Kit) to the vendors, integrating proprietary security equipment with INTELLECT™ software.

The above kit includes the software tools required for the development of integrated modules (auxiliary software) or modification of existing software to process messages, events and responses in the *Intellect* kernel format.

16.2.3 Internal video Server database

The internal video Server database contains the following information:

1. system settings (objects created in the system, their attributes, users and user rights and other additional data);
2. events registered by the system within the period specified at the system configuration stage (event logs).

The internal video Server database is maintained in the MS SQL format. The list of MS SQL Server versions, supported by Intellect, is given in the table below.

MS SQL Server version	**Supportes edition**
MS SQL Server 2008 R2 – see http://www.microsoft.com	Enterprise Edition (Restrictions– maximum number of processors and memory capacity, su
	Developer Edition (Restrictions– maximum number of processors and memory capacity, su
	Standard Edition (Restrictions - 4 supported processors; maximum memory capacity, suppo
	Express Edition (Restrictions- 1 supported processor, maximum database size -10 Gb)
	Web Edition (Restrictions - 4 supported processors; maximum memory capacity, supported
	Workgroup Edition (Restrictions - 2 supported processors; maximum memory capacity, sup
MS SQL Server 2012 - see http://www.microsoft.com	All
MS SQL Server 2014 - see http://www.microsoft.com	All
MS SQL Server 2016 - see http://www.microsoft.com	All
MS SQL Server 2017 - see http://www.microsoft.com	All
MS SQL Server 2019 - see http://www.microsoft.com	All

Note.

Free of charge version MS SQL Server 2014 Express (SP3) is installed with Intellect software on default.To get information about technical features and limitations of free version see https://www.microsoft.com.

Note.

If an error occurs while installing Microsoft SQL Server 2008 R2 Express, try to download the corresponding installation kit from https://www.microsoft.com and install manually.

Attention!

While exceeding maximum database memory capacity (when MS SQL Server edition with memory capacity is used) there is no guarantee of stable operation for INTELLECT™.

Information about the objects, settings of the digital video surveillance and audio monitoring system and event logs can be automatically replicated from the video Server database to the databases of all other video Servers of the system. Communication between full featured program kernels of INTELLECT system is supported by the TCP/IP environment (if the system configuration defines certain program kernels, between which communication is to be provided).

Information about system objects and their settings is initially stored to the database of the video Server where the objects belong to. Replication is initiated automatically whenever data is changed, the kernel is launched or communication is restored.

Replication is used to create a common event environment within the distributed digital video surveillance system. Replication is a hidden process for the user.

16.2.4 Communication environment

The communication facilities of INTELLECT™ software allows deployment of distributed digital video surveillance systems, which control lengthy and versatile objects. Remote system components interact automatically with each other forming a common security system.

Data exchange and communication between distributed digital video surveillance and the audio monitoring system is supported by the local access networks (LAN), Internet (WAN), telephone lines (Dial-Up) and leased communication channels, when TCP/IP telecommunications transportation protocol is used.

16.3 Intellect software package restrictions

The following restrictions are imposed in the *Intellect* software package when building video surveillance and audio control systems:

1. Maximum ptz devices (analog) which are in use on one computer is 64. For IP-devices, this number is limited by the Server hardware resources.
2. Maximum **Screen** objects assigned for one computer is 500.
3. Maximum number of video input channels for videosignal processing in the live video and/or multiplexing modes is limited by the Server hardware resources – processor power, RAM memory space, etc.
4. Maximum number of simultaneous output analog videosignals is limited by the number of video capture cards (with analog video outputs) in use on the Server.
5. Maximum number of remote workstations connected to the Server to receive videos is limited by the number and parameters of transmitted videosignals, video surveillance system architecture and network bandwidth.
6. Maximum number of Servers, videosignals from which are transmitted simultaneously to a remote workstation, is limited by the number and parameters of transmitted videosignals, video surveillance system architecture and network bandwidth.
7. Maximum number of simultaneous video images displayed on the screen of a remote work station is limited by video image parameters and network bandwidth.
8. Maximum video stream rate transmitted via a videogate is limited by the videogate hardware parameters and network bandwidth.
9. Maximum number of audio output channels (to the loudspeakers, earphones, etc.) depends on the audio card used for playback.

10. Enable 64-bit modules if more than 25 **Tracker** objects are to be used on one Server with video resolution higher than 800x600.
11. Digitization bandwidth depends on the audio card parameters and software limitation from 0 to 48 000 Hz.
12. Do not set the bitrate value 8 or 12 kb/s when sampling frequency is 8 kHz for correct sound registration from Axis IP-cameras using the AAC codec; it is recommended to use the bitrate value equals to 16, 24, 32, 48 or 64 kb/s.
13. Use the G.711 audio codec instead of G.726 codec for correct sound registration from Sony IP cameras.
14. Different Servers are not allowed to be connected to one database. Use of remote database by Server is allowed but it can cause increased requirements to the network and others resources and may cause delays when sending events and states between cores that can affect the system.
15. *Intellect* software package of one version is to be installed on all components of distributed system.
16. It is recommended to leave **Decompressor** field empty on the settings panel of the **Camera** object or use the Motion Wavelet decompressor when using WS7 and WS17 video capture cards. Correct operation of *Intellect* software is not guaranteed if other decompressors are selected.
17. Partial decompression is possible when using MPEG4, MJPEG, MXPEG, Motion Wavelet and H264svc codecs. Partial decompression for H263, H264avc and Mpeg2 codecs is not supported. Fps decreasing only is supported by H264svc-t codec.
18. If the MPEG4 format of recording to archive is selected, the loss of video record part is possible (about 0.5 seconds from the video recording beginning).
19. If the **Recording frame rate** parameter (**Camera** object, **Basic settings** tab) is set to non-zero, regardless of its value of recording to the archive is performed only by anchor frames if H.264 codec is in use. If the **Hot record rate** parameter for H.264 codec is also in use, then the recording to the archive will be performed by anchor frames too. If the **Recording frame rate** parameter is set to 0 or not set, all frames are recorded to the archive.
20. If 64-bits modules are in use the following items are not supported:
    a. The **Scene** object (see Configuring object's panoramic view by means of the Scene object).
    b. Some detection tools from *Detector Pack* (at the moment of writing the documentation - the barcode detection tool only).
    c. *Arena* module and *Auto-Uragan* license plate recognition as a part of *Auto Intellect*.
    d. *ACFA Intellect* modules.
21. Grooming on Videogate can be performed using MJPEG, Motion Wavelet, MPEG, H.264 and MxPeg codecs. If the grooming rate is 25 fps, then the first minute of video will be displayed at lower speed (~12 fps). For MXPeg codec the maximum allowed grooming rate is 12 fps.
22. Web server displays video only in MJPEG format. When transferring video to the Web server video stream is recompressed to MJPEG format.
23. It is required to add Web server address to the Java exceptions in order to Web server work with JRE 7u51 or later versions.
24. Video stream transferred via RTSP Server is to be compressed using H.264, H.265, MPEG4 or MJPEG codecs. Video with width and/or height more than 2048 pixels is not supported when MJPEG codec is in use.
25. Use of more than 100 scripts/programs on one computer may cause system instability.
26. Only files of .wav format can be in use as the **Play audio file** action parameter of the **Audio player** object. Otherwise, the **Play audio file** action is not performed.
27. The **External window** object is specialized on working with onebox applications. If the application contains several boxes, then all of them will be opened simultaneously when application is started.
28. PureVideo/CUDA technology in the *Intellect* software is applied only for video signals decompression in H.264 codec. PureVideo/CUDA technology is not used for video signal compression if resolution more than 1920x1088 is set in the camera.
29. Recording to the archive is performed only in the color mode if SC590N4 video capture card with h.264 format of video signal compression is in use. The black-and-white mode is not supported.
30. Video displaying on Server using SC3B0N16 (WS216) and SC390N16 (WS16) cards is performed only with 352x288(PAL)/ 352x240(NTSC) resolution.
31. Only key frames are played back when the archive is played back fast in H264 and MPEG4 formats.
32. Video signals are not transferred to *Intellect*-based vertical modules using the Videogate module. These modules always receive video signal directly like other modules.
33. There is no sound transmission to the RMW via the Videogate if different subnets are in use.
34. When working with *Intellect*, do not use power-saving modes, such as sleep mode or a “Power saver” power plan, so that the CPU clockspeed does not get lower that the base speed.

35. *Intellect* supports NVIDIA® Mosaic™ multi-display technology when NVIDIA Quadro Sync is used additionally with it (see the related NVIDIA documentation). Without NVIDIA Quadro Sync there can be ~10-200 ms discrepancies in video playback time between monitors.

16.4 Hashing procedure

The following hashing procedures are used in the *Intellect* software package:

1. The MD5 procedure is used for passwords hashing (hash length is 16 bits).
2. For digital signing of archive the following are used:
    a. RSA-256 encryption (key is 256 bits).
    b. SHA1 hashing (hash size is 20 bytes).

16.5 Traffic encryption in the Intellect software

A security and video surveillance system based on Intellect software should be built on a separate network that connects all the major components of the system without any connection to the main network. This significantly reduces the risk of being hacked and losing important data. If for some reason it is not possible to isolate the security system on a separate network, it is recommended that you secure access to it from external networks by using a VPN with dedicated ports and password protection.

Users can connect and work with Intellect software from their mobile devices or from a browser. In addition, the video signal can be transmitted over the secure HTTPS protocol.

In addition to encryption software, Intellect software supports hardware encryption of the channels between routers and all network nodes.

17 Requirements for the software and hardware platform

17.1 Requirements for base PCs

INTELLECT™ software is designed for use with IBM compatible PCs. Efficiency and performance of the Intellect system depends, in particular, on the technical parameters and performance of the PCs. Before you start system design, you should carefully study the requirements for the hardware components and check if they are able to support the target performance of the system.

17.1.1 General requirements for PCs

Requirements for PCs depend on *Intellect* software installation type. The following installation types are available:

1. **Servers** are designed for digitization, processing, recording, transmission and displaying the incoming video signals from the cameras of the video surveillance system.
2. **Remote Administrator Workstations** are designed for remote monitoring of video signals, for creating gateways and archives of video sequences, for logging the events registered by *Intellect* software and use as a web server for the transmission of video signals over HTTP (this protocol is used to transmit signals over the Internet and display them with standard Web-browsers). Configuration requirements for the Remote Administrator Workstation depend on the functions it is designed to perform.
3. **Remote Clients** are designed to playback incoming video and audio signals from video surveillance system servers and to control cameras, microphones, PTZ units, etc.

Minimum requirements for computer configuration are specified in the table.

Component	Server and RAW	Client	QTY per computer	Additional information
Tower	Any		1	—
Motherboard	Any type that supports required processor and has the necessary set of pins and slots		1	Pay attention to the number of free PCI (-e) slots and socket type of the processor
Processor	Select the processor in accordance with the computer configuration using the on-line calculator: https://sale.axxonsoft.com/calc/calculator.jsf. Documentation on the calculator is available here: Documentation		1	If the total number of processor cores is more than 8, it is recommended to use only 64-bit operating systems: Windows 7 x64 Ultimate, Windows 7 x64 Professional, Windows Server 2008 R2 x64 or higher. Processor supporting AVX instructions is required for the VA capture and recognition (the most recent *Face-Intellect* documentation is available in AxxonSoft documentation repository)
Memory	At least 2 GB		—	Memory operating speed increase by using memory with greater frequency or using memory in the dual stream (or more) mode results in less CPU load and, consequently, greater *Intellect* performance
Hard drive 1	Space required for installation of the OS + 10 GB for installation of Intellect software + 20 GB for installation of MS SQL Server	Space required for installation of the OS + 10 GB for installation of Intellect software	1 (+1)	Mirroring can be used to improve the fault-tolerance

Hard drive 2	To maintain video/audio archive compatible with the requirements for the archive depth	—	—	External disk systems can be connected via SAS, SCSI, Fiber Channel interfaces Will be installed in cases where video/audio archives are required
DVD-RW	Any type of DVD-RW		1	To write the archive to an external carrier, for fallback recovery (optional)
Video card	Discrete: NVIDIA GeForce GT520 1 GB RAM or more productive. On-board: Intel HD Graphics 530 or more productive		1	Optional if it is not required to display video on the monitor. *Intellect* can operate without a video card if the processor has a built-in video core
Audio card	Standard audio cards, MidiMan Delta, Comart Hera and Olkha 9P		1	Optional if audio surveillance is not required
Power supply unit	Any matching the PC tower. Capacity depends on the hardware configuration		1	Two fans are recommended: a suction fan and an induced draft fan. A redundant fan can also be installed
FAN & Temp Control	Any temperature control module		1	Optional
OS	OS Windows supported versions (see Operating system requirements)		1	Internet access is recommended to be switched off
Architecture	x86, x64		—	—

Attention!

If *Intellect* is installed on a computer with two processors, it is recommended to disable the Hyper-threading. If it is enabled, the operating system does not allow *Intellect* to run on two processors simultaneously.

Note.

The system clock on the server must be synchronized with the client's system clock, or run a couple of seconds ahead. Otherwise, problems during re-connecting (for example, on connection loss) may occur.

17.1.2 Operating system requirements

Intellect is compatible both with 32 (x86) and 64 bit licensed versions of Microsoft Windows operating system (OS). File system — NTFS.

Note

To ensure the correct *Intellect* operation, it is necessary that the OS is updated to the latest version.

Attention!

For stable and correct *Intellect* operation, the swap file (the size is selected according to system requirements) should NOT be enabled in OS.

Windows version	Supported architecture	Supported release	Restrictions	Installation types
Windows				
Windows 11	x64	All editions	No restrictions	Any type
Windows 10 IoT[2]	x86, x64	Enterprise ***Attention! Core edition is not supported***	No restrictions	Any type
Windows 10[2]	x86, x64	Home	No restrictions	Any type
		Pro		
		Enterprise		
Windows 8.1[2]	x86, x64	Core	No restrictions	Any type
		Pro		
		Enterprise		
Windows 8[2]	x86, x64	Windows 8 (Windows 8 Core)	No restrictions	Any type
		Windows 8 Pro		
		Windows 8 Enterprise		
Windows 7 SP1[2]	x86, x64	Starter (x64 edition does not exist)	Restrictions, imposed by the OS edition (2GB RAM, 1 physical processor, 1 monitor). See http://www.microsoft.com	Any type
		Home Basic	Restrictions, imposed by the OS edition (1 physical processor). See http://www.microsoft.com	
		Home Premium	Restrictions, imposed by the OS edition (1 physical processor). See http://www.microsoft.com	
		Professional	No restrictions	
		Enterprise		
		Ultimate		
Windows Server				

Windows version	Supported architecture	Supported release	Restrictions	Installation types
Windows Server 2022[1,3]	x64	Standard	No restrictions	Any type
Windows Server 2019[1,3]	x64	Standard	No restrictions	Any type. If you plan to use video capture cards for analog cameras, make sure to install all official Windows Server 2019 updates (see http://www.microsoft.com)
		Datacenter		
Windows Server 2016[1,3]	x64	Essentials	No restrictions	Any type
		Standard	No restrictions	Full Installation type is supported. Server Core and Nano Core Installation types are not supported
		Datacenter		
Windows Server 2012 R2[1,3]	x64	Foundation	Restrictions, imposed by the OS edition (1 physical processor). See http://www.microsoft.com	Full Installation type is supported. Server Core Installation type is not supported
		Essentials	Restrictions, imposed by the OS edition (2 physical processors). See http://www.microsoft.com	
		Standard	No restrictions	
		Datacenter		
Windows Storage Server 2012 R2[1,3]	x64	Standard	No restrictions	Any type
Windows Server 2012[1,3]	x64	Foundation	Restrictions, imposed by the OS edition (1 physical processor). See http://www.microsoft.com	Full Installation type is supported. Server Core Installation type is not supported
		Essentials	Restrictions, imposed by the OS edition (2 physical processors). See http://www.microsoft.com	
		Standard	No restrictions	
		Datacenter		
Windows Home Server 2011 SP1[3]	x64	-	No restrictions	Full Installation type is supported. Server Core Installation type is not supported
Windows Small Business Server 2011 SP1[3]	x64	Standard	No restrictions	Full Installation type is supported. Server Core Installation type is not supported
		Essentials		

Windows version	Supported architecture	Supported release	Restrictions	Installation types
		Premium Add-on		
Windows Storage Server 2008 R2 SP1[3]	x64	Essentials	Restrictions, imposed by the OS edition (1 physical processor). See http://www.microsoft.com	Full Installation type is supported. Server Core Installation type is not supported
		Workgroup	No restrictions	
		Standard		
		Enterprise		
Windows Server 2008 R2 SP1[2,3]	x64	Enterprise	No restrictions	Full Installation type is supported. Server Core Installation type is not supported
		Datacenter		
		Standard		
		Web		
		HPC		
		Foundation		

[1] The latest drivers should be installed on video adapter from the video adapter manufacturer for the correct operation of *Intellect* interface objects and vertical solutions in server OS.

[2] Face capture and recognition using the VA and VisionLabs modules is not supported in 32-bit operating systems.

[3] In order to use SC590N4, SC3B0N16, SC390N16, SC300Q16 (FX-4), SC300D16 (FX-8), SC310N16 (FX-16), SC200Q4 Low profile (FS-115), SC510N4 (FX HD4) video capture cards in Windows Server operating systems, enable the *Desktop Experience*. Find information on how to work with this component at https://technet.microsoft.com/en-us/library/cc754314(v=ws.11).aspx
In addition, to use SC300Q16 (FX-4), SC300D16 (FX-8), SC310N16 (FX-16) video capture cards in Windows Server operating systems, enable access to camera on the Server: type **Camera privacy settings** in the search field or go to the **Start** → **Settings** → **Privacy** → **Camera** menu, then allow access to the camera on this device in the window that opens.

17.1.2.1 Specific requirements for working with Intellect

Before installing *Intellect* on Windows 7, Windows 8, Windows Server 2008 R2 and Windows Server 2012 OS, it is necessary to pre-install .Net 4.0 or later. When the installation begins on these OS, the corresponding message will be displayed.

For the correct operation of FX-4 and FX-8 cards in *Intellect*, the KB3033929 update should be installed. Download this update at https://technet.microsoft.com/en-us/library/security/3033929.

For the correct start of the Elasticsearch service on 32-bit systems, you should limit the RAM allocated to this service (see Limiting RAM for Elasticsearch service).

17.1.3 Free disk space (video archive size) required

Intellect™ system allows saving the video recordings to the hard drives (maintain video recordings archive). Archived information can be saved to the hard drives of such types as SCSI, IDE, SATA, USB and also RAID arrays. SCSI disks and RAID arrays (in particular RAID-5) allow accelerating data search and recording.

The size of the redundant array defines the length (time based length) of the saved and archived video recording. The size of the redundant array is selected based on the required parameters of the video recording.

> **Attention!**
>
> For proper operation of video archive recording the disk space size must exceed «Ring» parameter, that has been stated in **Video Subsystem** section of advanced system settings utility (see The settings panel for the Video subsystem section).

To determine disk space required for storing archive from IP-cameras, please use the on-line calculator. Documentation on the calculator is available here.

Table below shows the average frame size of a PAL video signal depending on frame resolution, video signal compression, color grade of the image and frame resolution, frame chromaticity and motion level in the frame.

Video card type	Resolution	Colour	Frame size (Kb) with 50% of motion in the frame	Frame size (Kb) with 75% of motion in the frame	Frame size (Kb) with 100% of motion in the frame
SC390N16 (WS16)	704x576	colour	15	30	61
		black-and-white	10	22	42
	704x288	colour	6	10	30
		black-and-white	4	9	18
	352x288	colour	4	6	17
		black-and-white	2	5	10
SC3B0N16 (WS216)	704x576	colour	19	35	101
		black-and-white	11	33	65
	704x288	colour	8	12	49
		black-and-white	6	11	29
	352x288	colour	4	7	25
		black-and-white	3	6	15
FX416\MS416	To calculate required disk space for these cards, please use the on-line calculator.				
SL16-200 (FX116)					
SC310N16 (FX16)					
SC200Q4 (FS15)					

Video card type	Resolution	Colour	Frame size (Kb) with 50% of motion in the frame	Frame size (Kb) with 75% of motion in the frame	Frame size (Kb) with 100% of motion in the frame
SC200Q4 LOW PROFILE (FS115) **SC300Q16 (FX4)** **SC300D16 (FX8)** **SC230N4** **SC330Q16 (analogue of SC300Q16)** **SC330D16 (analogue of SC300D16)**					
FS5\FS6\FS8\FS16	704x576	colour	26	59	103
		black-and-white	24	42	91
	704x288	colour	17	26	52
		black-and-white	16	24	47
	352x288	colour	11	15	39
		black-and-white	10	14	37

Note.

Table shows the examples of frames for video cameras with set frame frequency – 25 f\s.

Archive size will be calculated on the basis of frame resolution and compression, image color grade, rate of video signal frames per second, number of cameras, recording events continuously to the hard drives.

Archive size can be calculated from formula no. 1:

Archive size (days) = (1024 (Mb/Gb) * 1024 (Kb/Mb) * Hard drive size (Gb)) / (60 (sec/min) * 60 (min/hr) * 24 (hr/day) * Frame size (Kb) * Frame rate (frames/sec) * Number of cameras)

Comments relating to Formula no. 1. To estimate the archive size, the following should be performed: the size of hard drive in Kb (the rates for converting Gb into Kb are included into the numerator of Formula no. 1) divide by the frame size, defined in Table A as a function of video signal parameters, and by the frame rate per camera and the number of cameras, connected to the video server. Archive size in this case will be measured in seconds. Now, the archive size expressed in seconds should be converted to the number of days (the rates to convert seconds to days are given in the denominator of Formula no. 1).

Note.

Archive size can also be calculated from a simplified formula, where numerical conversion factors are reduced to a numerical value (Formula no 2).
Archive size (days) = 12 (Kb/Gb * day/sec) * Hard drive size (Gb) / (Frame size (Kb) * Frame rate (frames/sec) * Number of cameras)

Example. If the size of a hard drive, for instance, is 40 GB, 4 cameras are continuously recording PAL video signals with 10 frames per second and 150Kb frame size. Based on the formula, you work out:

Archive size (days) = 12 (Kb/Gb * day/sec) * 40 (Gb) / (150 (Kb) * 10 (frames/sec) * 4) = 0.08 (days)

The arithmetic calculation shows, that the video archive size in the particular case will be 0.08 days (about 1 hour 55 minutes).

For the purpose of calculations, frame size can be defined in the table above.

Note.

To calculate the size of a hard drive, the following specific features should be accounted for: 1) About 5-10% of the hard drive size is taken up by the filing subsystem data. To ensure that Windows OS is operating properly, at least 20% of free disk space is required. By default, Windows OS auxiliary files are assigned 1000Mb. To modify the above value, Windows OS catalogue should be updated, using Tweaki.exe utility, supplied together with the INTELLECT distribution software package.

Table below shows archive sizes calculated for hard drives of various sizes, based on a continuous incoming PAL video signal recording, from 1 camera with a frame rate of 25 f/sec.

Resolution	**Hard drive size**			
	80 GB	160 GB	400 GB	750 GB
352x288 b/w	2,1	4,3	10,7	20,0
352 x 288 color	1,9	3,8	9,6	18,0
704x288 b/w	1,6	3,2	8,0	15,0
704 x 288 color	1,5	3,1	7,7	14,4
704x576 b/w	1,2	2,3	5,8	10,9
704 x 576 color	1,1	2,3	5,6	10,6

17.1.4 Defining disk space (audio archive size)

Intellect software package allows storing audio archive (recorded with the video archive) on hard disks (see Setting up the audio and video synchro recording). So, it is necessary to provide space for storing not only video recordings, but also audio recordings recorded synchronously, on the hard disk. Information on how to calculate the required disk space for storing the video archive is given in Free disk space (video archive size) required section.

Below one can find information about required disk space for storing audio recordings from 1 audio channel (microphone) depending on the audio digitization rate.

Important!

Regardless of the codec, the audio archive is recorded in PCM format.

Digitization rate	**Audio recordings for 24 hours, GB**	**Audio recordings for 30 days, GB**
8000	0.39	11

11025	0.49	15
22050	1	30
44100	1.8	54
48000	2	60
96000	4	120

The formula for calculating the depth of the video archive recorded synchronously with the audio archive is given below (to find info about frame size see Free disk space (video archive size) required):

Depth of video and audio archive (day) = Hard disk space (GB) / ((k (s/day* GB/Kb) * Frame size(Kb) * Frame rate (fps) * Number of cameras) + Volume of audio recording per day (GB/day) * Number of audio channels)

Here k is the unit conversion factor for the depth of the video archive, calculated like this:

*k = (60(s/min)*60 (min/h)*24(h/d))/(1024(Mb/GB)*1024(Kb/MB))~0.08*

17.1.5 Define required disk space (size of event log database)

The event log database can be stored with the Intellect configuration database or without it.

Disk space required for event log database storing is counted by formula:

Required disk space, Gb = N (pcs) * K (events/hour) * T (days) * 24 (h/day) * 1.2 (Kb) / 1024^2 (Kb/Gb)

where N – number of objects generated events.

K – average number of events per hour from one object. It is defined experimentally from real conditions. For example, to define the average number of events per hour for camera it is required to know how many times per hour motion appears in the camera field of view. Estimation from above: one event once per five seconds, on more frequently triggering detection haven't got enough time to disarm and events won't be record to the database.

T – the depth of events archive in days, specified at the system configuration.

1.2 – space required for storing one event in kilobytes.

Example. There are 250 objects, each of them generates one event per 5 seconds (i.e. 720 events per hour) with the archive depth of 20 days.

Required disk space, Gb = 250 (pcs) * 720 (events/hour) * 20 (days) * 24 (h/day) * 1.2 (Kb) / 1024^2 (Kb/Gb) = 98.9 Gb ~ 100Gb

17.1.6 Define required disk space (VMDA metadata storage)

When using the smart search in the archive, the VMDA metadata storage is created and configured (see Creating and configuring VMDA metadata storage).

The size of the VMDA metadata storage depends on the frame rate, minimum and maximum object size, tracker sensitivity: the higher the frame rate and larger the object size, the more disk space is required for storage.

If the video is recorded 24 hours a day, you can use the following formula to estimate the disk space required to store the object tracks database:

VMDA (GB) = 0,5 GB * (Number of cameras) * (Number of days)

17.1.7 Intellect software working in virtual machines

Intellect software package supports working in the following virtual machines:

Virtual machine	Client OS	Additional information
VMware Workstation Pro 15.5.1	see Operating system requirements	Neuroanalytics can be in use (including neural filter, neurotracker, as well as fire and smoke detection tools – see the Detector Pack subsystem documentation in the AxxonSoft documentation repository). USB-devices forwarding to virtual machine via the virtual machines means is available. Working for Carmen-freeFlow, Carmen-parking, VIT, Auto-Uragan LPR modules' hardware keys, as well as Guardant is checked.
VMWare Workstation version 15.0.0	see Operating system requirements	USB-devices forwarding to virtual machine via the virtual machines means is available. Working for Carmen-freeFlow, Carmen-parking, VIT, Auto-Uragan LPR modules' hardware keys, as well as Guardant is checked.
VMWare ESXI version 6.5.0	see Operating system requirements	USB-devices forwarding to virtual machine via the virtual machines means is available. Working for Carmen-freeFlow, Carmen-parking, VIT, Auto-Uragan LPR modules' hardware keys, as well as Guardant is checked.
Hyper-v 10.0.17134.1	see Operating system requirements	It is possible to use external program, for example USBoverLAN to forward USB-devices in this virtual machine.

Note

Officially Carmen software module does not support virtual machines, although Carmen software module operates on VMware and VirtualBox as they can handle the USB properly.

Use general requirements for PCs in order to define the requirements for RAM, processor, etc. It should be taken into account that the performance of virtual systems is less than one of real systems, so the estimated number of cameras should be reduced accordingly. Get more details from the sales department in your AxxonSoft branch.

Note

To implement other devices to the virtual machine see documentation of the corresponding virtual machine.

Attention!

The following restrictions are imposed when *Intellect* software is working in virtual machines:

1. Using of video capture devices is not supported.
2. Working of *Intellect* interface objects, Report.exe utility and Converter.exe utility is not guaranteed in virtual machines.
3. Demo mode operation of the VIT module (part of *Auto-Intellect* software) is not allowed.

17.2 Requirements for TCP/IP Network

On the page:

- Requirements for TCP/IP Network bandwidth for video signal transferring
- Requirements for TCP/IP network bandwidth for database synchronization functionality
- Requirements to the TCP/IP network quality

17.2.1 Requirements for TCP/IP Network bandwidth for video signal transferring

Throughput capacity of the network refers to the factors restricting performance of the distributed network. Data exchange flow is primarily made up of image data. For instance, where surveillance cameras are used to monitor remote objects, likes ATMs, the data flow (image flow) is transmitted over communication links.

In order to calculate the required bandwidth of TCP/IP network for video transmission from IP devices and some video capture cards, it is recommended to use the Axxon platform calculator, available here (the **Summary stream from ip devices (Mbit/s)** parameter). For video capture cards that are not supported by the platform calculator, use the calculation data below.

Table below shows the maximum number of remote surveillance cameras as a function of the throughput capacity of various communication links. The frame rate of the image flow (reference format is PAL) for calculation purposes was accepted as equal to 1 frame per second.

Note

In real conditions, the fluctuations of camera streams can be quite significant, depending on the scene illumination, the use of day/night mode, how much motion there is in the frame. To accurately calculate the required network bandwidth, it is necessary to measure the stream from cameras that are already installed on the protected facility.

Communication mode	**Link capacity**	**Black and white image**			**Color image**		
		standard	high	full	standard	high	full
Dial-Up	56 Kb/sec	<1*	<1*	<1*	<1*	<1*	<1*
ADSL, Ethernet	128 Kb/sec	1	<1*	<1*	<1*	<1*	<1*
ADSL, Ethernet	256 Kb/sec	2	1	1	1	1	<1*
ADSL, Ethernet	512 Kb/sec	4	3	2	3	3	2
ADSL, Ethernet	1 Mb/sec	7	5	4	6	5	4
ADSL, Ethernet	1.5 Mb/sec	11	8	6	10	8	6
Ethernet	2 Mb/sec	14	11	8	13	10	8
Ethernet	10 Mb/sec	71	53	39	64	51	38
Ethernet	100 Mb/sec	711	533	388	640	512	376

Communication mode	Link capacity	Black and white image			Color image		
		standard	high	full	standard	high	full
Ethernet	1 Gb/sec	7282	5461	3972	6554	5243	3855

*max. one surveillance camera, provided that maximum compression and/or additional grooming is applied.

To calculate the maximum number of remote cameras transmitting image flow to the network with a rate over 1 f/sec, the corresponding value shown in the table should be divided by the number of frames.

Example: To transmit live video, a 100 Mb/sec network should be used (25 frame/sec – PAL), video image – color; frame resolution – standard. As the table shows, the Mb/sec link can transmit the image flow at a rate of 1f/sec, specified color grade and resolution from max. 640 surveillance cameras. Consequently, if the image flow rate is 25 frames per second, the maximum number of cameras will decrease by 25 times and will be equal to: 640/25=25 cameras.

Note

More often than not, video signal processing, transfer and recording requirements take up only a small proportion of the digital video surveillance system resources. While calculating performance of the video surveillance system, the proportion of resources, consumed by audio monitoring, may be neglected.

17.2.2 Requirements for TCP/IP network bandwidth for database synchronization functionality

If the Intellect software operates in the distributed environment where several Servers and/or Remote Admin Workstations are combined the Configuration databases synchronization is performing (see Database synchronization setup).

The fulfilling of following minimal requirements for network is needed for correct synchronization of Configuration databases:

1. Minimal speed of data transferring by link channel (capacity) is 64 kbit/sec.
2. Maximal delay while packet transferring is 500 milliseconds.

With more badly parameters value the correct operation of databases synchronization functionality is not guaranteed.

17.2.3 Requirements to the TCP/IP network quality

The following connection quality requirements are imposed for the *Intellect* software video subsystem to work correctly when connecting IP devices via WAN:

1. Latency:
   - for live video no more than 10 seconds. If this value is exceeded, the connection to the IP device will be terminated.
   - for face recognition no more than 1500 milliseconds, if this value is exceeded, many faces will be missed due to the skipping of a large number of frames.
   - for service and smart detection tools no more than 400 milliseconds, if this value is exceeded, the quality of object detection will decrease, smart detection tools may incorrectly generate alarms.

2. Packet loss
   - for live video no more than 40%. If this value is exceeded, the connection to the camera will be terminated. With a packet loss of 10% to 40%, frame drops will be observed (the more losses, the more drops).
   - for face recognition, service and smart detection tools no more than 25%. If this value is exceeded, skipping of faces will be missed, and the tracks of smart detection tools will not correspond to objects.

17.3 Requirements for PTZ and control panels

INTELLECT™ software is compatible with PTZ units, control panels and tilt IP-cameras from such manufacturers as Panasonic, Samsung, Videotec, Sanyo, etc. You can find an updated list of PTZ units and control panels that are compatible with INTELLECT™ software on the sithe of AxxonSoft in the Integration section at: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php

17.4 Requirements for audio input units

Intellect software can use the following audio inputs:

1. FS/WS/FX/VRC video capture cards. These cards support simultaneous digitization of 1-16 audio signals, depending on the type of the card used. The list of video capture cards compatible with *Intellect* software and their features are given in the Installing and configuring security system components guide.
2. Standard sound cards, including cards, integrated with the motherboard. Standard sound cards, as a rule, support simultaneous digitization of up to 2 audio signals.
3. Multi-channel sound cards and converters for digitization of outgoing audio signals from microphones and telephone lines, software and hardware complex for the digital audio registration, etc. You can find an updated list of multi-channel audio inputs that are compatible with *Intellect* software on the AxxonSoft site in the Integration section at: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.
4. IP-units. You can find an updated list of IP-units for audio input that are compatible with *Intellect* software, as well as specific application features thereof on the AxxonSoft site in the Integration section at: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.
   The IP device shall transfer audio data encoded in any of the following formats:
   - G.711
   - G.726
   - AAC
   - PCM
   - MPEG2 LAYER2 (MP2L2)
   - IMA ADPCM

17.5 Requirements for IP devices

Intellect is compatible with IP devices of the following vendors: Axis, Panasonic, Sony, Arecont Vision and others.

> **Note**
>
> The current list of the IP devices compatible with *Intellect* and the range of IP device functionalities supported by *Intellect* are at the company's site in the **Integration** section: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.

Number of IP devices connected to one Server depends on TCP/IP network bandwidth (see Requirements for TCP/IP Network) and functions performed on the basis of these devices. For instance, virtual memory consumption (for video.run process) increases when VMDA detection tools are used (see Configuring smart video detection tools). One camera with a configured VMDA detection tool can use 30-40 MB (depending on camera resolution) of virtual memory. By default, not more than 2 GB of virtual memory is allocated for the video.run process, if you need to connect to one Server more than 25 IP cameras with the configured VMDA detection tools with video resolution higher than 800x600, use 64-bit modules (see the Configuring of using 64-bits modules).

In some cases, it is necessary to enable the synchronization of the Server and IP device time (if the device supports this setting):

1. In some cases (for example, if there is no video from the device), when connecting the camera via the ONVIF protocol, it may be necessary to synchronize the time and the time zone between the Server and the device.
2. For *Intellect* operation with the embedded IP device storage, it is necessary to synchronize the time between the Server and the device.
3. If there is no time synchronization for some IP devices, events of the onboard analytics may work incorrectly in *Intellect*.

Specific application features of certain IP devices:

1. To ensure correct sound recording from Axis IP cameras when AAC audio codec is used, avoid setting the audio stream bitrate at 8 or 12 Kb/s, if the digitizing rate is 8 kHz: the bitrate should be 16, 24, 32, 48 or 64 Kb/s.
2. To ensure correct sound recording from Sony IP cameras, avoid using G.726 audio codec: use G.711 codec instead.

Attention!

It is possible to install the up-to-date drivers and codecs, taking into account the changed distributive structure, irrespective of the general *Intellect* version update.

Hardware integrated into Intellect

17.6 Requirements for GSM Equipment

GSM equipment is used in the *Intellect* software to send SMS, whenever the program registers pre-defined events (detector alarms, Operator commands, etc.). The list of said GSM equipment includes GSM modems, GSM adapters or mobile phones supporting such standards as ETSI GSM 07.07 or ETSI GSM 07.05.

17.7 Requirements for voice modems

Voice modems are used in the *Intellect* software to automatically send out voice messages, whenever the program registers pre-defined events (detector alarms, Operator commands, etc.). *Intellect* software is compatible with the voice modems, which are not designed to code (compress) audio streams, or the voice modems, which support such audio stream coding standards as 4-bit Rockwell ADPCM 7200 Hz, 4-bit IMA ADPCM 4800 Hz, 4-bit IMA ADPCM 7200 Hz, 4-bit IMA ADPCM 8000 Hz, 8-bit unsigned linear PCM at 7200 Hz, 8-bit unsigned linear PCM at 8000 Hz, 4-bit Rockwell ADPCM 7200 Hz, 8 bit u-law (G.711) at 8000 Hz, 8 bit A-law (G.711) at 8000 Hz.

17.8 Requirements for software which is used while integrating

The *Intellect* software allows integrating with contiguous information systems, additional software or functional expansion modules.

Use InternetExplorer browser while working with Intellect software from browser through the CamMonitor Active X-object.

17.9 Requirements for anti-virus software

Correct working of some modules of the *Intellect* software package is not guaranteed if the anti-virus software installed on computer where the *Intellect* software package is installing analyses incoming/outgoing traffic.

17.10 Requirements for BIOS configuration

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

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

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

Attention!

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

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

17.11 Hardware requirements for Intellect and vertical solutions detection tools

Intellect software and vertical solutions include various detection tools, some of which can use video card resources (GPU) for operation.

See also Hardware requirements for the Tracker with neural filter operation. Please refer to the corresponding vertical solution documentation in AxxonSoft documentation repository for more detailed hardware platform requirements applied to the detection tools being part of the vertical solutions.

Detection tool(s)	CPU	GPU	VPU
Intellect base			
VMDA tracker	+	-	-
VMDA tracker with neural filter	+	+	+
Main motion detection tool	+	-	-
Basic detection tools	+	-	-
Face detection	+	-	-
Detector Pack			
Heat map detection	+	-	-
Detection of moving against crowd flow	+	-	-
Queue length detection	+	-	-
Smoke detection	+	+	+

Detection tool(s)	CPU	GPU	VPU
Fire detection	+	+	+
Stopped vehicle detection	+	-	-
People counter detection	+	-	-
Train detection	+	-	-
Detection of light indication control	+	-	-
Sweethearting detection	+	+	+
Barcode detection	+	-	-
Fluid level detection	+	-	-
Neurotracker	+	+	+
Person location tracker	+	+	+
Face-Intellect			
Face detection with any external capture	+	-	-
Auto-Intellect			
Any LPR module	+	-	-

18 Personnel skills requirements

The Administrator of a digital video surveillance system based on *Intellect* software should possess the following qualifications:

1. Windows local network administrator (see Operating system requirements).
2. AxxonSoft product expert. The above qualifications can be obtained through authorized training in AxxonSoft Products in the AxxonSoft Training Centre.

19 Installing and removing INTELLECT™ software

19.1 Installing Intellect

19.1.1 Description of INTELLECT™ software distribution package

INTELLECT™ software is offered as a software installation kit (distribution package) available on the company's official website: https://axxonsoft.com/resources/downloads/intellect.php.

The installation kit contains all software components necessary for the installation of INTELLECT™ software.

The software is made operable with the intellect.sec license key file provided by AxxonSoft manager. The key file defines the configuration of the INTELLECT™ software delivery package.

> **Note.**
>
> If there is no key file INTELLECT™ software will operate in demo mode within two month from the *i*ntellect.exe file creation date, from 8 a.m till 12 midnight.

To install and configure INTELLECT™ software, administrator rights are required.

The description of the main components of the Intellect installation package is given in the table below:

File or folder	Description
Drivers	The folder containing the drivers for the Intellect-integrated video capture cards, sensors/relays, USB WatchDog hardware performance monitoring devices
ipint.driverpack	The folder containing the drivers package installation kits (x32 and x64) for the Intellect-integrated IP devices - *IP Drivers Pack*
Key	The folder containing the license key file. If the installation kit was downloaded from the official AxxonSoft website rather than received on a disk, then this folder is empty.
languages	The folder containing the language packs for installation. By default, it contains only the Setup folder with the English (en) and Russian (ru) language packs in the corresponding folders. If the folder with the language pack is deleted, the correspondong language will not be available for the installer. Other language packs downloaded from the official AxxonSoft website can be added to the languages folder in order to install the Intellect in the required language - for details, see Installation of Intellect as a Server/Remote Administrator's workstation
Redist	The folder containing the installation kits of the prerequisites required for the Intellect operation - for details, see Using the Product.msi and Redist.exe for INTELLECT™ software installation
Product.msi	The installation file for installing the Intellect without additional components (drivers, prerequisites, etc.) - for details, see Using the Product.msi and Redist.exe for INTELLECT™ software installation
Redist.exe	The installation file for installing the additional components required for the Intellect operation (drivers, prerequisites, etc.) - for details, see Using the Product.msi and Redist.exe for INTELLECT™ software installation
setup.exe	The executable file to run the full installation of the Intellect with all the necessary drivers, prerequisites, etc.

19.1.2 Getting ready for Intellect installation

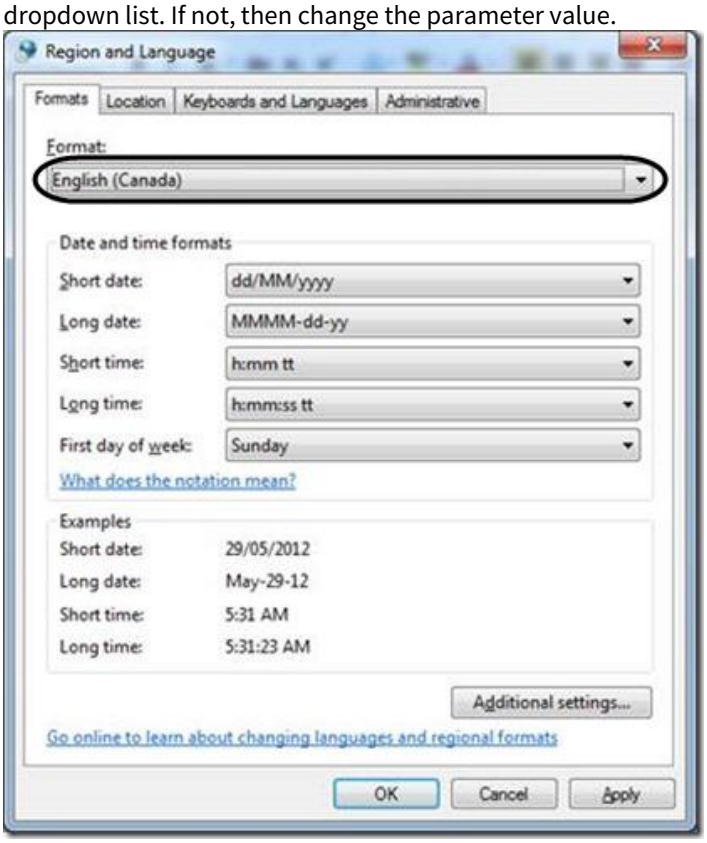
On the page:

- OS language settings
- System settings

19.1.2.1 OS language settings

Before installing Intellect in any language with any configuration (Server, Client or RAW) make sure that appropriate language and regional options are set in the OS. Do the following:

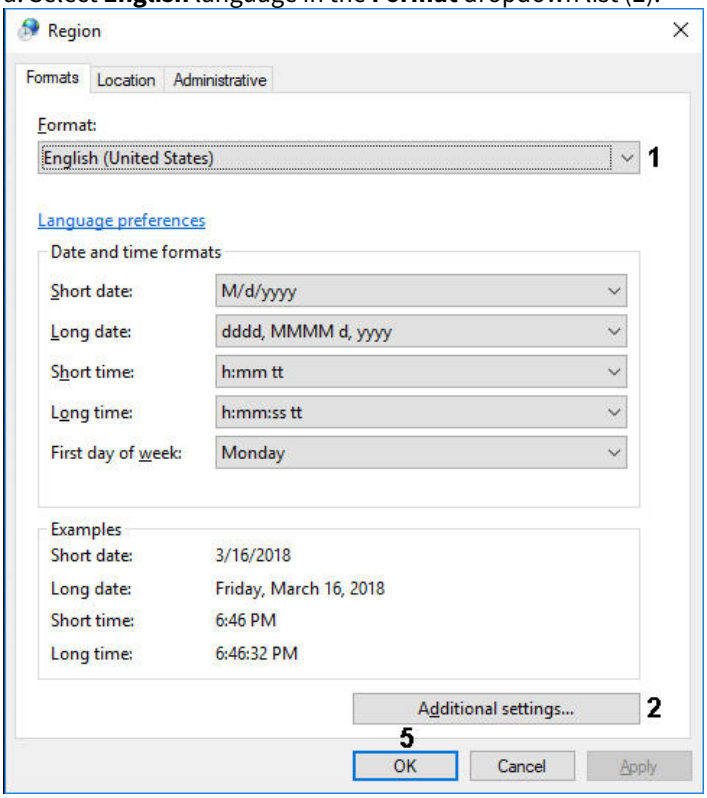
1. Go to the **Start – Control Panel – Regional and Language Options** menu. The **Regional and Language Options** window is displayed.
2. Go to the **Formats** tab. Make sure that the language that is used for Intellect installation is selected in the **Format** dropdown list. If not, then change the parameter value.



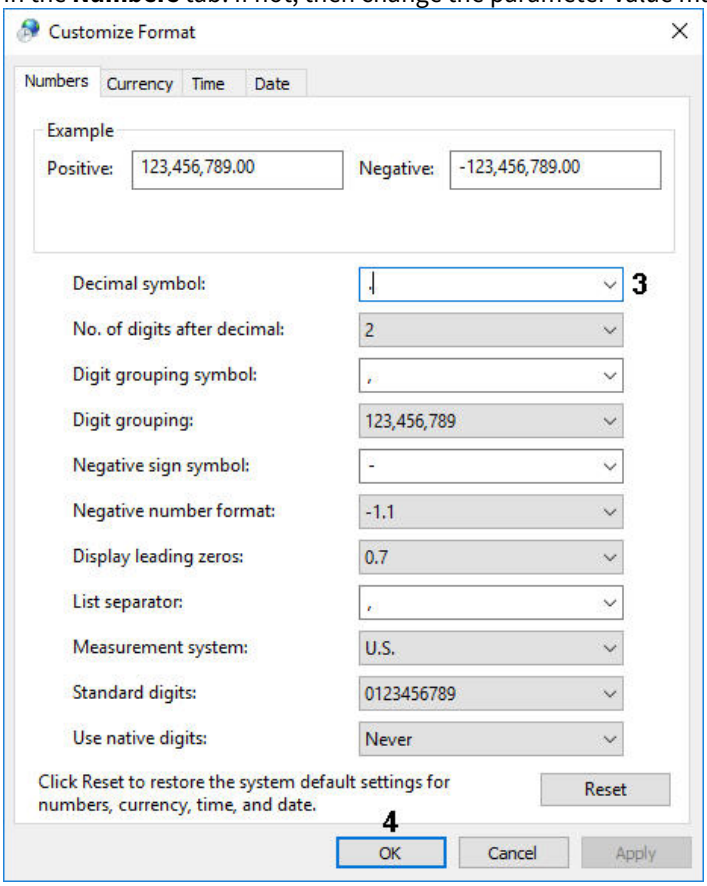
> **Important!**
>
> If **English** is to be in use, then '.' is to be specified as the decimal symbol.

Specify '.' as the decimal symbol as follows:

a. Select **English** language in the **Format** dropdown list (**1**).

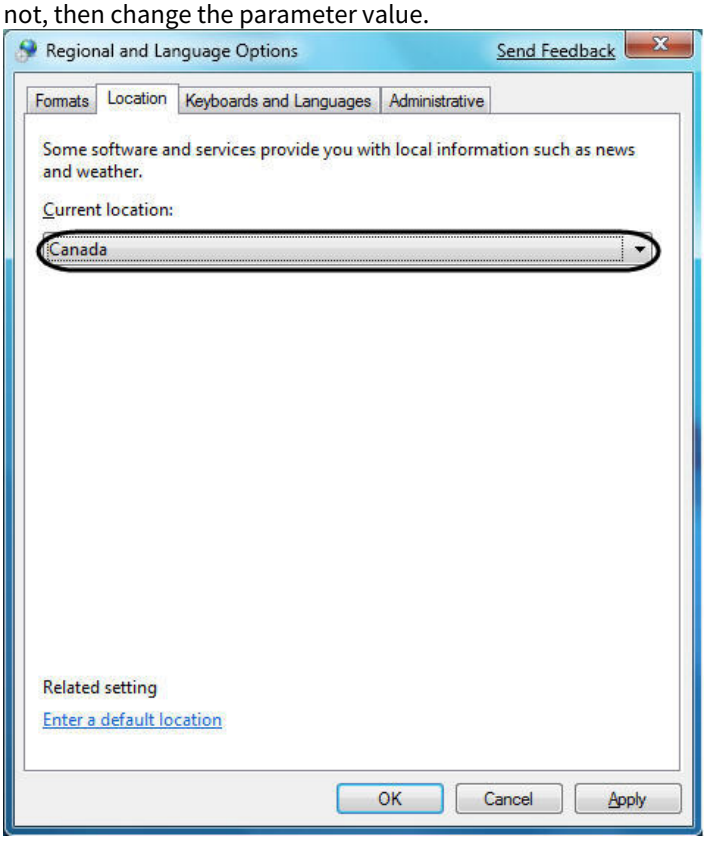


b. Click the **Additional settings...** (2) button and make sure the '.' value is selected for the **Decimal symbol (3)** parameter in the **Numbers** tab. If not, then change the parameter value manually.

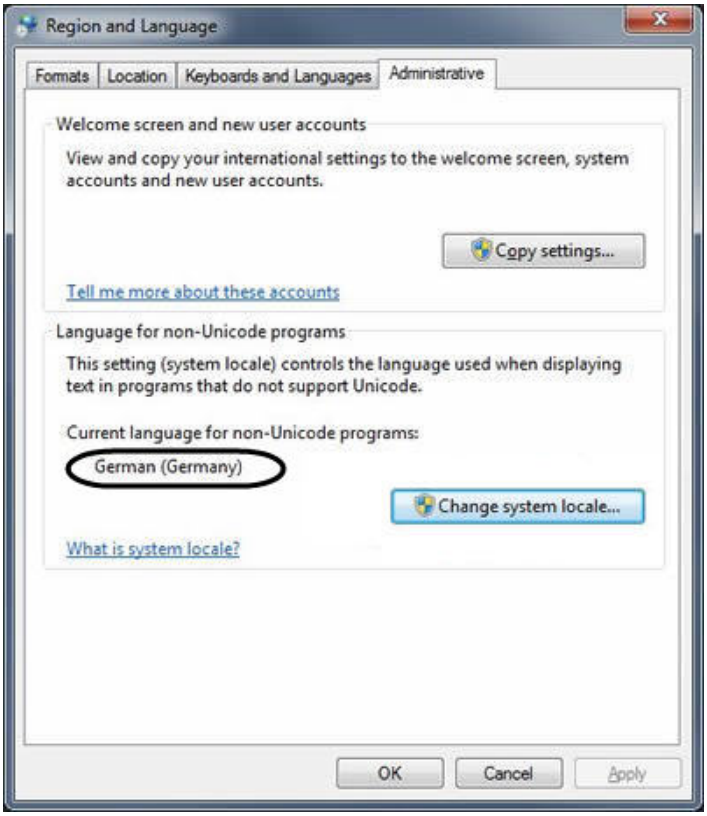


c. Click **OK** (**4**).
d. Click **OK** (**5**).

3. Go to the **Location** tab. Make sure that the real computer location is selected in the **Current location** dropdown list. If not, then change the parameter value.



4. Go to the **Administrative** tab. Make sure that the language that is used for Intellect installation is specified in the **Current language for non-Unicode programs** field. If not, then change the parameter value using the **Change system locale...** button.



19.1.2.2 System settings

Before starting the *Intellect* software installation, make sure that the name of the computer it is installed on does not exceed 15 characters. If the computer name is longer than 15 characters, the installation will not complete correctly. Rename the computer.

For example, GATE-SERVER is a valid computer name that contains 11 characters, and BACKUP-ARCHIVE-SERVER is too long because it contains 21 characters.

19.1.3 Installation of Intellect as a Server/Remote Administrator's workstation

This section outlines a step-by-step instruction on how to install *Intellect* software as a “Server”.

> **Note**
>
> The following features are to be taken into account while installing *Intellect* software:
> - *Intellect* software is to be installed on a “clean” Windows OS (see the Operating system requirements section).
> - To install *Intellect* software, administrator rights are required.

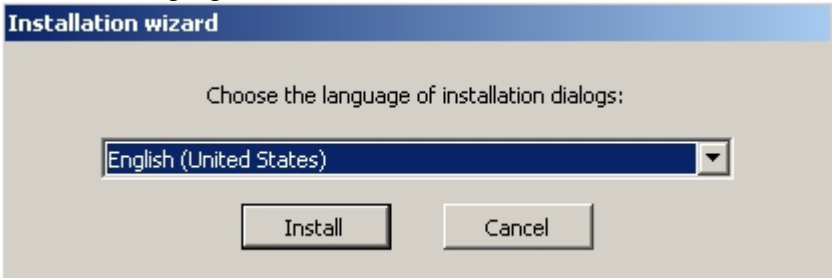
To install *Intellect* software, do the following:

1. Unpack the installation kit as described in Getting ready for Intellect installation; the destination folder will show the contents of the kit.

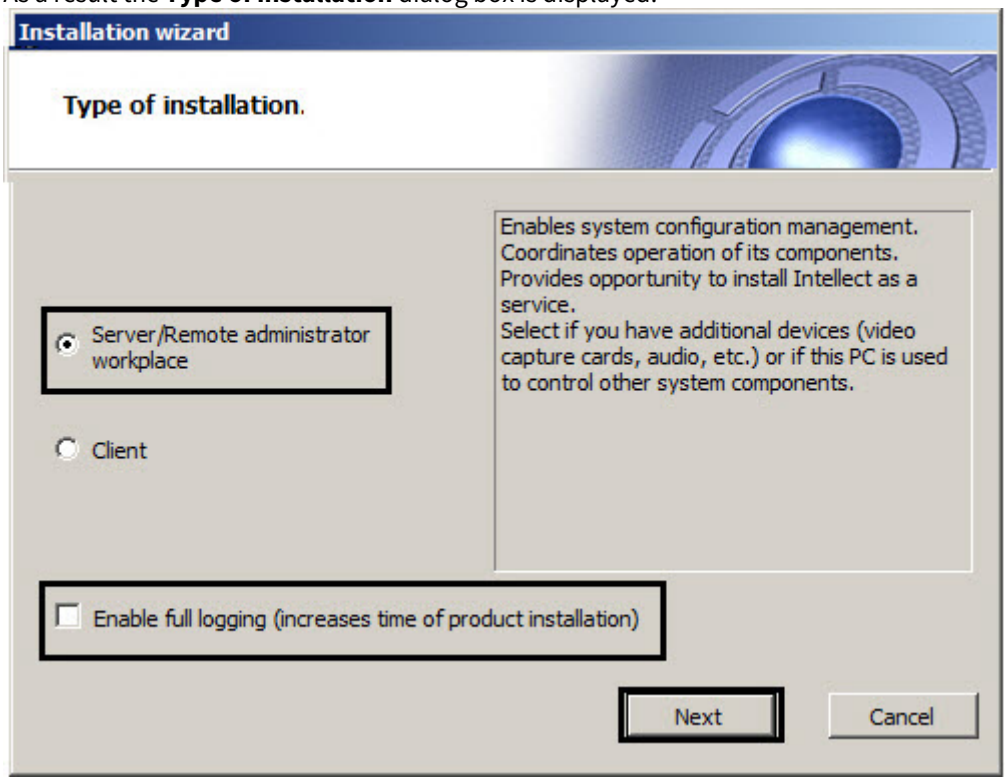
2. Run the setup.exe file to start the *Intellect* software installation procedure.
   As a result the dialog box of choosing language is displayed.

   > **Note**
   >
   > *Intellect* requires Microsoft.Net Framework 4.0 or later installed. It is usually included in the Windows OS installation kit and does not require separate installation. Otherwise, an installation window will open—you should agree to automatic installation. For more information about the Microsoft.Net Framework, see the official documentation https://learn.microsoft.com/en-us/dotnet/framework/.

3. Choose the language of *Intellect* software installation and click **Install**.



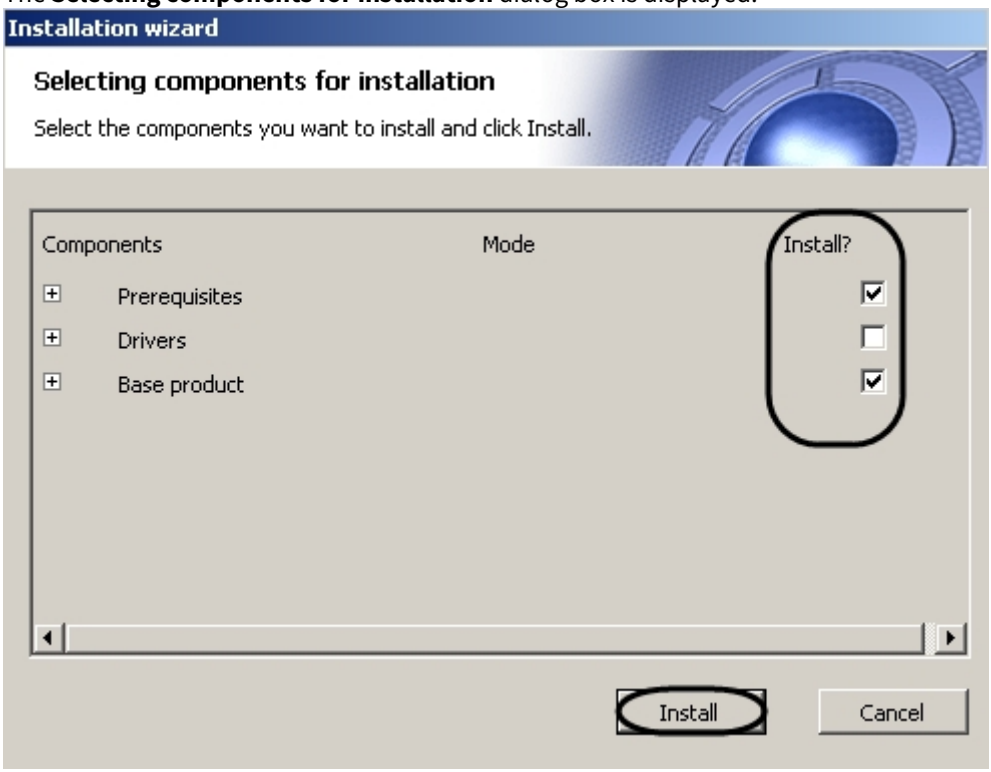
As a result the **Type of installation** dialog box is displayed.



4. Select the **Server/Remote administrator's workstation** type of installation.
5. To log all installation events, set the **Enable full logging (increases time of product installation)** checkbox.

> **Note**
>
> While installing and uninstalling the software events are logged to Intellect.log and Intellect uninstall.log correspondingly. To collect log-files, the “Support.exe” tool is to be used (see The utility for collecting configuration data on servers and RWS for the Technical Support section).

6. Click the **Next** button.
   The **Selecting components for installation** dialog box is displayed.

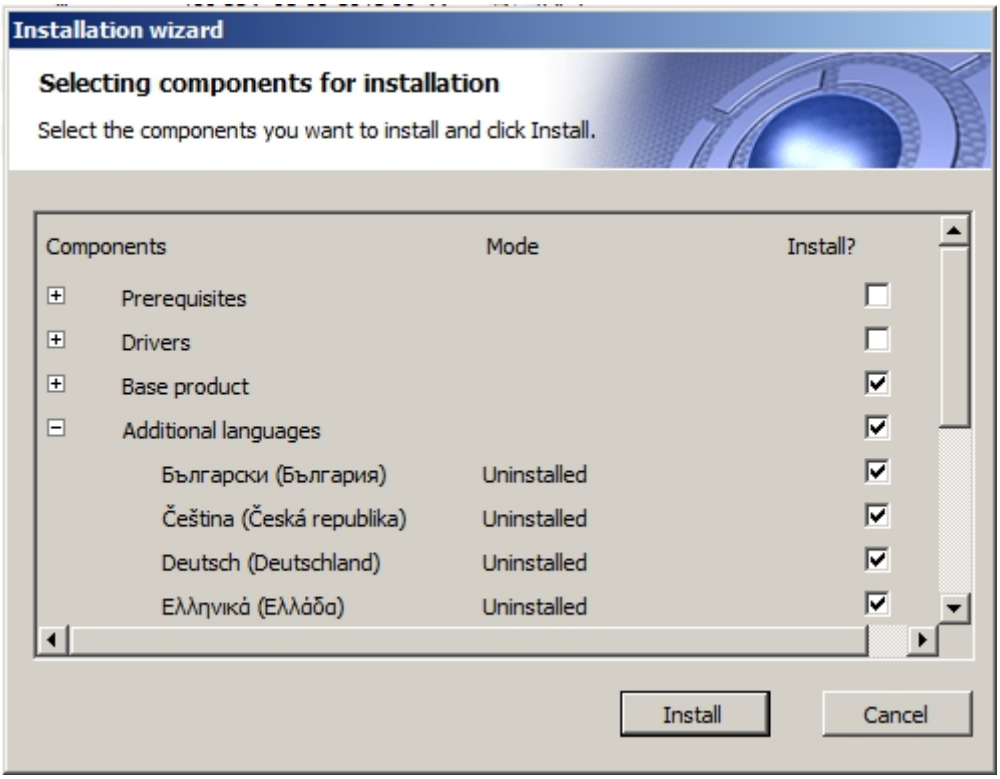


7. Set the checkboxes next to the components that are to be installed.

> **Note**
>
> All offered components are recommended to be installed.
> However, if installation is performed using the integrated software package (with vertical solutions modules), then there will be an option to select vertical solutions that are to be installed. Only those vertical solutions that will be in use are to be selected. There is no need to install all vertical solutions.
> Vertical solutions will be installed after installing Axxon Intellect Enterprise. Information on how to install vertical solutions can be found in the corresponding documentation.

> **Note**
>
> At this stage it is possible to deny installing MS SQL Express database server. In this case it will be required to configure connection to the remote database at step 16.
> When installation of *Intellect* is complete database connection parameters can be changed using the idb.exe utility—see INTELLECT™ software database connection.
> Pay attention that *Intellect* operation will be impossible without connection to any database source.

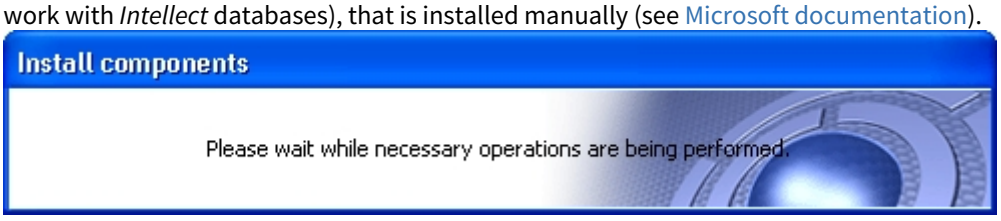
If you are not installing from a disk, you will also be able to select the languages to be installed. To do this, download the language pack from AxxonSoft official website (https://www.axxonsoft.com/) before beginning the installation and put the archive's files into the languages folder in the installer's directory. As a result, a list of **Additional languages** will be displayed in the **Components** section of the **Selecting components for installation** window, and you can select the languages that need to be installed.



Note

If this method of installing languages is not suitable, each language can be installed separately later (see Installing the language). After the installation, use the utility tweaki.exe to switch languages (see Switching languages in the Intellect Software System).

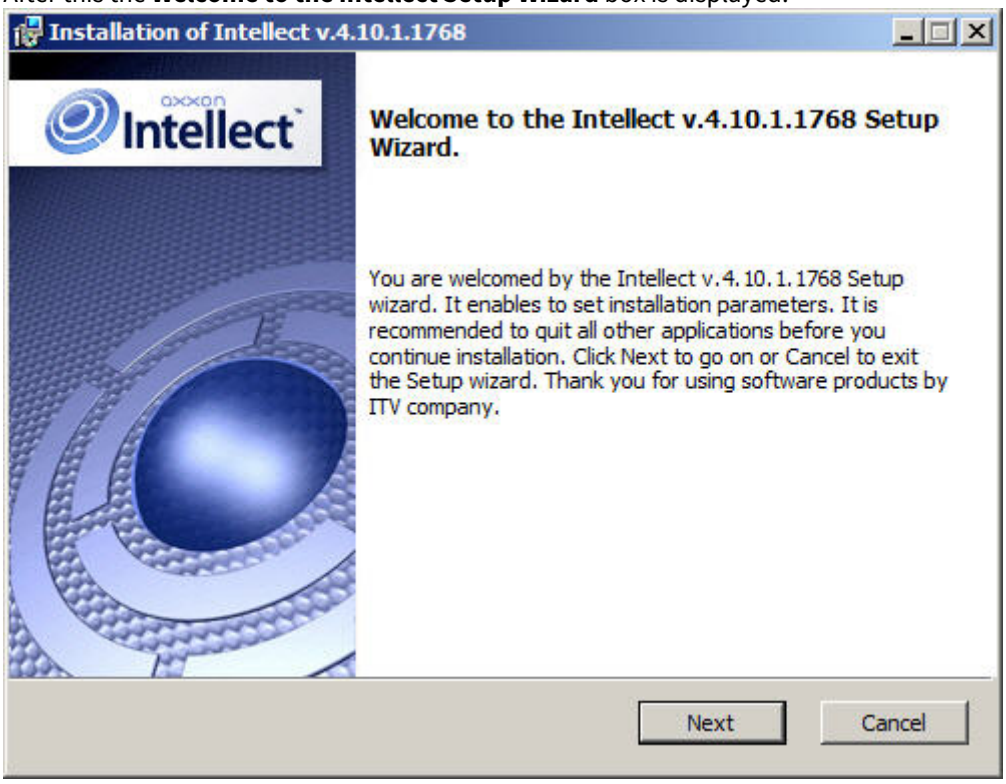
8. Click the **Install** button.
The selected components are automatically installed except Microsoft SQL Server Express 2014 database (necessary for work with *Intellect* databases), that is installed manually (see Microsoft documentation).



Important!

Auto installation of necessary prerequisites may take more than 10 minutes.

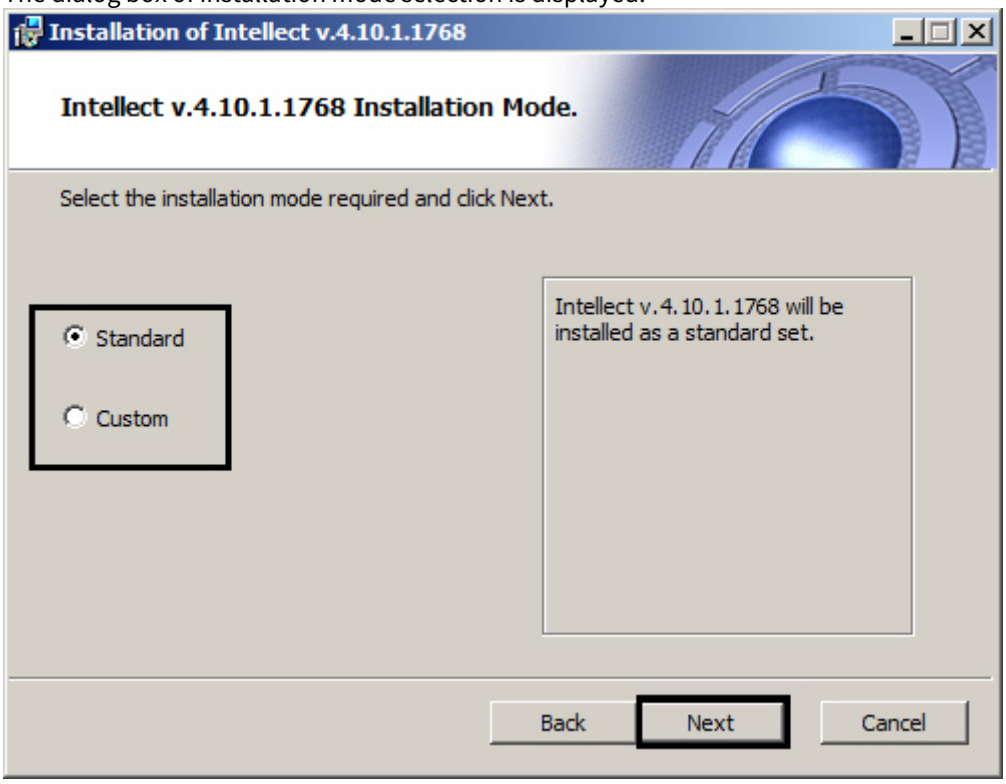
After this the **Welcome to the Intellect Setup Wizard** box is displayed.



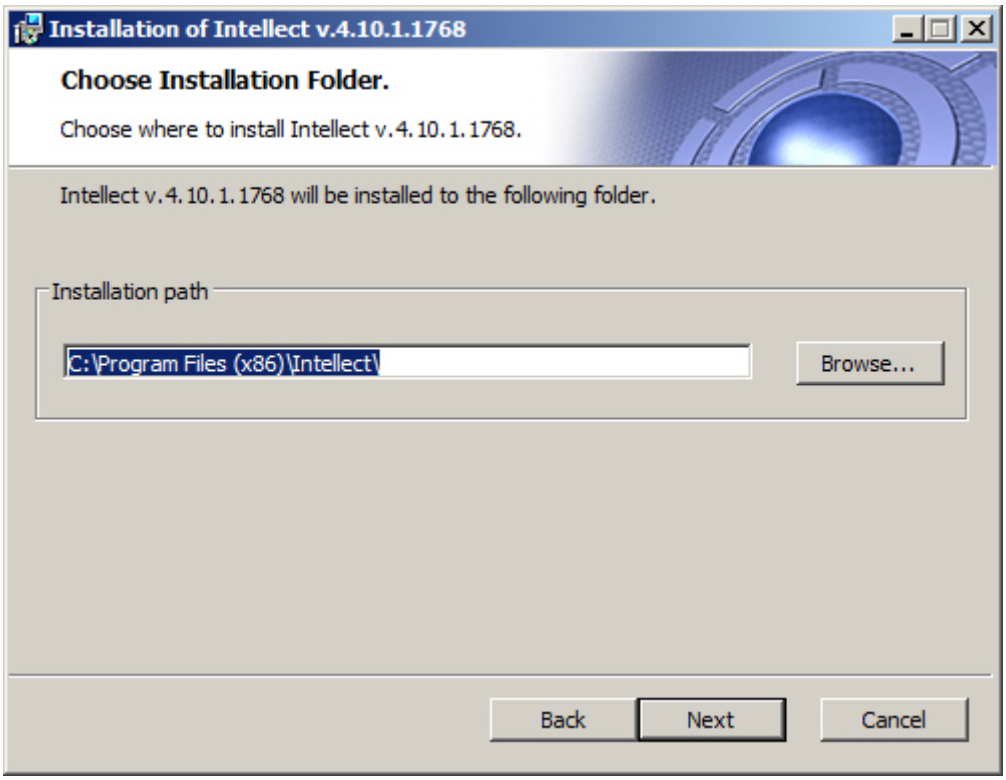
9. Click the **Next** button.
   The **License Agreement** dialog box is displayed.

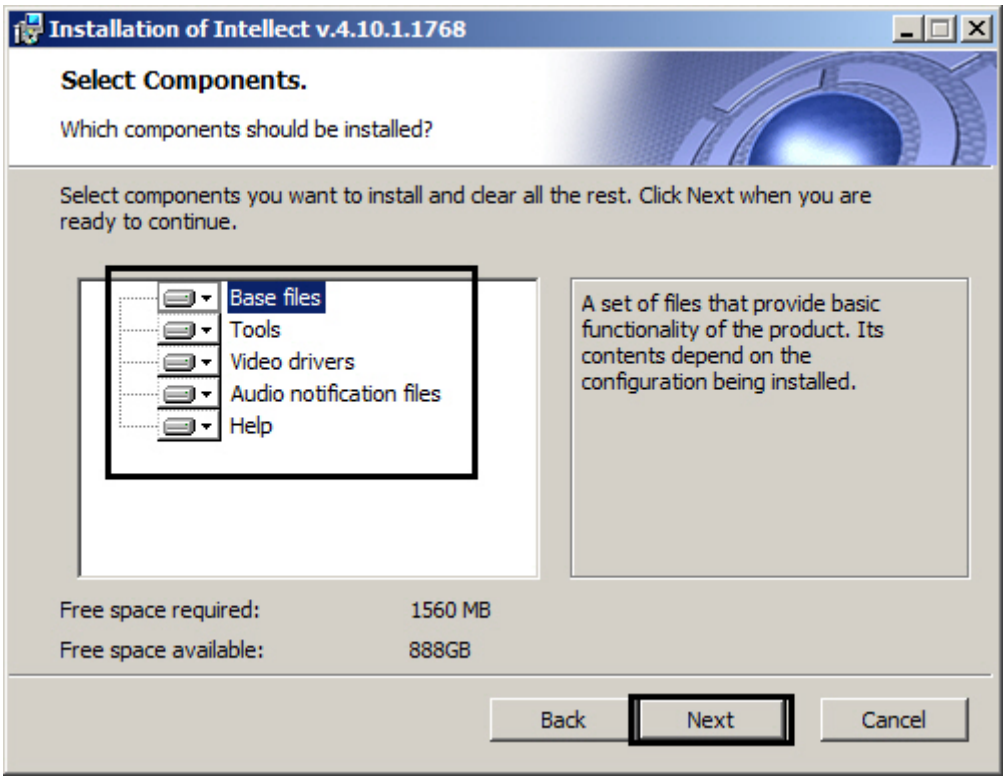
10. Read the License agreement and accept its terms by setting the switch into the **I accept the terms of the License agreement** position, otherwise the *Intellect* installation will be stopped.

11. Click the **Next** button.
    The dialog box of installation mode selection is displayed.



12. Select the installation mode.
13. Click the **Next** button.
    When the **Custom** installation mode is selected, the dialog box of choosing the installation folder is displayed, and then the **Select components** dialog box is displayed. This step is omitted when the **Standard** installation mode is selected.

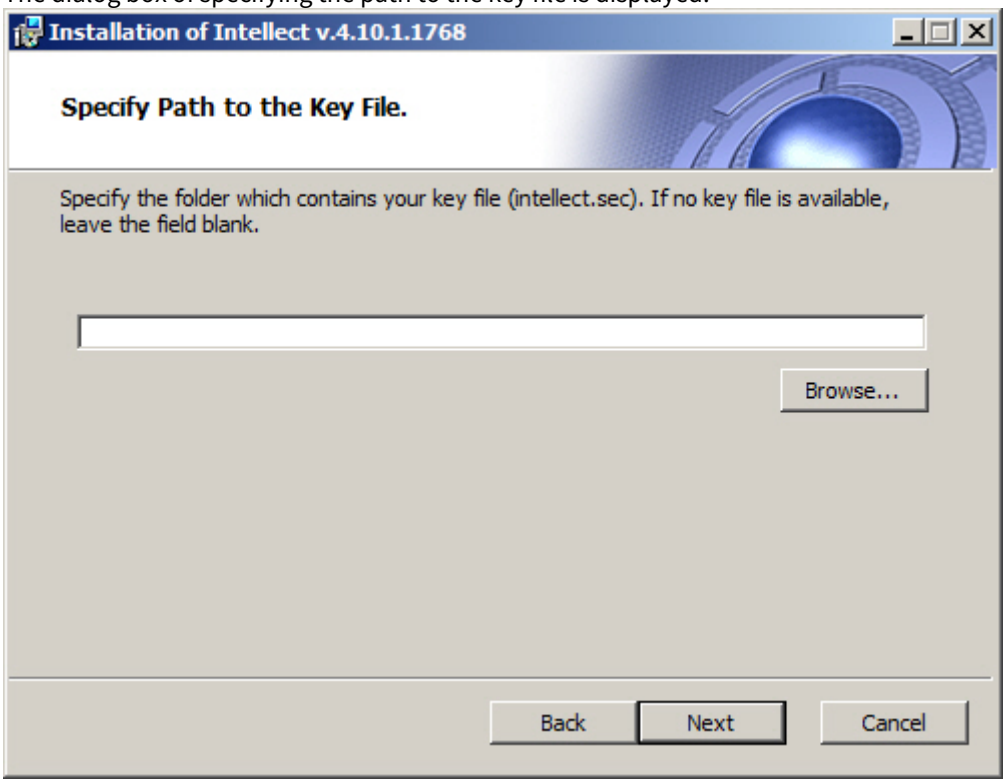




Note

The description of the component is displayed in the installation box when this component is selected.

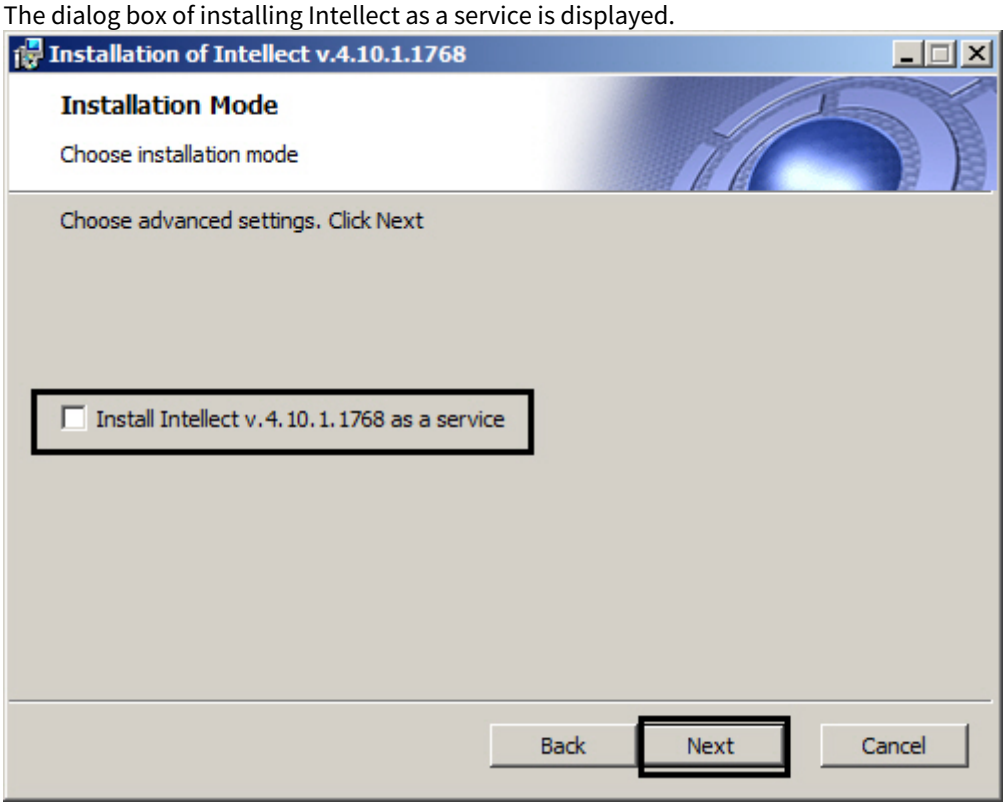
The dialog box of specifying the path to the key file is displayed.



Note

Keep the field blank if the key file will be copied later.

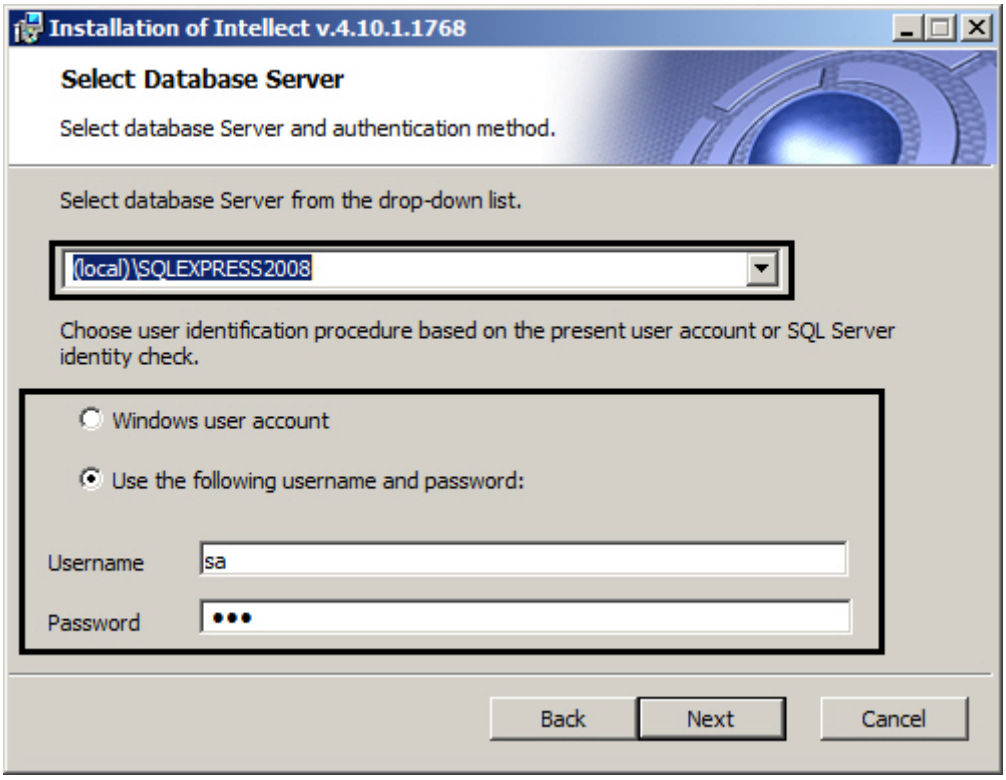
14. Click the **Next** button.
The dialog box of installing Intellect as a service is displayed.



Note

The 64-bit version of *Intellect* is not available when installed as a service. If this checkbox is set checked, then 32-bit modules will be started after installing *Intellect* as a service.

15. Set the **Install Intellect as a service** checkbox if *Intellect* software is to be started before the user is authorized by the Windows OS and before Windows applications are started (including the Explorer application) that is used for starting Windows OS interfaces and various other applications installed on the Server (see Working with Windows OS services for operating Intellect™ installed as a Service section).
16. Click the **Next** button.
The dialog box of MS SQL Server database server selection is displayed. Specify the authentication parameters to connect to it.



Important!

Access of some user to the database is impossible without additional settings of the idb.exe utility and knowing of the login and password of Administrator if installation of the *Intellect* software package is performed by Administrator and Windows account data are in use for SQL authentication. So it is highly recommended not to use such authentication method of the SQL server.

17. Select the SQL-server using the drop-down list.

Note

If there is necessity to use the SQL-server installed on this (local) computer, the “(local)\SQLEXPRESS2014” item (set by default) is to be selected.

Important!

You cannot connect different Servers to one database.
Server can use remote database, but requirements to network and other resources become higher and this can cause delays while transmitting events and states of cores.

18. Set the authorization parameters that will be used by *Intellect* while connecting to the SQL-server.

Note

If *Intellect* is installed as a service, select the SQL Server identity check, i.e. set the **Use the following username and password** checkbox and specify the username and password to login the Server database. If the database is to be connected via the Windows account, then for proper operation of *Intellect* any other the user is to have corresponding SQL Server permissions.

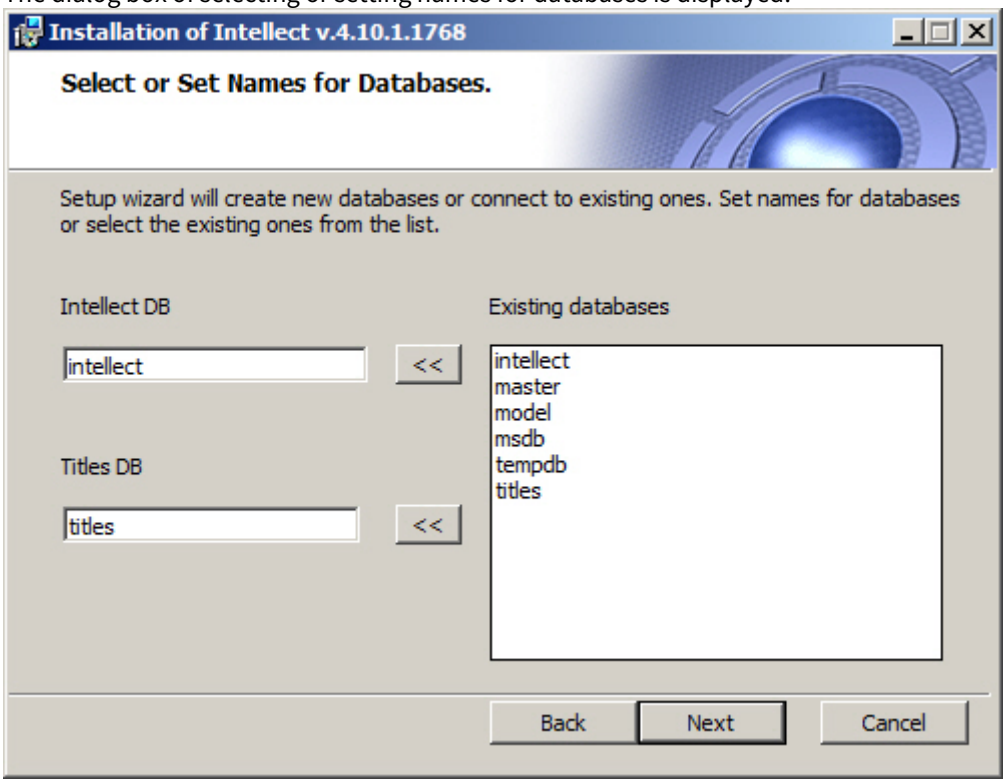
Ways of authorization performed in the dialog box.

Ways of authorization	**Windows user account**	**Use the following username and password (recommended)**
Usage	SQL Server from *Intellect* distributive (or from the distributive of the external vendor) and *Intellect* is installed on the same computer	SQL Server from *Intellect* distributive and *Intellect* are installed on the same computer. Meanwhile connection to SQL Server with the set username (login) and password may be performed from any remote computer that is in the same net domain of TCP/IP net with a computer, where SQL Server is being installed
	SQL Server and *Intellect* are installed on different computers that are connected through TCP/IP net and are in the same net domain. Meanwhile the account for the user currently authorized in Windows OS on the computer, where *Intellect* is being installed is to be created in Windows OS on the computer with installed MS SQL Server	SQL Server from *Intellect* distributive and *Intellect* are installed on different computers that are connected through TCP/IP net and are in the same net domain. Meanwhile the username (login) and password are to correspond to the username (login) and password used for access to SQL-server
	Full-scale SQL Server (supplementary installed) and *Intellect* are installed on different computers, connected through TCP/IP net and are in the same net domain. Meanwhile the account for the user currently authorized in Windows OS on the computer, where *Intellect* is being installed is to be created on the remote SQL Server	Full-scale SQL Server (supplementary installed) and *Intellect* are installed on the same or different computers that are connected through TCP/IP net and are in the same net domain. Meanwhile the username (login) and password are to correspond to the username (login) and password used for access to SQL-server

Note

For SQL Server installed from *Intellect* distributive, the “sa” username and “*Intellect_default_DB_4*” password are used by default. While installing the *Microsoft SQL Server Express 2014* the password may be changed for any other.

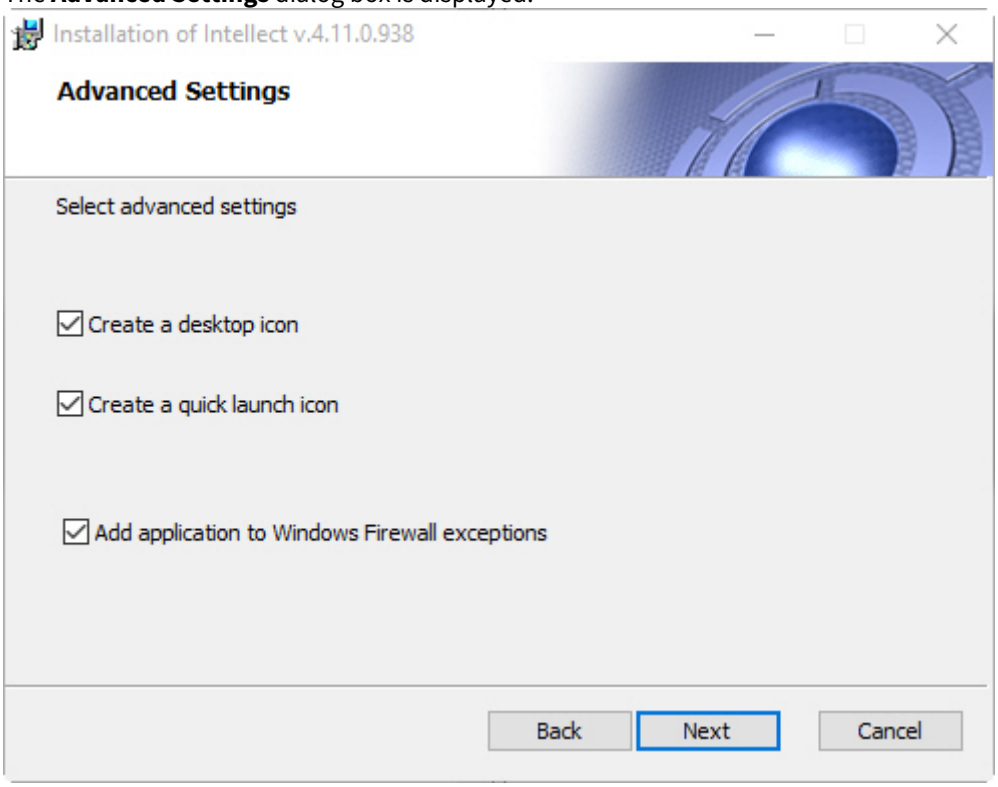
19. To continue the installation, click the **Next** button.
    The dialog box of selecting or setting names for databases is displayed.



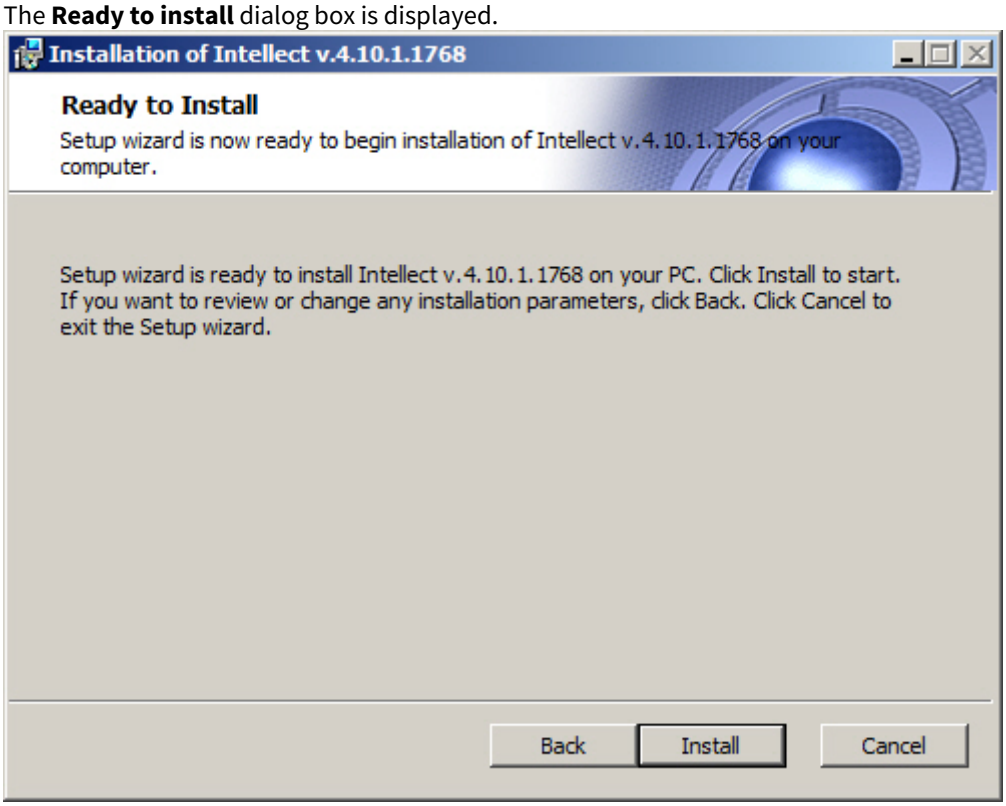
20. By default the *Intellect* database is in use as the main database. To set another database select the required database from the **Existing databases** list and click the button near the **Intellect DB** field.
21. By default the titles database is in use as a database of titles. To set another database select the required database from the **Existing databases** list and click the button near the **Titles DB** field.
22. Click the **Next** button.

> **Note**
>
> If the system while being installed displays the “Rights are required to create or edit databases” message, then the installation process must be stopped and then restarted again.

The **Advanced Settings** dialog box is displayed.



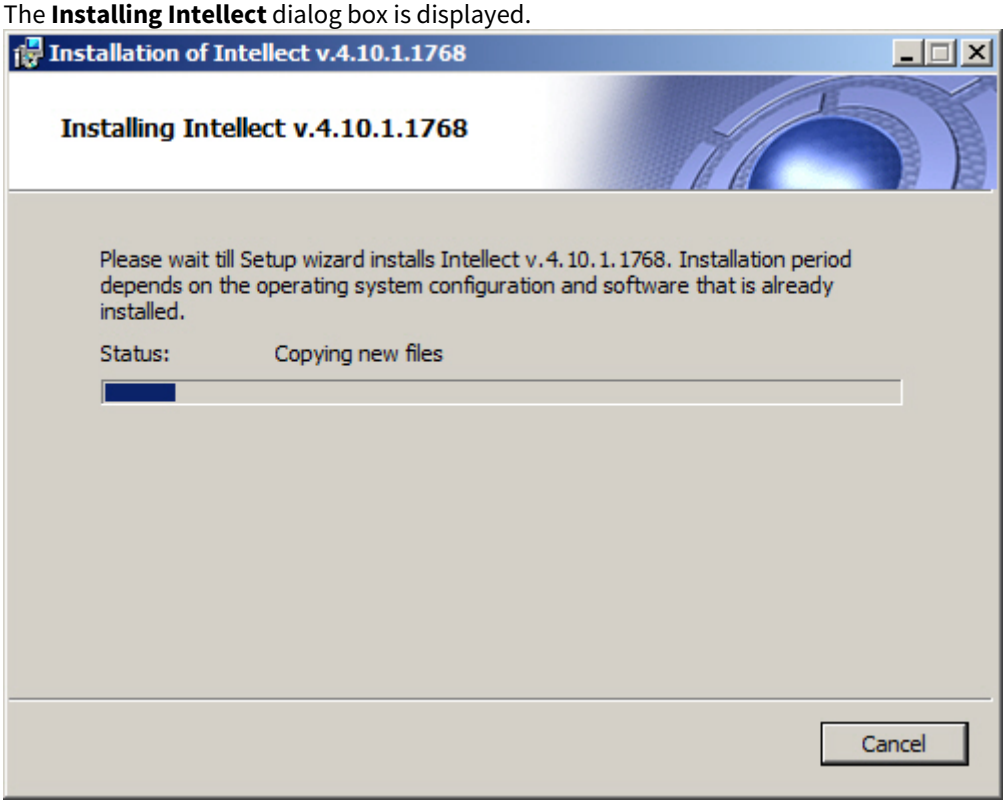
23. If a desktop icon is to be created, set the corresponding checkbox.
24. If a quick launch icon is to be created, set the corresponding checkbox.
25. If it is required to add *Intellect* and all its components to the Windows Firewall exceptions, set the corresponding checkbox.
26. Click the **Next** button.
27. The **Ready to install** dialog box is displayed.



Note

To change the setting, click the **Back** button.

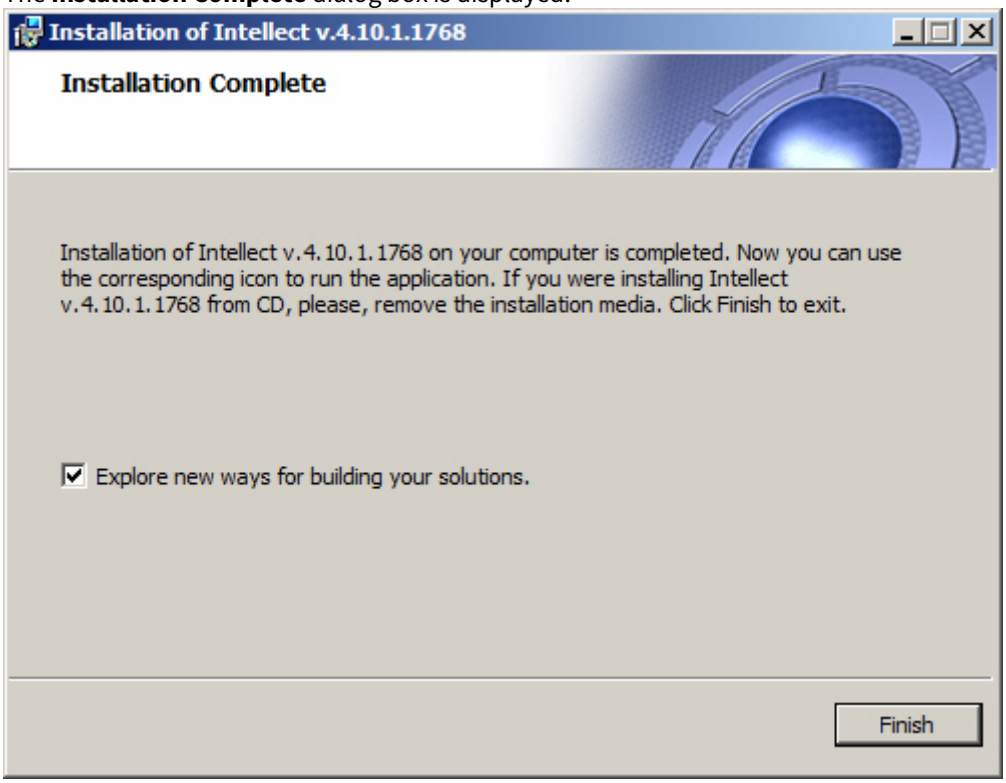
28. Click the **Install** button.
The **Installing Intellect** dialog box is displayed.



Note

Error of driver installation for the FX4 card can occur while the *Intellect* software installation on the Windows 7 SP1 operating system without Internet connection. To eliminate this error install the following missing Windows updates:
https://support.microsoft.com/en-us/kb/3004394
https://support.microsoft.com/en-us/kb/3033929

29. The **Installation Complete** dialog box is displayed.

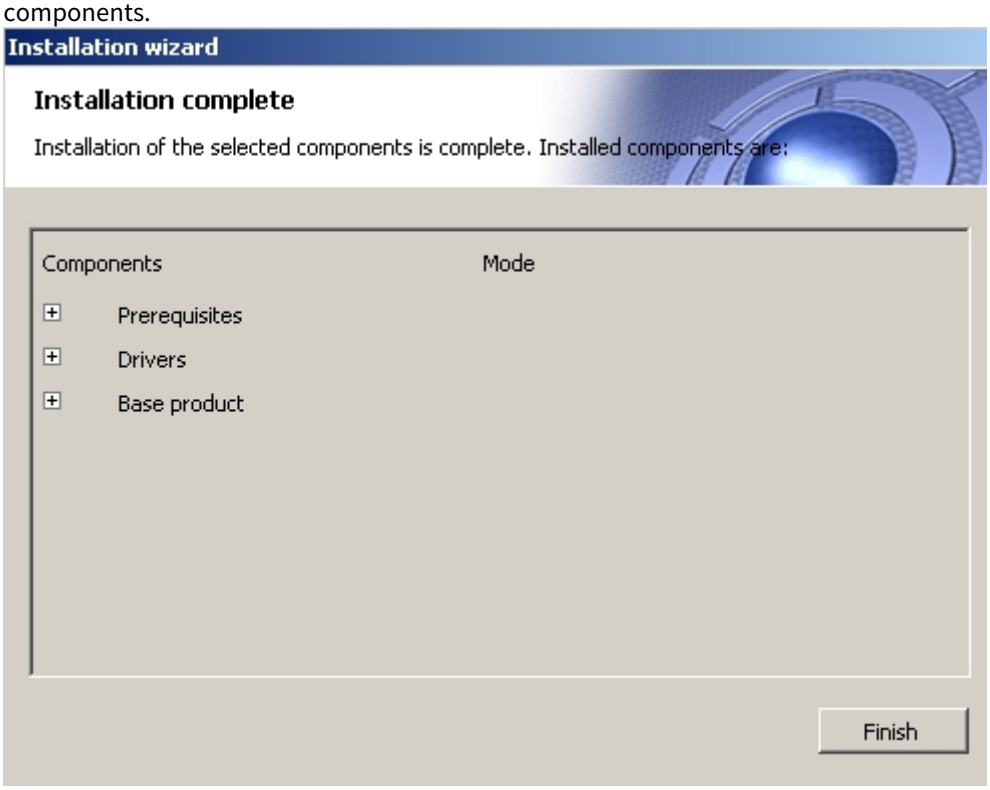


30. Set the **Explore new ways for building your solutions** checkbox, to view the document containing information about new features of the installed *Intellect*.
31. Click the **Finish** button.

> **Note**
>
> Then the Driver Pack will be installed. Starting from the Driver Pack 3.51, this driver package requires the Windows KB2999226 update to be installed. If this update is not installed on the system, a corresponding warning will be displayed. To continue the installation, it is necessary to install the update from the official Microsoft website:
> https://www.microsoft.com/en-us/download/details.aspx?id=49093
> If KB2999226 is installed, but there is no software ability to identify it, run the Driver Pack installation from the command prompt with the SOFT_INSTALL = "yes" parameter.
> `C:\>start /i IPDriverPack-x64.msi SOFT_INSTALL="yes"`

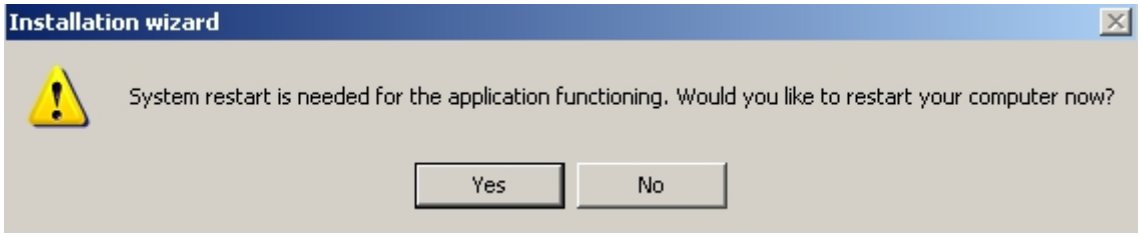
Then the Installation wizard dialog box is displayed, containing the information on the mode (installed or not) of *Intellect*

components.



32. Click the **Finish** button.

The dialog box offering to restart the system is displayed.



Restarting the computer is required to correctly complete the *Intellect* installation. If choose not to restart your computer now, you will need to do it yourself after installing *Intellect*.

The *Intellect* as a Server is now installed.

19.1.4 Installation of INTELLECT™ software to the Client

This section outlines a step-by-step instruction on how to install INTELLECT™ software onto a Client workstation.

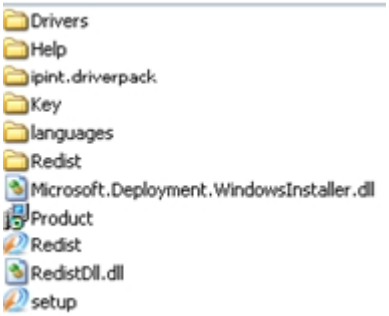
Note.

The following features are to be taken into account while installing INTELLECT™ software:

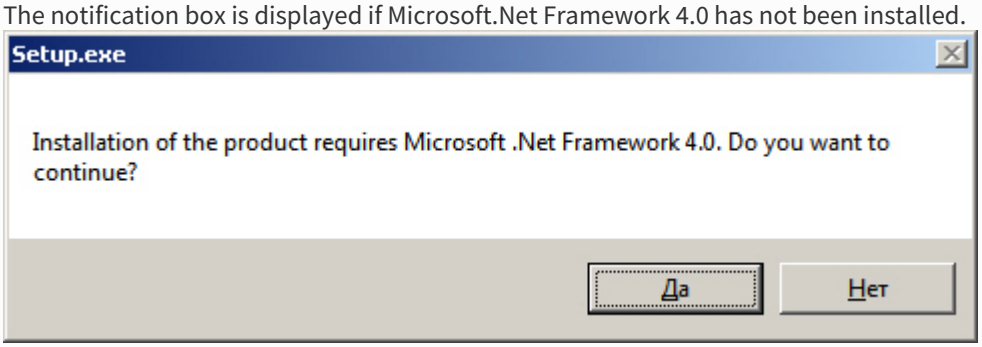
- INTELLECT™ software is to be installed on a “clean” Windows OS (see the Operating system requirements section).
- To install INTELLECT™ software, administrator rights are required.
- INTELLECT™ software is to be installed in the folder, which appears by default in the corresponding dialog box of the installation program (i.e., “C:\Program Files \ Intellect”). It is not recommended to change the names of the logical disk and folder for the installation.
- Versions of INTELLECT™ software installed on the Client and Server/Administrator's workstation are to be the same. Otherwise, their operation is not guaranteed.

To install INTELLECT™ softwareas a **Client**, do the following:

1. Unpack the installation kit as described in Getting ready for Intellect installation; the destination folder will show the contents of the kit.

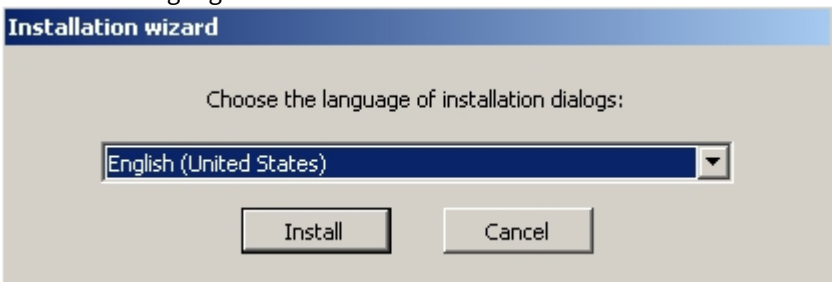


2. Run the setup.exe file to start the INTELLECT™ software installation procedure.
As a result the dialog box of choosing language is displayed.

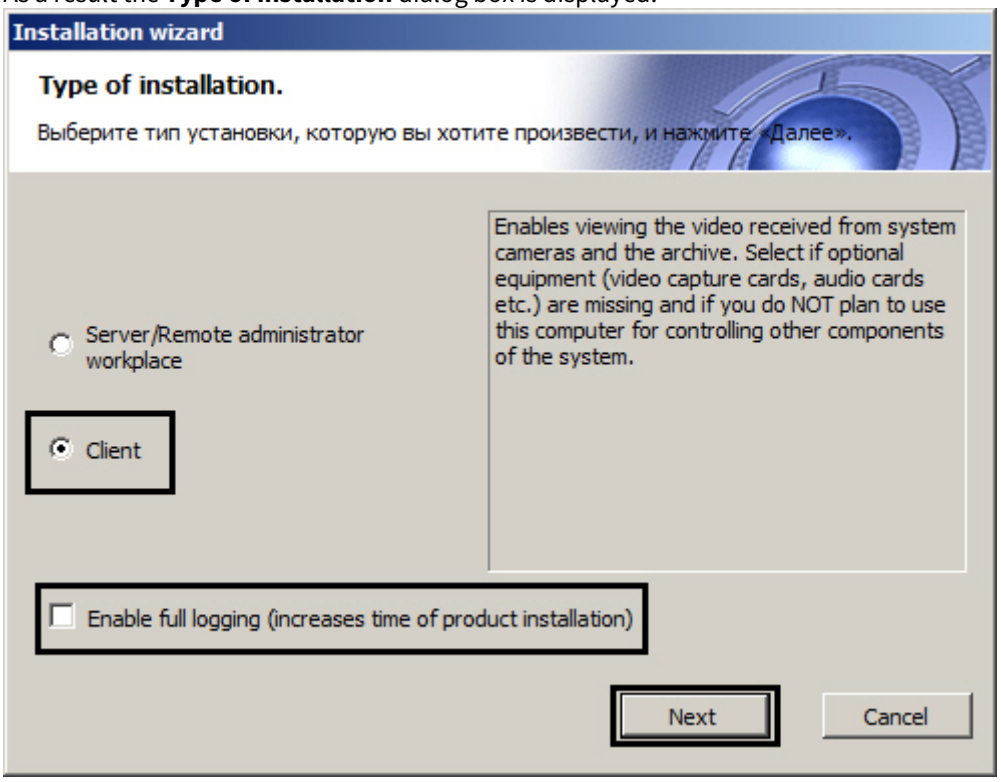
> **Note**
>
> The notification box is displayed if Microsoft.Net Framework 4.0 has not been installed.
>
> 
>
>
> Click **Yes** for Microsoft.Net Framework 4.0 auto installation.

> **Attention!**
>
> When INTELLECT™ is installed on Windows 8 and Windows Server 2012 OS, the Microsoft.Net Framework 4.0 or later is to be pre-installed. If the Microsoft.Net Framework 4.0 or later has not been installed, then the warning is displayed. In this case stop installing INTELLECT™ and install the Microsoft.Net Framework 4.0 or later. You will find the instructions on how to install it at: http://msdn.microsoft.com/en-gb/library/hh506443.aspx

3. Choose the language of INTELLECT™ software installation and click **Install**.



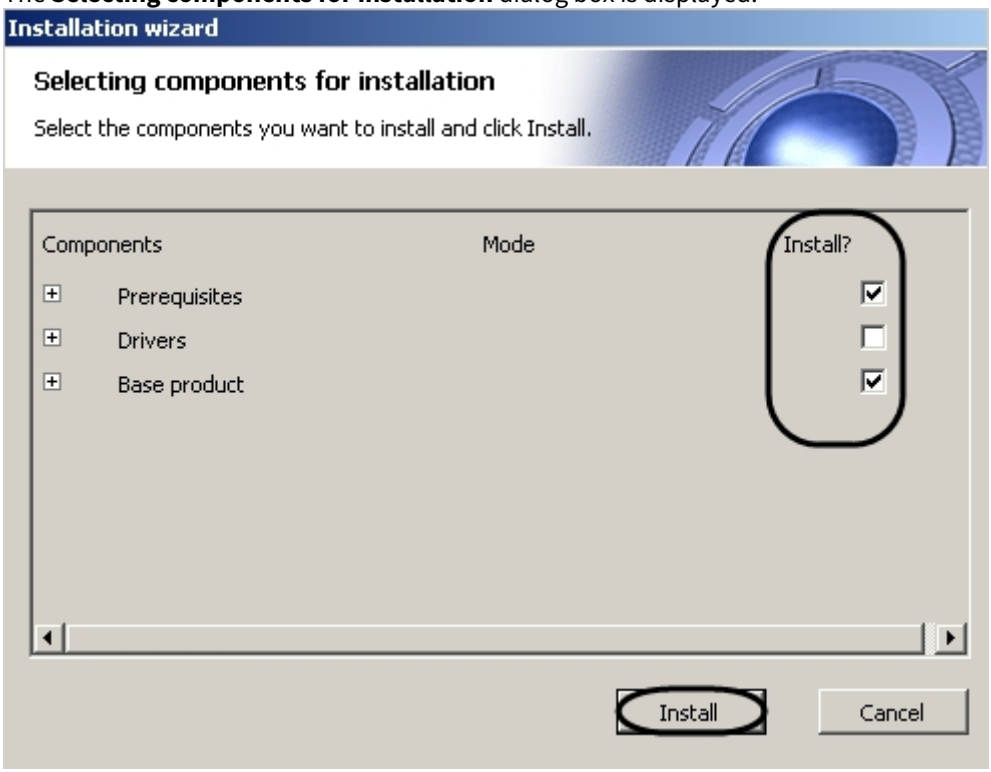
As a result the **Type of installation** dialog box is displayed.



4. Select the **Client** type of installation.
5. To log all installation events, set the **Enable full installation log** checkbox.

> **Note**
>
> While installing and uninstalling the software events are logged to Intellect.log and Intellect uninstall.log correspondingly. To collect log-files, the “Support.exe” tool is to be used (see The utility for collecting configuration data on servers and RWS for the Technical Support section).

6. Click the **Next** button.
   The **Selecting components for installation** dialog box is displayed.

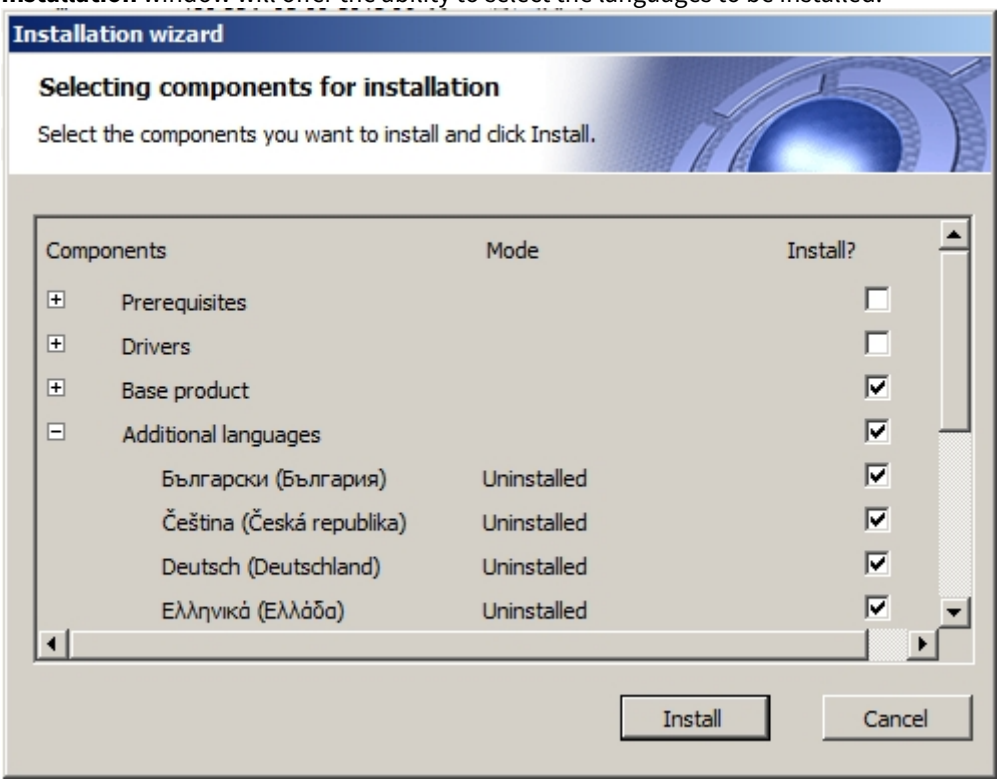


7. Set the checkboxes next to the components that are to be installed.

> **Note**
>
> All offered components are recommended to be installed.

If you are not installing from a disk, you will also be able to select the languages to be installed. To do this, download the language pack from AxxonSoft official website (https://www.axxonsoft.com/) before beginning the installation and put the archive's files into the languages folder in the installer's directory. As a result, the **Selecting components for**

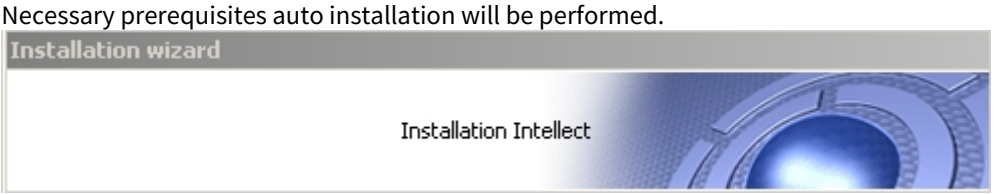
installation window will offer the ability to select the languages to be installed.



Note

If this method of installing languages is not suitable, each language may be installed separately (see Installing the language). After the installation, use the utility tweaki.exe to switch languages (see Switching languages in the Intellect Software System).

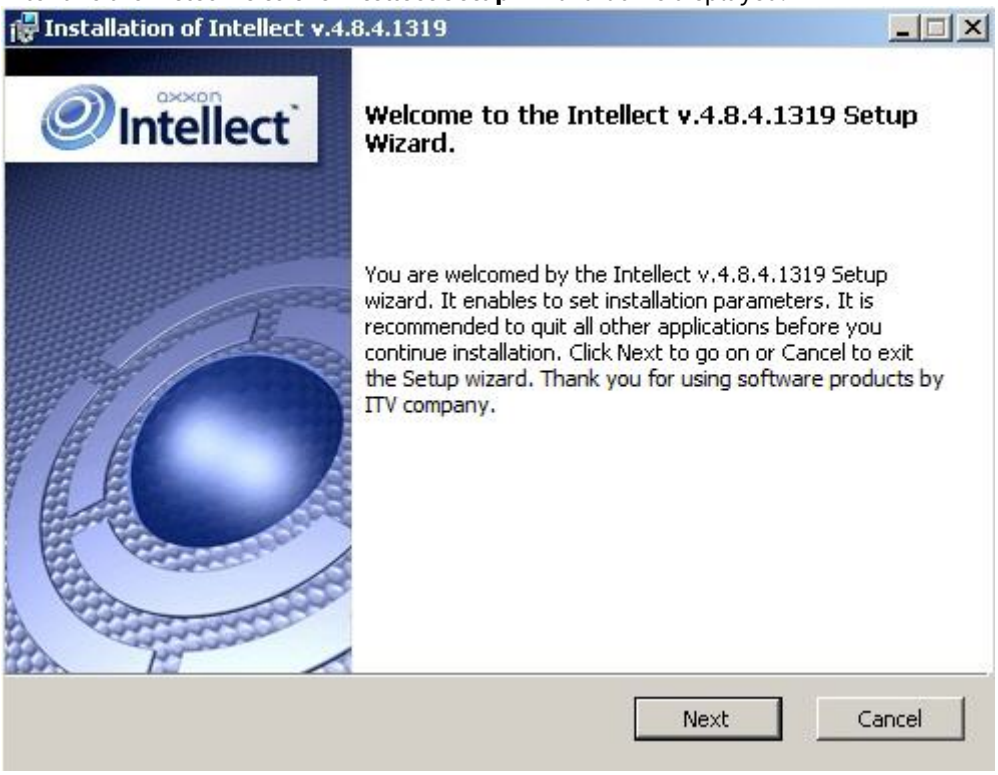
Click the **Install** button.
Necessary prerequisites auto installation will be performed.



Attention!

Auto installation of necessary prerequisites may require more than 10 minutes.

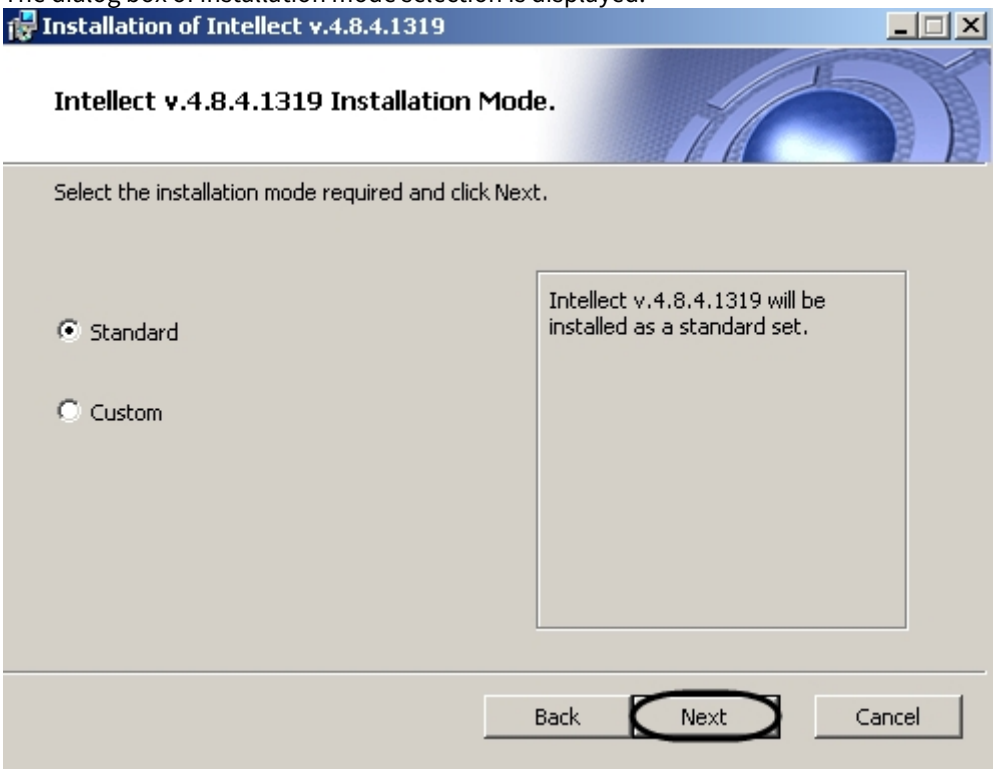
After this the **Welcome to the Intellect Setup Wizard** box is displayed.



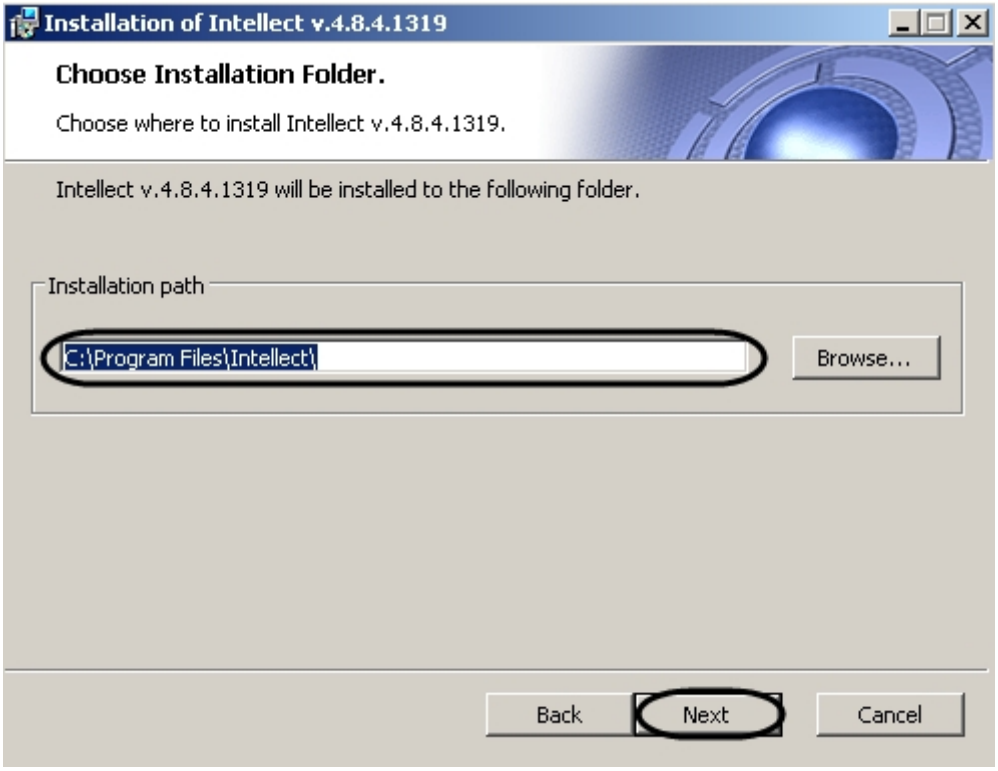
8. Click the **Next** button.
   The **License Agreement** dialog box is displayed.

9. Read the License agreement and accept its terms by setting the switch into the **I accept the terms of the License agreement** position, otherwise the INTELLECT™ installation will be stopped.

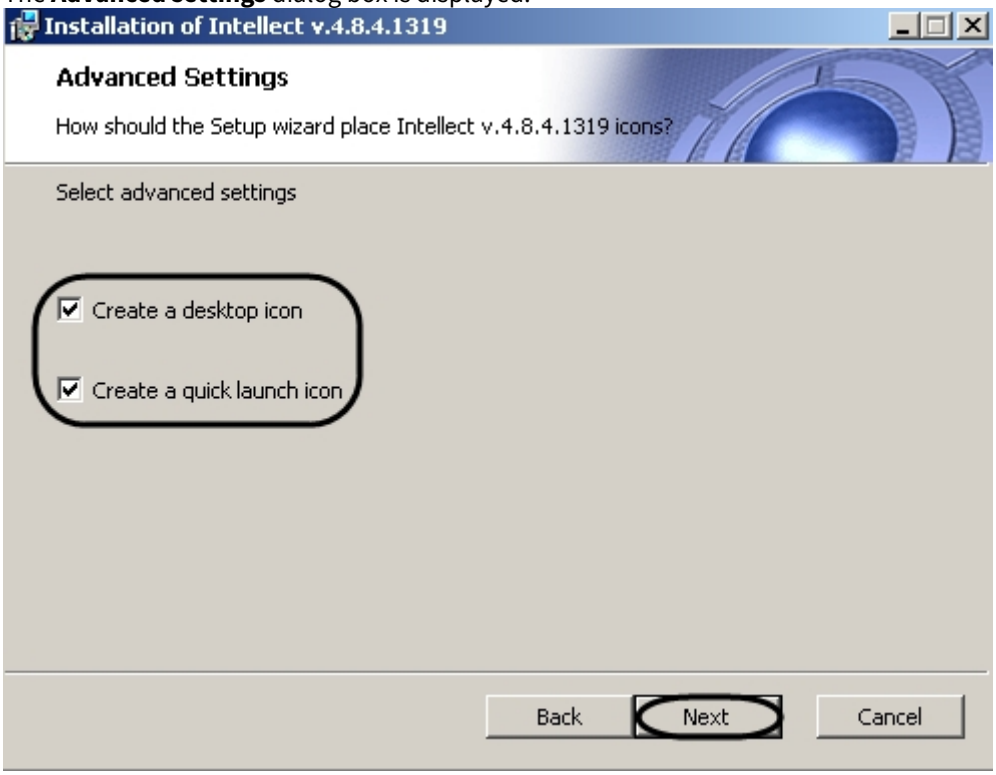
10. Click the **Next** button.
    The dialog box of installation mode selection is displayed.



11. Select the installation mode.
12. Click the **Next** button.
    When the **Custom** installation mode is selected, the dialog box of choosing the installation folder is displayed. This step is omitted when the **Standard** installation mode is selected.

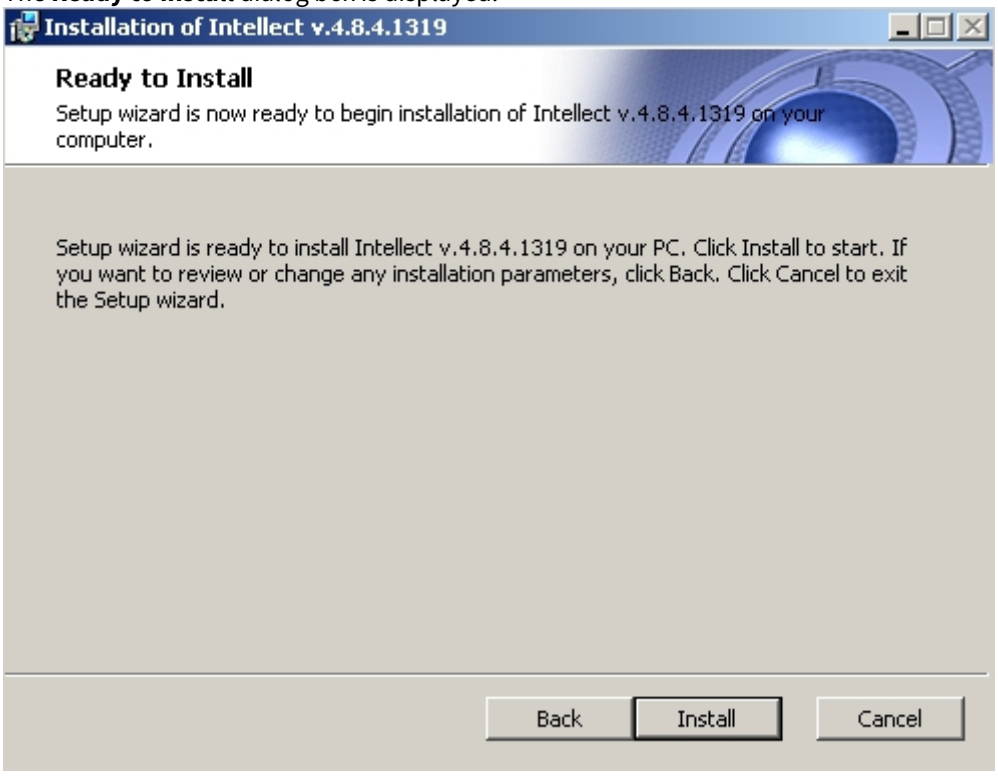


The **Advanced settings** dialog box is displayed.



13. If a desktop icon is to be created, set the corresponding checkbox.
14. If a quick launch icon is to be created, set the corresponding checkbox.
15. Click the **Next** button.

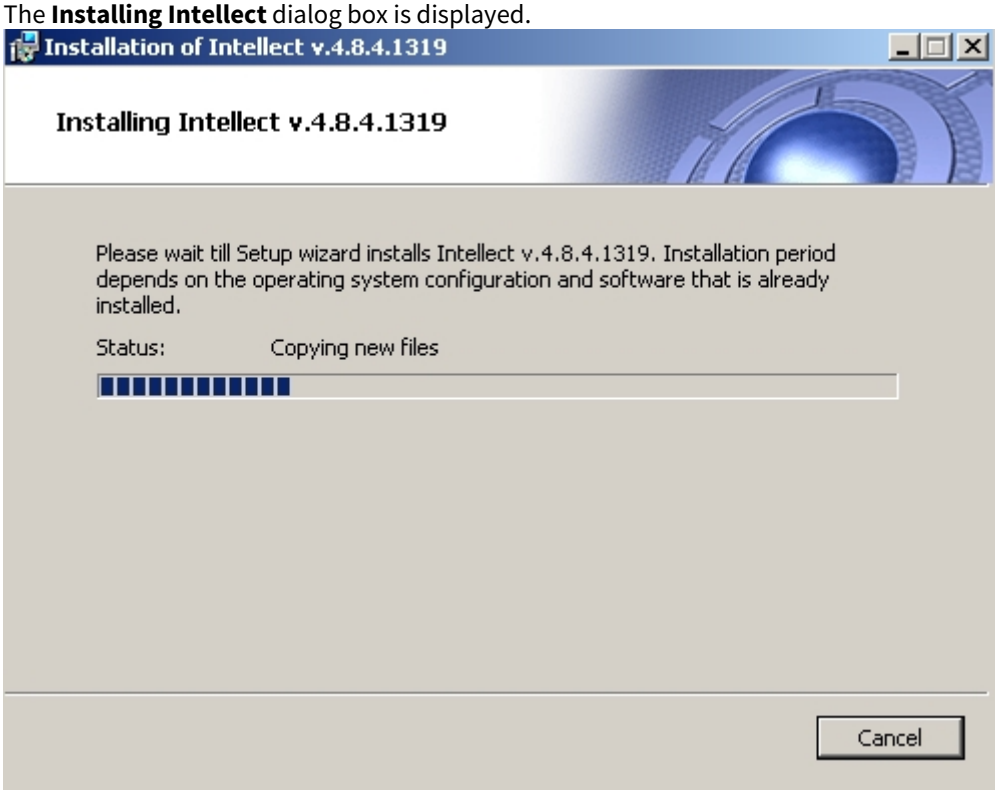
The **Ready to install** dialog box is displayed.



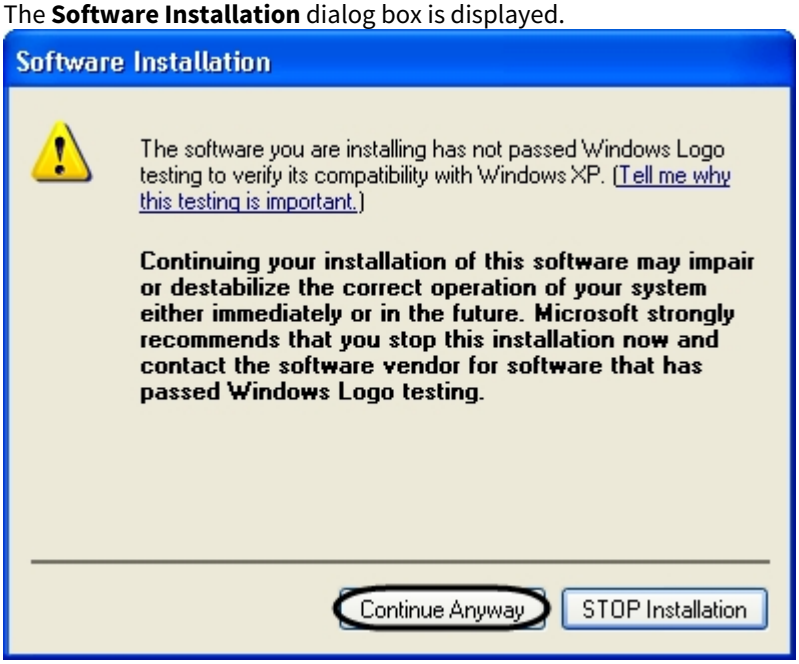
Note.

To change the setting, click the **Back** button.

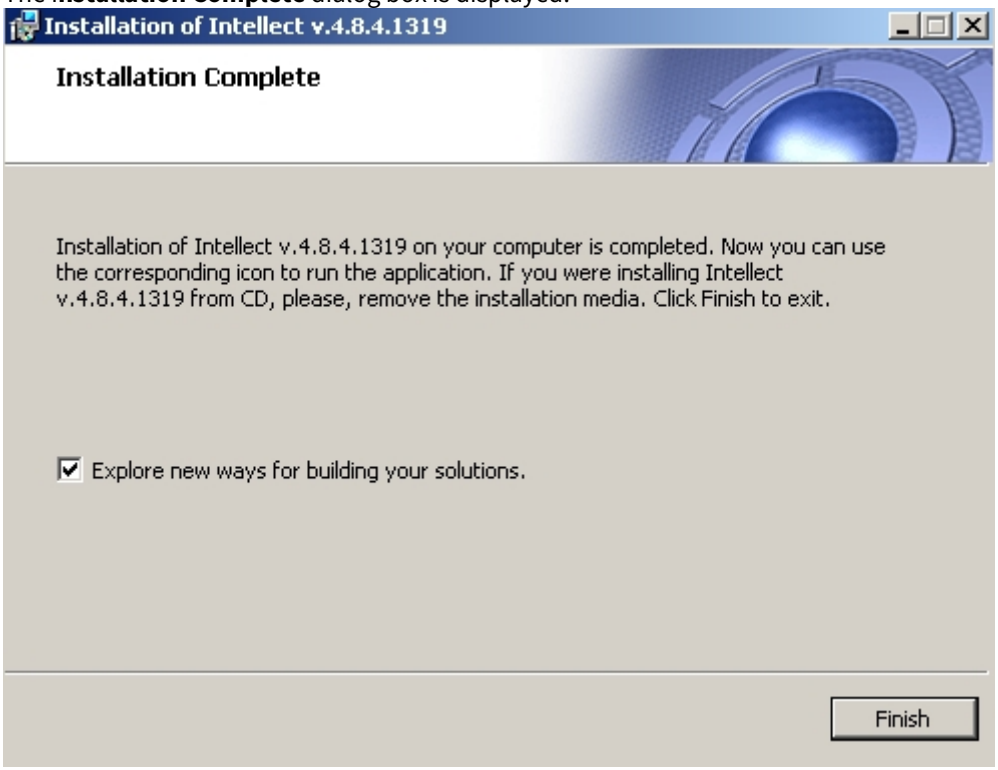
16. Click the **Install** button.
    The **Installing Intellect** dialog box is displayed.



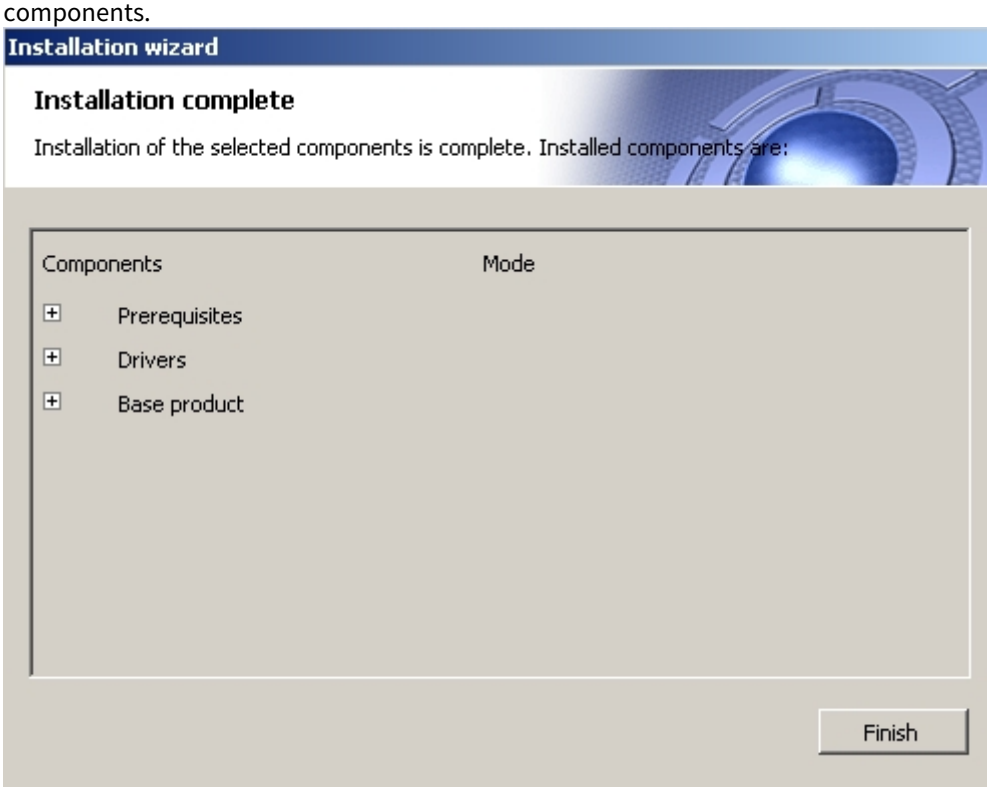
    The **Software Installation** dialog box is displayed.



17. To continue the installation, click the **Continue Anyway** button.
    The I**nstallation Complete** dialog box is displayed.



18. Set the **Explore new ways for building your solutions** checkbox, to view thw document containing information about new features of the installed *Intellect*.
19. Click the **Finish** button.
    Then the Installation wizard dialog box is displayed, containg the information on the mode (installed or not) of *Intellect* components.



20. Click the **Finish** button.

The *Intellect* with the **Client** type of installation is now installed.

19.1.5 Updating Intellect

If you install *Intellect* on a computer where an earlier version is used, then the installation will be in the updating mode.

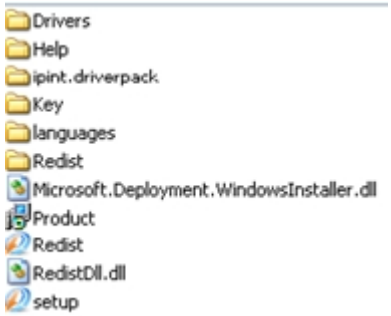
Attention!

Important to know before updating *Intellect:*

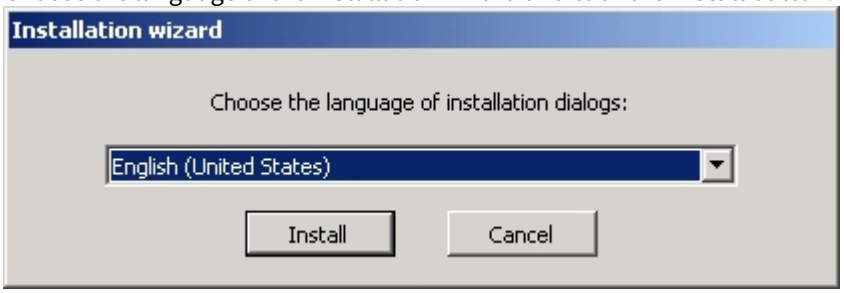
1. Before updating, we recommend you to back up all databases that you use—see Creating the database backup copy. Also, copy and save the **intellect.sec** license file (located in the root of the *Intellect* installation directory, by default: C:\Program Files/Intellect).
2. *Intellect* can be updated if there is a difference in the third digit of the version number and the first two digits are the same. If the first and/or second digits are different, you must reinstall *Intellect* instead of updating, i.e. uninstall the previous version and install the new one.
   Examples:
   a. you can update from version 4.11.1 to version 4.11.3;
   b. you cannot update from version 4.10.1 to 4.11.2, you need to reinstall.
3. Before starting the update, *Intellect* must be uploaded, if it is running.
4. You must run the update as Windows Administrator.
5. When you update *Intellect* on the Server or Remote Administrator's workstation, you should also update *Intellect* on Remote Client. The compatible versions of *Intellect* should be installed on Remote Clients and on the Server/ Remote Administrator's workstation, i.e. the first two digits of the version number should be the same (e.g. versions 4.10.4 and 4.11.0 aren't compatible, but versions 4.10.3 and 4.10.4 are compatible).
6. Starting with version 4.10.2, *Intellect* isn't compatible with the earlier versions in the distributed configuration.

To update *Intellect*, do the following:

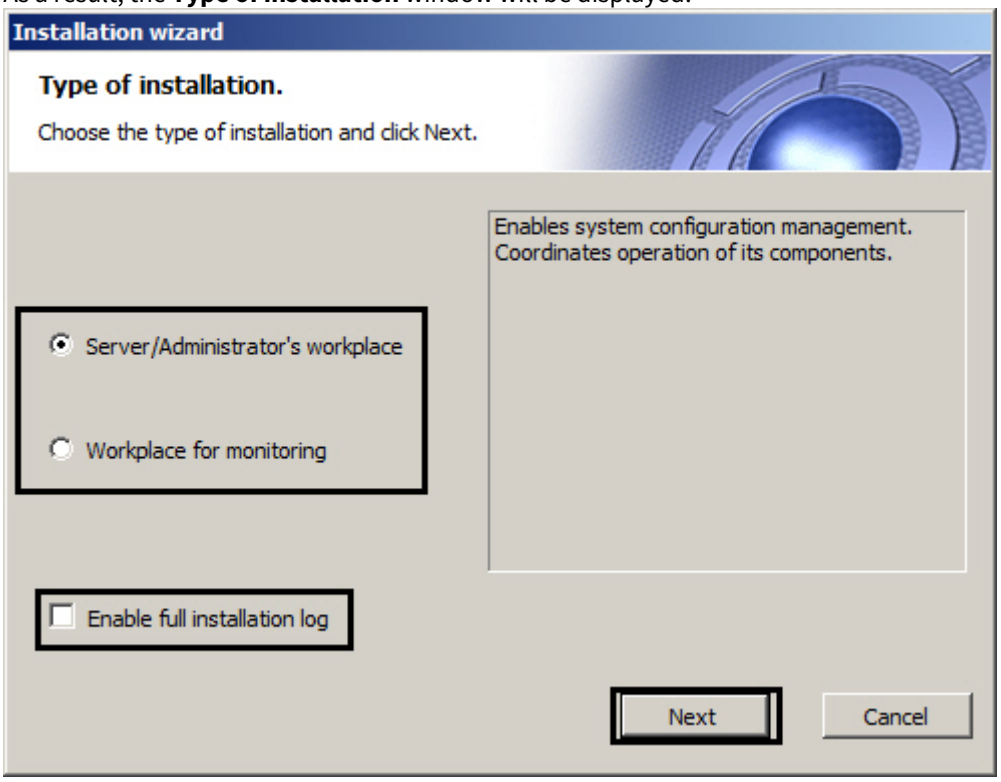
1. Unpack the installation kit as described in Getting ready for Intellect installation. The destination folder will show the contents of the kit.



2. Run the setup.exe file to start the *Intellect* installation procedure.
   As a result, a window for choosing the Installation wizard language will be displayed.
3. Choose the language of the Installation wizard and click the **Install** button.



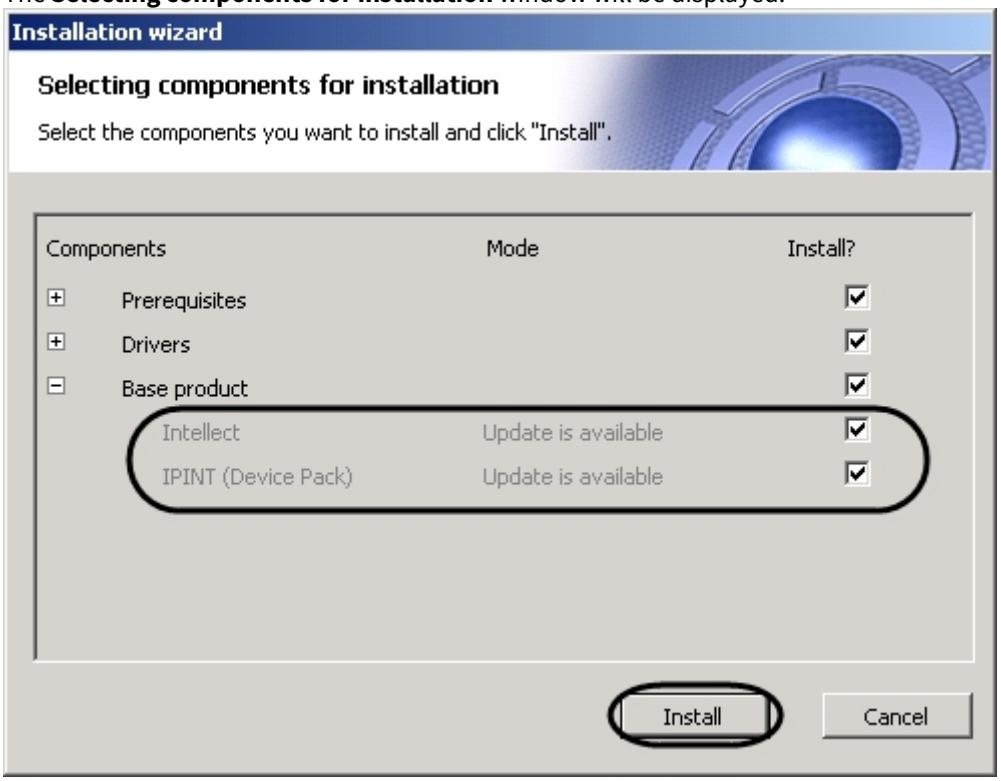
As a result, the **Type of installation** window will be displayed.



4. Choose the type of installation needed.
5. To log all installation events, set the **Enable full installation log** checkbox.

> **Note**
>
> While installing and uninstalling, the software events are logged to Intellect.log and Intellect uninstall.log correspondingly. To collect log files, use the Support.exe tool (see The utility for collecting configuration data on servers and RWS for the Technical Support*).*

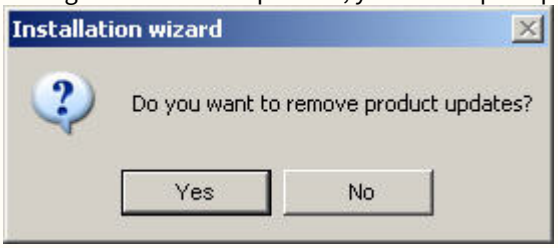
6. Click the **Next** button.
   The **Selecting components for installation** window will be displayed.



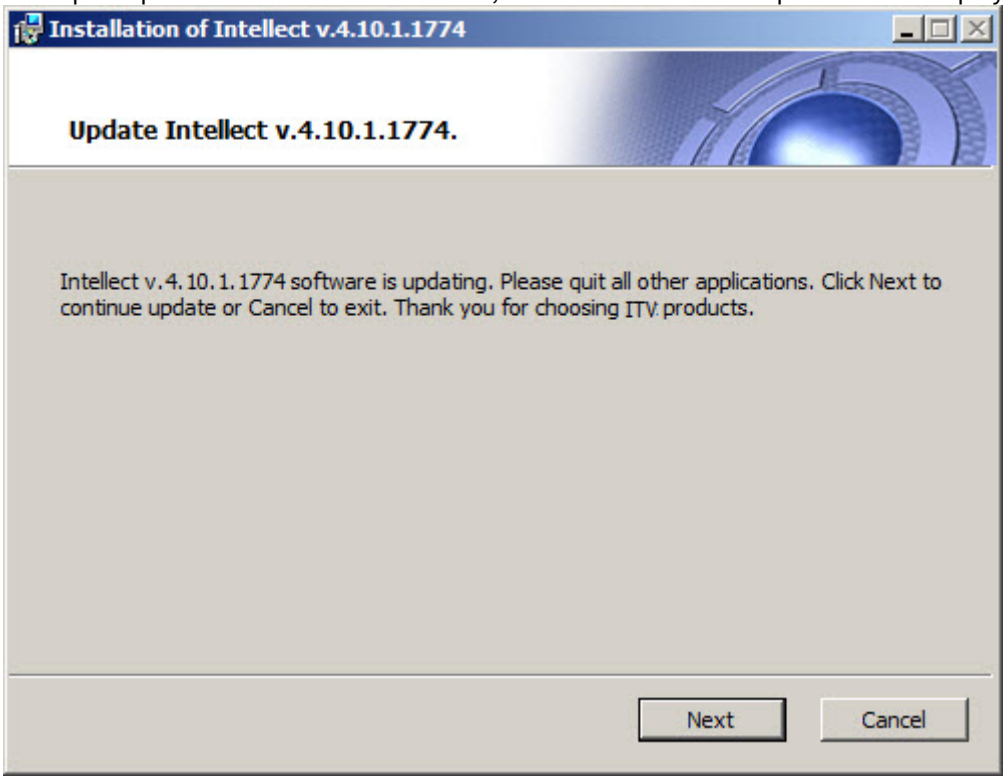
7. Set the checkboxes next to the components that you want to install.

> **Note**
>
> It is recommended to install all suggested components.

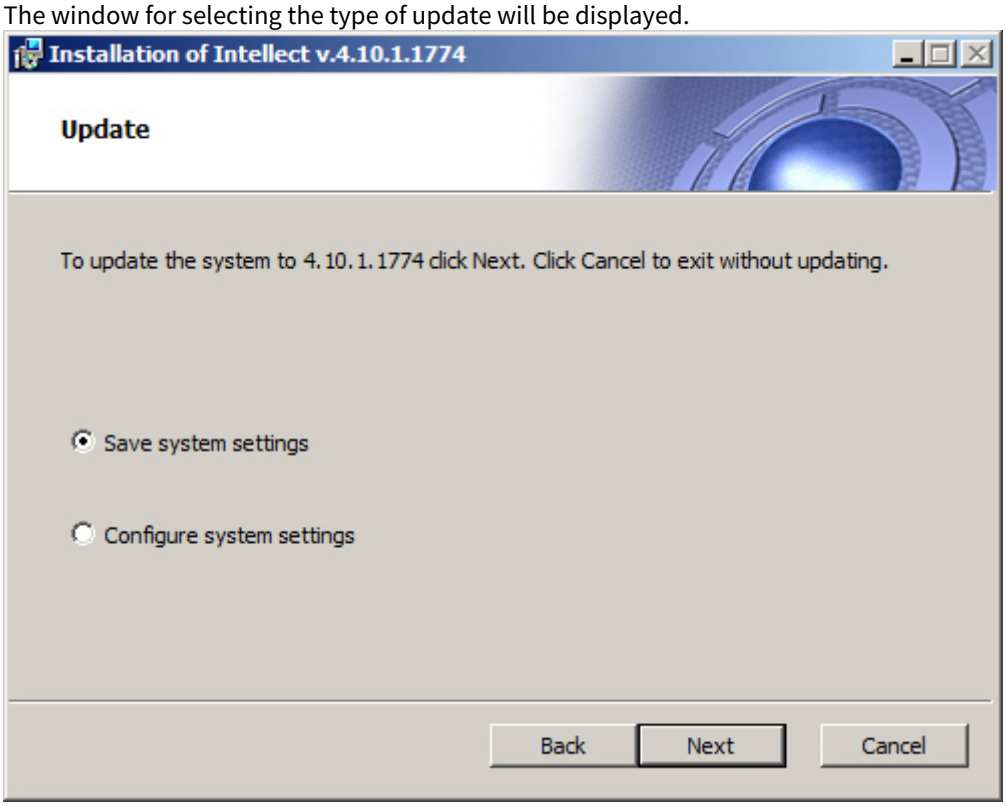
8. Click the **Install** button.
   The selected prerequisites and drivers will be installed.

> **Attention!**
>
> During the installation process, you will be prompted to remove the installed vertical solutions:
>
> 
>
>
> Two options are possible:
>
> a. If you click the **Yes** button, the vertical solutions will be removed during the update process. In this case, you will need to reinstall them after the update. Installation manuals are available in the documentation for each solution, links are on the main documentation page for Intellect 4.11.0-4.11.3. You should also consider version compatibility: General information about product releases and version compatibility.
> b. If you click the **No** button, the vertical solutions won't be removed and will be compatible with the new version of *Intellect* after the update.

When prerequisites and drivers are installed, the window of *Intellect* update will be displayed.



9. Click the **Next** button.
The window for selecting the type of update will be displayed.

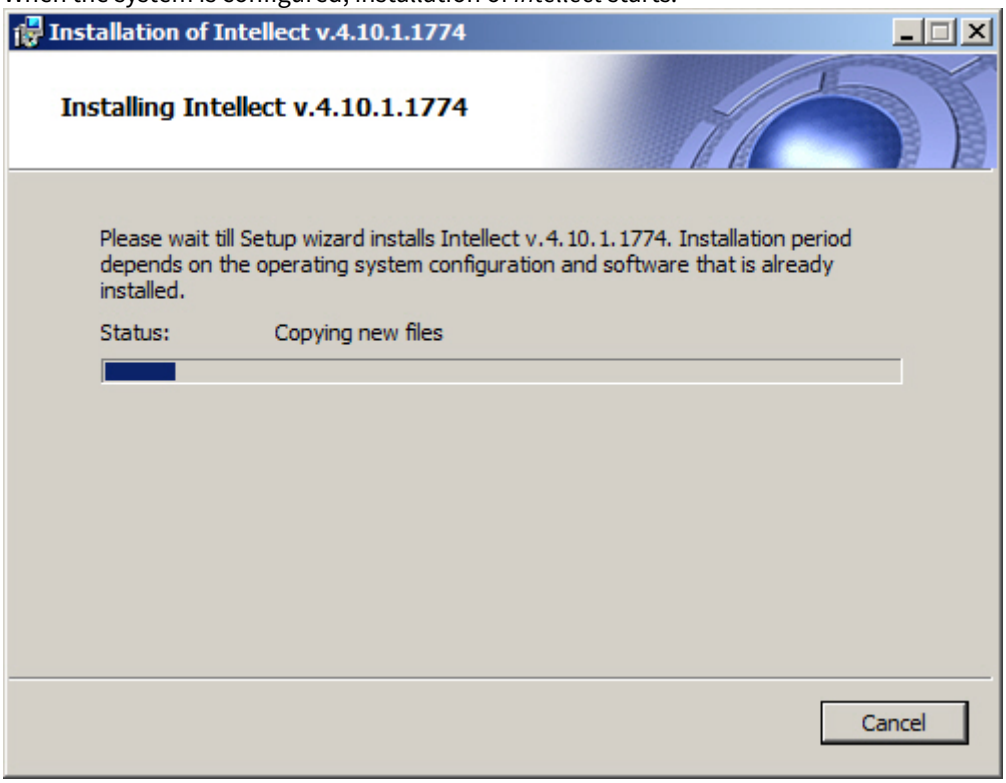


10. Select one of the suggested types of update. The types of update are described in the table below.

The types of update	Description
Save system settings	Use of settings chosen for installation of an earlier version

Configure system settings	Switch to step-by-step system configuration. Step-by-step configuration is described in Installation of Intellect as a Server/Remote Administrator's workstation

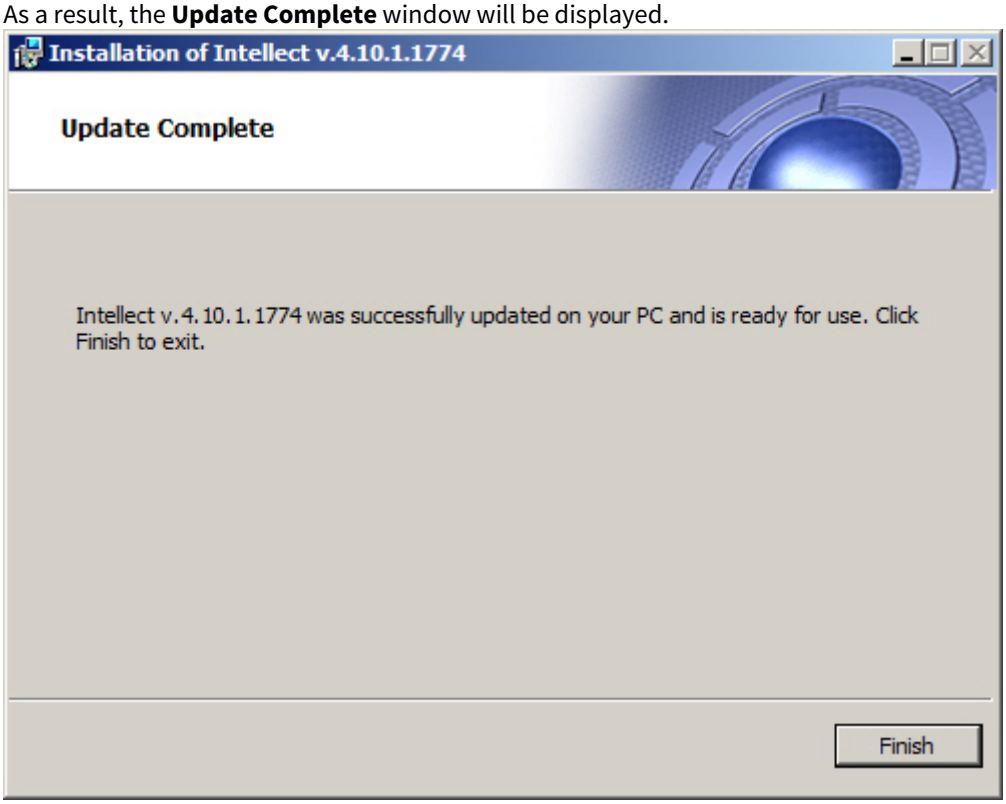
11. Click the **Next** button.
When the system is configured, installation of *Intellect* starts.



Note

When updating *Intellect* on Windows OS 7 SP1 without Internet connection, an error may occur during the installation of the drivers for the FX4 card. To eliminate this error, install the following missing Windows updates:
https://support.microsoft.com/en-us/kb/3004394
https://technet.microsoft.com/en-us/library/security/3033929

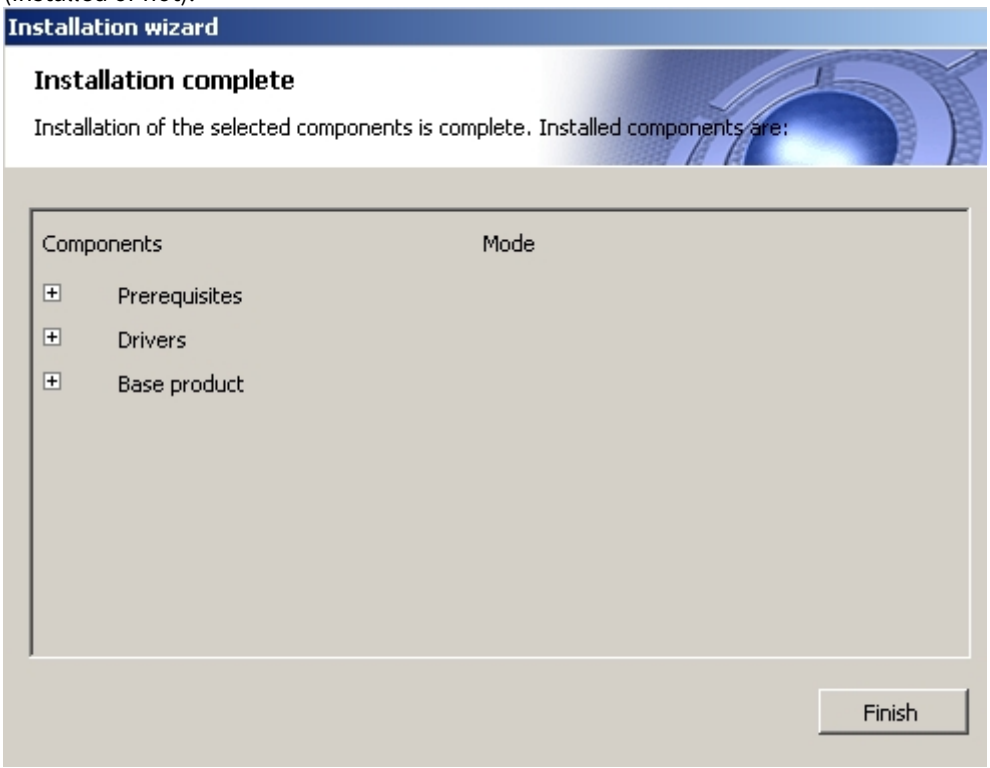
12. As a result, the **Update Complete** window will be displayed.



13. Click the **Finish** button.

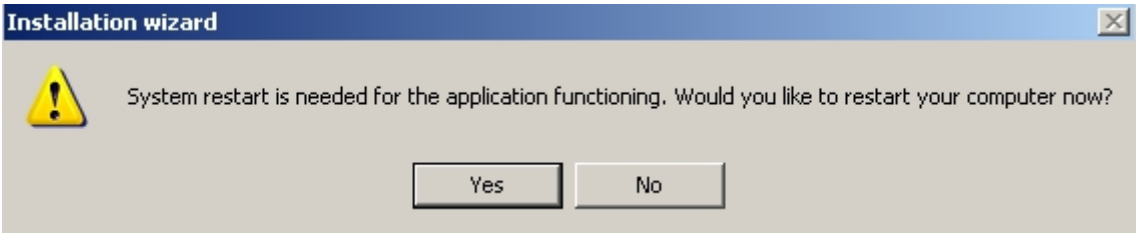
> **Note**
>
> Then the *DriversPack* will be installed if you selected this component.

The **Installation complete** window will be displayed. It contains the information about the *Intellect* components mode (installed or not).



14. Click the **Finish** button.

A window prompting to restart the computer will be displayed.



To correctly finish the installation of *Intellect,* you must restart the computer. If you don't choose to restart now, you will have to do it yourself after the installation.

Intellect is now updated.

Note

If you try to update *Intellect* to an older version, the updating process will go as described above, but the version will remain the same and there will be no changes in the software.

Updating Intellect installed as a Service
Remote update of Intellect
The Automatic Update Service

19.1.6 Using Product.msi and Redist.exe for Intellect installation

Besides running Setup.exe file for the the INTELLECT™ software installation, Product.msi and Redist.exe files can be used:

1. Product.msi is designed for INTELLECT™ software installation with step-by-step configuration of main parameters such as type of installation, installation directrory etc.

   Note.

   Product.msi is worth being used when all drivers, prerequisits and other components necessary for proper operation of INTELLECT™ being installed.

2. Redist.exe enables selection and installation of necessary components for INTELLECT™ operation (for example drivers, prerequisits and the very product).

The use of these files allows reducing installation time of INTELLECT™ software due to less steps during installation.

19.1.7 Separate installation of components for Intellect operation

The components that are required for *Intellect* operation are installed automatically when *Intellect* is installed, and you don't need to install anything additionally (see Installing Intellect). When updating *Intellect,* the latest versions of components are also installed. They match the version of *Intellect* that is being updated (see Updating Intellect).

Attention!

It is strongly recommended to install or update the components together with *Intellect* installation/update. A component separate update can lead to incompatibility with the main product. In this case, you will have to reinstall everything.

If you need to install or update the components without updating the main product, the following options are available:

1. For all components: run the Redist.exe executable file, which is included in the distribution package of the required version, select the necessary components to install (see Using Product.msi and Redist.exe for Intellect installation).
2. For IP Drivers Pack, two ways are described on the page Updating Drivers Pack separately from the main product.
3. For the language pack: install LanguagePack downloaded from the website (see Installing the language).

19.1.7.1 Updating Drivers Pack separately from the main product

The version of Drivers Pack that matches the *Intellect* base version is installed together with *Intellect.* It is not recommended to update Drivers Pack separately, as this may cause its incompatibility with the main product. In this case, you will have to reinstall everything.

This manual describes the options for updating Drivers Pack separately from the *Intellect* update, in cases when you want to revert to an earlier version of Drivers Pack or install a newer version of Drivers Pack saving the current *Intellect* version.

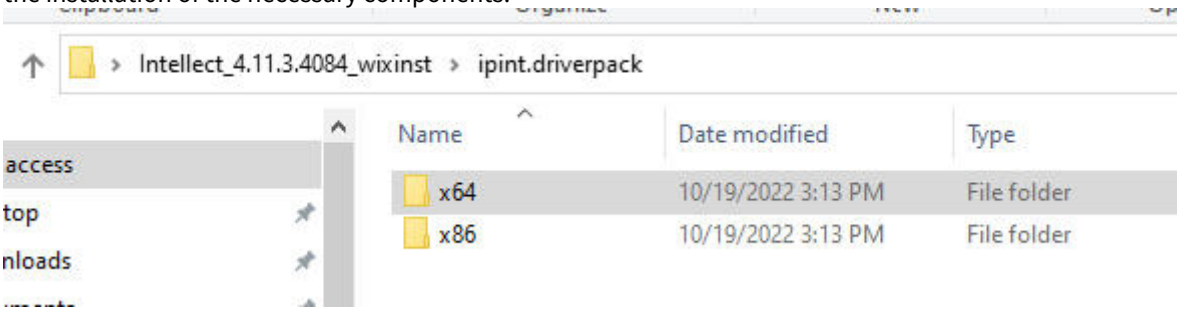
For the information on the *Intellect* versions and Drivers Pack compatibility, see Documentation Drivers Pack and the webpage https://www.axxonsoft.com/products/integration/supported-ip.

Attention!

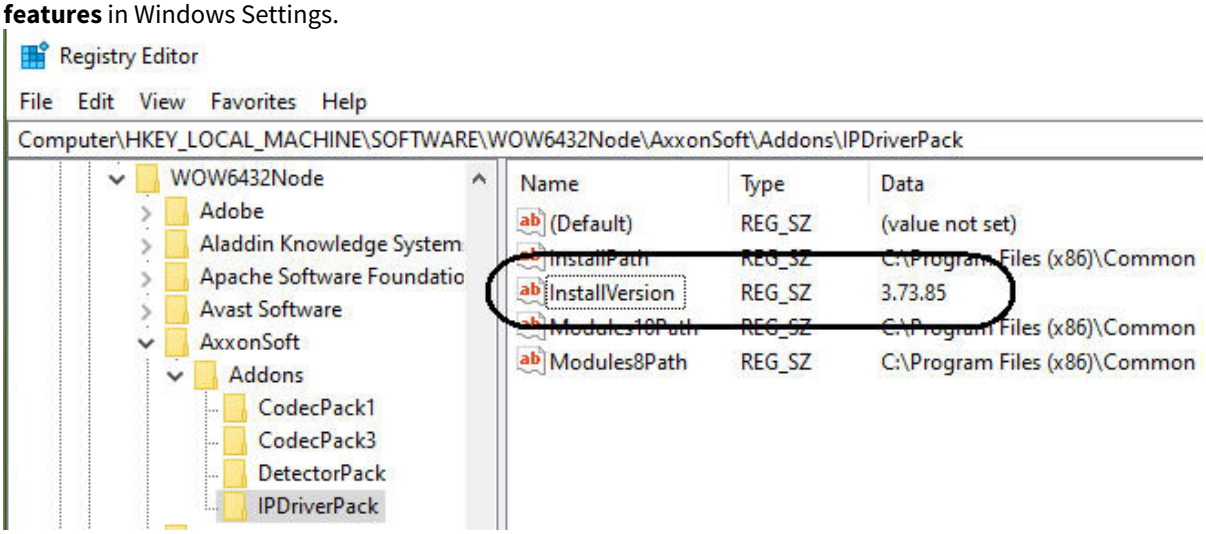
If you want to install a newer version of Drivers Pack, you don't need to uninstall the previous version.
If you want to install an earlier version of Drivers Pack, you will need to uninstall the current version and then install the version you need.

19.1.7.1.1 Installation without uninstalling the previous version

1. In the *Intellect* distribution package containing the required version of Drivers Pack, go to the **ipint.driverpack** folder and one-by-one run the **IPDriverPack.msi** files for x64 and x86 (located in the x64 and x86 folders respectively). Each file starts the installation of the necessary components.

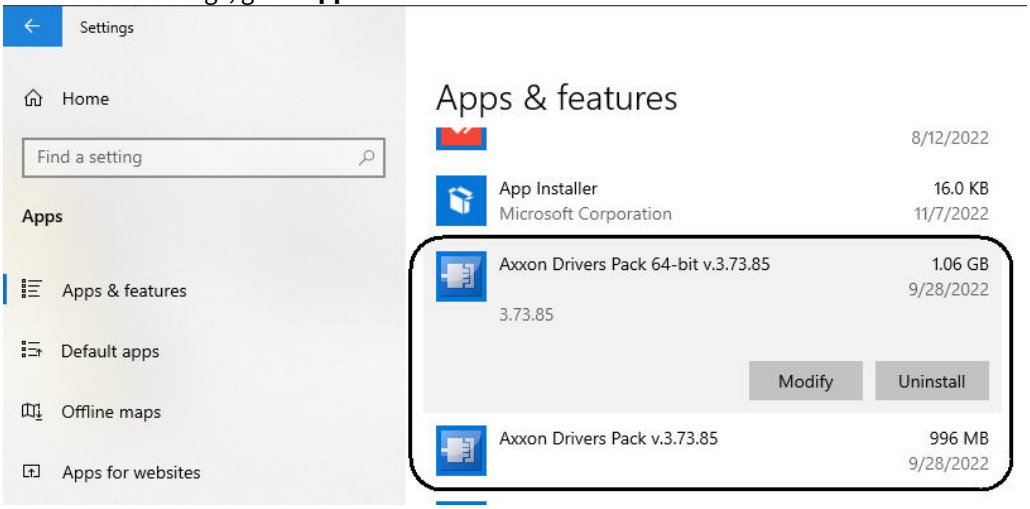


2. After the installation is finished, check if it was successful. To do this, in the **Registry Editor** in the path Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\AxxonSoft\Addons\IPDriverPack, check the **InstallVersion** key. The version you installed should be specified. You can also check the version of Drivers Pack in **Apps & features** in Windows Settings.

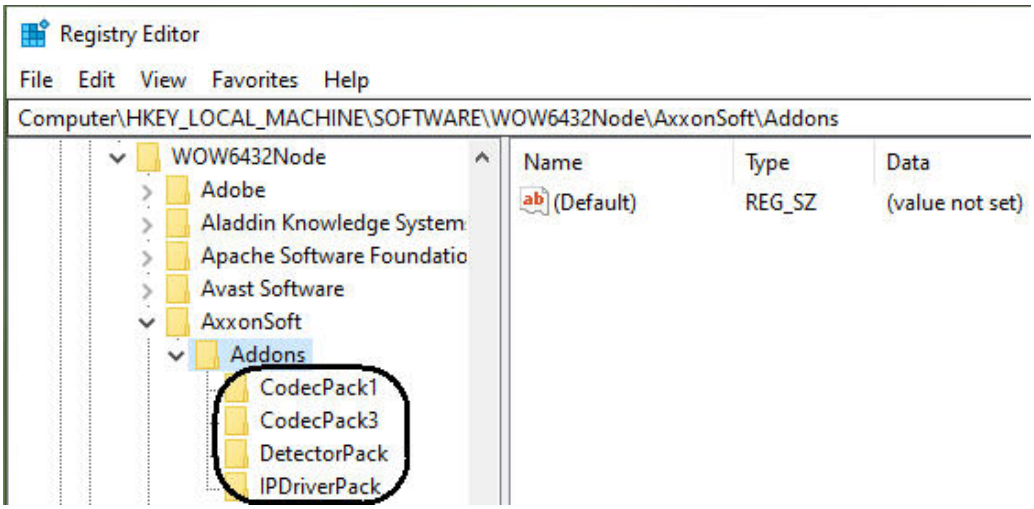


19.1.7.1.2 Installation with uninstalling the previous version

1. In Windows Settings, go to **Apps & features** and uninstall **Axxon Drivers Pack 64-bit** and **Axxon Drivers Pack**.



2. In the **Registry Editor** on the path Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\AxxonSoft\Addons\IPDriverPack, delete all contents of the **Addons** subsection.



3. Delete all contents of the **C:\Program Files\Common Files\AxxonSoft** folder.
4. Install Drivers Pack by running the **IPDriverPack.msi** files of the correct version as described above. Check if the installation was successful.

As a result, the new version of Drivers Pack will be installed, but the *Intellect* version will remain the same.

19.1.8 Possible installation problems and their solutions

On the page:

- Error while installing driver for the FX4 card
- Error code 26352

19.1.8.1 Error while installing driver for the FX4 card

Error of driver installation for the FX4 card can occur while the *Intellect* software installation on the Windows 7 SP1 operating system without Internet connection. To eliminate this error install the following missing Windows updates:

https://support.microsoft.com/en-us/kb/3004394

https://support.microsoft.com/en-us/kb/3033929

19.1.8.2 Error code 26352

Error 26352 may occur if *Intellect* is being installed on an operating system with applied information security policies. This error code means that the problem is related to installing driver signature certificates. These certificates are valid for one year. If the OS security settings do not allow to install drivers with expired certificates and the certificates themselves, the installation is interrupted with an error.

To solve this problem, please download a newer *Intellect* distribution kit. It is available on the web-site https://www.axxonsoft.com/resources/downloads/intellect.php or by request to the technical support at https://support.axxonsoft.com.

19.2 Restoring Intellect

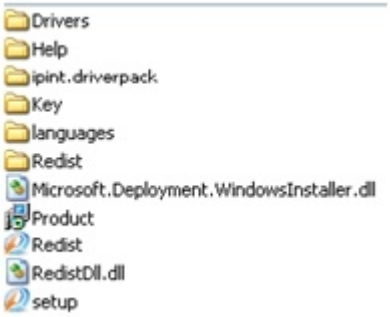
The restore mode is used to reinstall all *Intellect* components. Use this function when, for example, some files were accidentally deleted from the installation directory.

To launch the restore mode, you need to restart *Intellect* installation without deleting the previous version. To restore *Intellect* correctly, make sure that the distribution package is located in the same path as it was during installation or that the operating system is configured to save the *.msi files in the cache.

> **Note**
>
> To reinstall *Intellect* correctly, close all applications on the computer before the reinstallation startup.

To restore *Intellect*, do the following:

1. Open the folder containing the unpacked distribution package.



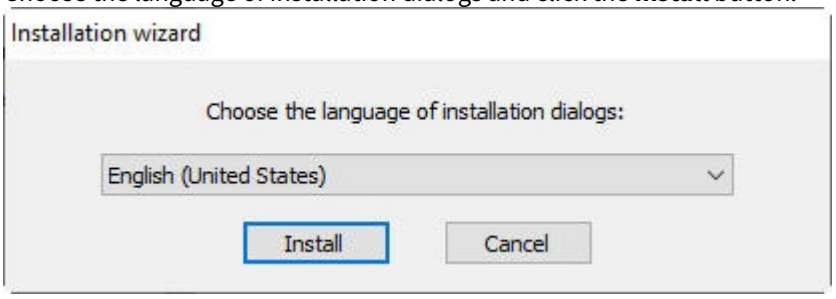
> **Note**
>
> Here we describe how to restore *Intellect* using the installer. The same process can be started using the uninstaller: open Windows Start menu → Settings → Apps, find *Intellect* in the list and click **Uninstall**. The uninstaller window will open, select the **Repair** option and proceed according to this manual.

2. Run the Setup.exe executable file used for running *Intellect* installation program.
   As a result, the Installation wizard dialog box is displayed.

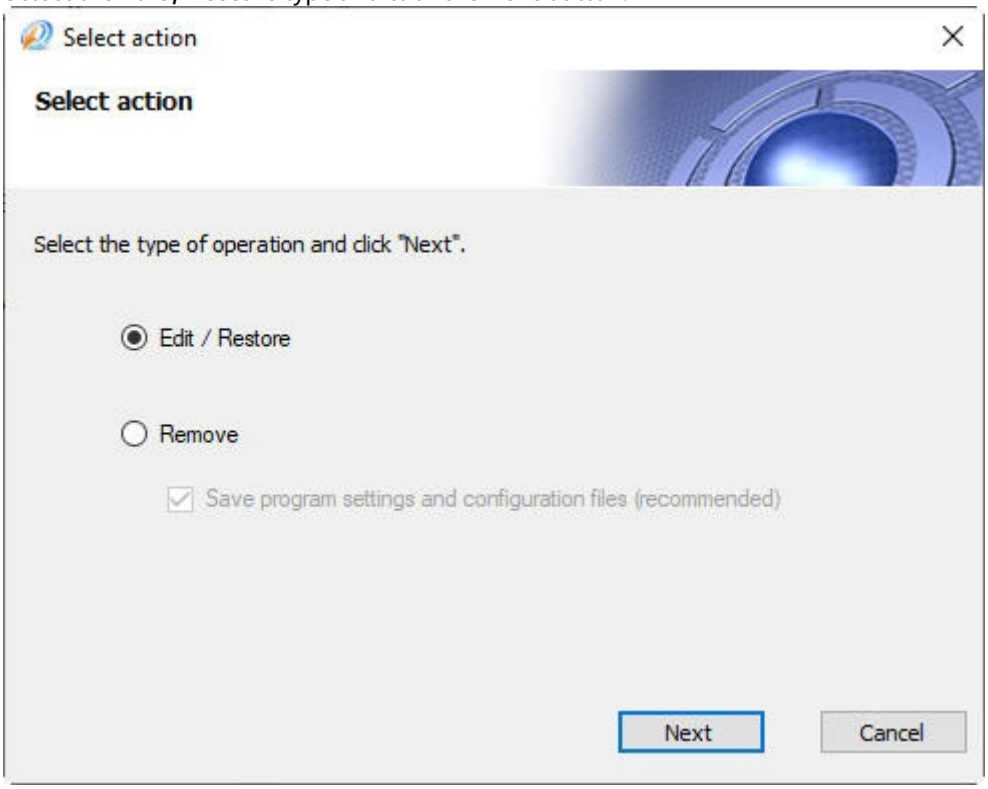
> **Note**
>
> The following files may be run for restoring *Intellect* instead of Setup.exe:

a. Product.msi—to restore *Intellect*;
b. Redist.exe—to install additional components.

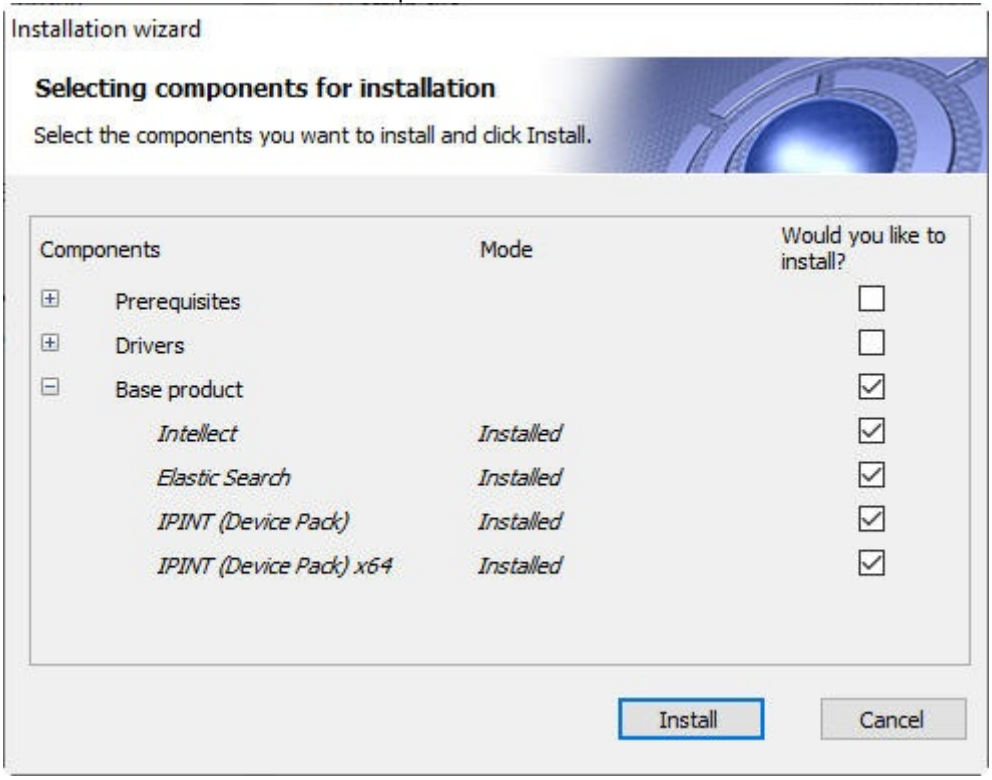
3. Choose the language of installation dialogs and click the **Install** button.



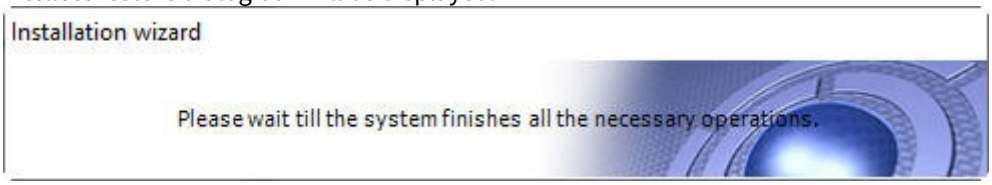
4. Select the **Edit / Restore** type and click the **Next** button.



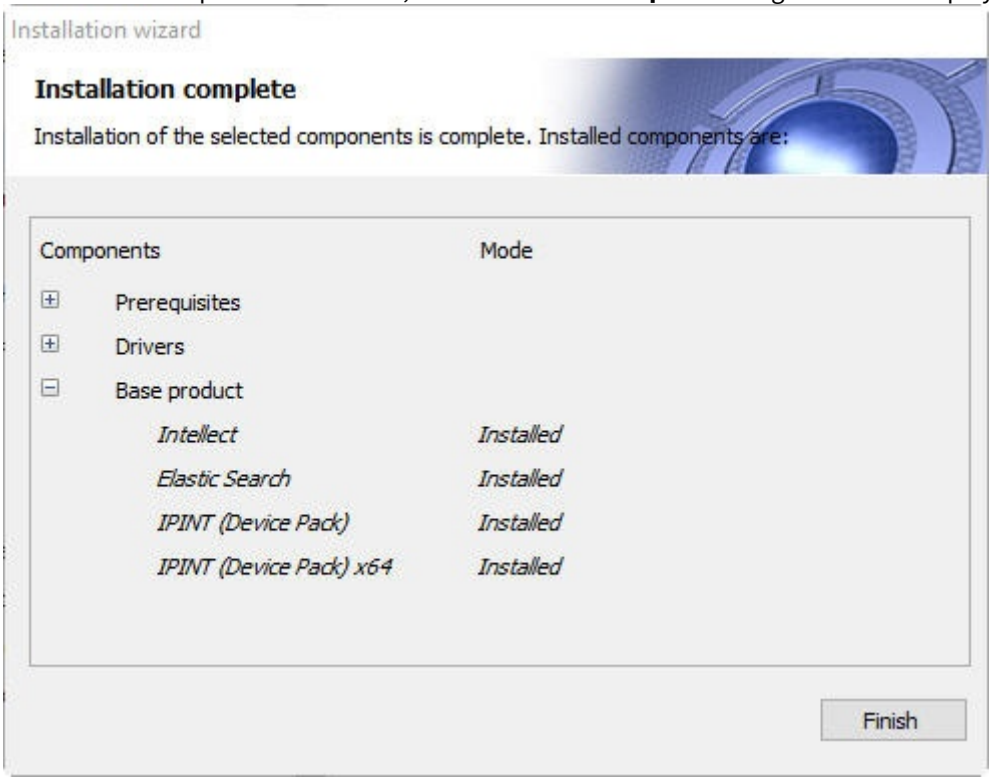
5. Set the checkboxes next to the components that need to be restored and click the **Install** button.



Intellect restore dialog box will be displayed.



When the restore process is finished, the **Installation complete** dialog box will be displayed.



6. Click the **Finish** button.

Intellect is now restored.

19.3 Removing INTELLECT™ software

Intellect software installation program works in a deletion mode. This mode is required when all the components of the *Intellect* software should be deleted.

> **Note.**
>
> Before starting the deletion process of the *Intellect* software all the other applets should be closed on the computer.

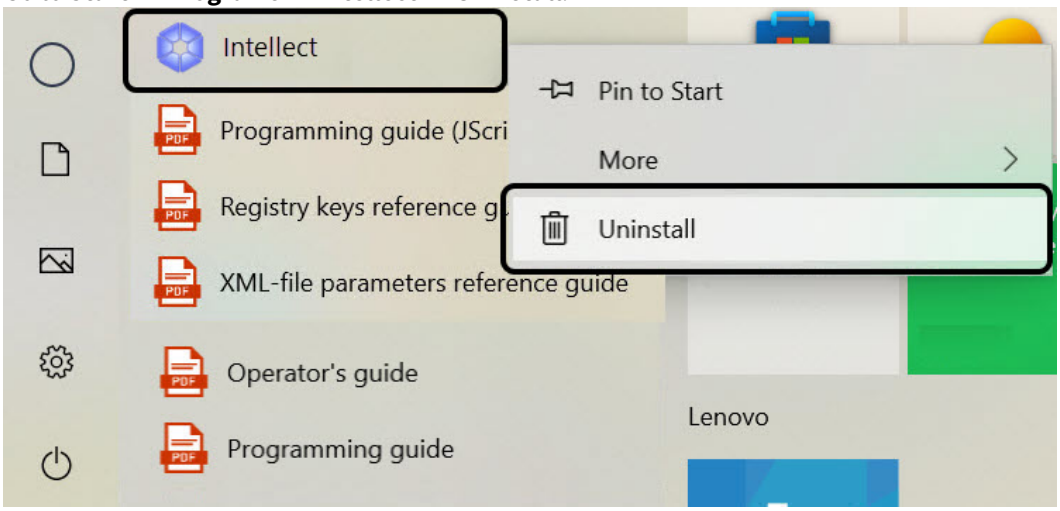
The *Intellect* software removal process can be launched using one of the following ways:

1. Using the Start menu;
2. Using OS Windows panel «Add or remove programs»;
3. Using the installation kit.

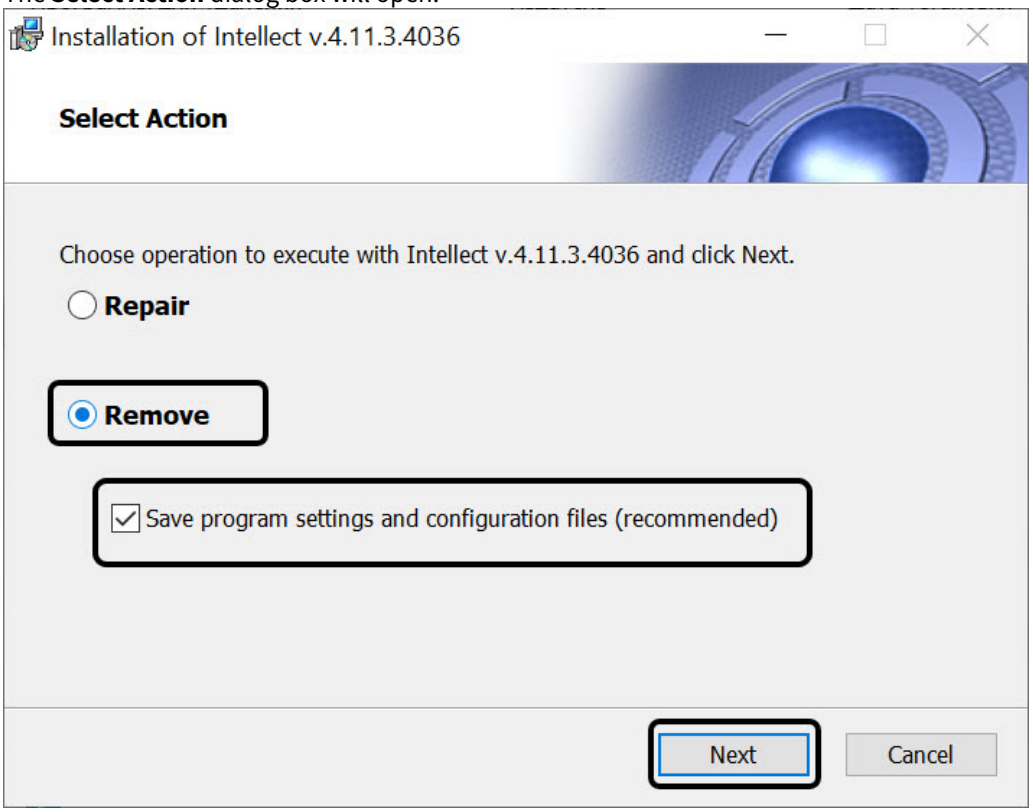
19.3.1 Removing Intellect from the Start menu

To remove *Intellect* from the **Start** menu, do the following:

1. Go to **Start** → **Programs** → **Intellect** → **Uninstall**.



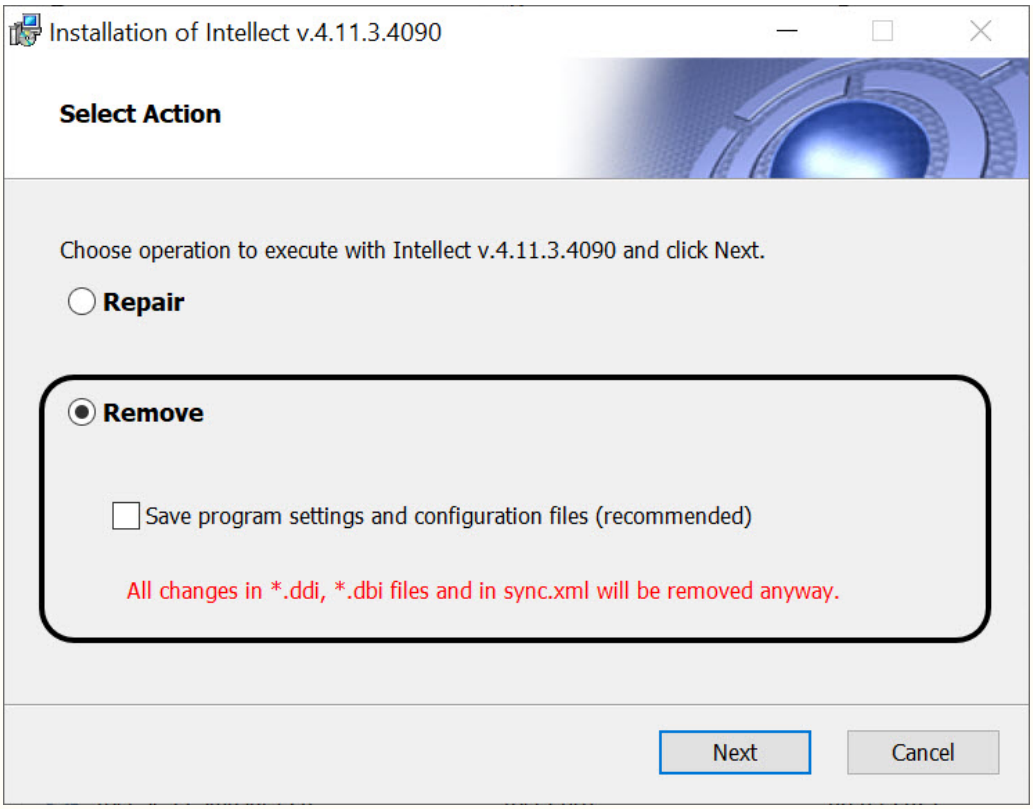
The **Select Action** dialog box will open.



2. Select the **Remove** action.
3. If you want to save *Intellect* settings in the database, set the **Save program settings and configuration files (recommended)** checkbox.

> **Note**
>
> If the sync.xml file was changed, then after removing with the configuration saved, the file will not be deleted, but the next time you install *Intellect,* it will be overwritten.
> If you made changes to the ddi or dbi files installed with *Intellect*, using the ddi.exe utility, then these files will be deleted when removing *Intellect* with configuration saved. If you created new ddi or dbi files, they will be saved.

> **Attention!**
>
> If the **Save program settings and configuration files (recommended)** checkbox is clear, a warning message will appear.

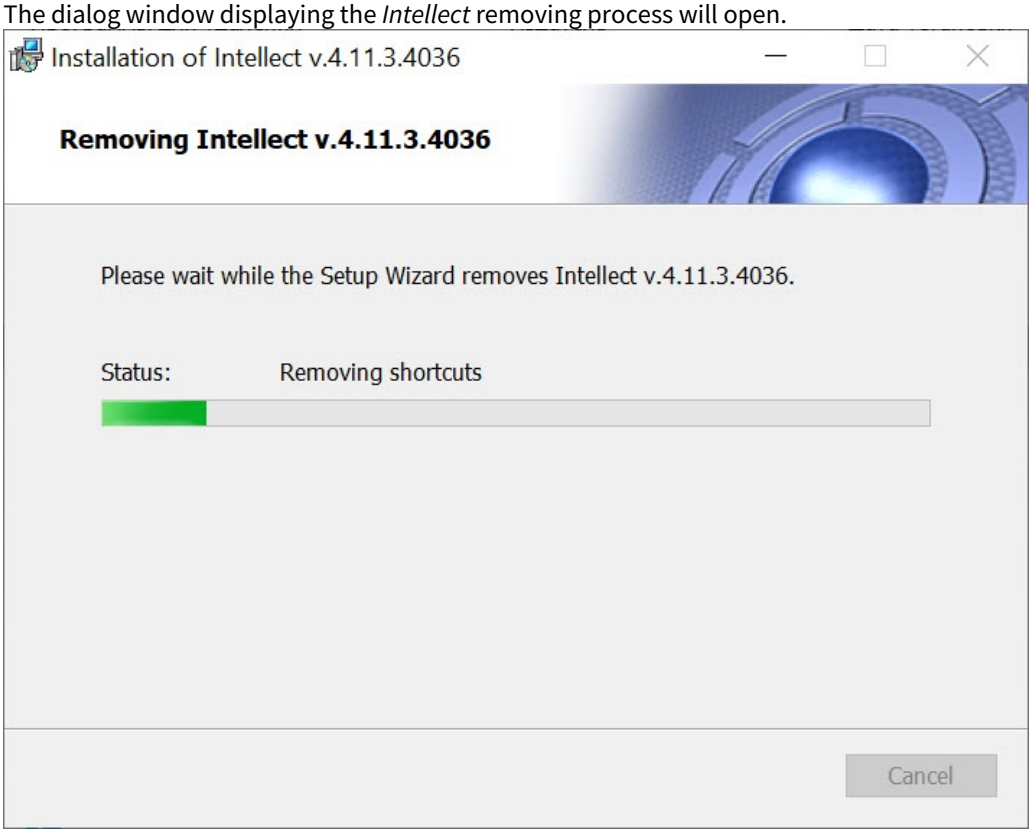


When removing *Intellect* without configuration saved, all ddi and dbi files, as well as the sync.xml file, will be deleted.

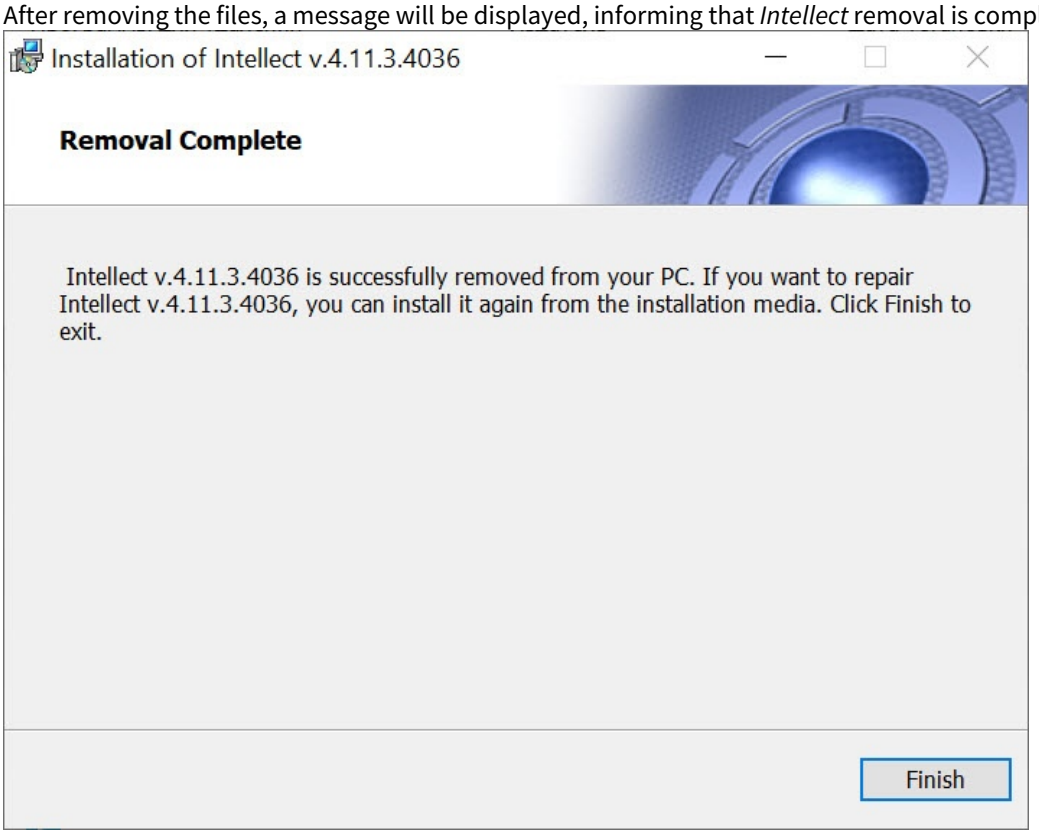
4. Click the **Next** button.

> **Note**
>
> Click the **Cancel** button to cancel *Intellect* removing.

The dialog window displaying the *Intellect* removing process will open.



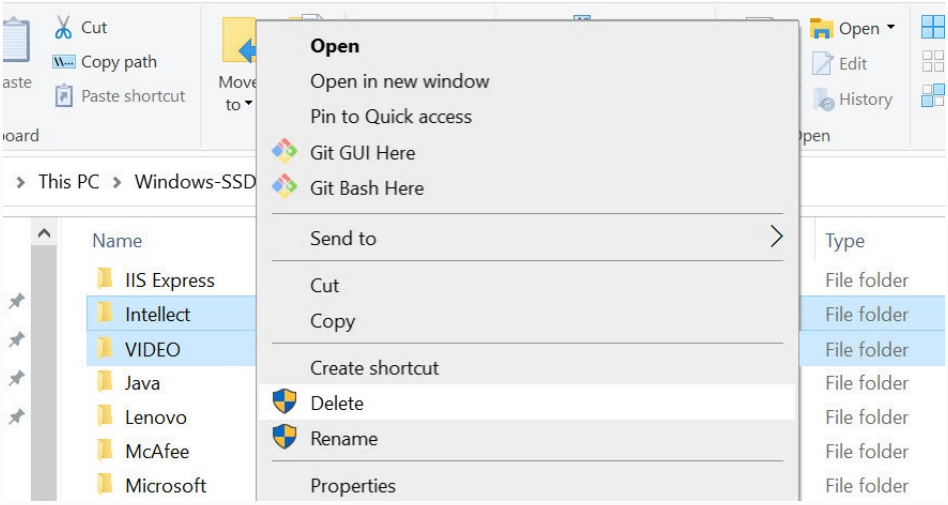
After removing the files, a message will be displayed, informing that *Intellect* removal is complete.



5. Click the **Finish** button.

Note

To completely remove *Intellect,* you should manually delete the *Intellect* installation directory and all Video folders created for storing audio and video recordings.



Note

Note, that the name of the *Intellect* installation directory may differ from the default name (C:\Program Files\Intellect).

Note

In some cases, you may need to restart Windows OS before removing the *Intellect* installation directory (for instance, folders/Intellect).

Note

We don't recommend removing the *Intellect* installation directory, if you plan to re-install *Intellect*. The directory contains:

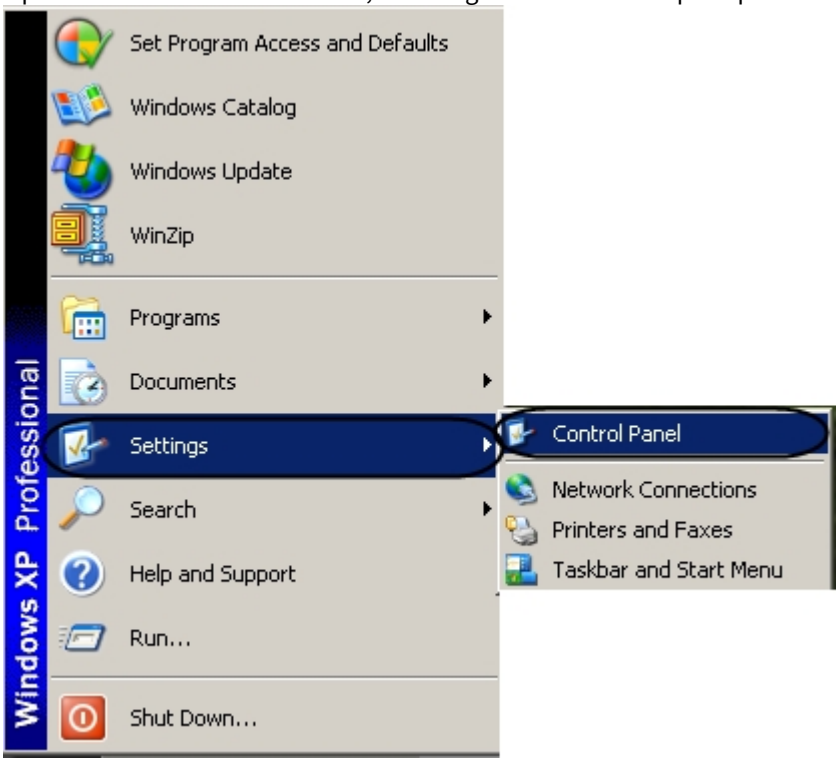
1. Folders with video recordings and video recordings frames exported during *Intellect* operation.
2. Log files containing the information about *Intellect* module operations.
3. Backup copies of these files.

Removing *Intellect* from the **Start** menu is complete.

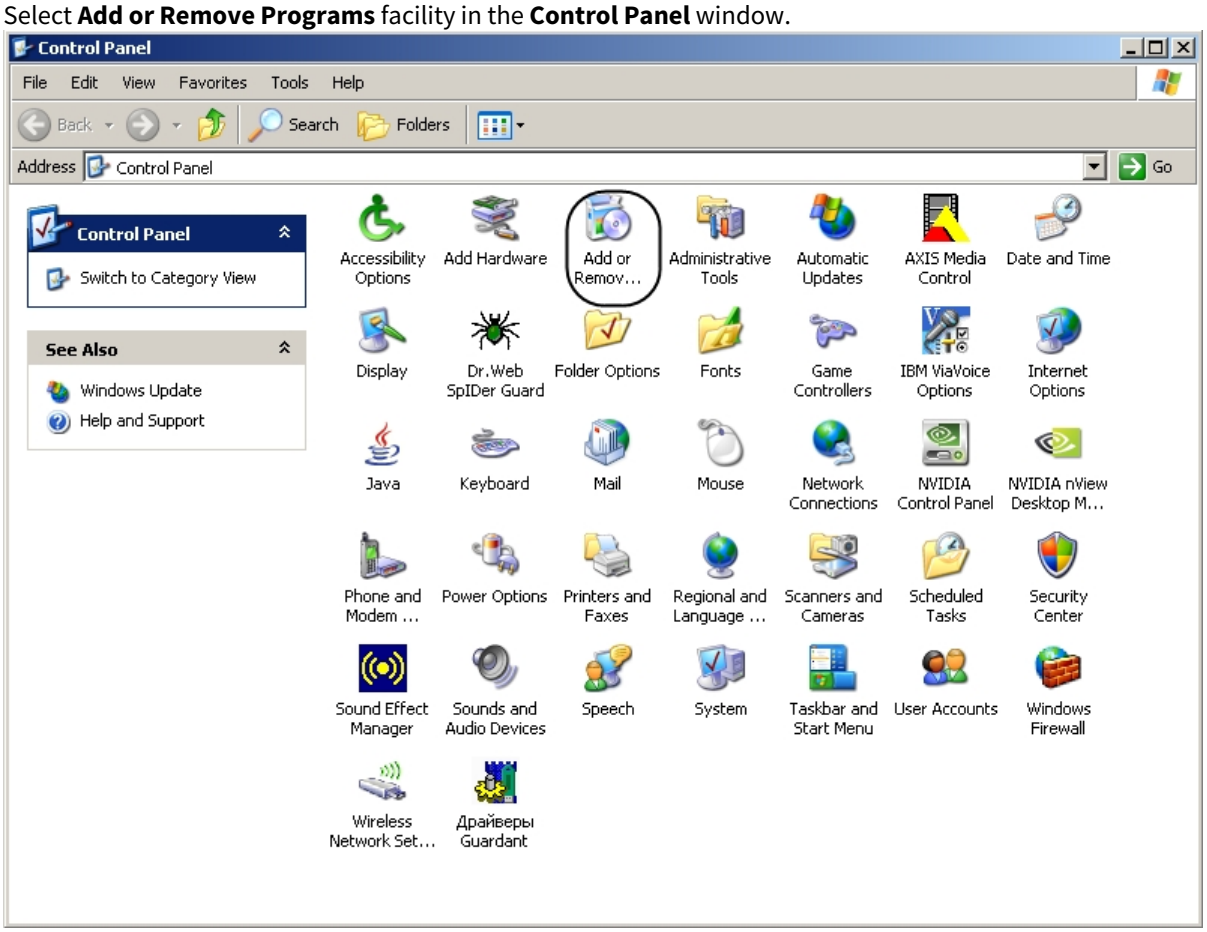
19.3.2 Removing INTELLECT™ software from the OS Windows panel Add or Remove programs

To uninstall Intellect™ system using A**dd or Remove Programs** facility, follow the next steps:

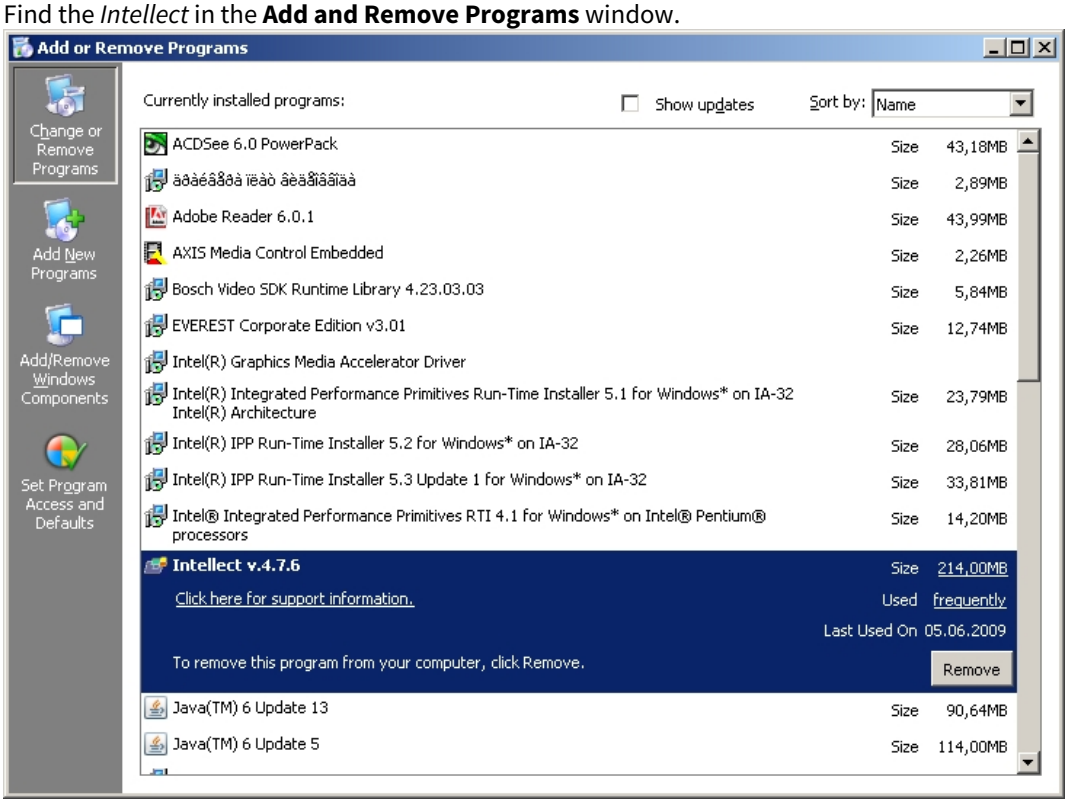
1. Open the **Control Panel** window, selecting in the command prompt: **Start ->Settings ->Control Panel**.



2. Control panel dialog window will be displayed.
3. Select **Add or Remove Programs** facility in the **Control Panel** window.



Find the *Intellect* in the **Add and Remove Programs** window.



4. Click the **Remove** button next to the name of Intellect program.
   As a result the **Select Action** dialog box is displayed.
5. Follow steps 2-5 of the instruction in section Removing Intellect from the Start menu.

At this stage the deletion process of Intellect software with the help of OS Windows **Add or Remove program** panel is over.

19.3.3 Removing INTELLECT™ software using the installation kit

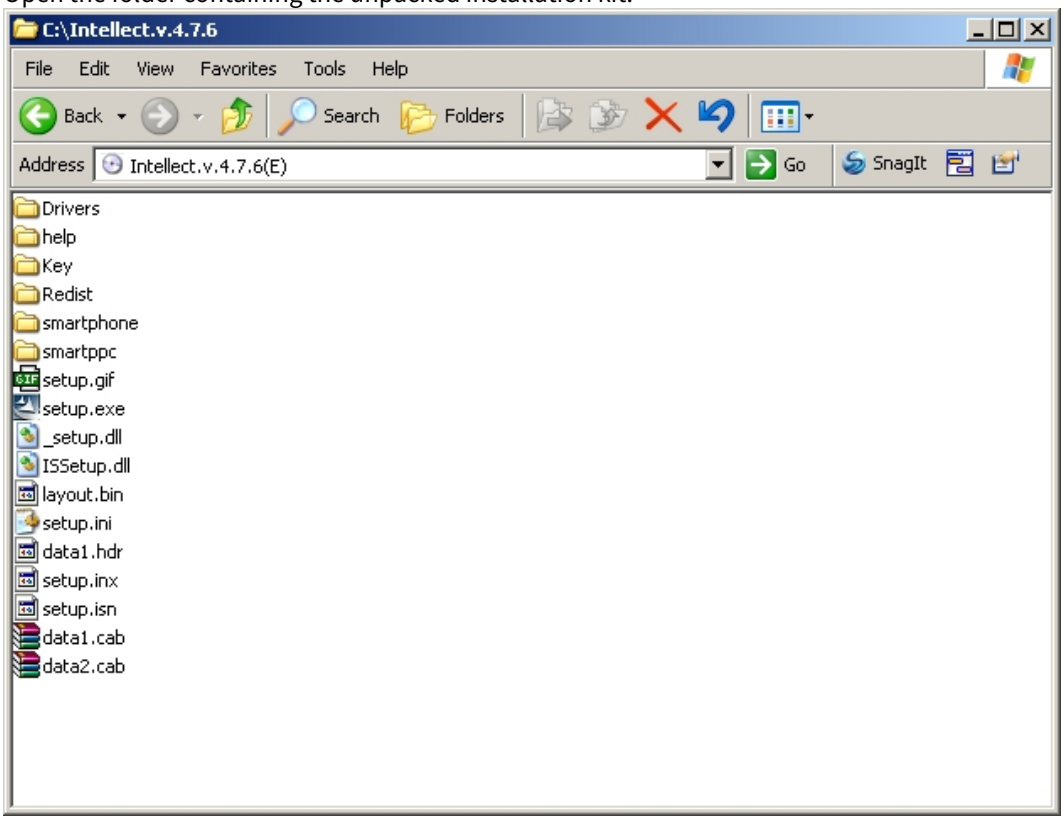
Intellect installation wizard can run in a deletion mode. This mode is required when all the components of the *Intellect* software should be deleted.

Run the installation wizard without removing the previous version of the *Intellect* software to run installation program in a deletion mode.

> **Note.**
>
> Before starting the deletion process of the *Intellect* software all the other applets should be closed on the computer.

To delete Intellect software do the following:

1. Open the folder containing the unpacked installation kit.



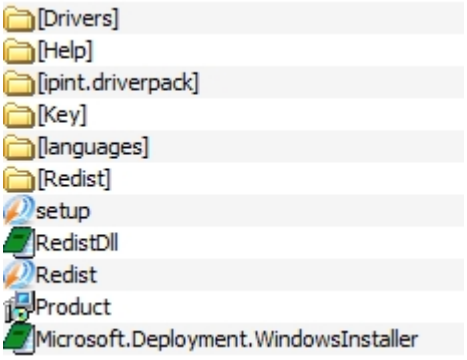
2. Launch the file Setup.exe
   As a result the **Select Action** dialog box is displayed.
3. Follow steps 2-5 of the instruction in section Removing INTELLECT™ software from the Start menu.

At this stage the deletion process of Intellect software with the help of installation kit is over.

19.3.4 Removing INTELLECT™ software installed as a Service

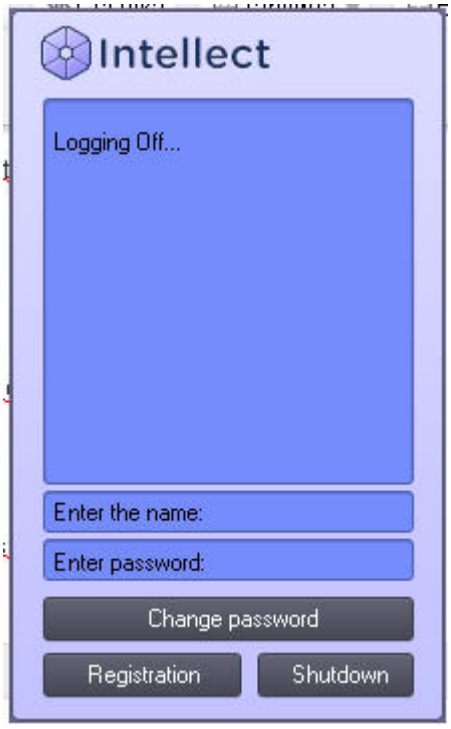
To remove *Intellect* software , installed as a Service, do the following:

1. Open the folder containing the unpacked installation kit.



2. Run setup.exe.
   As a result the **Select Action** dialog box is displayed.

When *Intellect* works it will be automatically logged off.



3. Follow steps 2-5 of the instruction in section Removing INTELLECT™ software from the Start menu

At this stage the deletion process of *Intellect* software installed as a Service is over.

19.4 Installing INTELLECT™ software in a silent mode

There is possibility to run the *Intellect* software in a silent mode (without user interface).

Note.

While installation program operation it may be required to restart the system. The installation will be continued automatically after the system is restart.

Note.

When installing in invisible mode on Windows 7 and Windows Server 2008 R2, all Windows Update updates are to be installed, then use HotFix available at link on the Microsoft website or here. As a result, there will be no messages about the unreliable publisher during the installation of drivers.

Important!

Consider version compatibility when performing silent update. If *Intellect* is updated to a version whose second and/or third number is larger than that of the currently installed version (for example, from version 4.10.4 to 4.10.5, or 4.9.5 to 4.10.5), compatibility is lost with industry-specific vertical solutions built for old versions. This is why all vertical solutions are deleted by default unless you use the /saveaddons parameter.
If build number differs, e.g. 4.10.5.200 is updated to 4.10.5.300, vertical solutions remain unchanged.

The redist.exe process finish in Windows task manager indicates that the program has been installed.

This installation type is performed by setting setup.exe install file parameters in the OS Windows command prompt. The install file parameters are given in the table below.

The install file parameter in the command prompt	Description

/?	Help window call
/help	Help window call
/x /removeall	The Intellect software deletion without saving the configuration
/x /uninstall	The Intellect software deletion saving the configuration
/r	The Intellect software repair
/repair	The Intellect software repair
/qn	The Intellect software installation/update
/quiet	The Intellect software installation/update
/norestart	Disabling the auto restart of the system while it is being installed
/LANG=”ru”	Russian language selection of installation program
/LANG=”en”	English language selection of installation program
/INSTALLTYPE="Client"	Selecting the **Monitor workstation** installation type
/INSTALLTYPE="Server"	Selecting the **Server** installation type
/INSTALLTYPE="Admin"	Selecting the **Admin workstation** installation type
/ADD="[]"	A list of components necessary for installation. Is used if a component that is not installed by default is to be installed. Possible values are given in the next table.
/REMOVE="[]"	A list of components that are not to be installed. Possible values are given in the next table
/CMD="[commands]"	Values of functions for basic installation program. Where commands mean [Function] =\"[Value]\" or [Function] ='[Value]'. Available functions of installation program are given in the last table in the section.
/debug	Enable verbose logging.
/noOSCheck	Supress checking OS version
/dpcmd="INSTALL_BOSCH_VIDEOSDK=\"no\""	Installation of Bosch VideoSDK driver (see Note): no – do not install; yes – install.
/saveaddons	Do not delete any vertical solutions

Important!

In some cases **Bosch VideoSDK** installation results in displaying of the command prompt window which must be closed in order to proceed with the installation.

Note.

In the help window of installation program there are two examples identical in functional which differ by type of parameter's entering /CMD (table above, parameter's value /CMD).

Possible values of /ADD and /REMOVE parameters:

Architecture x86	**Architecture x64**
BaseIntellect	BaseIntellect
IPDriverPack_x86	IPDriverPack_x86
-	IPDriverPack_x64
Acrobat	Acrobat
dotnetfx35_x86	dotnetfx35_x86
JRE_x86	JRE_ amd64
MsXml	MsXml
Redist2005_x86	Redist2005_x86
SQLServer_x86	SQLServer_ amd64
WindowsInstaller_x86	WindowsInstaller_ amd64
WindowsPowerShell20_x86	WindowsPowerShell20_x amd64
Guardant_x86	Guardant_ amd64
Dotnet40	Dotnet40
Redist2010_x86	Redist2010_x86
-	Redist2010_x64
ReportViewer	ReportViewer

Installation program features:

Installation program features	**Description**
CREATE_QUICKLAUNCH_SHORTCUT='1'	Create quick launch shortcut (is used by default)
CREATE_QUICKLAUNCH_SHORTCUT='0'	Do not create quick launch shortcut
CREATE_DESKTOP_SHORTCUT='1'	Create shortcut on the desktop (is used by default)

CREATE_DESKTOP_SHORTCUT='0'	Do not create shortcut on the desktop
ADDLOCAL='[]'	A list of components for installation. Available values : 1) Utils – the utilities included in the Intellect system are installed 2) AxxonSoft VideoDrivers – drivers by AxxonSof company are installed; 3) Wav – sound notification files are installed. All the components are installed without ADDLOCAL='[]' command. Example. ADDLOCAL='Wav' – Intellect system and sound notification files are installed.
REMOVE='[]'	A list of components that are not to be installed. Available values: 1) Utils – the utilities included in the Intellect system are not installed; 2) AxxonSoft VideoDrivers – drivers by AxxonSoft company are not installed; 3) Wav – sound notification files are not installed. All the components are installed without REMOVE='[]' command. Example. REMOVE ='Utils' – Intellect, divers and sound notification files are installed. The utilities are not installed.
Functions of the “Server” and “Admin workstation” installation types	
INSTALL_AS_SERVICE='1'	Installation as a service
PATHTOKEYFILE='[%SourceDir%]'	Specify the path to the Key folder with license key
LANGUAGE='[en]'	Select the language of the Intellect system
SQL_AUTHTYPE='Windows'	Selecting the ”Windows accounts” user authentication method
SQL_AUTHTYPE='Sql'	Selecting the “SQL authentication” user authentication method
SQL_USERNAME='[sa]'	Setting the user name for the “SQL authentication” method
SQL_PASSWORD='[]'	Setting the password for the “SQL authentication” method
General functions:	
DB_INTELLECT_NAME='[intellect]'	Specifying the main database. It is not relevant when SQL_AUTHTYPE='Windows'
DB_TITLES_NAME='[titles]'	Specifying the titles database. It is not relevant when SQL_AUTHTYPE='Windows'
SQL_INSTANCE='[(local)\SQLEXPRESS]'	Specifying the database server. It is not relevant when SQL_AUTHTYPE='Windows'

Example of running the Intellect system installation program in a hidden mode:

setup.exe /quiet /LANG="ru" /INSTALLTYPE="Admin" /REMOVE="Acrobat Guardant_x86" /
CMD="CREATE_QUICKLAUNCH_SHORTCUT=\"0\" INSTALL_AS_SERVICE=\"1\" LANGUAGE=\"de\" SQL_AUTHTYPE=\"Sql\"
SQL_USERNAME=\"username\" SQL_PASSWORD=\"pass\" SQL_INSTANCE=\"(local)\SQLEXPRESS2014\"
DB_INTELLECT_NAME=\"intellectNew\" DB_TITLES_NAME=\"titlesNew\" INSTALLDIR=\"%ProgramFiles%\IntellectNew\"
REMOVE=\"Wav,Utils\""

In result the installation file setup.exe will be run with following parameters:

1. Installation program will install the Intellect software in a hidden mode (/quiet);
2. Installation program language– Russian(/LANG="ru");
3. Installation type – «Administrator workstation» (/INSTALLTYPE="Admin");
4. The following components are not installed: Adobe Acrobat, Guardant drivers. (/REMOVE="Acrobat Guardant_x86");
5. Installation is performed with following features (/CMD=):
    a. Without creating the quick launch shortcut (="CREATE_QUICKLAUNCH_SHORTCUT=\"0\");
    b. The Intellect software is installed as a service (INSTALL_AS_SERVICE=\"1\");
    c. Language of installed Intellect software is German (LANGUAGE=\"de\");
    d. Authentication method – «SQL authentication » (SQL_AUTHTYPE=\"Sql\");
    e. Login – username (SQL_USERNAME=\"username\");
    f. Password – pass (SQL_PASSWORD=\"pass\");
    g. Database server – (local)\SQLEXPRESS2014 (SQL_INSTANCE=\"(local)\SQLEXPRESS2014\");
    h. Main database– intellectNew (DB_INTELLECT_NAME=\"intellectNew\");
    i. Titles database – titlesNew (DB_TITLES_NAME=\"titlesNew\");
    j. Installation path - %ProgramFiles%\IntellectNew (INSTALLDIR=\"%ProgramFiles%\IntellectNew\");
    k. Utilities and voice notification files are not installed (REMOVE=\"Wav,Utils\").

19.5 Remote installation, removal and update of Intellect software

Remote installation, removal and update of *Intellect* software are performed using the wmic.exe utility of the command prompt. This utility is a part of Windows OS. Enter «wmic» without quotations in the Windows command prompt to run the utility.

Detailed information about this utility is presented in the http://msdn.microsoft.com reference web-site.

Note.

The wmic.exe utility works incorrectly with VMWare virtual computers. The utility working with other virtual computers is not guaranteed.

It is required to disable UAC for wmic operation on the remote computer (instruction on disabling is presented in the OS settings for correct operation of Remote Admin Workstation or Server section).

The method of installation, removal and update described in this section is applicable for computers in the domain and for installation on computers outside the domain.

First copy the *Intellect* distributive to local disks of these computers.

For this use the following script of the command prompt:

xcopy %Path_to_folder_with_distributive% %Network_folder_on_target_PC% /e

Where:

%Path_to_folder_with_distributive% – path to the folder with distributives on the local computer.

%Network_folder_on_target_PC% – path to the folder on computer where the software installation is supposed. Access for writing is to be granted for it.

Attribute /e – causes the copying of all catalogues and their contents, including empty catalogues.

Note.

UNC-path is specified in the\\<server IP-address>\<General folder on this server>\... format.
Here dots define path from general folder to folder with distribution. If installation is performed on off-domain computers with specifying of server IP-address on which installation is performed. If installation is performed on computers in domain the address of server containing the folder with distribution available for all computers is specified.

Detailed information about working with the xcopy utility is presented on the Microsoft reference web-site. At the time of writing this documentation the utility description is located on http://technet.microsoft.com/en-gb/library/bb491035.aspx.

The method of installation described in this section allows installing and updating only basic product without prerequisites, drivers and other additional components.

19.5.1 Remote installation of Intellect software

To install the *Intellect* software on the remote computer, do the following command using the wmic.exe utility:

/NODE:"Computer_name" /USER:"User_name" /PASSWORD:"Password" productcallinstalltrue, "%installer parameters%", "%Path_to_folder_with_distributive%\Product.msi"

Where:

- /NODE – the target computer name on which the *Intellect* software is to be installed.

> **Note.**
>
> Instead of NODE list the text file in which names of target computers are listed in column can figure.

- /USER and /PASSWORD – login and password of user who has the corresponding rights for the *Intellect* software installation on the remote computer.
- "% Path_to_folder_with_distributive %\Product.msi" – path to the Product.msi installer file which is to be run, namely a local path to the folder in which the distributive was copied.
- %installer parameters% – installer options. The following parameters can be applied to the Product.msi:

1. which can be applied to all msi files (to get the reference execute the msiexec.exe /? command in the command line from the <WINDOWS>\system32\ directory).
2. parameters described in the setup.exe reference in the /CMD="[commands]" section (to get the reference execute the setup.exe /? command in the command line from the installer folder, all commands are described in the Installing INTELLECT™ software in a hidden mode section.
3. Parameters which are specified in the setup.exe while installation, i.e.:
    a. CMD_INSTALLTYPE – Client, Server, Admin.
    b. REMOVEALL (0, 1) – removing with/without configuration saving
    c. NOOSCHECK=1 – disable the check for compatibility with OS.

> **Note.**
>
> Working of specified parameters is not guaranteed if there is a thread in the registry:
> - For x86 system: HKEY_LOCAL_MACHINE\SOFTWARE\ITV\INTELLECT\InstallPropertyInfo
> - For x86 system: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\INTELLECT\InstallPropertyInfo
>
> It contains parameters of previous installation.

> **Example**
>
> Example of the line with installer parameters:
> REBOOT=ReallySuppress LANGUAGE="es" TRANSFORMS="%Path_to_folder_with_distributive%\languages\Setup\es\es.mst" CMD_INSTALLTYPE="Server"
> Where
> REBOOT=ReallySuppress – cancel computer reboot when installation finished,
> LANGUAGE="es" – select the language of product. Default product language is English.
> TRANSFORMS="%Path_to_folder_with_distributive%\languages\Setup\es\es.mst" – specify path to the language mst-patch of installer (specify the installer language).
> CMD_INSTALLTYPE="Server" specifies the type of the Intellect software package installation – Server. The “Admin” value is also available (if the Remote Administrator Workstation installation type is required) and “Client” (if the Remote Client installation type is required).

19.5.2 Remote update of Intellect software

For remote update of the Intellect software up to a newer version:

1. Install the new version as described in Remote installation of Intellect software section.
2. In the command, make sure to specify the path to Product.msi for a new version.

In this case the old version will be automatically removed with configuration saving and the newer version will be installed.

19.5.3 Remote removal of Intellect software

> **Note**
>
> When *Intellect* is removed remotely, its configuration is kept.

For remote removal of the *Intellect* software, run the following command in the wmic.exe utility:

```
/NODE:"Computer_name" /USER:"User_name" /PASSWORD:"Password" product where name="Product_name"
 call uninstall
```

Where **Product_name** – the name under which the *Intellect* software installed. Usually it is «Intellect v.Build_number». These names can be found in the registry catalogue in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall section.

19.6 Configuring Cluster Service for Intellect

Cluster is a group of independent computers operating together as a whole system providing clients with a general set of services. Cluster enables expanding both accessibility of services and scalability and controllability of their OS.

To set up a cluster for INTELLECT, stick to the following rules:

1. INTELLECT is to be installed on all the computers forming the cluster.
2. INTELLECT configuration (paths to the installed INTELLECT software and video archive disks) is to be identical on all computers.
3. All computers, forming the cluster, are to be in one network domain.
4. All computers are to run one OS Windows Server.
5. If the Intellect software is installed as a service, the InheritServiceEnvironment registry key must be created and set to 1 (the key is created in the HKEY_LOCAL_MACHINE\SOFTWARE\ITV\INTELLECT\IntellectRunService\ section for 32-bit and in the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\INTELLECT\IntellectRunService\ for 64-bit systems).
6. The specific name and password must be used for database connection.

> **Note.**
>
> Nets organization and setting up order are given in the Windows Server reference manual (see https://learn.microsoft.com/en-us/windows-server/failover-clustering).

19.6.1 Example. Consolidation of two Servers into cluster and Intellect configuration

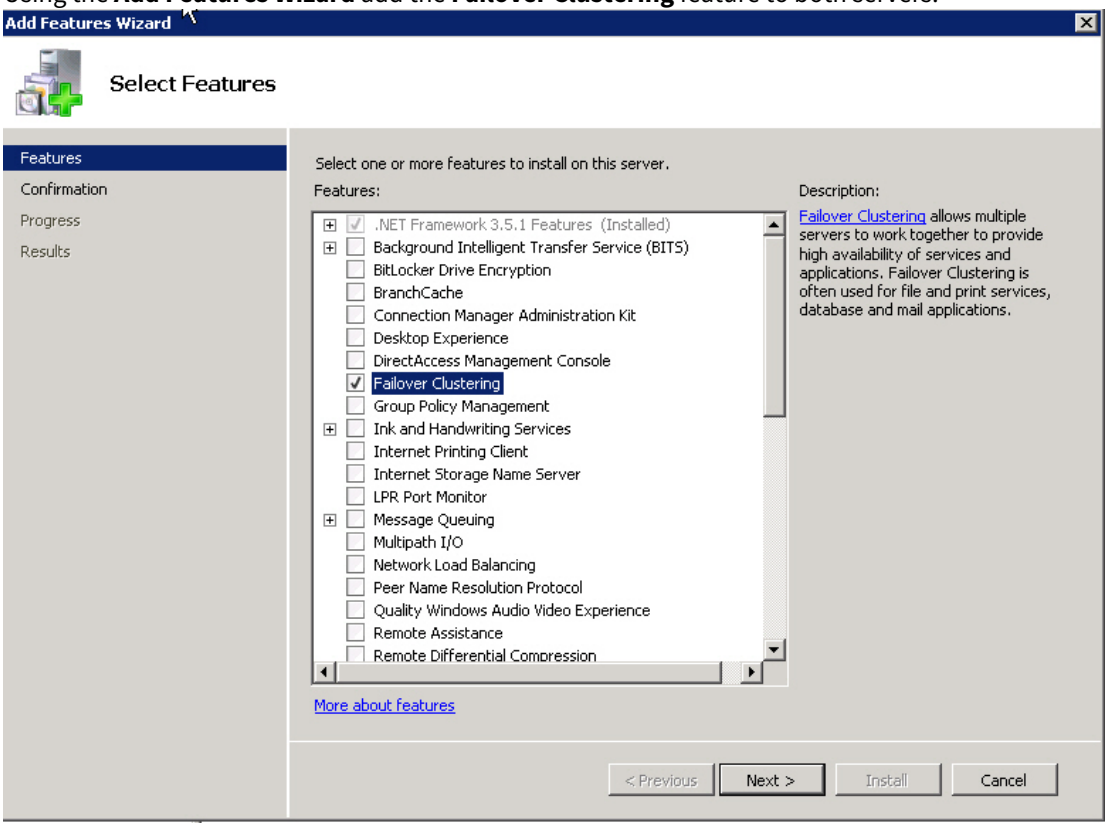
On the page:

- Preconfiguration of servers
- Consolidation of two Servers into cluster and Intellect configuration

19.6.1.1 Preconfiguration of servers

Before consolidating the Servers into cluster, do the following:

1. Install Windows Server of one of the following edition to both Servers:
   a. Windows Server 2008 R2 Enterprise
   b. Windows Server 2008 R2 Datacenter
   c. Windows Server 2012 R2 Standard
2. Add both servers to one domain.
3. Using the **Add Features Wizard** add the **Failover Clustering** feature to both servers.



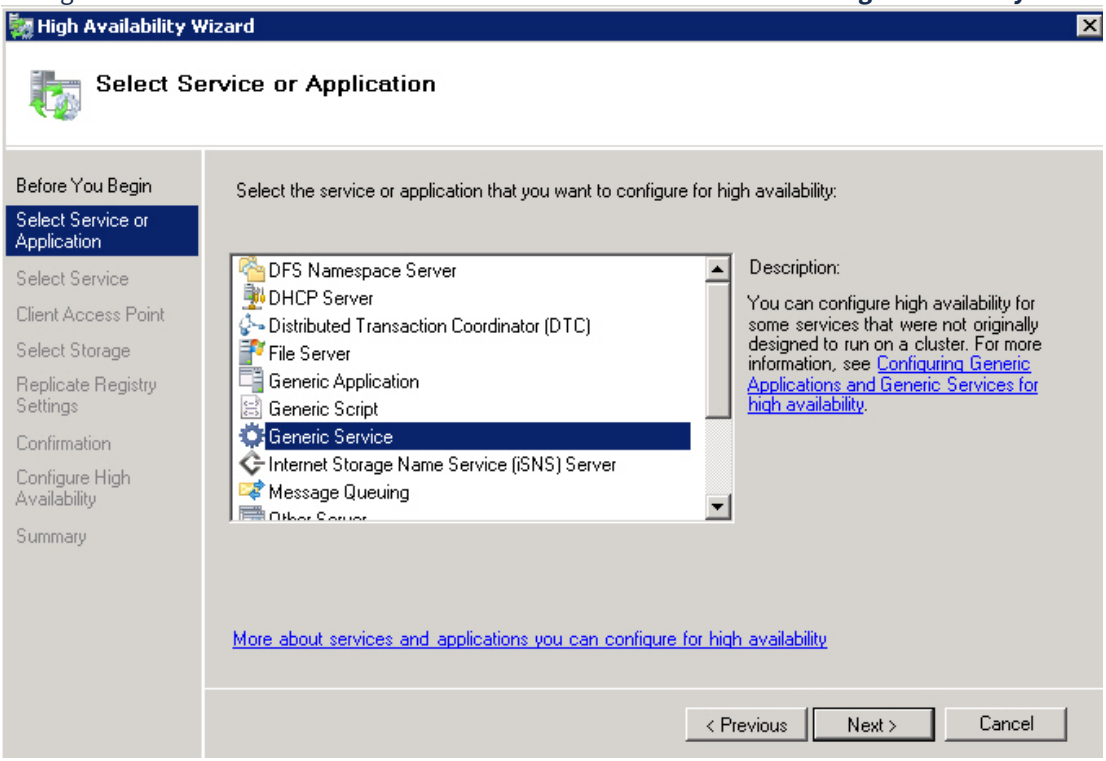
4. Enter the following parameter for the RAID supporting as a storage for cluster to the register:
   Location—HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ClusDisk\Parameters
   Name—AllowBusTypeRAID
   Type—DWORD
   Value—1
   (see Working with Windows OS registry).
5. Restart both Servers.
6. Create three disks on the common RAID array:
   a. to work in quorum and to store the cluster configuration
   b. to store the *Intellect* database
   c. to store video archive
7. In the **Storage** → **Setup** menu, set **Assignment Mode** in the **Multiple Assignment** position.
8. In the **Virtual Disks** → **Assign** menu, set the **Full Access** value for all servers.
9. Enter the **first server**. Start the disks control consol and initialize all three disks.
10. Switch the disks to online mode, create sections on all disks and format them.
11. Switch the disks to offline mode.
12. Enter the **second server** and initialize the disks in the same way.

19.6.1.2 Consolidation of two Servers into cluster and Intellect configuration

To consolidate two Servers into cluster and configure *Intellect*, do the following:

1. Install the required version of *Intellect* on both Servers before consolidating them into cluster (see Installing and removing Intellect).
2. Set the AxxonSoft\INTELLECT\IntellectRunService\InheritServiceEnvironment parameter with the value 1 in the registry.

3. Stop the **SQL Server (SQLEXPRESS)** and **Intellect Core Server** services on both Servers and switch them to the manual type of start.
4. Start the **Failover Cluster Manager** on the one of Servers (or remotely).
5. Select **Act** → **Create cluster**. The **Cluster Creation Wizard** will launch.
6. Add both servers which are supposed to use for the failover cluster.
7. Specify NetBios name and the IP address for the failover cluster (this data will be used for connection of the settings console).
8. Complete the cluster creation.
9. Configure the role on cluster. Select **Add service** → **Generic Service** in the **High Availability Wizard**.



10. Select the**Intellect Core Server** service.
11. Configure the NetBios name and the IP address for the service (these parameters will be used for connection to *Intellect).*
12. Complete the role configuration.
13. Set the dependence on the Name and the IP address on the **Dependence** tab in the service settings.
14. Set the **Use network name for computer name** checkbox (regardless of the letter case in the cluster settings, the name will be transmitted in capital lettters) on the **General** tab.
15. Go to the role settings and select **Add service** → **Generic Service**.
16. Select the **SQL Server (SQLEXPRESS)** service.
17. Complete the adding of the service.
18. Select the **Intellect Core Server** service and perform **Off the line** action.
19. Enter the Server, which is specified as the Owner unit. Disconnect the *Intellect* database in SQL, move the database files to the disk in the failover array and connect the database again.
20. In the idb.exe, set the username and password for the database connection (see The idb.exe utility for converting databases, selecting database templates and making backup copies of databases).
21. Start the Tweaki.exe and rename the computer to the name of the failover cluster (see Tweaki.exe utility for advanced setup of the Intellect software system).
22. In the cluster settings, select **Additional actions** → **Replace primary cluster resources** → **Select unit**. Specify the second Server.
23. In the SQL, disconnect the old databases and connect new databases from the disk in the failover array.
24. Change the username and password for the database connection in the idb.exe.
25. Start the **Intellect Core Server** in the **Failover Cluster Manager**.
26. Start *Intellect*. Make sure that the start is correct.

Consolidation of two Servers into cluster and *Intellect* configuration are complete.

20 License key

Functionality (configuration) of the system is restricted by the license key supplied together with the *Intellect* software installation package. Operations with the license files are described in the Installing and removing INTELLECT™ software section.

The license key activates the system functionality. Whenever the system configuration needs to be extended (for instance, where a subsystem, which is not included in the basic configuration, is required), to enable functionality of the program module corresponding to the subsystem which needs to be installed, the previous license key is to be replaced with a new one, which will restrict updated system functionality.

Replacement of the previous license key with a new license key initiates the updated set of functional subsystems when the system is reset.

> **Important.**
>
> It is obligatory to restart *Intellect* after replacing the activation key. If *Intellect* is installed as a service, restart the **Intellect Core Server** service (see also Working with Windows OS services for operating Intellect™ installed as a Service).

In a distributed system the configuration of each computer depends not only on this computer's license key, but on the license keys of other computers in the distributed system. That is, the maximum functionality of each computer in the distribute system is limited by the license key of the computer with minimum capabilities. Thus, the same license key is recommended to be used on all computers in the distributed system.

The license key is bound to computer equipment. The bind is performed in one of the following ways:

1. Binding to "Guardant" hardware dongle of one of the following type:
    a. Guardant Stealth II;
    b. Guardant Sign;
2. Binding to dallas-codes of video capture cards with cryptochip (FS5\6\8\16, WS7\17) of Axxonsoft production;
3. Binding to computer equipment (HID).

> **Important!**
>
> It is recommended to use Guardant dongle to bind the license key. This method is the most convenient, since it does not depend on the computer hardware (HID). The Guardant dongle allows avoiding errors in case of any board or card replacement.

License key is required when the *Intellect* software installing with the Remote Administrator Workstation or Sever installation type. If the Remote Client installation type is selected, the license key is not required.

20.1 Binding the license key to computer equipment

HID (Hardware ID) – is encrypted information about computer equipment which is gathered by CodeReader utility and is transferred to AxxonSoft for license key generation.

The binding of following elements has been realized:

1. motherboard;
2. processor;
3. hard disk;
4. RAM;
5. video card;
6. netcard

If main utilities of Server are replaced, then the licence is not active. For instance, simultaneous replacement of motherboard and processor will cause the license loss. However, simultaneous replacement, installation or deinstallation of hard disk, RAM, video card or netcard will not cause the key deactivation.

20.2 Match search in the license key

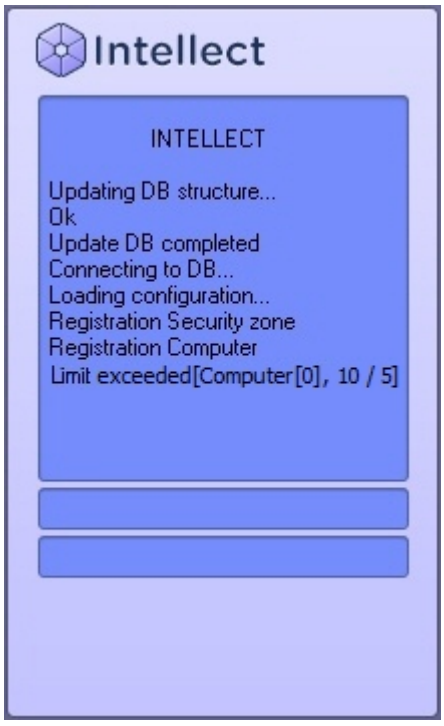
Codes match search in the license key with devices codes in the computer is performed in the following way:

1. Computer HID is read where the Intellect software is run.
2. License key is read.
3. For every computer, stated in the license key, the following actions are performed:
    a. If the computer in license key is bound via HID:
        i. If there are video capture cards manufactured by AxxonSoft company in the license key , the match search of board codes on the computer and board codes in the license key will be performed (if there is no match , the following computer in the key will be checked);
        ii. If there are no video capture cards manufactured by AxxonSoft Company in the license key, the match search of computer HID and computer equipment codes in the key will be performed (if there is no match, the following computer in the key will be checked).
    b. If the computer in license key is not bound via HID, the match search of video capture cards manufactured by AxxonSoft company on the computer and board codes in the license key will be performed (if there is no match , the following computer in the key will be checked).

If there is at least one match found the Intellect software will be run.

20.3 Features of the Intellect software operation when the object limit is exceeded

When *Intellect* is launched with a key and equipment limit exceeded, the **Limit exceeded** message is displayed in the loading window indicating the object which caused the excess and the number of created in the "created/allowed" format. Square brackets indicate the internal ID of the object type in the license key.

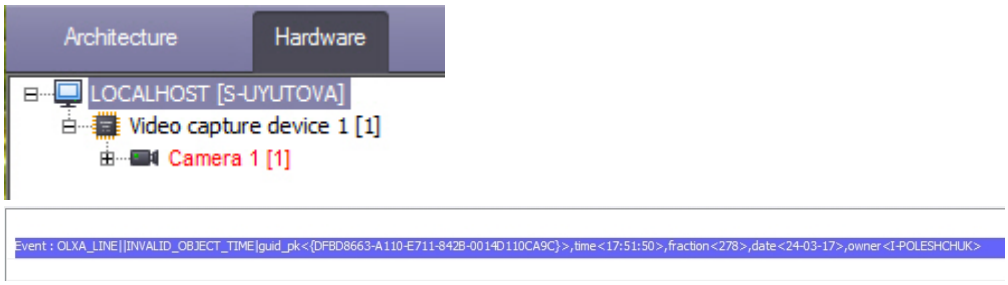


In this case to start the *Intellect* software operation, do the following:

1. Forward the intellect.sec key from the *Intellect* directory to another folder, e.g. "D:\Temp".
2. Run the *Intellect* software in a demo mode.
3. Remove a redundant object.
4. Shutdown the *Intellect* software.
5. Restore the key from the "D:\Temp" folder to the *Intellect* installation directory.
6. Start the *Intellect* software.

If the object is not provided by the license key, then it will not be possible to add it to the equipment tree, since it will be absent in the **Create object** function (see The Create object function). Similarly, it will not be possible to create another object if the limit on the number of such objects provided by the license key is reached.

Moreover time of action of certain objects can be set in the intellect.sec license key. If the action of the objects expired, *Intellect* starts as usual, but the expired object is colored red in the hardware tree, and the INVALID_OBJECT_TIME event from this object comes to the Debug window.



After the expiration of the object, it is impossible to use it in *Intellect*: it continues to be displayed in the object tree, but events are not received from it and it does not respond. Other modules cannot communicate with an expired object.

To resume work with an expired object, you need to request the intellect.sec license key from the AxxonSoft manager and update it. If the object is no longer needed, you can delete it (see Deleting).

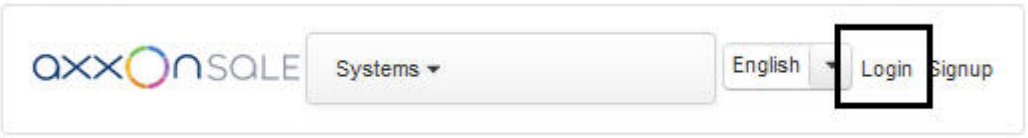
> **Note**
>
> The validity period of the object cannot be longer than the validity period of the temporary key.

20.4 Decoding license key

You can find out what objects and how many of them are available thanks to the activation key, as well as hardware codes to which the key is bound.

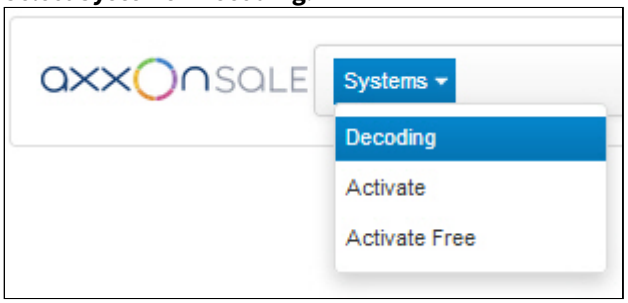
For this, do the following:

1. Go to https://sale.axxonsoft.com/sale/.
2. Log in to the site. To do this, click **Login** and enter your username and password.



> **Note**
>
> License key decoding is available only to registered users of the site. If you do not have a username and password, then you need to register by clicking **Signup**.

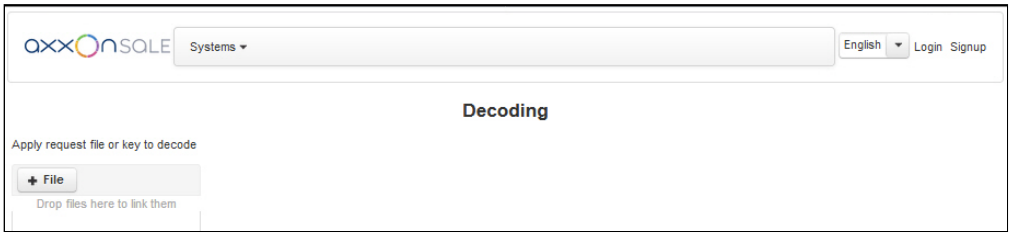
3. Select **Systems** - **Decoding**.



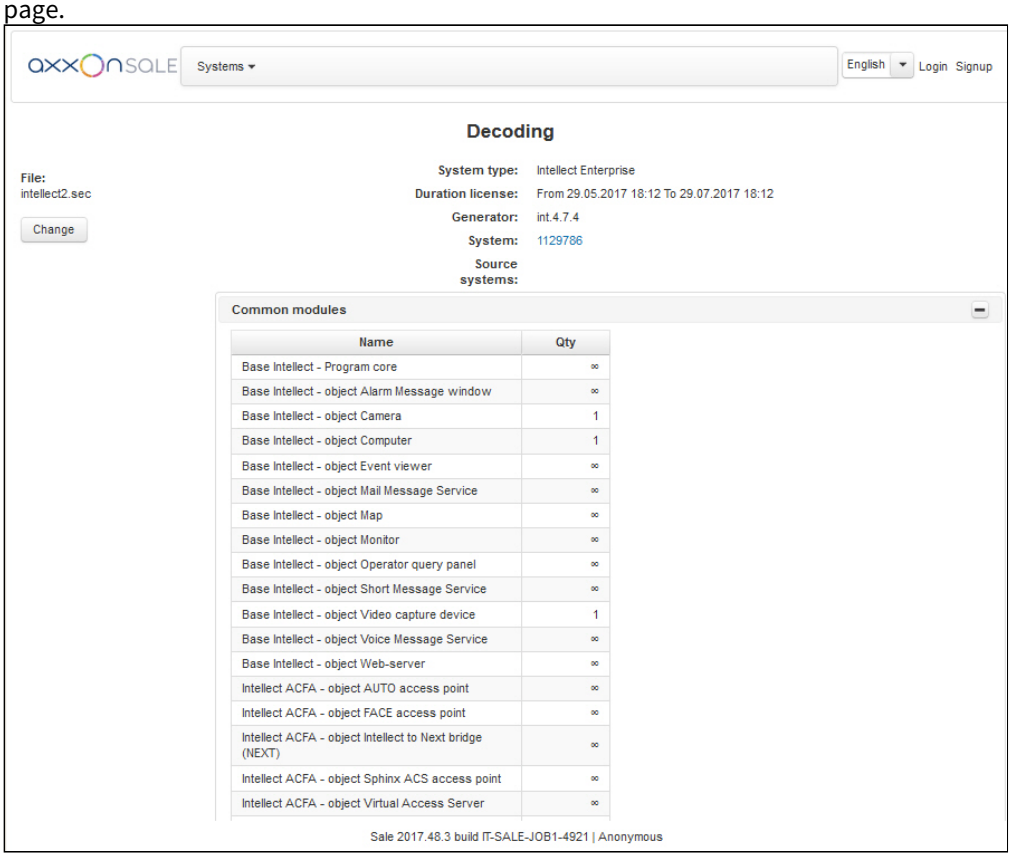
4. Add intellect.sec license file to the **File** form.

Note

The license file is in the *Intellect* installation directory root, by default: C:\Program Files (x86)\Intellect\.



5. After adding the file, the information about available objects and hardware codes will be automatically displayed on the page.



21 Configuring system startup and shutdown

21.1 Configuration of Intellect™ software startup

21.1.1 Possible options for Intellect™ software startup

Intellect™ software is launched in one of the following ways:

1. Manual launch;
2. launch from Windows OS Start menu;
3. launch from Windows OS command prompt;
4. automatic launch;
5. launch from Startup of the Windows OS;
6. launch with the PC switched on, without starting Windows OS;

Manual launch of *Intellect*™ software does not require additional settings. Automatic launch of *Intellect*™ software using one of the above methods, requires certain additional Windows OS settings. Windows OS settings are given in the corresponding sections of this chapter.

If the video surveillance system uses pre-defined rights and authorizations for the users, *Intellect*™ software launch starts with user authorization. Depending on the *Intellect*™ system settings, the following user authorization options are available:

1. By entering the login and password. In this case, when the system is launched, the user will be able to access only those functions of *Intellect*™ system, which comply with his rights and authorities.
2. Without entering any login and password. In this case *Intellect*™ system makes available only those functions, which comply with the rights and authorities of the default user.

By default, *Intellect*™ system authorizes a user through a password. To launch *Intellect*™ software without a password, an Operator should identify a user, whose rights and authorities will be used to launch the *Intellect*™ system. Procedures for identification of the default user are described in the Rights administration chapter.

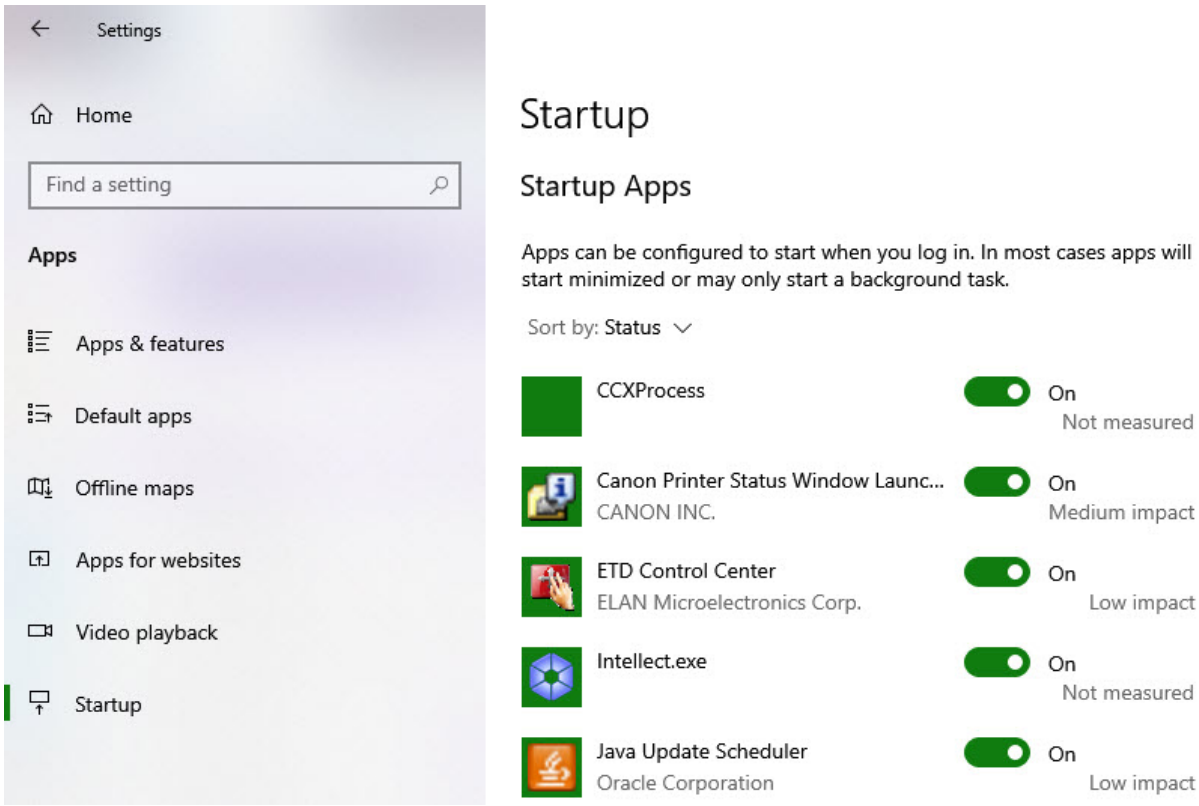
Note.

If the *Intellect* software is installed as a service, and the user rights and privileges are not set, password authorization is required upon entering the *Intellect*. Otherwise the *Intellect* modules and services will not be launched.

21.1.2 Configuring Intellect system automatic startup from Windows OS Startup

Intellect software can be launched automatically from the **Startup** function, as soon as Windows OS services and shell start downloading.

To configure the *Intellect* system launch using the **Startup** function, you need to add *Intellect* to the Startup Apps list: Start → Settings → Apps → Startup. You can refer to the Windows OS documentation (depending on the installed version); a link to the relevant documentation will be in the Startup window.



Important!

In **Windows 8.1** and **Windows 10** for the proper operation of the Startup function, create a registry key with an arbitrary name in the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run (if the OS is 64-bit) or HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (if OS is 32-bit).
The path to the executable file is to be specified as the key value, for instance: C:\Program Files\Intellect\Intellect.exe
Also, disable UAC completely as described in OS settings for correct operation of Remote Admin Workstation or Server.

21.1.3 Configuring Intellect system automatic startup bypassing standard Windows OS

Automatic start of *Intellect* system, instead of starting the standard Windows OS shell is used in cases, when access to the basic PCs of the video surveillance system need to be restricted: to prevent start of various applications, file copying and deletion, operations with Windows OS and other non-standard PC operations.

In cases where Startup is set for launching instead of Windows OS, the *Intellect* system will start downloading after Windows OS, instead of Explorer. This makes start of various applications installed in a PC, and operations with the program dialog boxes, inaccessible for a user.

Attention!

Configuration of the local security policy is required for full disabling of UAC in the Windows 8 and Windows 8.1 OS—see the OS settings for correct operation of Remote Admin Workstation or Server section.

To set up *Intellect* software automatic startup bypassing the standard Windows OS (Explorer), the following string parameters of the Windows OS registry are to be modified:

Registry section: HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\.

Folder: Winlogon.

Parameter: Shell.

Default parameter value: Explorer.exe.

Required parameter value: entire path to the *Intellect* software startup file.

For instance, to set up *Intellect* system automatic start for configuration of the Server, the “Shell” parameter is to be identified as: “C:\ Program Files\Intellect\intellect.exe”.

To set up *Intellect* system automatic start for configuration of the Remote Client, the “Shell” parameter is to be identified as: “C:\Program Files\Intellect\slave.exe”.

If the rules of safety of distributed network, a part of which the configured PC is, require that the PC be authorized in the domain, Windows OS may be configured to start without requesting the name (login) and password of the user, who is registered in the domain of the distributed network. To do this, you need to specify the user name (login) and password, which will be used to authorize the computer in the domain by default. To set up Windows OS start without user name (login) and password request, change the following string parameters of the Windows OS registry:

Registry section: HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\.

Folder: Winlogon.

#	Parameter	Default parameter value	Required parameter value
1	AutoAdminLogon	0	1
2	DefaultUserName	One of the registered user names (logins)	User name (login) for authorization in the domain
3	DefaultPassword	If parameter does not exist, it is to be created	User name for authorization in the domain

Registry parameters are edited either using the Tweaki.exe utility (recommended), or manually. Setup of *Intellect* system automatic startup with the Tweaki.exe utility is shown in Tweaki.exe utility for advanced setup of the Intellect software system. Basic information required for manual system registry editing is outlined in the Working with Windows OS registry section.

Working with Windows OS services for operating Intellect™ installed as a Service

21.2 Configuring Intellect™ system shutdown

The *Intellect*™ system is always closed manually. If the video surveillance system uses pre-defined rights and authorizations for the users, *Intellect*™ software should be closed by entering a user password.

Intellect™ system may be closed using the following options:

1. using an authorized user login and password
2. using an administrator password.
3. using an administrator password entered in the displayed administrator password request window.

Intellect™ system closure is configured at the stage of administration of user rights and authorizations, and is described in the corresponding sections of the Rights administration chapter..

22 Working with the System settings dialog box

22.1 General information about the System settings dialog box

The *Intellect*™ system is configured using the **System settings** dialog box.

The **System settings** dialog box is designed to configure and set up the digital components of the video surveillance system.

The **System settings** dialog box helps to solve the following key objectives:

1. creation and configuration of the system objects corresponding to the function modules (groups) of the *Intellect*™ system;
2. configuration of video surveillance and audio monitoring functions;
3. user interface configuration;
4. administration of user rights and authorizations.

The interface of the **System settings** dialog box is described in Description of the System settings dialog box.

22.2 Startup and shutdown of the System settings dialog box

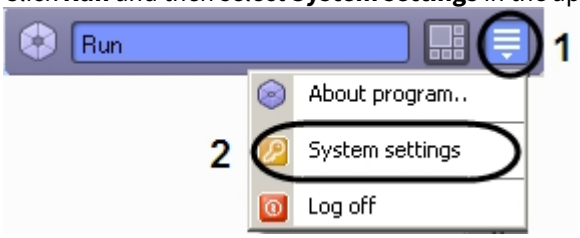
22.2.1 Startup of the System settings dialog box

To start up the System settings dialog box follow the next steps:

1. Display the main control panel on the monitor. For this purpose, drag the mouse cursor to the upper left corner of the monitor.

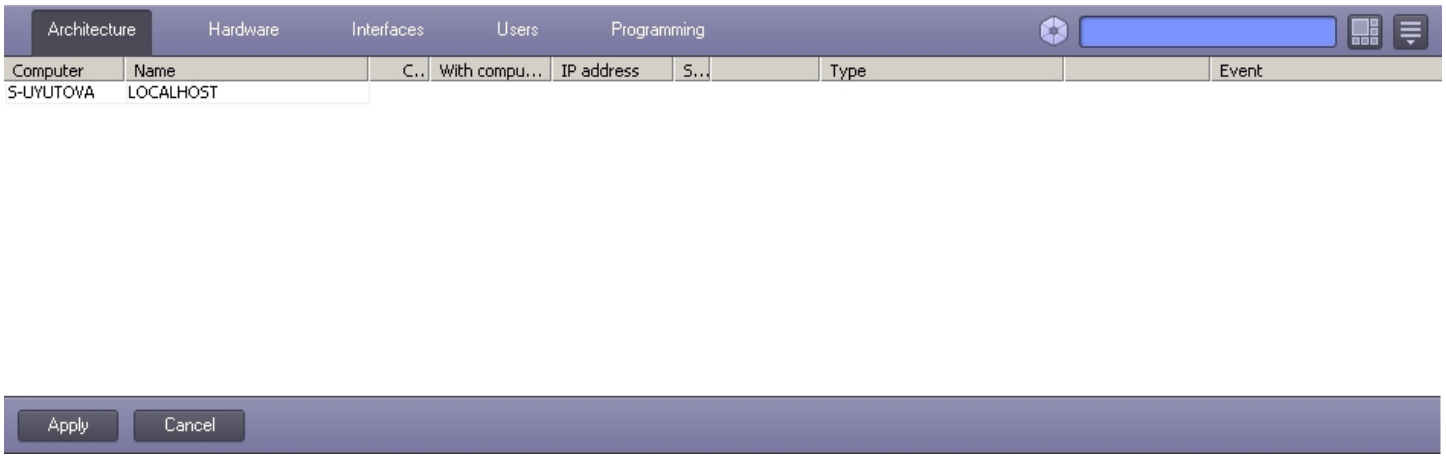
> **Note.**
>
> By default, the Main Control Panel is displayed on the primary monitor. The number of monitor for displaying the Main Control Panel can be set by the cur_monitor registry key (see Registry keys reference guide).

2. Click **Run** and then select **System settings** in the appearing dropdown menu.



> **Note.**
>
> The **System settings** item is also available in the menu that appears on clicking the icon in the Windows notification area (system tray), or by short-time holding the “hot” button F8.

Now you have the **System settings** dialog box displayed on the monitor.



Note.

The interface of the INTELLECT™ **Main Control Panel** is given in Appendix 1. Interface.

Attention!

While changing the screen resolution it is necessary to restart the *Intellect* software for dialog windows correct displaying.

Note.

In case of the **System settings** dialog window exceeds the bounds of the screen, use one of the following ways to solve this problem:

1. Set the font size 96 pixels per inch (the screen scale is 100%). To perform this operation, go to the **Control panel -> Appearance and personalization -> Settings of screen resolution**.
2. If the first way doesn't solve the problem, use settings_height and settings_width registry keys and specify the height and width of the **System settings** dialog window in pixels (see the Registry keys reference guide).

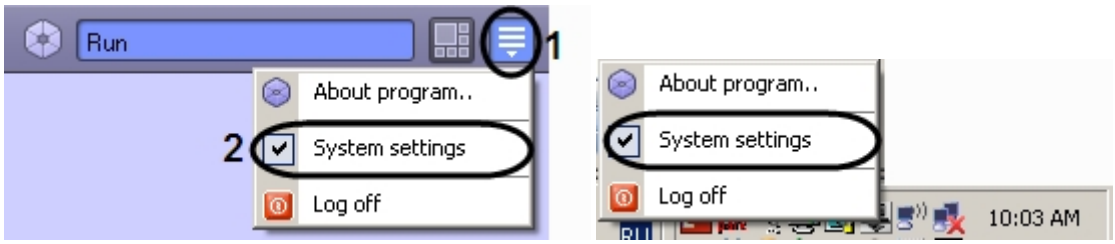
Note.

If captions are displayed incorrectly in the interface because there is no such font in the system, then install the font located in the Redist\Font folder. Information on how to install fonts in Windows up to 7 can be found at https://support.microsoft.com/en-us/help/314960/how-to-install-or-remove-a-font-in-windows.
On Windows 8, Windows 8.1, Windows 10 fonts are installed in the other way:

1. Select **Run** in the **Start** menu.
2. Enter the following command:
   %windir%\fonts
3. Click **OK**.
4. Copy or move font files to the folder opened.

22.2.2 Shutdown of the System settings dialog box

To exit the **System settings** dialog box, select **Run** in the **Main Control Panel**, or in the Windows notification area (system tray), or by short-time holding the "hot" button F8, and then select **System settings** in the appearing dropdown menu, which will already be checked.



The **System settings** dialog box will be closed after repeated selection of the **System settings** in the menu.

22.3 Setting procedure for system objects

On the page:

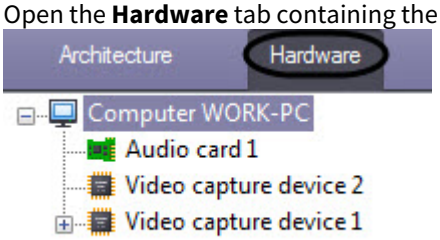
- Select an object
- Create an object
- Edit an object
- Change the parent object
- Copy objects
- Enable or disable objects
- Delete an object

Configuration of *Intellect* system objects generally includes the following stages:

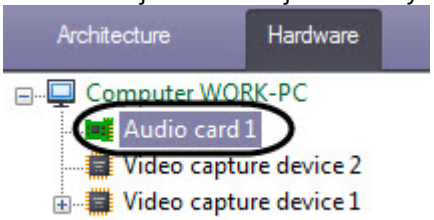
22.3.1 Select an object

To select an object, do the following:

1. Open the **Hardware** tab containing the objects tree.



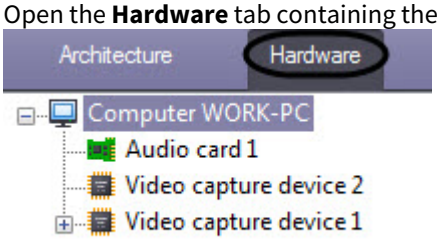
2. Select an object in the objects tree by clicking it with the mouse.



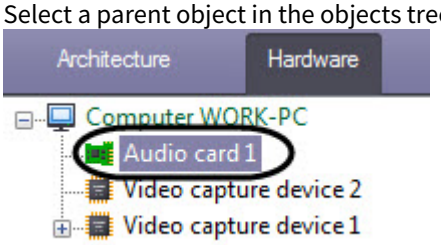
22.3.2 Create an object

To create an object, do the following:

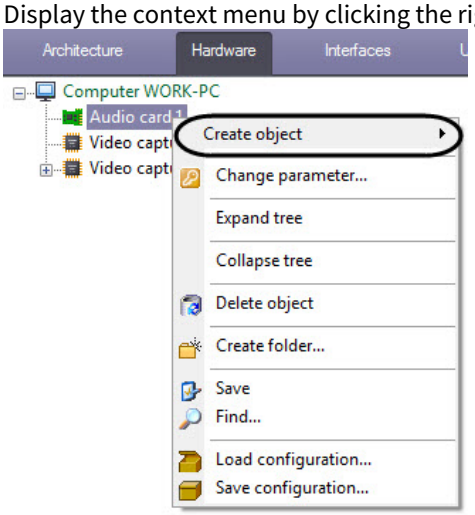
1. Open the **Hardware** tab containing the objects tree.



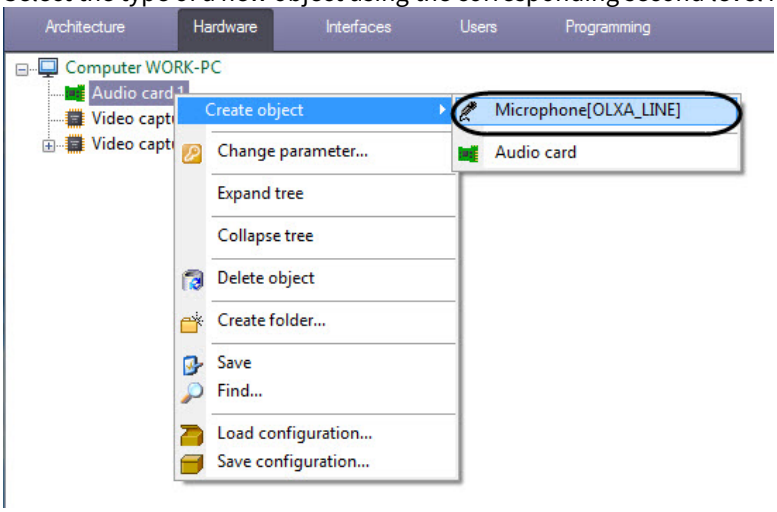
2. Select a parent object in the objects tree, which should be used as a basis for the creation of a child object.



3. Display the context menu by clicking the right mouse button and select **Create object**.



4. Select the type of a new object using the corresponding second level menu.

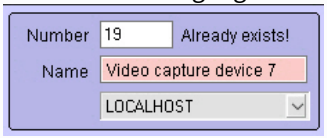


As a result of the above operations, the object settings panel will display an identification panel for the new object.

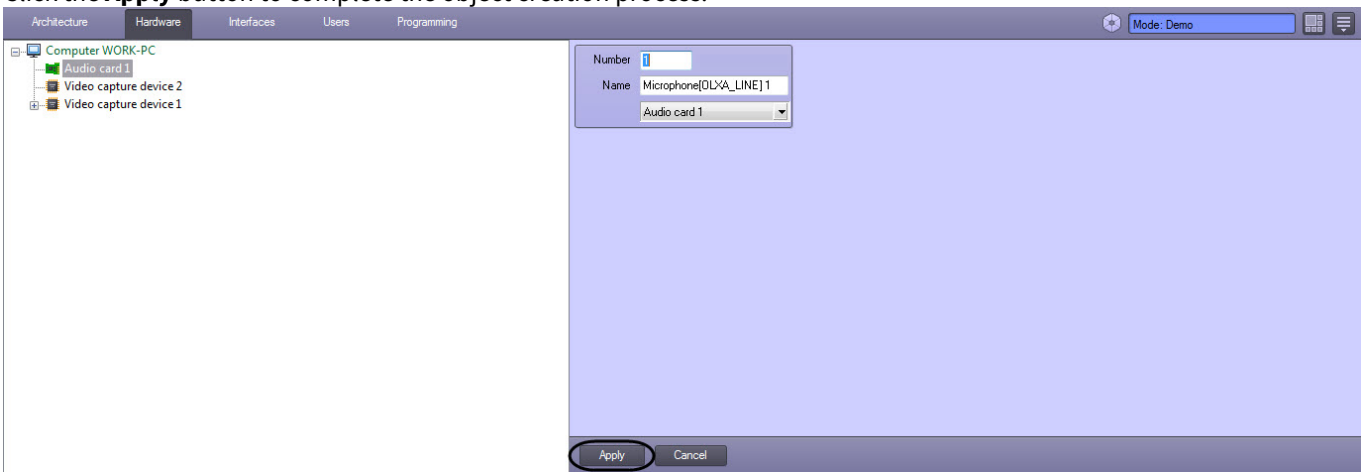
5. Specify a unique identification number in the **Number** field (**1**) and the unique name of a new object (the **Microphone** object in the example on the figures) in the **Name** field (**2**).

Note

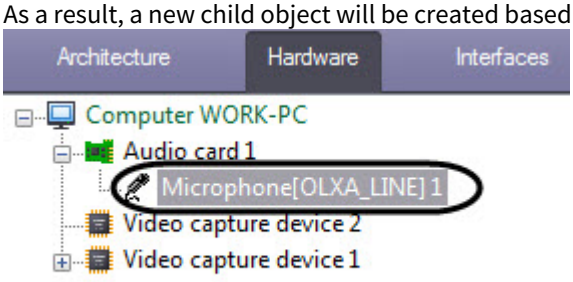
For the list of restrictions on the use of characters for object identifiers (Numbers), see Identifiers (numbers) of system objects.
You should not use the > and < characters in the **Name** filed. If these characters are used in the object name, they will be removed when settings are applied.
If the identifier or the name already exist in the system, the corresponding message is displayed on the panel, and the field is highlighted in red.



6. Click the **Apply** button to complete the object creation process.



7. As a result, a new child object will be created based on the selected parent system object.



Note

If the parent system object has one or more child objects, then you can expand the list of the child objects using the ⊞ icon, and collapse the list using the ⊟ icon.

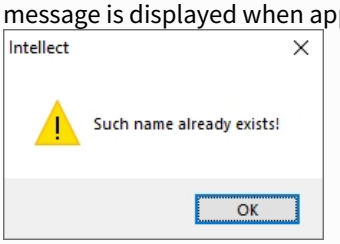
22.3.3 Edit an object

Editing means any modification of the object settings, i.e. changes in the object parameter values. The settings panel of the system object is the key configuration instrument of the object setup.
To edit an object, do the following:

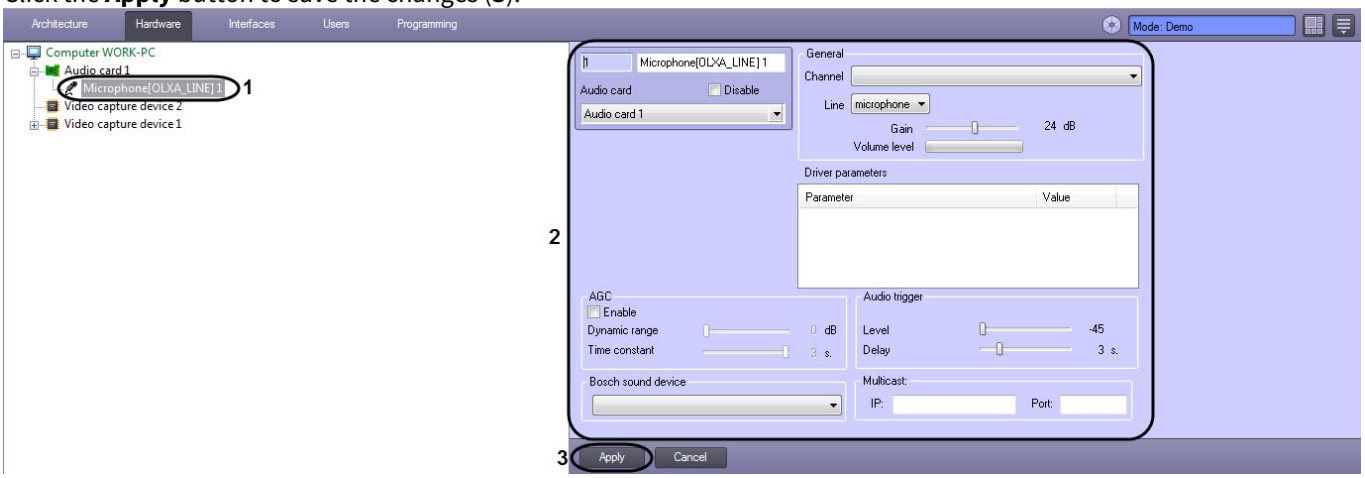
1. In the objects tree, select a system object the parameters of which should be edited by clicking the object (**1**).
2. Edit the object parameters using the settings panel of the object (**2**).

Note

The object ID cannot be edited.
The object name can be changed, however, if an object with the same name already exists, the corresponding message is displayed when applying the settings:



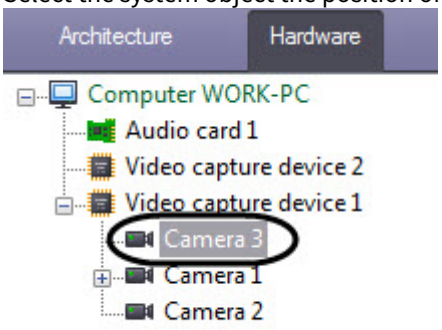
3. Click the **Apply** button to save the changes (**3**).



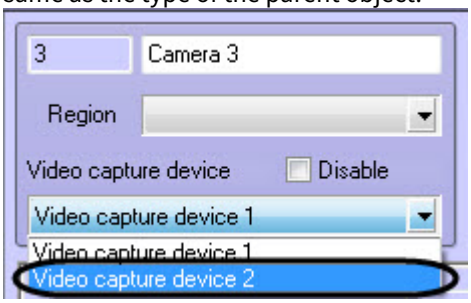
22.3.4 Change the parent object

When changing the parent object, you can move the created object in the objects tree of *Intellect* without losing the settings. To change the parent object, do the following:

1. Select the system object the position of which should be changed in the objects tree.

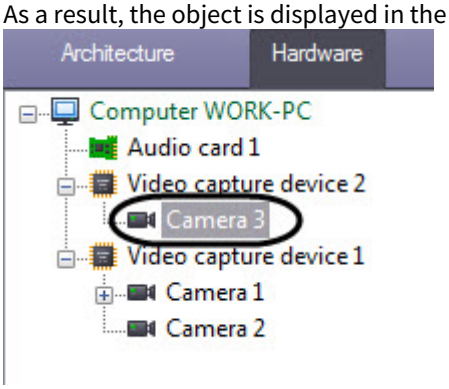


2. Select a new parent object in the drop-down list on the settings panel of the object. The name of the drop-down list is the same as the type of the parent object.



> **Note**
>
> If the object is moved to another computer, *Intellect* should be restarted on both computers—on the one the object is moved to and on another the object is moved from.

3. As a result, the object is displayed in the objects tree of the selected parent object.



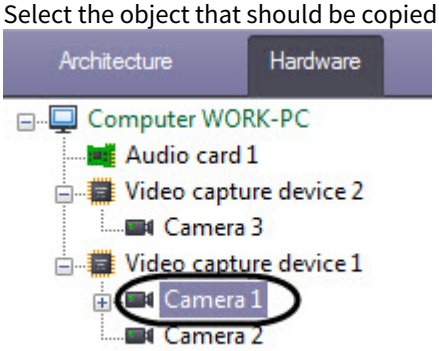
22.3.5 Copy objects

The copy function enables cloning the objects created in *Intellect* objects tree (for copying objects using a template, see also The Save function).

> **Note**
>
> The copy function is guaranteed for the **Video capture device** object and its child objects: **Camera**, **Sensor**, **Relay**, **Embedded detection tool**, **Face detection tool**, **Detection zone**, **Tracker**, **VMDA detection tool** and **Captioner**. For other objects this function is not guaranteed.

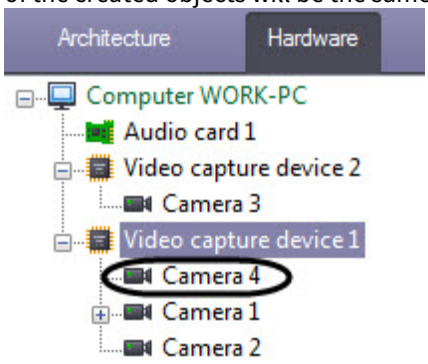
To copy the objects, do the following:

1. Select the object that should be copied in the objects tree.



2. To copy the object press the **Ctrl+C** key combination.
3. Select the parent object on the basis of which the copy of the selected object should be created or one of the objects created on the basis of the parent object.
   If the copy should be created on the basis of the same parent object as the source object, then this step can be skipped.
4. Paste the object using one of the following key combinations:
   a. **Ctrl+V**—paste only the copied object.
   b. **Ctrl+Shift+V**—paste the copied object with all child objects.

The object or objects will be created with the default names, and they will be assigned the next free ID in order. The parameters of the created objects will be the same as those of the corresponding source objects.



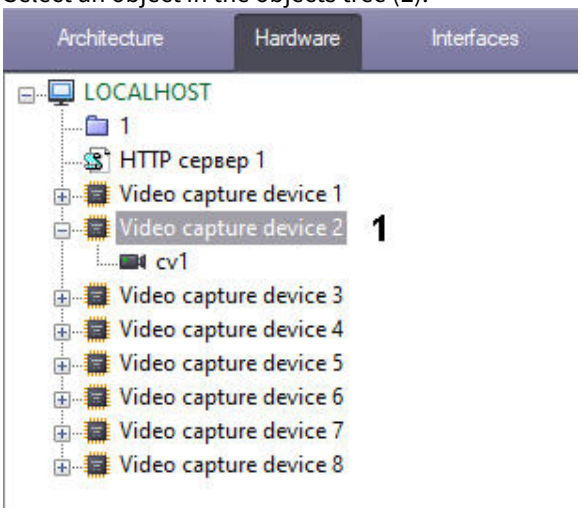
Note

Once copied, object can be pasted multiple times.
The copied object will be stored in the clipboard until *Intellect* restart, or until the clipboard clipping is replaced with a new copied object.

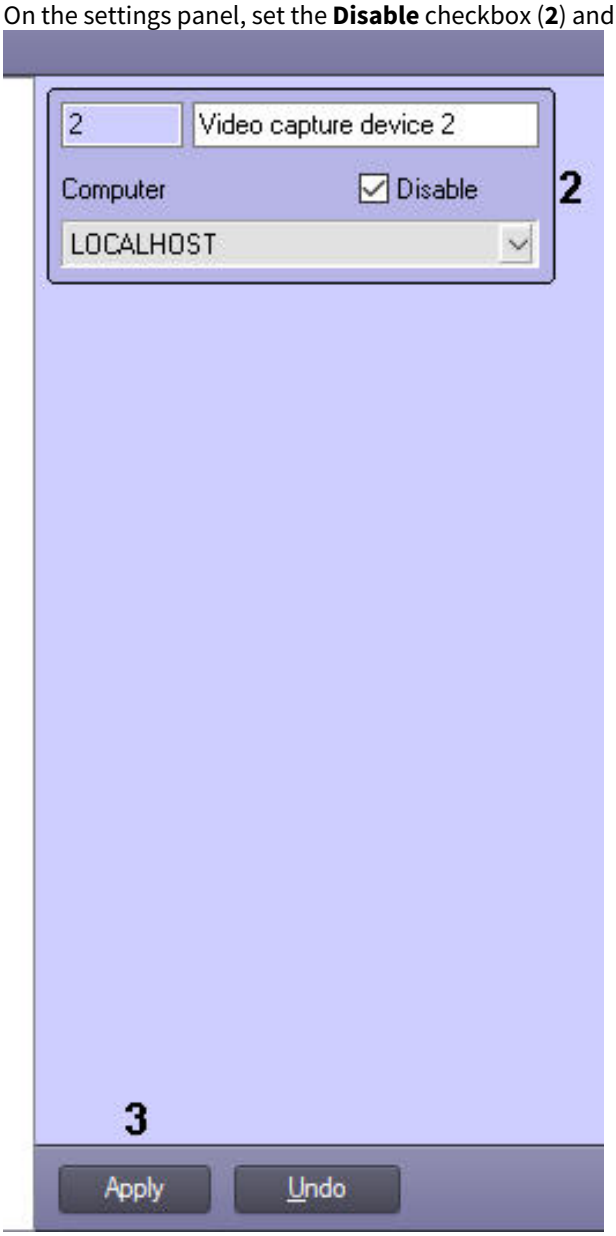
22.3.6 Enable or disable objects

In order to disable an object, do the following:

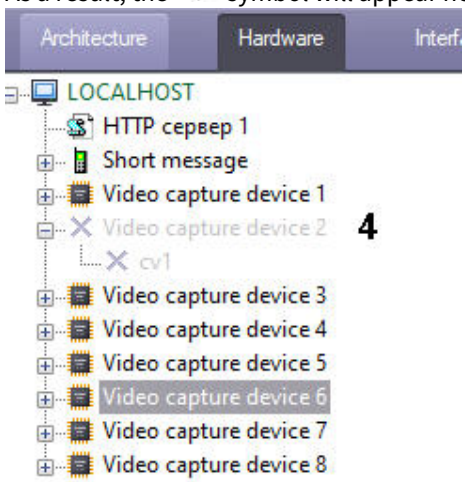
1. Select an object in the objects tree (**1**).



2. On the settings panel, set the **Disable** checkbox (**2**) and click the **Apply** button (**3**).



3. As a result, the symbol will appear next to the disabled object (**4**).



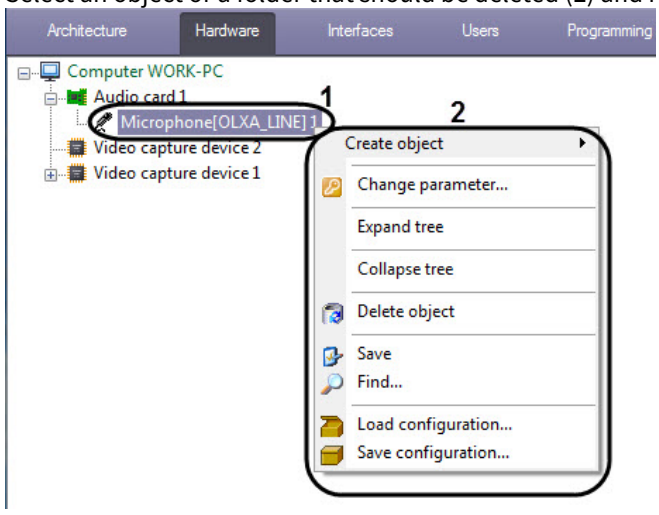
To enable an object, set the **Disable** checkbox clear in the settings panel and click the **Apply** button.

> **Note**
>
> Disabling an object also disables all of its child objects.

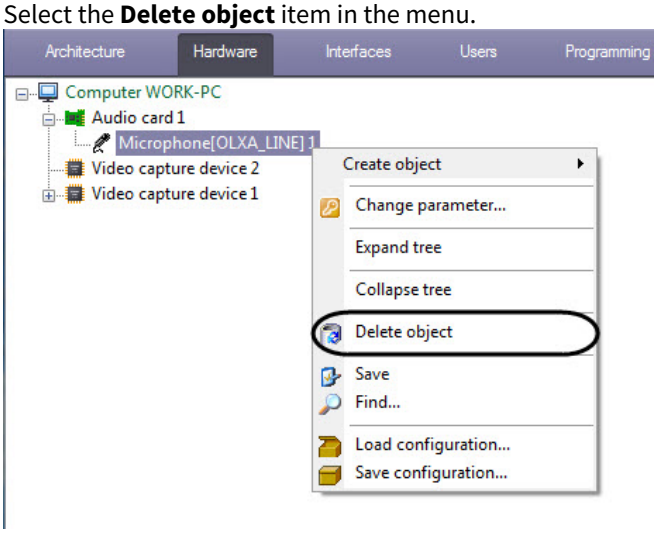
22.3.7 Delete an object

To delete an object, do the following:

1. Select an object or a folder that should be deleted (**1**) and right-click to display the context menu (**2**).



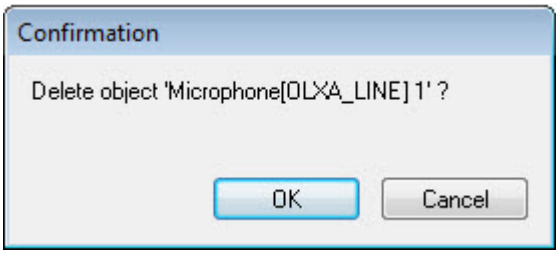
2. Select the **Delete object** item in the menu.



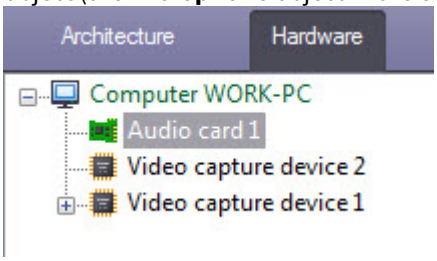
> **Note**
>
> You can also select the object that should be deleted and press **Ctrl+Del** instead of using the context menu.

As a result, a dialog box requesting confirmation of the object deletion will appear on the monitor.

3. Click the **OK** button.



4. The figure below displays the result of an object deletion (objects tree contents after the object was deleted). The deleted object (the **Microphone** object in the example) is no longer displayed in the objects tree.



> **Note**
>
> The object settings are applied after switching to another fragment, regardless of clicking the **Apply** button.

Description of the System settings dialog box

22.3.8 Identifiers (numbers) of system objects

When you create any system object, its number is automatically set by the system in order and depends on how many objects of the same type have already been created. At the same time, you can change the number by setting it yourself, taking into account the restrictions given in the table below.

Features:

- you cannot create objects of the same type with the same identifiers in the system;

- you can change the identifier only when creating an object (see Create an object). After creation, the identifier cannot be changed.

22.3.8.1 The Hardware tab

№	Object type	You can use in the Number
1	Alarm notification window	Numbers, letters, periods, hyphen, dash, and underscore
2	ATM	Numbers, letters, periods, hyphen, dash, and underscore
3	Audio card	Only numbers from 1 to 2147483647
4	Microphone	Only numbers from 1 to 32767
5	Audio playback card	Only numbers from 1 to 2147483647
6	Speaker	Only numbers from 1 to 255
7	NGP manager	Numbers, letters, periods, hyphen, dash, and underscore
8	Backup archive	Numbers, letters, periods, hyphen, dash, and underscore
9	Backup audio archive	Numbers, letters, periods, hyphen, dash, and underscore
10	BacNet	Numbers, letters, periods, hyphen, dash, and underscore
11	Control device	Only numbers from 1 to 2147483647
12	Data replication service	Numbers, letters, periods, hyphen, dash, and underscore
13	Event counter	Numbers, letters, periods, hyphen, dash, and underscore
14	Failover service	Numbers, letters, periods, hyphen, dash, and underscore
15	HTTP Server	Only numbers from 1 to 2147483647
16	IIDK Interface	Numbers, letters, periods, hyphen, dash, and underscore
17	Incident server	Numbers, letters, periods, hyphen, dash, and underscore
18	Incident handler	Numbers, letters, periods, hyphen, dash, and underscore
19	Intercom subsystem	Numbers, letters, periods, hyphen, dash, and underscore
20	Intercom	Numbers, letters, periods, hyphen, dash, and underscore
21	ISD integration server	Numbers, letters, periods, hyphen, dash, and underscore
22	Special keyboard	Numbers, letters, periods, hyphen, dash, and underscore

№	Object type	You can use in the Number
23	LDAP service	Numbers, letters, periods, hyphen, dash, and underscore
24	Mail Message Service	Numbers, letters, periods, hyphen, dash, and underscore
25	Mail message	Numbers, letters, periods, hyphen, dash, and underscore
26	Failover manager	Numbers, letters, periods, hyphen, dash, and underscore
27	Manitou	Numbers, letters, periods, hyphen, dash, and underscore
28	Map server	Numbers, letters, periods, hyphen, dash, and underscore
29	ONVIF-Server	Numbers, letters, periods, hyphen, dash, and underscore
30	ONVIF-Server Profile	Numbers, letters, periods, hyphen, dash, and underscore
31	Operator query panel	Numbers, letters, periods, hyphen, dash, and underscore
32	RTSP Server	Numbers, letters, periods, hyphen, dash, and underscore
33	Short Message Service	Numbers, letters, periods, hyphen, dash, and underscore
34	Short Message	Numbers, letters, periods, hyphen, dash, and underscore
35	SIP-terminal	Numbers, letters, periods, hyphen, dash, and underscore
36	SIP trunk	Numbers, letters, periods, hyphen, dash, and underscore
37	Address book	Numbers, letters, periods, hyphen, dash, and underscore
38	SIP-device	Numbers, letters, periods, hyphen, dash, and underscore
39	SIP-operator	Numbers, letters, periods, hyphen, dash, and underscore
40	SNMP service	Only numbers from 1 to 2147483647
41	SNMP trap	Only numbers from 1 to 2147483647
42	Sound notification	Only numbers from 1 to 2147483647
43	System restart service	Numbers, letters, periods, hyphen, dash, and underscore
44	Telegram bot	Numbers, letters, periods, hyphen, dash, and underscore
45	Telemetry Controller	Numbers, letters, periods, hyphen, dash, and underscore
46	Control panel	Numbers, letters, periods, hyphen, dash, and underscore

№	Object type	You can use in the Number
47	PTZ device	Numbers, letters, periods, hyphen, dash, and underscore
48	Video capture device	Only numbers from 1 to 2147483647
49	Camera	Only numbers from 1 to 2147483647
50	Analog sensor	Only numbers from 1 to 2147483647
51	Edge storage	Numbers, letters, periods, hyphen, dash, and underscore
52	Relay	Only numbers from 1 to 2147483647
53	Sensor	Only numbers from 1 to 2147483647
54	Captioner	Only numbers from 1 to 2147483647
55	Detection zone	Numbers, letters, periods, hyphen, dash, and underscore
56	ECHD channel	Only numbers from 1 to 2147483647
57	Embedded detection	Only numbers from 1 to 2147483647
58	Face Detection	Numbers, letters, periods, hyphen, dash, and underscore
59	MPEG4 encoder	Only numbers from 1 to 2147483647
60	Tag&Track	Numbers, letters, periods, hyphen, dash, and underscore
61	Tracker	Only numbers from 1 to 2147483647
62	Neurofilter	Only numbers from 1 to 2147483647
63	VMDA detection	Only numbers from 1 to 2147483647
64	VideoIntellect detection	Numbers, letters, periods, hyphen, dash, and underscore
65	Video.run watcher	Only numbers from 1 to 2147483647
66	Videogate	Only numbers from 1 to 2147483647
67	VideoGuard integration client	Only numbers from 1 to 2147483647
68	VideoGuard message filter	Only numbers from 1 to 2147483647
69	VideoIntellect Client	Numbers, letters, periods, hyphen, dash, and underscore
70	VMDA metadata storage	Numbers, letters, periods, hyphen, dash, and underscore

№	Object type	You can use in the Number
70	Search channel	Numbers, letters, periods, hyphen, dash, and underscore
72	Voice Message Service	Numbers, letters, periods, hyphen, dash, and underscore
73	Voice message	Numbers, letters, periods, hyphen, dash, and underscore
74	Voice Notification Service	Numbers, letters, periods, hyphen, dash, and underscore
75	Web-server	Only numbers from 1 to 2147483647
76	Web-server 2.0	Only numbers from 1 to 2147483647
77	Yitu client	Numbers, letters, periods, hyphen, dash, and underscore
78	Computer	Numbers, letters, periods, hyphen, dash, underscore, and any symbols. Maximum 15 characters

22.3.8.2 **The Interfaces tab**

№	Name	You can use in the Number
1	Display	Numbers, letters, periods, hyphen, dash, and underscore
2	Audio player	Numbers, letters, periods, hyphen, dash, and underscore
3	Panel of Backup archive	Numbers, letters, periods, hyphen, dash, and underscore
4	Captions search	Numbers, letters, periods, hyphen, dash, and underscore
5	Charts	Numbers, letters, periods, hyphen, dash, and underscore
6	Configuration check	Numbers, letters, periods, hyphen, dash, and underscore
7	Display manager	Numbers, letters, periods, hyphen, dash, and underscore
8	Event Viewer	Numbers, letters, periods, hyphen, dash, and underscore
9	External window	Numbers, letters, periods, hyphen, dash, and underscore
10	HTML Interface	Only numbers from 1 to 2147483647
11	HTML page	Only numbers from 1 to 2147483647
12	Incident manager	Numbers, letters, periods, hyphen, dash, and underscore
13	Intercom Control Monitor	Numbers, letters, periods, hyphen, dash, and underscore

№	Name	You can use in the Number
14	Live sound switch	Only numbers from 1 to 2147483647
15	Map	Only numbers from 1 to 2147483647
16	Layer	Only numbers from 1 to 2147483647
17	Monitor	Numbers, letters, periods, hyphen, dash, and underscore
18	Operator protocol	Numbers, letters, periods, hyphen, dash, and underscore
19	Scene	Numbers, letters, periods, hyphen, dash, and underscore
20	SIP-panel	Numbers, letters, periods, hyphen, dash, and underscore
21	State statistics	Numbers, letters, periods, hyphen, dash, and underscore
22	Telemetry control panel	Numbers, letters, periods, hyphen, dash, and underscore

22.3.8.3 The Users tab

№	Name	You can use in the Number
1	Department	Numbers, letters, periods, hyphen, dash, and underscore
2	User	Numbers, letters, periods, hyphen, dash, and underscore
3	User permissions	Numbers, letters, periods, hyphen, dash, and underscore

22.3.8.4 The Programming tab

№	Name	You can use in the Number
1	Area	Numbers, letters, periods, hyphen, dash, and underscore
2	Region	Only numbers from 1 to 65534
3	Rule of states transition	Only numbers from 1 to 65534
4	Time schedule	Only numbers from 1 to 65534
5	Timer	Only numbers from 1 to 2147483647
6	Script	Only numbers from 1 to 2147483647
7	Program	Numbers, letters, periods, hyphen, dash, and underscore

№	Name	You can use in the Number
8	Macro event	Numbers, letters, periods, hyphen, dash, and underscore
9	Macro	Numbers, letters, periods, hyphen, dash, and underscore
10	Objects link	Numbers, letters, periods, hyphen, dash, and underscore
11	Access level	Only numbers from 1 to 65534

For **virtual objects**, you can use numbers, letters, periods, hyphen, dash, and underscore in the identifier.

23 Intellect configuration and setup

23.1 Configuration procedure for servers, clients and remote workstations

23.1.1 Server settings

23.1.1.1 Server hardware and software platform

The video surveillance system based on INTELLECT™ software uses Servers to receive and process video signals from analog and IP surveillance cameras. The Server hardware and software platform generally contains:

1. A personal computer that meets the requirements of INTELLECT™ software.
2. Embedded video capture cards or Guardant dongle that enables receiving video from IP devices only.
3. INTELLECT™ software with the **Server** configuration (see Installation of Intellect as a Server/Remote Administrator's workstation).
4. The license key with rights to use video capture cards or IP devices along with INTELLECT™ software.
5. MS SQL server software for INTELLECT™ system database control.

> **Attention!**
>
> The same set of program modules specified in the intellect.sec license key is to be set for proper operation of the system on all Servers (see Program modules section).

> **Attention!**
>
> Proper operation of INTELLECT™ is possible only if the user has OS Windows administrator rights.

23.1.1.2 Setting up a Server

The main task of the Server is receiving and processing of video signals. It provides several options: audio signal receiving and processing, PTZ control, security services, user's auto functions (macros), etc. Server setup sequence depends on its hardware configuration and the options to be realized.

To configure the Server, follow the steps:

1. Start the INTELLECT™ program on the Server (see Operator's Guide).
2. With remote Server setup (e.g., from the administering Server), register the **Computer** object, which corresponds to the Server, and set the interaction parameters with the Servers, Remote Admin Workstations, Remote Clients of the distributed video surveillance system (see Configuration of distributed architecture section). While local setting up the Server the relevant **Computer** object is created automatically in the **Hardware** tab during the first startup.
3. Configure hardware that is connected to the Server (see Configuration of hardware section). This includes the following steps:
    a. Configure the Server video subsystem (see Configuring video subsystem section).
    b. Configure the Server audio subsystem if there are microphones (see Configuring audio subsystem section).
    c. If there are sensors and relays, create and configure the relevant objects (see Installing and configuring security system components guide).
    d. Configure backup video archiving on the Server, if necessary (see Configuring backup archiving section).
    e. Configure the hardware performance tester and restart service, enable and configure the notification services (see Notification services and Configuring the System restart service sections).
    f. Set up logging of events registered for the Server system objects (see Configuring events logging).
4. If the Server is to be used as the Operator's workstation, configure the user interface: video surveillance monitor, audio player, map etc. (see Configuring the user interface section).
5. Assign the users rights to work with Server system objects (see Configuration of users and permissions section).
6. If auto options are to be used, create the macros and time zones, etc. (see System settings (the Programming tab) section).

23.1.2 Configuring a Remote Admin Workstation

23.1.2.1 Remote Admin Workstation hardware and program platform

The video surveillance system based on INTELLECT™ software uses Remote Admin Workstations for remote administering of INTELLECT™ software installed on Servers and other Remote Admin Workstations of the distributed video surveillance system, as well as the specialized platforms: videogate, remote archive server, remote web server etc. The Remote Admin Workstation can perform several of these functions or one of them.

> **Note.**
>
> Audio and video from IP devices can be processed at Remote Admin Workstations.

Remote Admin Workstation hardware and software platform contains:

1. Personal computer that meets the requirements of INTELLECT™ software.
2. Guardant dongle.
3. INTELLECT™ software with the “Remote Admin Workstation” configuration (see Installation of Intellect as a Server/ Remote Administrator's workstation).
4. License activation key.
5. MS SQL server software to control the *Intellect*™ database.

23.1.2.2 Remote Admin Workstation configuration

In a simple case a Remote Admin Workstation may be used for remote administering only.

To configure a Remote Admin Workstation, follow the steps:

1. Start the INTELLECT™ program on Remote Admin Workstation (see Operator's Guide).
2. With remote setup (e.g., from the administering Server), register the **Computer** object, which corresponds to the Remote Admin Workstation, and set the interaction parameters with the Servers, Remote Admin Workstations, Remote Clients of the distributed video surveillance system (see Configuration of distributed architecture section). While local setting up the Remote Admin Workstation the relevant **Computer** object is created automatically in the **Hardware** tab during the first startup.
3. Configure the hardware performance tester and restart service (see Configuring the System restart service section).
4. Set up logging of events registered for the Remote Admin Workstation system objects (see Configuring events logging).
5. If the Remote Admin Workstation is to be used as the Operator’s workstation, configure the user interface: video surveillance monitor, audio player, map etc. (see Configuration of interfaces section).
6. Assign the users rights to work with Remote Admin Workstation system objects (see Rights administration section).
7. If auto options are to be used, create the macros and time zones, enable and configure the notification services (see System settings (the Programming tab) and Notification services sections).

23.1.2.3 Videogate configuration

Videogates are used in large-scale distributed video surveillance systems for video signal routing among the Servers, Remote Admin Workstations and Remote Clients that are in different subnets.

To configure the gateway, do the following:

1. Start the INTELLECT™ program on the videogate (see Operator's Guide).
2. With remote setup of the videogate (e.g., from the administering Server), register the **Computer** object, corresponding to the Remote Admin Workstation, and set the parameters of interaction with Servers, Remote Admin Workstations and Remote Clients of the distributed video surveillance system (see Configuration of distributed architecture section). While local setup of the videogate the relevant **Computer** object is created automatically in the **Hardware** tab during the first startup.
3. Enable and configure the **Videogate** module (see Configuring the Videogate module section).
4. Configure the hardware performance tester and the restart service (see Configuring the System restart service section).
5. Set up logging of events registered for the **Videogate** system objects (see Configuring events logging).
6. Assign the rights to users in order to work with the **Videogate** system objects (see Configuration of users and permissions section).

7. If auto options are to be used, create the macros and time zones, enable and configure the notification services (see System settings (the Programming tab) and Notification services sections).

23.1.2.4 Configuring backup archive server

INTELLECT™ software has a backup archiving option for video records from the video surveillance Servers. As the archiving process requires great computer resources, archiving is not to be performed on the Servers directly. It is strongly recommended to choose the individual Remote Admin Workstation as the archiving Server.

To configure the archiving server, do the following:

1. Start the INTELLECT™ program on the archive server (Operator's Guide).
2. With remote setup of the archive server (e.g., from the administering Server), register the **Computer** object, corresponding to the archive server, and set the parameters of interaction with the Servers, Remote Admin Workstations and Remote Clients of the distributed video surveillance system (see Configuration of distributed architecture section). While local setup of the archive server the relevant **Computer** object is created automatically in the **Hardware** tab during the first startup.
3. Enable and configure the **Backup archive** module (see Configuring backup archiving section).
4. Configure the hardware performance tester and the restart service (see Configuring the System restart service section).
5. Set up logging of events registered for the **Videogate** system objects (see Configuring events logging).
6. Assign the rights to users in order to work with the **Videogate** system objects (see Configuration of users and permissions section).
7. If auto options are to be used, create the macros and time zones, enable and configure the notification services (see System settings (the Programming tab) and Notification services sections).

23.1.2.5 Configuring remote Web-server

The video surveillance system based on INTELLECT™ software uses the remote web-server to transmit video signals and to receive Operator's commands via the Internet. It is recommended for large-scale systems with a distributed structure to use the remote web server on the individual Remote Admin Workstation instead of a local one on one of Servers.

> **Note.**
>
> The remote web-server should be allocated in the individual subnet and on the outer IP address (for its operation as an Internet HTTP server). Therefore the web server should be set to receive video signals via the videogate. The videogate can be the remote one (remote computer with installed and configured *Videogate* module) or the local one (*Videogate* module is installed and configured on the same computer with the web-server).

To configure the remote web server, follow the steps:

1. Start the INTELLECT™ program on the web-server.
2. With web-server remote setup (e.g., from the administering Server), register the **Computer** object, which corresponds to the web-server, and set the interaction parameters with the Servers, Remote Admin Workstations, Remote Clients of the distributed video surveillance system (see Configuration of distributed architecture section). While local setting up the web-server the relevant **Computer** object is created automatically in the **Hardware** tab during the first startup.
3. Enable and configure the *Web-server* module (see Configuring the Web-server module section).
4. If no remote videogate is used, then enable and configure the *Videogate* module (see Configuring the Videogate module section).
5. Configure the hardware performance tester and restart service (see Configuring the System restart service section).
6. Set up logging of events registered for the **Web-server** system objects (see Configuring events logging).
7. Assign the users rights to work with the **Web-server** system objects (see Configuration of users and permissions section).
8. If auto options are to be used, create the macros and time zones, enable and configure the notification services (see System settings (the Programming tab) and Notification services sections).

23.1.3 OS settings for correct operation of Remote Admin Workstation or Server

The user who does not belong to the "Administrators" group can work with Intellect software correctly if the following requirements are fulfilled:

1. UAC (Users account control) is disabled for Windows 7, Windows 8, Windows 8.1, Windows 10 OS. UAC can be disabled on the Control panel by Administrator of computer.

   > **Attention!**
   >
   > Low position of the **Do not notify me** slider on the **User account control parameter** page doesn't mean the full UAC disabling in the Windows 8, Windows 8.1 or Windows 10. Configuration of the local security policy is required for full disabling the UAC. Configuration is performed on the **Control panel** → **Administrating** → **Local security policy** window.
   > It is required to disable all policies names of which are started from "User Account Control", apart from:
   > **User Account Control: request action to increase rights for administrators in the mode of administrator approval**—set the Increasing without request item in the **Security parameter** value.
   > **User Account Control: request action to increase rights for users**—set the Account request item in the **Security parameter** value.

2. User is to have the free access to the AxxonSoft thread in the registry HKEY_LOCAL_MACHINE\Software\AxxonSoft section for 32-bit system (HKEY_LOCAL_MACHINE \Software\Wow6432Node\AxxonSoft for 64-bit system).
3. User is to have the free access to the folder in which the Intellect software is installed.
4. User is to have the free access to the VIDEO and AUDIO folders on all logical disks in the system.
5. If the HKEY_LOCAL_MACHINE\Software\AxxonSoft\Intellect\BackupFolder key is in the registry (HKEY_LOCAL_MACHINE \Software\Wow6432Node\AxxonSoft\Intellect\BackupFolder for 64-bits system), the free access to the folder specified in the BackupFolder key is to be granted to user. For more information on this key please see Creating the database backup copy.
6. The free access to the following folders is needed if there is no the BackupFolder key:
   a. C:\ProgramData\—for Windows 7 OS;
   b. C:\ Documents and Settings\All Users\Application Data\—for Windows XP OS.
7. The user is to have SeCreateGlobalPrivilege rights. Open the **Local security policy** tool (**Control panel** → **Administration**), select **Local policies** → **Assign User rights** → **Global objects** creation and add the existing user to the folder.
8. In Microsoft SQL Server Management Studio, assign the sysadmin role to the BUILTIN\Users group:
   a. In the Microsoft SQL Server Management Studio object explorer, select **Security** → **Logins**;
   b. In the **BUILTIN\Users** context menu select **Properties**;
   c. In the properties, select **Server Roles** and set the **sysadmin** checkbox, then click **OK**.

23.1.4 Configuring Remote Clients (RC)

23.1.4.1 Remote Client hardware and software platform

Remote Clients are used as Operator's workstations and provide remote video surveillance and audio monitoring: video and audio monitoring, sensor status control, cameras and PTZ units control and so on.

At a Remote Client administering options (one cannot create, delete and configure objects in the system as well as register users and administer their rights) as well as local database (database on the remote computer with installed INTELLECT™ system is in use) are inaccessible.

The Remote Client hardware and program platform generally contains:

1. A personal computer, that meets the requirements of INTELLECT™ software.
2. The *Intellect*™ software with the **Client** configuration (see Installation of INTELLECT™ software to the Client section).

23.1.4.2 Configuring Remote Client

The basic function of the remote Client is receiving video and audio signals from video surveillance system Servers, video and audio monitoring, cameras, microphones and PTZ units control via various components of the Operator interface (video surveillance monitor, audio player, map, PTZ window etc.).

To configure the Remote Client, follow the steps:

1. Register the **Computer** object, which corresponds to the Remote Client, and set the interaction parameters with the Servers, Remote Admin Workstations, Remote Clients of the distributed video surveillance system on the administering

server (see Configuring the INTELLECT™software system with distributed architecture of the digital video surveillance system section).
2. Configure the User interface by creating screen(s) and setting up the Remote Client access to them. The screen(s) should contain the user interface components: video surveillance monitor, audio player, map etc. (see Configuring the user interface section).

23.1.4.3 OS settings for correct operation of Remote Client

Fulfill the following conditions to work correctly with INTELLECT™ software which is installed as Remote Client by the user who does not belong to the “Administrators” group:

1. User is to have the free access to the ITV thread in the registry HKEY_LOCAL_MACHINE\Software\ITV section for 32-bit system (HKEY_LOCAL_MACHINE \Software\Wow6432Node\ITV for 64-bit system).
2. User is to have the free access to the folder in which INTELLECT™ software is installed.

23.2 Configuration of distributed architecture

23.2.1 General principles of designing the digital video surveillance system with distributed architecture

The digital video surveillance system generally contains:

1. Servers – hardware and program platforms used to receive and process video and audio signals from analog and IP surveillance cameras.
2. Remote Admin Workstations – hardware and program platforms used for remote administering of the video surveillance system and as the specialized platforms for: video gateway, remote archive server, remote web server etc.
3. Remote Client – hardware and program platforms used as Operator’s workstations to realize remote video surveillance and audio monitoring:

Servers, Remote Admin Workstations and Remote Clients are integrated into the video surveillance system, fitting the system set of functions, safety requirements, specific features of the guarded location etc. The video surveillance system may include several subnets, that interact via selected (node) servers and Remote Admin Workstations. The distributed architecture of the video surveillance system provides synchro data exchange (events, commands, setting parameters, etc) among its components.

Servers, RAWs and ROWs communicate with each other in LAN, WAN, VPN, Wireless networks using TCP protocol.

Note.

One version of the *Intellect* software package is to be installed on all components of the distributed system. This is due to the database structure of the *Intellect* software package can differ in different versions so the data loss can occur.

Requirements for the software and hardware platform

23.2.2 Configuring procedure for the distributed system

To configure the distributed video surveillance system, follow the steps:

1. Design the surveillance system structure project, if it has not been developed before (see Selecting the structure of the distributed system).
2. Set up database synchronization for all servers and Remote Admin Workstations in compliance with the system structure project (see Synchronizing the databases of servers and remote workstations).
3. Register the servers, Remote Admin Workstations and Remote Clients from the same subnet on the administering server of this subnet (or at node Remote Admin Workstations and servers, that optionally realize the administering server function, if there are any subnets). If any selected subnets are present in the system, register the servers and Remote Admin Workstations that provide interaction of subnets (see Registration of servers, clients and remote workstations on the administering server).

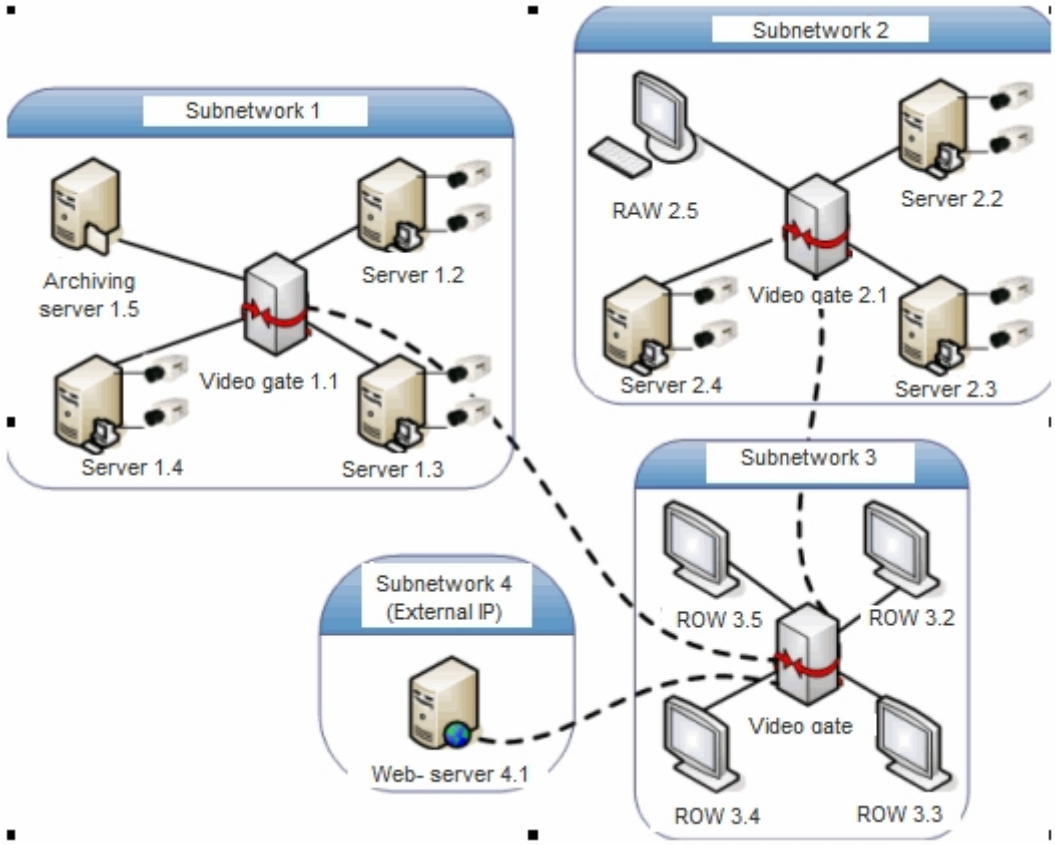
4. Set up interaction of servers, Remote Admin Workstation and Remote Clients in compliance with the system structure project (see Configuring the interaction of distributed system components).
5. Set up time synchronization in the distributed system, if necessary (Configuring time synchronization in the distributed system).
6. Specify computers in the distributed system which will be used only as Clients (see Role-assignment in distributed system).

23.2.3 Selecting the structure of the distributed system

While designing the distributed video surveillance system structure you should take into account:

1. The number of servers, Remote Admin Workstations and Remote Clients to be installed on the guarded location.
2. The distances between video surveillance system components and their comminication channels capacity. For example, servers are divided by long stretches of land, and the Remote Admin Workstation and Remote Client are within the same room – the central surveillance station. Given the engineering constraints, servers will have the low capacity channels, and the Remote Admin Workstation and Remote Client will have high capacity channels. Then Remote Admin Workstation and Remote Client will interact with the servers via the gateway only.
3. The system security requirements, for example, to prevent unauthorized administering, subnets with servers and Remote Admin Workstations and subnets with Remote Clients, are separated. Subnets interact via the gateway only.

An example of organization of the distributed video surveillance system is shown in the figure.



23.2.4 Synchronizing the databases of servers and remote workstations

INTELLECT™ software servers and Remote Admin Workstations configuration parameters are stored in the distributed database. Each server and Remote Admin Workstation store local copies of the distributed database. Local database copies should be synced to provide distributed operation of INTELLECT™ software and data replication (synchro alteration of local database copies).

The following synchronization mechanisms are used in *Intellect*:

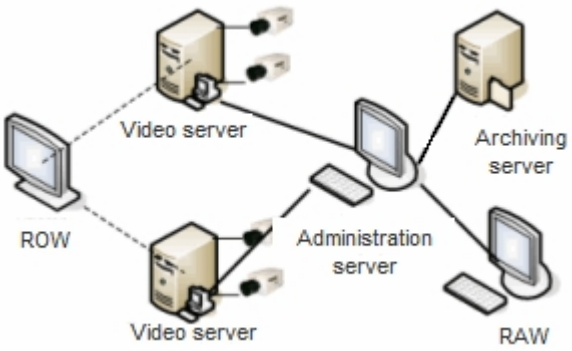
1. Internal synchronization. All changes are applied to computers automatically. This mechanism is used by default and does not require any further configuration. Internal synchronization can be disabled – see Configuring internal synchronization.
2. DB synchronization of recipients with sources when starting *Intellect*:

1. Configuration synchronization (see Database synchronization setup).
2. Configuration and protocol synchronization (see Database synchronization setup and make changes to sync.xml file).

> **Note.**
>
> DB tables that are not synchronized during synchronization are in the sync.xml file. It is highly recommended not to change this file.

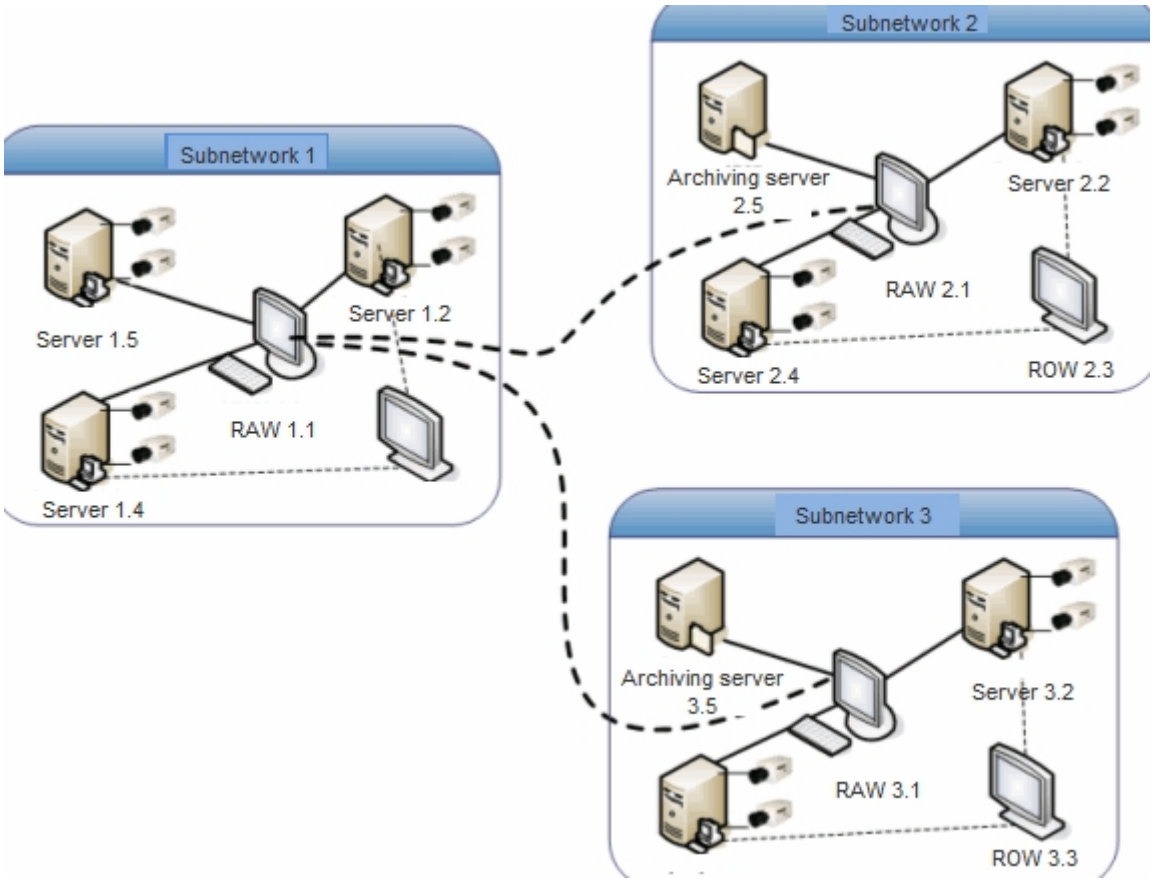
3. Only protocol synchronization (see Configuring the Event Viewer databases synchronization).

In the simplest case, database synchronization is performed for all servers and Remote Admin Workstations with the database of the administering server.



> **Note.**
>
> The Remote Client has no database; therefore the administering server database should not be synced with it.

If any selected subnets are present in the system, the servers and Remote Admin Workstation databases should be synced with the node server or Remote Admin Workstation database (see, for example, figure below).



For example, to set up database synchronization for the servers of the distributed system shown in the figure, you need:

1. to sync the databases of 1.2, 1.4, 1.5 servers with 1.1 Remote Admin Workstation database;
2. to sync the databases of 2.2, 2.4 servers and 2.5 archiving server with 2.1 Remote Admin Workstation database;
3. to sync databases of 3.2, 3.4 servers and 3.5 archiving server with 3.1 Remote Admin Workstation database;
4. to sync databases of 3.1 and 2.1 and Remote Admin Workstations with 1.1 Remote Admin Workstation database;

For detailed instructions on database synchronization setup see INTELLECT™ software database management.

23.2.5 Registration of servers, clients and remote workstations on the administering server

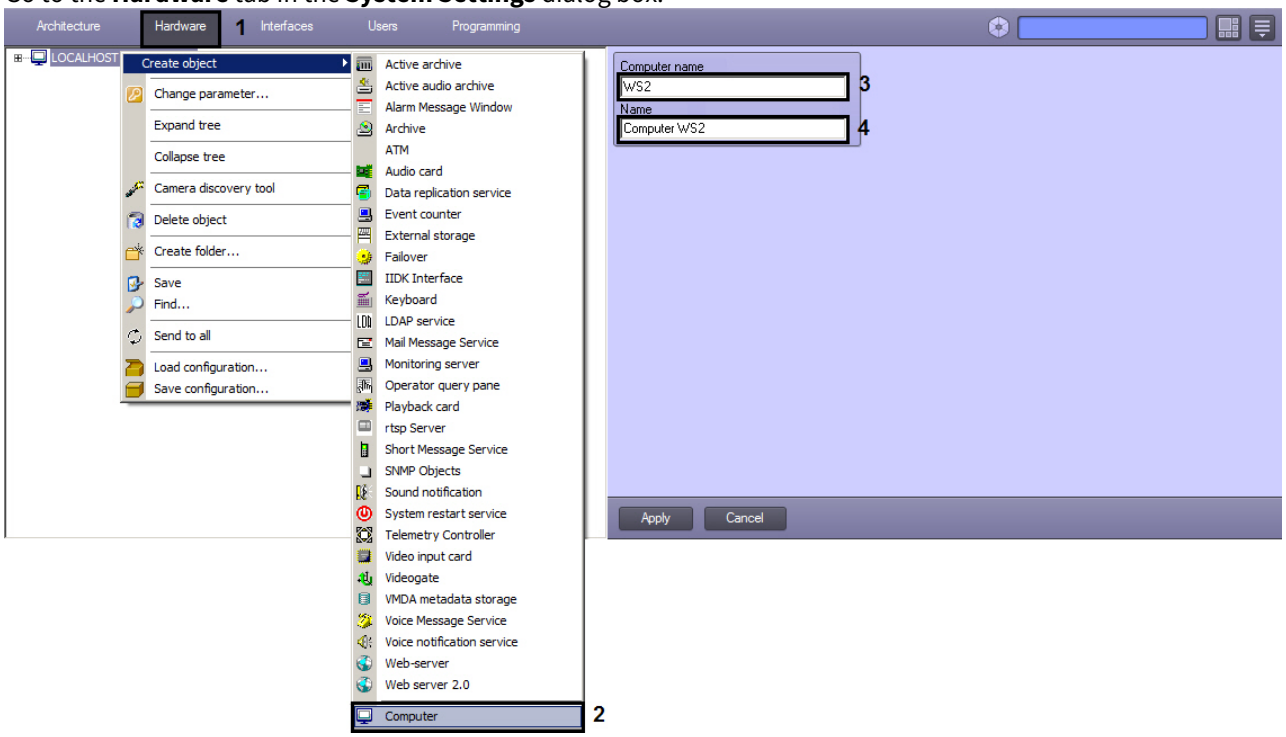
Administering the servers and Remote Admin Workstations is usually performed from one selected Workstation – the administering server. It is recommended to have one administering server for any single selected video surveillance subnet (e.g. for security reasons).

All servers, Remote Admin Workstations and Remote Clients should be registered on the administering server.

To register the servers and remote Workstations on the administering server, follow the procedure:

1. Make sure that the synchronization of all servers and Remote Admin Workstations databases with the administering server database is set properly (see the previous section).
2. Check the servers, Remote Admin Workstations and Remote Clients connections to the subnet.
3. Launch the INTELLECT™ program on the administration server.
4. Register the **Computer** system object on the administering server for each server. Remote Admin Workstation or Remote Client. For that follow the steps:

a. Go to the **Hardware** tab in the **System Settings** dialog box.



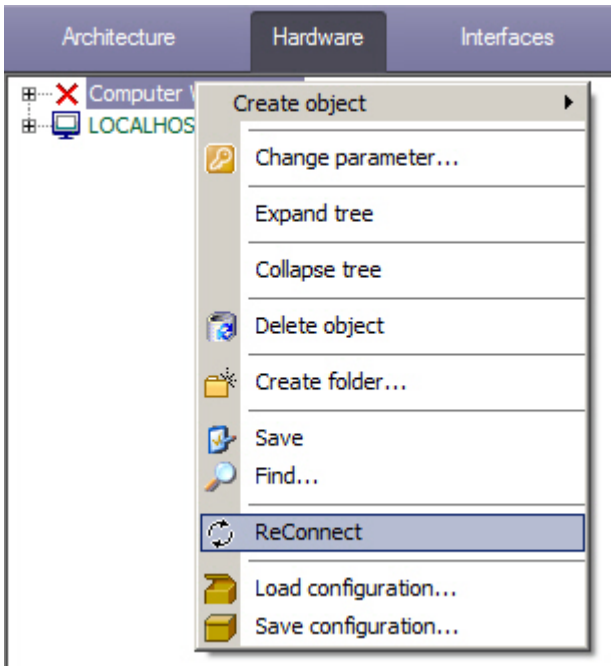
b. Create a **Computer** object on the base of the **Computer** object.
c. Enter the network name of the server, Remote Admin Workstation or Remote Client in the **Computer name** field.

> **Note.**
>
> The maximum length for the network name is 15 characters. If the network name is longer than 15 characters, then first 15 characters are to be specified as the network name in this field.
> The computer name may only consist of Latin characters and digits.

d. Enter the name, used for the computer by the INTELLECT™ software, in the **Name** field.
e. Click the **Apply** button.

5. Repeat the 4th step for each server, Remote Admin Workstation and Remote Client of the distributed video surveillance system (or its subnet).
6. Start the INTELLECT™ program on all operator and administration workstations and servers.
7. If communication exists between the administering server and the server, Remote Admin Workstation or Remote Client, the **Computer** object will be assigned the «» icon on the objects tree.
8. If no connection exists between the administering server and the server, Remote Admin Workstation or Remote Client, the **Computer** object will be assigned the «» icon on the objects tree. The most probable causes of disconnection are INTELLECT™ software failure on the server, Remote Admin Workstation or Remote Client; network disconnection, faulty database synchronization, wrong network name. Detect and remove the cause of disconnection before continuing to configure the system, then try to connect the administering server to the server, Remote Admin Workstation or Remote Client again.

To connect to the the server, Remote Admin Workstation or Remote Client from the remote administering server without restarting INTELLECT™ software, right click the relevant **Computer** object to display the context menu and select **Reconnect**.



Registration of servers, Remote Admin Workstations and Remote Clients on the administering server is completed.

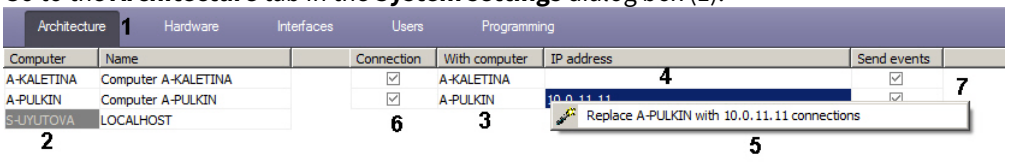
23.2.6 Configuring the interaction of distributed system components

To provide distributed system operation, Servers, Remote Admin Workstations and Remote Clients interactions are to be configured. Servers, Remote Admin Workstations and Remote Clients interaction means database replication (for Servers and Remote Admin Workstations only) and event exchange. For each Server, Remote Admin Workstation and Remote Client lists of interacting and non-interacting Servers, Remote Admin Workstations and Remote Clients are to be created.

Configuration of the surveillance system interaction is performed from the administering Server or, if there are dedicated subnets, from the node Server or Remote Admin Workstation.

To configure the interaction between the distributed system components, do the following:

1. Go to the **Architecture** tab in the **System settings** dialog box (1).



2. The **Computer** column displays the list of names of Servers, Remote Admin Workstations and Remote Clients registered in the **Hardware** tab (2). In the **Computer** column left click the name of the Server, Remote Admin Workstation or Remote Client to change its interaction settings. Text in the selected cell becomes grey.

> **Note**
>
> To search computer by name use Ctrl+F hotkeys combination. The **Search in tree** window will be opened, enter the full computer name or its part in it and click the Enter button. Found computer will be highlighted in grey in the list.
>
>
>

3. The **With computer** column displays the list of those Servers, Remote Admin Workstations and Remote Clients, with which the selected Server, Remote Admin Workstation or Remote Client is able to interact (3).
4. In the **IP address** column, specify the addresses of the computers you are connecting to (4). By default, the IP address is to be specified. If the **DNS instead of IP allowed** checkbox is set checked on the settings panel of the **Security zone** object in the **Programming** tab, then DNS name can be specified instead of IP address. If computer addresses are set automatically (DHCP is configured), then **IP address** field can be left blank.

> **Note**
>
> If the computer name is correct, then the IP address can be filled in automatically. For this, specify the question mark "?" in the **IP address** field and press the Enter key on the keyboard.

5. If the specified IP address is to be set for all communications with this computer in the distributed system, right-click in the **IP address** field and select **Replace links from <Computer name> to <IP-address>** in the opened feature menu (5). This is allowed if computers with one network interface are used in the system and the specified IP address is to be used to communicate with these computers.

> **Important!**
>
> When clicking the **Apply** button (see step 10), the changes will be saved only for the current computer. In order for the IP address to be saved for all computers in the distributed system, click the **Apply** button holding down the **Ctrl** key on the keyboard.

6. If the box next the **Connection** column and the row, corresponding to the Server, Remote Admin Workstation or Remote Client is checked, then the data on system configuration of the selected Server, Remote Admin Workstation or Remote Client with any Server, Remote Admin Workstation or Remote Client is exchanged (6). To forbid exchange of configuration data with the selected Server, Remote Admin Workstation or Remote Client, set the checkbox in the **Connection** column unchecked.

> **Note**
>
> Server or Remote Admin Workstation always exchange configuration parameters with Remote Client, even if the Connection checkbox is unchecked for this Remote Client.

7. If the box next to the **Send events** column and the row, corresponding to the Server or Remote Admin Workstation is checked, then events are exchanged between selected Server or Remote Admin Workstation and any Server or Remote Admin Workstation (7). To forbid event exchange with the selected Server, Remote Admin Workstation or Remote Client, set the checkbox in the **Send event** column unchecked.

> **Note**
>
> Server or Remote Admin Workstation always exchange configuration parameters with Remote Client, even if the **Send events** checkbox is unchecked for this Remote Client.

> **Note**
>
> In order to set all checkboxes in the **Connection** or **Send events** columns, highlight a box in the required column and click Ctrl+A. To set all the checkboxes unchecked, highlight a box and click Shift+A.

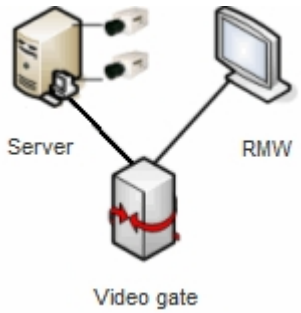
8. If modems are used for connecting the distributed system components, then fill in the **Connection, User and Password** fields in the **Hardware** tab of the **Computer** object according to the Windows modem configuration used.
9. Repeat steps 2-5 for each twain of Servers, Remote Admin Workstations and Remote Clients.
10. Click the **Apply** button

Interaction of the distributed video surveillance system components is now configured.

Let's consider setup of a Server and Remote Client connection via video gate as an example. A diagram of interaction of relevant components is shown in the figure.

Note.

Videogate is used in large distributed video surveillance systems for routing the video signals among servers and clients (or administrator workstations used as operator workstations) located in different subnetworks. See General information on the videogate for details.



According to the diagram, shown in the figure above, interaction must be disabled between the server (SERVER1) and Remote Client (MN1). As a result, the **Architecture** tab is to display the settings:

1. For the video gate (GATE), interaction is to be set with the Server (SERVER1) and with the Remote Client (MN1).

Architecture | Hardware | Interfaces | Users | Programming

Computer	Name	Connection	With computer	IP address	Send events
GATE	GATE	☑	MN1	192.168.1.2	☑
MN1	MN1	☑	SERVER1	192.168.1.3	☑
SERVER1	SERVER1				

2. For Remote Client (MN1), interaction is to be set up with the video gate (GATE), and interaction with the server (SERVER1) is to be disabled.

Architecture | Hardware | Interfaces | Users | Programming

Computer	Name	Connection	With computer	IP address	Send events
GATE	GATE	☑	GATE	192.168.1.1	☑
MN1	MN1	☐	SERVER1	192.168.1.3	☐
SERVER1	SERVER1				

3. For the server (SERVER1), interaction is to be set up with the video gate (GATE), and interaction with the Remote Client (MN1) is to be disabled.

Architecture | Hardware | Interfaces | Users | Programming

Computer	Name	Connection	With computer	IP address	Send events
GATE	GATE	☑	GATE	192.168.1.1	☐
MN1	MN1	☐	MN1	192.168.1.2	☐
SERVER1	SERVER1				

The Remote Client (MN1) **Computer** object in the **Hardware** tab in the **System settings** dialog box on the server (SERVER1) will not be displayed in the *Intellect* software package.

However, if the **Send events** checkbox is set (the **Connection** checkbox is to be deselected), the **Computer** object corresponding to the Remote Client (MN1) will be displayed on the **Hardware** tab on Server (SERVER1) tab but it will be marked with ⊗ and the object name will be highlighted by grey color. This indicates that administering of the given object is forbidden.

23.2.7 Configuring time synchronization in the distributed system

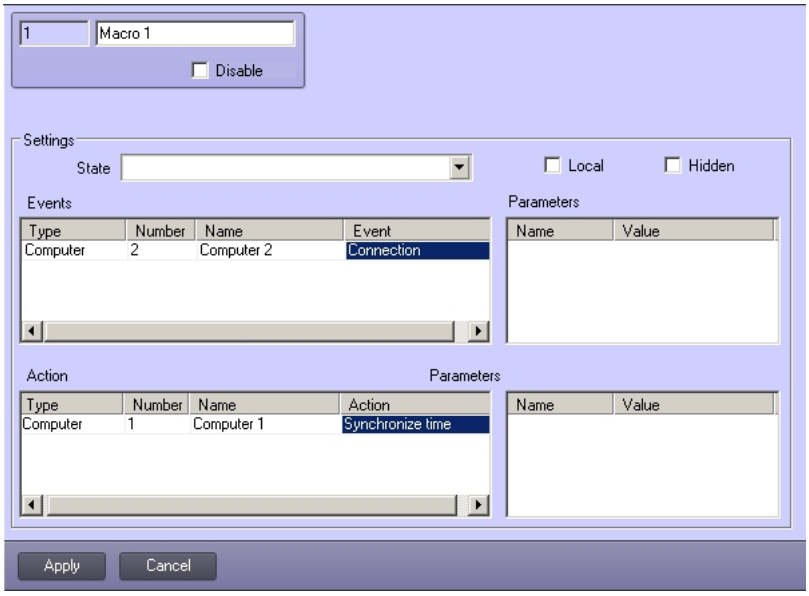
If Server is to synchronize its time with Servers connected to it when INTELLECT™ is started, do one of the following:

1. Set the **Synchronize time** checkbox on the settings panel of the **Computer** object corresponding to the Server that is the source of time synchronization (see The Settings panel of the Computer object section).
2. Set the **Time synchronization** checkbox in the tweaki.exe utility on the Server that is the source of time synchronization (see The Settings panel of the Intellect section section).
3. Create the SyncTime parameter with 1 value in the HKEY_LOCAL_MACHINE \Software\ITV\INTELLECT for 32-bit system (HKEY_LOCAL_MACHINE \Software\Wow6432Node\ ITV \INTELLECT for 64-bit system) registry on the Server that is the source of time synchronization.

Time is automatically synchronized at midnight every 24 hours or when INTELLECT™ is started on the Server that is the source of time synchronization. Synchronization can also be started by SYNC_TIME command of the SLAVE system object (see The Script object. Programming using the JScript language).

You can run a macro if time is to be synchronized when connecting the Servers that are time receivers. The details are in the Creating and using macros section.

The example of macro that synchronizes time of all Servers in the distributed system when connecting to Computer 2 if Computer 1 is configured as the source of time synchronization:



23.2.8 Role-assignment in distributed system

If it is certain that a computer is to be used as the Client only in the distributed systems (more than 30 computers), then it is to be specified on the settings panel of the corresponding **Computer** object. In this case software operation will be optimized.

Note.

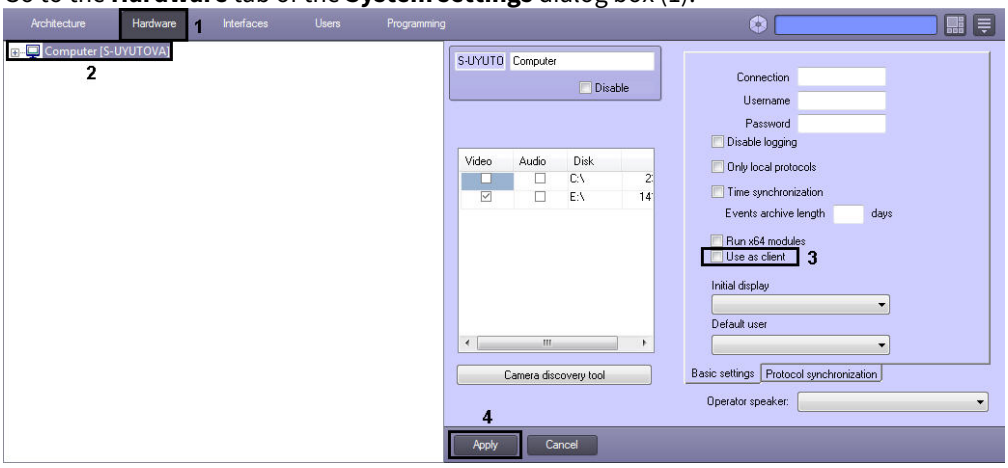
There is no need to use this setting in the smaller distributed systems.

Important!

If the computer is in use as Server/RAW and it is set to be used as the Client, then the distributed system will not operate correctly.

Role-assignment is performed as follows:

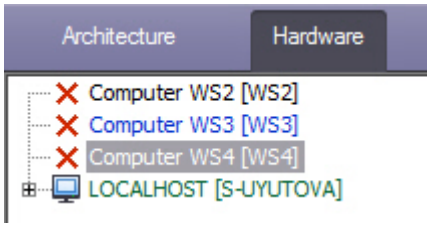
1. Go to the **Hardware** tab of the **System settings** dialog box (1).



2. Select the **Computer** corresponding to the Client (2).
3. Set the **Use as client** checkbox checked (3).
4. Click the **Apply** button (4).

The role of the computer in a distributed system is displayed in color in the object tree:

- The current Server operated locally is highlighted in **green**.
- The Clients are highlighted in **blue**.
- The other remote Servers in the system are highlighted in **black**.



The role is now assigned to the computer in the distributed system.

Requirements for TCP/IP Network
Operations using the Client

23.2.9 Features of distributed system operation using NAT

If the distributed system is built on the basis of a network in which Servers and/or Clients are behind NAT, then it is recommended to use VPN technology for the operation of such system. However, this is not a requirement: the distributed architecture may be configured in the usual way as described in Configuring the interaction of distributed system components. In this case, make sure to specify Server external IP address for Client-to-Server connection and do not specify the Client IP address.

When you configure NAT the ports that are used by started INTELLECT™ modules are to be opened — see The list of TCP ports used in INTELLECT™ section. Moreover the ports that are used by MS SQL Server for database synchronization are to be opened.

Note.

By default MS SQL Server uses 1433 TCP port and 1434 UDP port.

If an ONVIF IP-camera is behind NAT, then proper operation of this camera is not guaranteed. This limitation is due to the special features of the ONVIF protocol.

23.3 Configuration of hardware

23.3.1 Configuring of using 64-bits modules

In *Intellect* software it is possible to use modules specialized for working in 32-bits and 64-bits OS. Video.run and vmdadb.run modules, codecs, part of IP-cameras and video capture cards drivers are converted to the 64-bits platform.

Modules specialized for working on the 64-bits system allow removing restrictions on the number of connected and simultaneously displayed video channels in *Intellect* software. Using of 64-bits modules allows the system performance improvement up to 10 % comparing with 32-bits modules.

64-bit version of the **Scene** object (see Configuring object's panoramic view by means of the Scene object) is not available in *Intellect*. Some modules of vertical solution may not support 64-bits mode, while others, on the contrary, only support 64-bits mode. Please refer to the documentation for the corresponding vertical solution in here.

64-bits modules are loaded by default, and if there is no corresponding bit module, then a 32-bits module is started.

Important!

If two detection tools of DetectorPack are created in the configuration and one supports 32-bits operation while another supports only 64-bits operation, then detection module will start in 32-bits mode and 64-bits detection tool won't operate (similarly for other vertical solutions as the part of one module).

Using of 64-bits system is recommended:

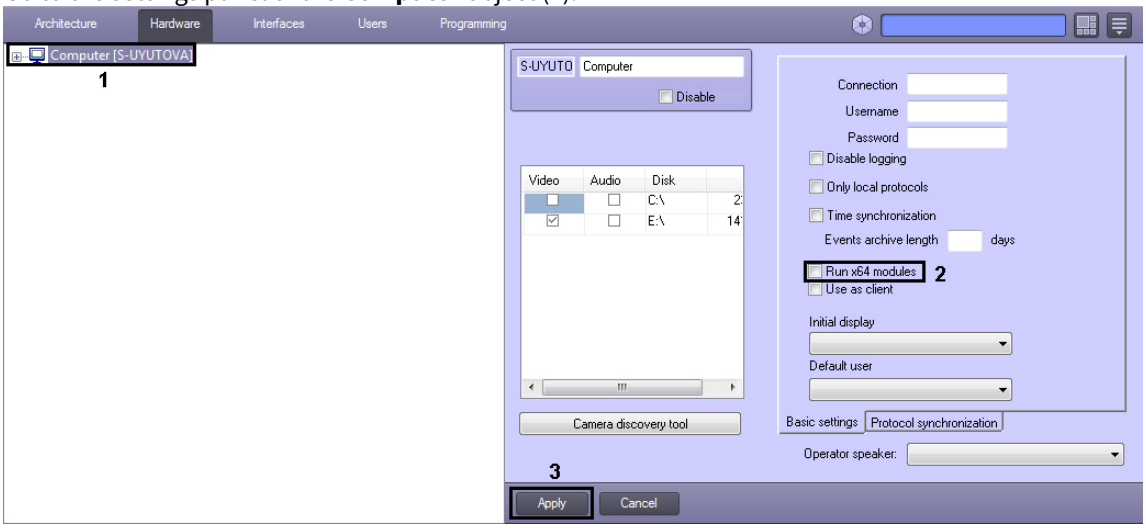
1. if the large number of cameras are to be displayed simultaneously (over 100 cameras);
2. if the large number of cameras are to be displayed in the ultrahigh resolution (over 50 cameras with 5Mpxls resolution in format without local unpacking);
3. if the large number of channels of forensic detections with search are to be in use (over 25 **Tracker** objects on the Server when video resolution is higher than 800x600).

Note

There is no 64-bits decoder for WS7 and WS17 cards with hardware compression. So video from these cards is not displayed on the remote client when 64-bits modules are in use.

To use the 64-bits modules do the following:

1. Go to the settings panel of the **Computer** object (1).



2. Set the **Run x64 modules** checkbox (2).
3. Click the **Apply** button (3).
4. Restart *Intellect*.

As a result, modules specialized for 64-bits OS will be loaded. If the 64-bits module is not found, the corresponding 32-bits module will be loaded.

Configuring of using 64-bits module is completed.

23.3.2 Configuring video subsystem

23.3.2.1 General information on configuring video subsystem

23.3.2.1.1 Video subsystem components description

In the video surveillance systems based on *Intellect,* the video subsystem is the set of software modules and hardware devices used to receive, transmit, digitize, process, record, and display video signals from video surveillance system cameras on monitor screens.

Video subsystem hardware includes:

1. video capture cards;
2. analog video camera (cameras);
3. IP devices.

Video subsystem software includes:

1. components for configuring the video capture cards;
2. components for digitized video signal compression and decompression;
3. components for digitized video signal recording;
4. components for digitized video signal transmission to Remote workstations;
5. components for displaying video signal on the monitor.

Installing security system components
Configuring video capture cards in INTELLECT™ software
Configuring IP devices
Hardware integrated into Intellect

23.3.2.1.2 Configuring video capture cards

Video capture cards are configured in the course of INTELLECT™ software administering. Video capture cards are configured by video signal digitization and processing settings, which comply with:

1. signal format (PAL or NTSC);
2. frame rate;
3. frame resolution;
4. brightness;
5. contrast;
6. color depth;
7. color rendition format.

Each camera has its individual video signal processing and digitization settings (except for the signal format, which is set for all cameras, and is attached to the same ADC).

Note.

In multistream mode (see Configuration of multistream video) settings of signal format parameters (PAL or NTSC), frames frequency, frame resolution is performed for each video stream separately on the **Camera** object's settings panel on the **Video stream** tab (see the The Settings panel of the Camera object section).

Moreover, configuring the video grabber involves setting up a proper switching of the video input channels.

Configuring video capture cards in INTELLECT™ software

Configuring the video signals processing mode while using video capture cards and analog video cameras

23.3.2.1.3 Configuring IP-devices

IP-devices are configured via the web server or any other software, supplied together with the device, and via INTELLECT™ software.

Video signal compression and processing settings (format, frame rate, frame resolution, brightness, contrast, color depth, color rendition format) are performed via the web server or any other software, supplied together with the device.

The INTELLECT™ software system receives the image, processes it with detectors, records the video signals from IP-devices and transfers it to the Remote Client.

Be sure before using an IP-device that processing and digitization settings of IP-devices (especially codecs), set via the web server, are supported by INTELLECT™ software. For actual information on IP-device compatibility, see the “Integration” section on the site of AxxonSoft company: https://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php

Requirements for IP devices
Configuring IP devices

23.3.2.1.4 Video signal compression and decompression

Video signal compression is digital video processing aimed at reducing video stream size. Compression is performed according to a specific software algorithm.

INTELLECT™ software uses a specific MotionWavelet algorithm to compress video signals received from video capture cards. This algorithm allows reducing video stream size by tens of times (from 5 to 30, subject to video signal features and compression rate).

To compress video signals from IP-devices, standard (MPEG4) or vendor designed algorithms are in use.

With compression, video stream size decreases at the cost of its quality. That is why INTELLECT™ software compresses the video signal in two modes only: in disk recording mode and in transmission to the Remote Workstation mode. The video signal is not compressed before displaying on a video server monitor.

Before displaying the compressed video signal it is decompressed. Decompression is automatically performed while displaying video signals (both real-time and archive footage playback) at Remote Workstations and video recordings playback on the videoserver.

If video resolution on the Monitor is less than resolution of compressed video, then INTELLECT™ partly decompresses video (it allows reducing load of CPU that decompresses video). Network load is reduced if the MotionWavelet codec is in use; if other codecs are in use, then the network load stays the same. Partial decompression is supported by MPEG4, MJPEG, MXPEG, Motion Wavelet and H264svc codecs. Partial decompression is not supported by H263, H264avc and Mpeg2 codecs. Only fps reduction is supported by H264svc-t codec.

Description of decompressors is shown in the table.

Decompressor	**Description**
FfmpegAllInOneDecoder	A module with a set of Ffmpeg library decoders (with an open source code). It allows converting multimedia data compressed by MxPEG, MPEG2, MPEG4 and Motion JPEG codecs.
H264InterlacedIppDecoder H264IppDecoder MPEG2IppDecoder MJPEGIppDecoder MPEG4IppDecoder	Decompressors included into the Intel Integrated Performance Primitives (Intel IPP) library. A compression format is specified in the decompressor name.
H264SvcEx	A decompressor for converting video signals in H264Svc format received from Stretch devices into the H264Avc format.

Decompressor	Description
H264SvcTex	A decompressor for converting video signals in H264Svc-t format received from VIVOTEC devices into the H264Avc format.
MxPEG Mobotix	A decompressor for converting video signals received from Mobotix devices.
Motion Wavelet 7.1	A decompressor for wavelet-converting video signals.
BOSCH	A decompressor for converting video signals received from BOSCH devices.
Intel Quick Sync	QuickSync-based decompressor decompresses video in H.264 format using embedded Intel graphic processor greatly reducing CPU load. To enable operation of this decompressor include the integrated video card into BIOS and install latest Intel drivers. The maximum resolution differs depending on Intel Quick Sync version, please see https://www.intel.com/ for more details.

Note

When decompressors included into the Intel IPP library are in use, there can be video distortions for some resolutions. In these cases resolutions divisible by 16 are recommended to be used (e.g, 1280x720 or 1360x768) or another decompressor is to be selected.

Compression and decompression algorithms are set on the settings panel of a **Camera** object using the **Compressor** and **Decompressor** list correspondingly (see the Settings panel of the Camera object section). The decompression algorithm set in the camera settings is used when a video signal is displayed on a video surveillance monitor and for detection operation.

Important!

By default compression and decompression algorithms are not available for selecting and **Compressor** and **Decompressor** dropdown lists are not available for editing. To enable this feature set the “1” value for EnableCodecSettings registry parameter (see Registry keys reference guide).

Note

In multistream mode (see Configuration of multistream video) the codec selecting and settings of video signal quality is performed separately for each video stream on the **Camera** object’s settings panel on the **Video stream** tab.

If the compressor/decompressor (default value) is not selected on the settings panel of a **Camera** object or the incorrect one is selected, then INTELLECT ™ software automatically selects the first compressor/decompressor in alphabetical order. If it does not fit too, the following one is selected and so on, until the correct one is selected.

Note

When WS7 and WS17 video capture cards are in use, the **Decompression** field is to be left blank otherwise use Motion Wavelet decompressor. If another decompressor is selected, then INTELLECT™ operation is not guaranteed.

Important!

If for some reasons the automatic decompressor selection is not right, then you are to select a decompressor manually.

23.3.2.1.5 How to record digitized video signals

Video signals archiving provides post-event analysis of evidence footage.

The archive is located on the local disks of the videoserver. Having reached the end of the archive disk volume, the archive is overwritten.

Before archiving on the videoserver, the video signal is compressed. It is compressed to reduce the size of the video recordings.

INTELLECT™ software is capable of auto recording, initiated by cameras (Main detectors) and detectors alarm detection or by Operator command.

Pre-event, post-event, and Hot (higher frame rate) recording can be performed to make post-event analysis of evidence footage more effective.

Configuring video archiving

23.3.2.1.6 Digital video signal transmission to Remote Workstations

INTELLECT™ software provides video surveillance from Remote Workstations based on:

1. A PC (IBM PC–based) personal computer, connected to the videoserver via local TCP/IP net;
2. An IBM PC, connected to the videoserver via the “web server” module by HTTP protocol;
3. Mobile device on the basis of iOS or Android connected to the videoserver with the help of mobile client.

Both real-time and archive video signals may be transmitted to Remote Workstations. Prior to being transmitted to a Remote Workstation, video signals are compressed.

Configuring video transmission to Remote Workstations

23.3.2.1.7 Video signal display

Video signals are displayed using the **Video Surveillance Monitor** interface object. The Video monitor is especially used to display video signals, received from cameras, and to play back the video recordings.

The video monitor has several options: detectors, PTZ units and microphones control, image processing and exporting.

Different video monitors are used with different video signal transmission modes:

1. Video server surveillance Monitor.
2. Video surveillance Monitor of the Remote Workstation, connected to the videoserver via the TCP/IP net, identical to the videoserver surveillance Monitor.
3. Video monitor of the web server, depicted in web browsers on Remote Workstations, connected to the videoserver via the web server module by HTTP protocol.
4. Video monitor of the mobile client based on iOS or Android operation system.

The above video surveillance monitors have different components and functions. Any video monitor can be set up to display real-time video and play back archive footage.

Configuring video display on Video Surveillance Monitor

23.3.2.2 Registrating Video Capture Devices and cameras in INTELLECT™ software

To configure video subsystem in INTELLECT™ software, create the **Video Capture Device** objects on the base of which the **Camera** objects are created (see Installing and configuring security system components guide).

23.3.2.3 Configuring the video signals processing mode while using video capture cards and analog video cameras

23.3.2.3.1 Setting up format (PAL or NTSC) for the input analog video signal

Different digitization and processing algorithms are used with different input video signal formats. The input signal format is individually set for ADC of every video capture card. Any single ADC processes and digitizes single format signals only: either PAL or NTSC.

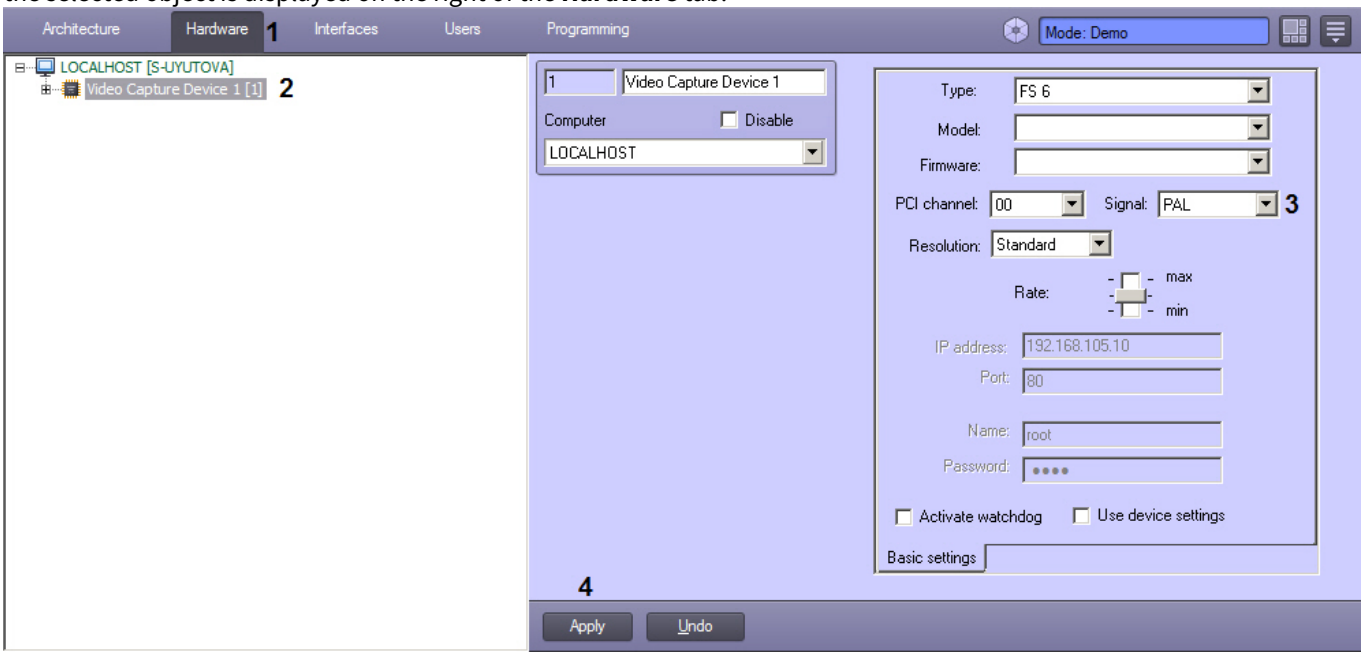
In INTELLECT™ all ADCs of video capture cards by default are set to digitize video signal in PAL format.

> **Note.**
>
> While using Stretch VRC6004, VRC 6008, VRC 6416, VRC 7008L and VRC 6404HD video capture cards, the input video signal (PAL or NTSC) is selected automatically depending on cameras, connected to the card. Changing the parameter does not affect the card workability.

> **Note.**
>
> While using SL16-200 (FX116) and FX416 video capture cards, restart INTELLECT™ software after changing the format of video input. Otherwise the initial settings will be active.

To set the ADC of a video capture card to digitize and process video signal in NTSC format, do the following:

1. Go to the **Hardware** tab in the **System Settings** dialog box (1).
2. In the objects tree of the **Hardware** tab, select the **Video Capture Device** object, created before (2).The settings panel for the selected object is displayed on the right of the **Hardware** tab.



3. In the **Signal** drop-down list, select the **NTSC** value (3).
4. Click the **Apply** button (4).

The input video signal format is now selected.

23.3.2.3.2 Frame rate settings

On the page:

- Video capture card resources
- Operation modes of the video capture cards' ADC
- Frame rate setup procedure
- Configuring video subsystem with disabled video channels
- Actual frame rate
- Changing frame grooming
- Allocation of video capture card's resources
- Video signal processing priorities
- Setting video processing priority
- Setting video recording priority

23.3.2.3.2.1 Video capture card resources

By default the resources of video capture cards are uniformly distributed between cameras video signals of which are digitized and processed by this ADC. The frame rate of the digitized video signal is limited by the ADC resources for video signal processing and digitization.

Video capture cards may be configured, so as to give to one or more cameras additional ADC resources, and thus to increase the frame rate of video signals from these cameras. At the same time the frame rate of video signals from other cameras is decreased.

Intellect and video capture cards sharing allows reallocating video capture card resources to the cameras:

Option 1. Reallocation of cameras between ADCs of a video capture card.

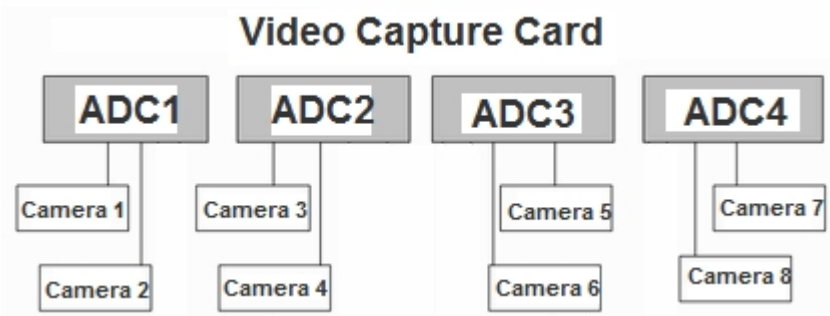
ADC resources are generally characterized by the maximum total frame rate of video signals. By default ADC resources are uniformly distributed between cameras to the assigned cameras. So, the more camera video signals are digitized and processed by the ADC, the lower the frame rate of the single video signal is.

Reallocation of cameras between ADCs allows increasing the frame rate for some cameras by means of others.

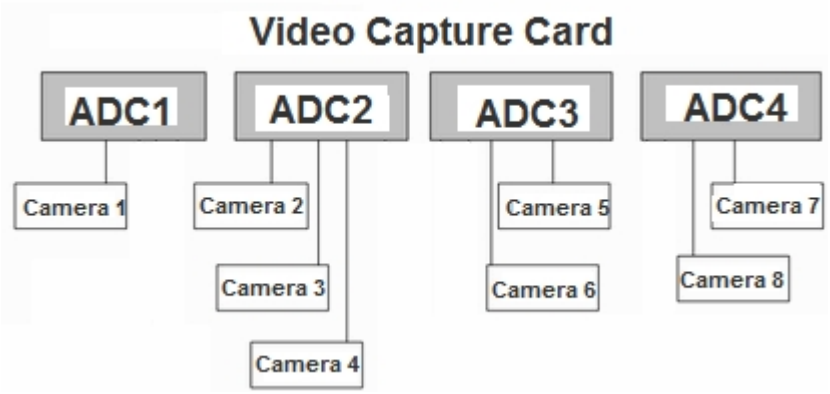
If all allowable cameras are connected to a video capture card, then only uniform distribution on ADC is possible. In this case every ADC of a video capture card digitizes and processes video signal from an equal number of cameras. So, the maximum frame rate is the same for all video signals (except for video signals of different formats and different resolutions).

If the number of cameras connected to a video capture card is less than their maximum number, then it is possible to reallocate them between ADCs of a video capture card. For this, those cameras, which frame rate is to be increased, are allocated separately to one ADC, or allocated in number that is less than the maximum allowable one. Cameras allocated to a given ADC and not subject to strict frame rate requirements, are reallocated to other ADCs.

An example of allocating cameras to ADCs is shown in the figure.



A. Uniform camera allocation between ADCs



B. reallocating the cameras between ADCs to allocate extra resources to Camera1

Option 2. Reallocation of resources of one ADC between cameras video signal of which are to be processed and digitized by one ADC.

By default the ADC resources are uniformly distributed between cameras video signals of which are digitized and processed by this ADC.

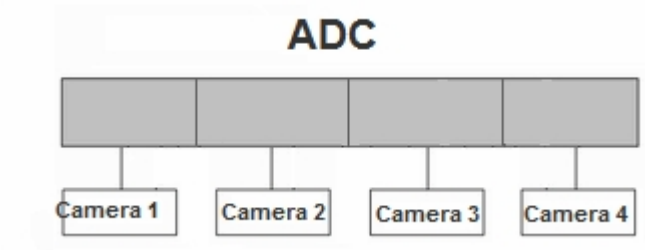
Reallocation of cameras between ADCs allows increasing the frame rate for some cameras by means of others. Reallocation of resources of one ADC to the cameras is much less effective than camera reallocation between the ADC. Therefore this is to be done only if camera reallocation to the ADC is impossible or if it does not help.

With reallocation of resources from 1 ADC to the cameras, one of the cameras gets extra ADC resources for its video signal processing and digitization. Extra ADC resources are formed by removing them from other cameras video signals of which whose are processed by the ADC.

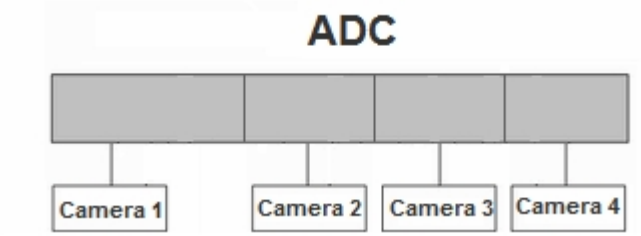
So, for a single ADC, when the frame rate of a certain camera increases, the frame rates of other cameras decrease.

To perform this operation, a selected camera is to have priority in the process queue.

An example of reallocation of resources of one ADC between cameras is shown in the figure below.



A. Uniform camera allocation between ADCs



B. reallocating the cameras between ADCs to allocate extra resources to Camera1

23.3.2.3.2.2 Operation modes of the video capture cards' ADC

ADC operation mode is defined by the number of processed and digitized video signals. There are two modes:

1. Live video.
2. Multiplexing.

In the Live video mode all resources of an ADC are used to process the single video signal. The mode provides digital video stream with a maximum frame rate of 25 FPS in PAL format and 30 FPS in NTSC format.

If the ADC processes two or more video signals, its resources are used in the multiplexing mode. Then the ADC resources are uniformly allocated between the cameras, and part of its resources support the multiplexing process. So, in the multiplex mode the total frame rate of video signals, digitized by a single ADC, is much lower than in the Live video mode.

The maximum permissible total frame rate in the multiplexing mode depends on the frame resolution.

For ADC that digitizes all video signals with standard (352 x 288 pixels in PAL format, 352 x 240 pixels in NTSC format) and/or high (704 x 288 pixels in PAL format, 640 x 240 pixels in NTSC format) frame resolution, the total frame rate is 16 FPS in PAL format and 20 FPS in NTSC format.

When ADC digitizes at least one of the video signals with full resolution (704 x 576 pixels in PAL format, 640 x 480 pixels in NTSC format), the maximum permissible total frame rate is reduced to 12 FPS in PAL format and 15 FPS in NTSC format.

23.3.2.3.2.3 Frame rate setup procedure

Default settings for the digitized video signals frame rate are 2 FPS in PAL format and 2.5 FPS in NTSC format.

While settings it is possible to increase or to reduce the frame rate.

To set up the frame rate, do the following:

1. Switch off the **Camera** objects, which are assigned to the idle video channels. This allows allocating the resources between working cameras only and thus increasing the frame rate.
2. Change frame grooming.
3. Reallocate cameras on ADC of the video capture card.
4. Reallocate resources of one ADC between cameras (priority process queues).

In most cases 1 and 2 steps are sufficient to set the frame rate. 3 and 4 steps are necessary only with high frame rate requirements to one or more cameras.

23.3.2.3.2.4 Configuring video subsystem with disabled video channels

By default resources of video capture cards' ADC are allocated uniformly between all video channels whether there is any signal passing through it or not. So, even if a video channel has no signal, the resources of ADC are allocated to it.

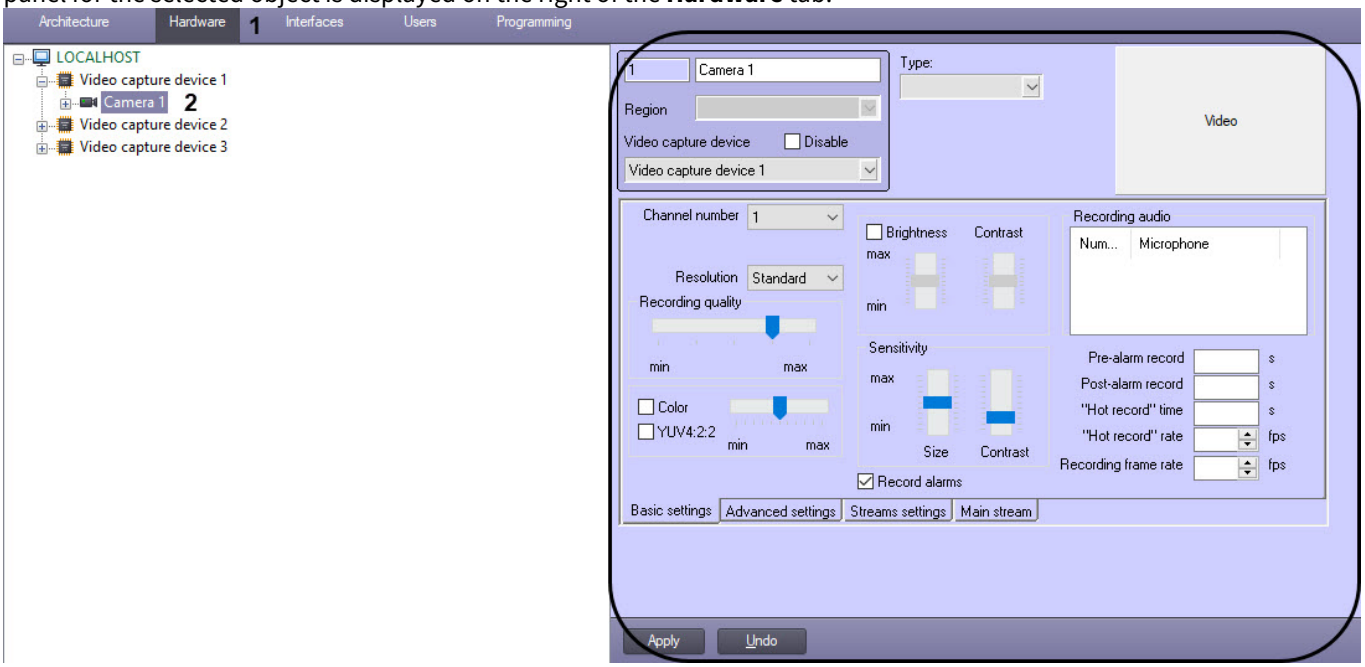
Several **Camera** objects are disabled in turn.

To prevent allocation of ADC resources, the **Camera** objects are to be disabled in *Intellect*, assigned to the disabled video channels.

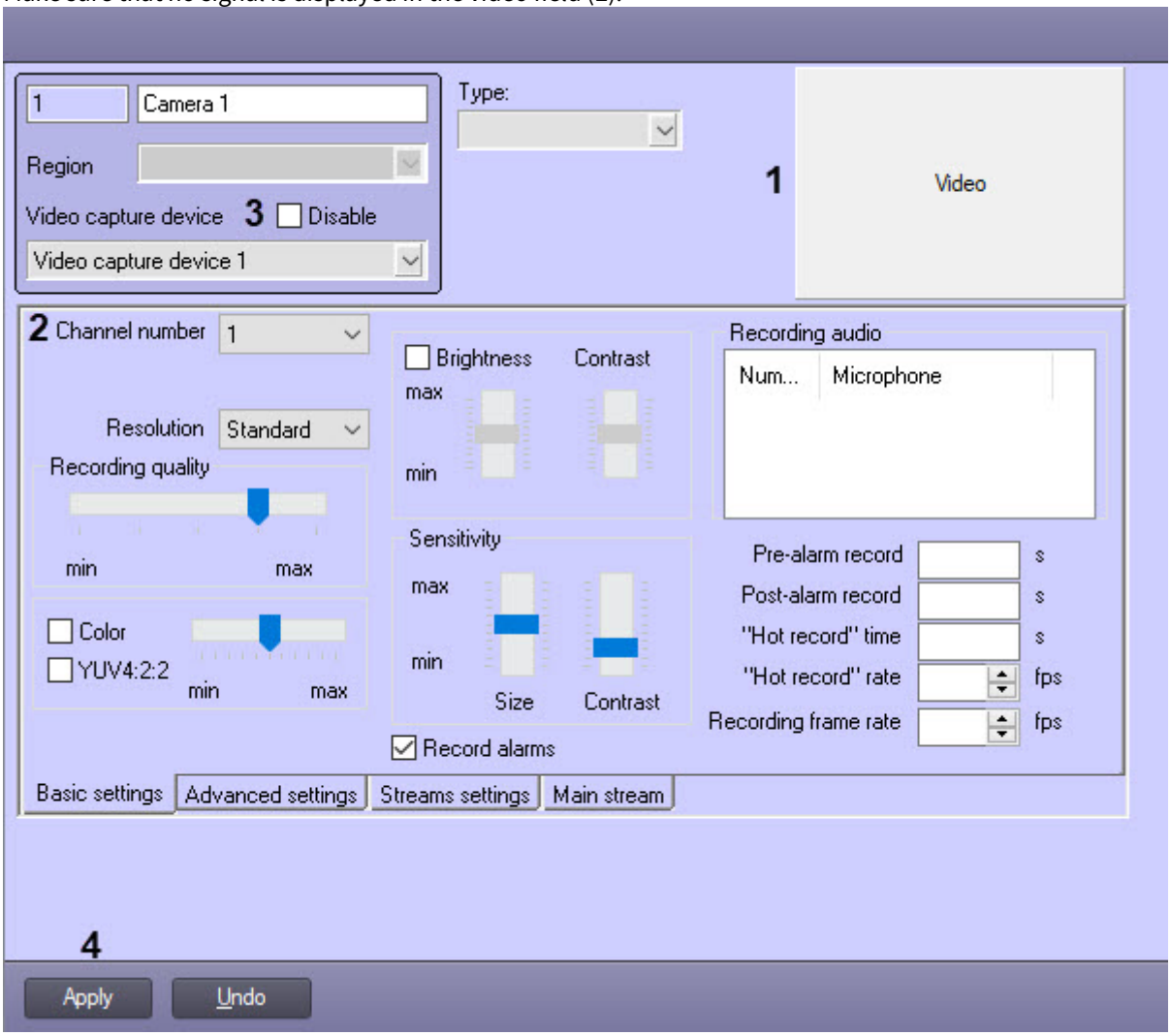
To disable the **Camera** objects in *Intellect*, do the following:

1. Define the numbers of the idle video capture channels (taking into account BNC plug numbering).
2. Go to the **Hardware** tab in the **System settings** dialog box (**1**).

3. Select the **Camera** object, created before, with the same channel number as the BNC plug (idle channel) (**2**). The settings panel for the selected object is displayed on the right of the **Hardware** tab.



4. Make sure that no signal is displayed in the video field (**1**).



5. The signal displayed in the video field indicates that the **Camera** object is matched to another video channel.The video channel number is specified in the **Channel number** drop-down list in the **Basic settings** tab (**2**). Match the **Camera** object with the channel number, which corresponds to the BNC plug number and the **Camera** object number, or scan for a **Camera** object, matched with the desired channel number.
6. Set the **Disabled** checkbox (**3**).
7. Click the **Apply** button (**4**).

The disabled **Camera** object is indicated with a cross mark.

Video subsystem with disabled video channels is now configured.

23.3.2.3.2.5 Actual frame rate

It is recommended to define the actual frame rate of video signal digitization and then to set up the frame rate for video signals from video surveillance system cameras.

Frame rate setup is to be done only if video signal frame rates from one or more cameras do not meet the requirements.

Actual frame rates are defined for each camera individually.

To define the actual frame rate for a selected camera, do the following:

1. Configure the video surveillance monitor (see Configuring video display on Video Surveillance Monitor section);
2. Enable the debug mode in *Intellect* using the tweaki.exe utility (see Tweaki.exe utility for advanced setup of the Intellect software system section).

In *Intellect* actual frame rates of digitized video signals in the debug mode are displayed on the Monitor. To define the frame rate of video signal from a selected camera, do the following:

1. Display the selected camera box on the Monitor.
2. Activate the selected camera box by left clicking on it.
3. The actual frame rate of the selected window video signal is displayed in the information window in the top right corner of the Monitor.

Note

For Stretch video cards of standard compression (h264) the frame rate that is displayed on Monitor in *Intellect* can be less than the frame rate that is indicated by the video card manufacturer. This is due to the fact that while displaying the frame rate of video signal digitization on Monitor in *Intellect* blank frames that are distributed by the video card, are not taken into account. «Blanck frames» do not contain the information about the image and are created by the video capture card when there are no changes in the video stream and a new video frame is the same as the previous one (for example, there is no motion in the frame).

23.3.2.3.2.6 Changing frame grooming

By default *Intellect* digitizes video signals with the frame rate lower than maximum allowed one. This is caused by the following:

1. Video signal processing and digitization with a high frame rate is a resource-intensive process. When the video signal frame rate increases, configuration requirements increase for the computer used as a Server.
2. Video signal is transmitted to the Remote Workplaces with the same frame rate as it was digitized. So, network capacity requirements increase together with the frame rate increase.

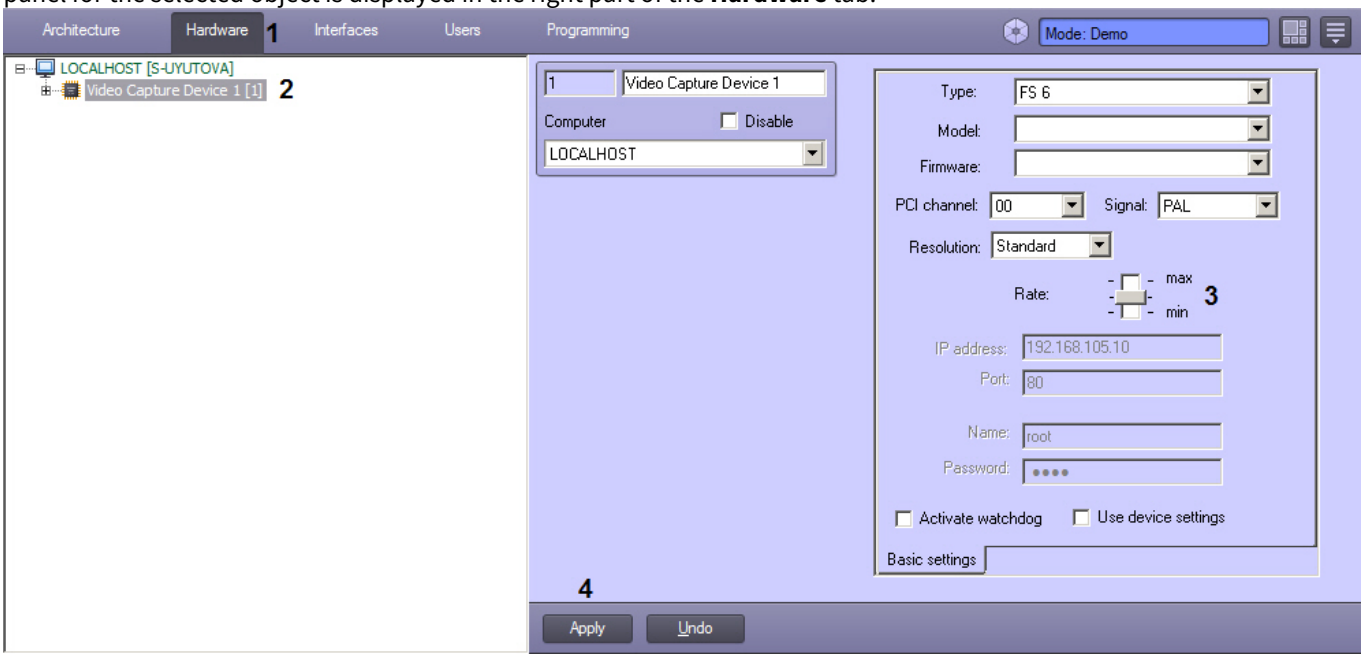
By default the total frame rate of video signals, which are digitized and processed by the same ADC, is 2 times lower than the maximum allowed one. This ratio is provided by frame grooming, which allows every second frame to be processed by the program.

Settings allow reducing (total frame rate increases) or increasing (total frame rate decreases) the grooming.

Frame grooming is changed separately and independently for every ADC.

To change grooming of ADC video signals, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).
2. Select the relevant **Video Capture Device** object, created before, in the **Hardware** tab in the objects tree (**2**). The settings panel for the selected object is displayed in the right part of the **Hardware** tab.



3. If it is necessary to increase the total frame rate up to the maximum allowed value, move the **Rate** slider to the **Max** position (**3**).
4. If it is necessary to reduce the total frame rate to the minimum allowed value, move the **Rate** slider to the **Min** position. The minimum total frame rate of video signals, digitized and processed by selected ADC, is 3 times lower than the maximum allowed one.
5. If it is necessary to return the default grooming settings, move the **Rate** slider to the middle position. The default total frame rate is 2 times lower than the maximum allowed one.
6. Click the **Apply** button (**4**).
7. Close the **System settings** dialog box and restart *Intellect*.

Note

Without restart, changes in video signal grooming may be applied incorrectly.

23.3.2.3.2.7 Allocation of video capture card's resources

By default all cameras are uniformly allocated to ADC of video capture card. Thus ADC resources are uniformly distributed to the cameras, attached to the video capture card, and all cameras have the same frame rate.

If the number of cameras connected to a video capture card is less than their maximum allowed number, it is possible to reallocate them between different ADCs of the video capture card. Reassigning of cameras allows increasing the frame rate for some cameras by means of a decrease in the frame rate of others.

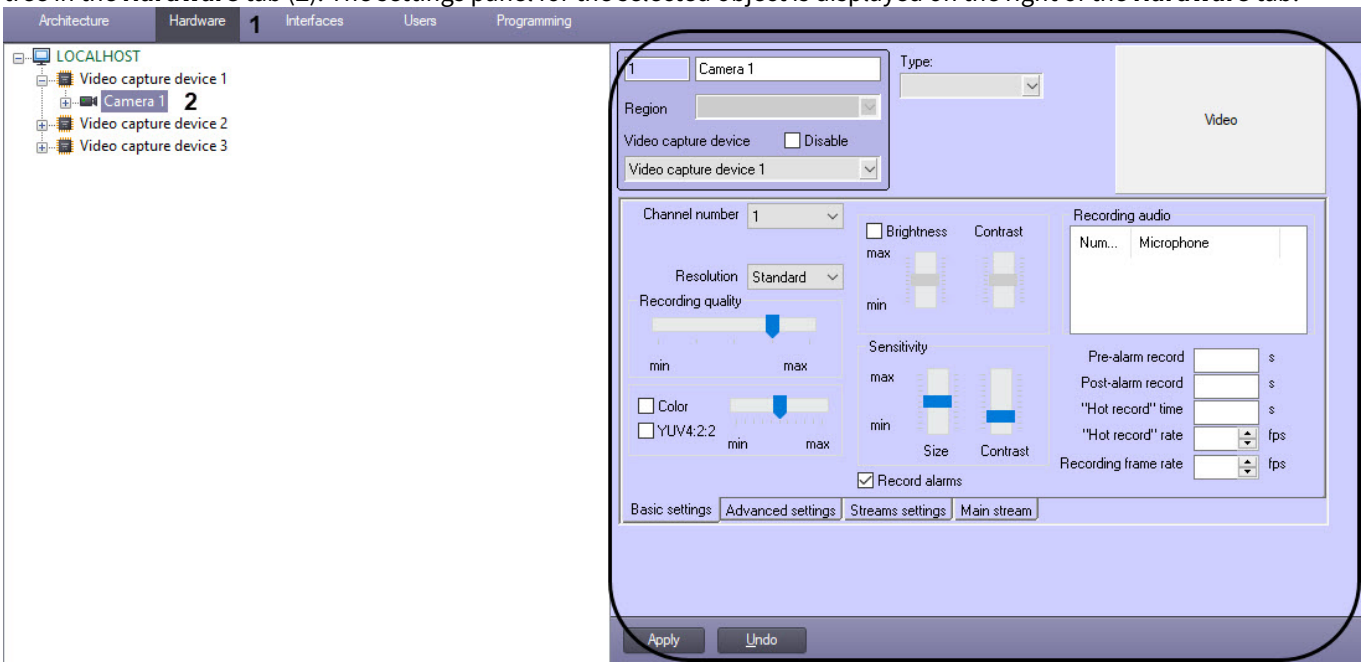
Before reassigning the cameras to ADCs of the video capture card, disable the **Camera** objects corresponding to disabled cameras (see Configuring video subsystem with disabled video channels section).

Note

Video inputs numeration of SC300Q16 (FX4) and SC300D16 (FX8) video capture cards does not correspond to the numeration of PCI channels in *Intelect*. It is impossible to allocate video inputs to chips one after another (i.e. the first corresponds to 1 and 2 chips, the second upper input corresponds to 3 and 4 etc.) because OS determines it.

To increase the frame rate of the video signal from one or more cameras, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).
2. Select the **Camera** object, created before, corresponding to the camera, which frame rate is to be increased, in the objects tree in the **Hardware** tab (**2**). The settings panel for the selected object is displayed on the right of the **Hardware** tab.



3. To increase the frame rate of a camera up to the Real time rate (25 FPS in PAL format and 30 FPS in NTSC format), reallocate other cameras serviced by the same ADC as with the camera above, to other ADCs.

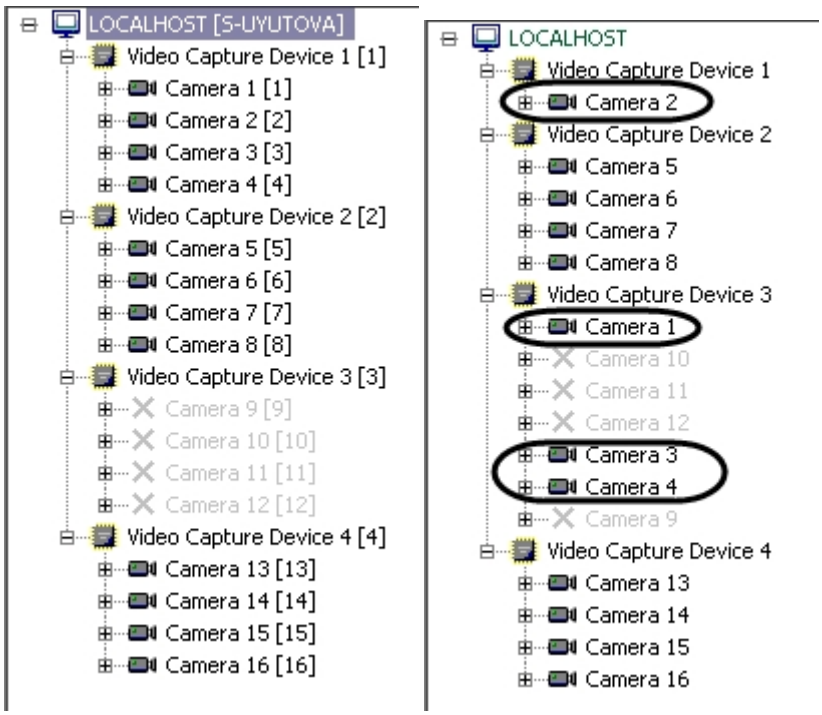
For this move **Camera** objects to parent branches of other **Video Capture Device** objects. The parent **Video Capture Device** object for a **Camera** object is set by selecting the number of the parent object in the **Video Capture Device** list of settings panel for the **Camera** object. As a result the **Camera** object moves to a subdirectory of the selected **Video Capture Device** object.

Example 1. Configuring video signal digitization with the Real time frame rate.

Task. Video signal on Camera 2 is to be digitized with the Real time frame rate.

Initial data. The card has 4 ADCs. They are matched to 4 **Video Capture Device** objects in the objects tree. The video capture card may have up to 16 cameras connected to it. 8 cameras are actually connected to the video capture card. The objects matched to

the remaining 8 cameras are disabled. Each of two ADCs, matched to the **Video Capture Device 1** and **Video Capture Device 2** objects, is configured to digitize the signals from 4 cameras. The ADCs matched to the **Video Capture Device 3** and **Video Capture Device 4** objects are not configured to digitize signals from any cameras. An example of the objects tree is given in figure A:



A. Initial data B. Result

Solution. Do the following:

1. Select the **Camera 1** object in the objects tree. The settings panel for the selected object is displayed.
2. Select **Video Capture Device 3** in the **Video Capture Device** list.
3. Click the **Apply** button.
4. The **Camera 1** object moves to the subdirectory of the **Video Capture Device 3** object (see B).
5. Repeat (1) – (4) steps for the **Camera 3** and **Camera 4** objects.
6. Select the **Video Capture Device 1** object in the objects tree.
7. Make sure that the **Speed** slider is in the max position.
   If the **Speed** slider is in the max position, then setup is completed.
   If the **Speed** slider is in another position, move it to the max position and do (8) - (10) steps.
8. Click the **Apply** button.
9. Close the **System settings** dialog box and restart *Intellect*.
10. The frame rate of the selected camera increases up to the Real time rate (for information on testing the frame rate change, see the Actual frame rate section).
11. If the number of connected cameras prevents the configuration of video signal digitization from one of the cameras with the Real time rate (for example, when 15 of 16 allowed cameras are connected), or if the frame rate on several cameras is to be increased simultaneously to the rate, lower than the Real time one, then the cameras, the frame rate of which is to be increased, are allocated between ADCs and they do not exceed the maximum allowable number. The frame rate is increased by as many times, as the number of cameras on ADC is reduced.

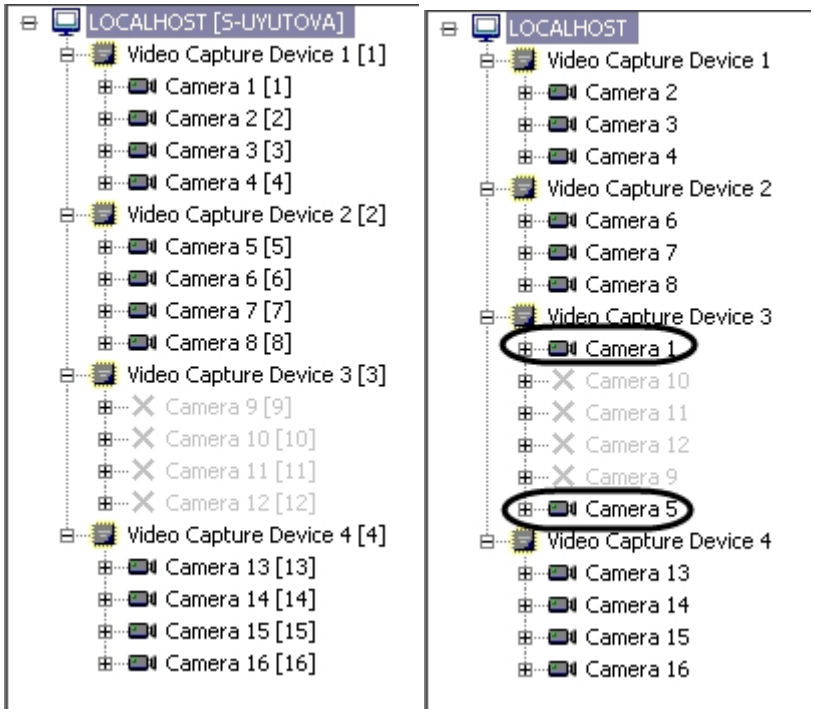
Video capture card's resources are now allocated.

Example 2. Configuring video signal digitization from 2 cameras with increased frame rate

Task. Video signal on **Camera1** and **Camera 5** is to be digitized with increased frame rate.

Initial data. The card has 4 ADCs. They are matched to 4 **Video Capture Devices** objects in the objects tree. The video capture card may have up to 16 cameras connected to it. 12 cameras are actually connected to the video capture card. The objects matched to the remaining 4 cameras are disabled. Each of 3 ADCs, matched to the **Video Capture Device 1**, **Video Capture Device 2** and **Video Capture Device 4** objects, is configured to digitize the signals from 4 cameras. The ADC, matched to the

Video Capture Device 3 object, is not configured to digitize the signals from any camera. An example of the objects tree is given in figure A.



A. Initial data B. Result

Solution. Do the following:

1. Select the **Camera 1** object in the objects tree. The settings panel for the selected object is displayed.
2. Select **Video Capture Device 3** in the **Video Capture Device** list.
3. Click the **Apply** button.
4. The **Camera 1** object moves to a subdirectory of the **Video Capture Device 3** object (B).
5. Repeat 1 – 4 steps for the **Camera 5** object.
6. The frame rate on **Camera1** and **Camera5** increases twofold (for information on testing the frame rate change see the Actual frame rate section).
7. Click the **Apply** button.

Video capture card's resources are now allocated.

Note

Ways of resources allocation (given in examples) are not used for SC200Q4 (FS15)\SC200Q4 LOW PROFILE (FS115)\SC300Q16 (FX4)\SC300D16 (FX8) video capture cards, because for these cards numbers of PCI channels (specified in settings of the **Video Capture Device** objects) are connected with physical inputs (BNC connectors).

23.3.2.3.2.8 Video signal processing priorities

The ADC resources are uniformly distributed to the assigned cameras by default.

ADC resources reallocation allows increasing the frame rate for a camera by means of other cameras. Reallocation of resources from 1 ADC between the cameras is much less effective than camera reallocation on the ADC. Therefore it should only be done if camera reallocation on the ADC is impossible or if it does not help.

With reallocation of resources from 1 ADC between the cameras, one of the cameras is allocated with additional ADC resources for its video signal processing and digitization. Additional ADC resources are formed by removing them from other cameras, video signals of which are processed by the ADC.

A camera is allocated with additional ADC resources via the priority process queue.

Intellect provides 1/2 and 1/3 process queues.

When a camera has a 1/2 process queue, its video signal is processed in every second frame. So, the digitization frame rate on this camera is the half of total frame rate of the considered ADC.

When a camera has a 1/3 process queue, its video signal is processed in every third frame. So, the digitization frame rate on this camera is one third of total frame rate of the considered ADC.

Example 1. The ADC is configured to digitize video signal from 4 cameras.

If all the cameras have a common queue, the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 3, Camera 4, Camera 1, Camera 2, Camera 3…

Let us suppose that Camera 1 has 1/2 queue, and the rest of the cameras are in the common queue. Then the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 1, Camera 3, Camera 1, Camera 4, Camera 1…

So, the frame rate on Camera 1 is increased by 2 times and becomes the half of total frame rate of the considered ADC. The frame rate of each of the remaining cameras becomes 1.5 times less and makes up 1/6 of total frame rate of the considered ADC.

Example 2. The ADC is configured to digitize the video signal from 3 cameras.

If all the cameras have a common queue, the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 3, Camera 1, Camera 2, Camera 3…

Let us suppose that Camera 1 has a 1/2 queue, and the rest of the cameras are in the common queue. Then the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 1, Camera 3, Camera 1, Camera 2…

So, the frame rate of Camera 1 is increased by 1,5 times and becomes the half of total frame rate of the considered ADC. The frame rate of each of the remaining cameras becomes 1.33 times less and makes up 1/4 of total frame rate of the considered ADC.

Example 3. The ADC is configured to digitize video signal from 4 cameras.

If all the cameras have a common queue, the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 3, Camera 4, Camera 1, Camera 2, Camera 3…

Let us suppose that Camera 1 has 1/3 queue, and the rest of the cameras are in the common queue. Then the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 3, Camera 1, Camera 4, Camera 2, Camera 1…

So, the frame rate of Camera 1 is increased by 1.33 times and becomes one third of total frame rate of the considered ADC. The frame rate of each of the remaining cameras becomes 1.125 times less and makes up 2/9 of total frame rate of the considered ADC.

Example 4. The ADC is configured to digitize video signal from 4 cameras.

If all the cameras have a common queue, the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 3, Camera 4, Camera 1, Camera 2, Camera 3…

Let us suppose that Camera 1 and Camera 2 have 1/2 queue, and the rest of the cameras are in the common queue. Then the ADC digitizes video signals in the following sequence:

Camera 1, Camera 2, Camera 3, Camera 1, Camera 2, Camera 4, Camera 1…

So, the frame rate of Camera 1 is increased by 1.33 times and becomes equal one third of total frame rate of the considered ADC. The frame rate of each of the remaining cameras becomes 1.5 times less and makes up 1/6 of total frame rate of the considered ADC.

Note1. If Camera 1 and Camera 2 have 1/3 queue and Camera 3 and Camera 4 are in the common queue, then allocation of the ADC's resources is as it is showed in the Example4.

Note2. It has no sense to enqueue one of two cameras, with 1/2 priority allocated to the same ADC, because this camera video signal will be processed as if it were in the common queue.

Note3. It has no sense to enqueue one of three cameras with 1/3 priority allocated to the same ADC, because this camera video signal will be processed as if it were in the common queue.

Reallocation of resources of 1 ADC between the cameras is possible in two modes:

1. in the processing mode, i.e. with video signal digitization and processing before it is displayed;
2. in the recording mode, i.e. with video signal digitization and processing before it is recorded into the Server archive. When cameras are switched to the recording mode, video signals are displayed with the rate, corresponding to the given ADC resources allocation.

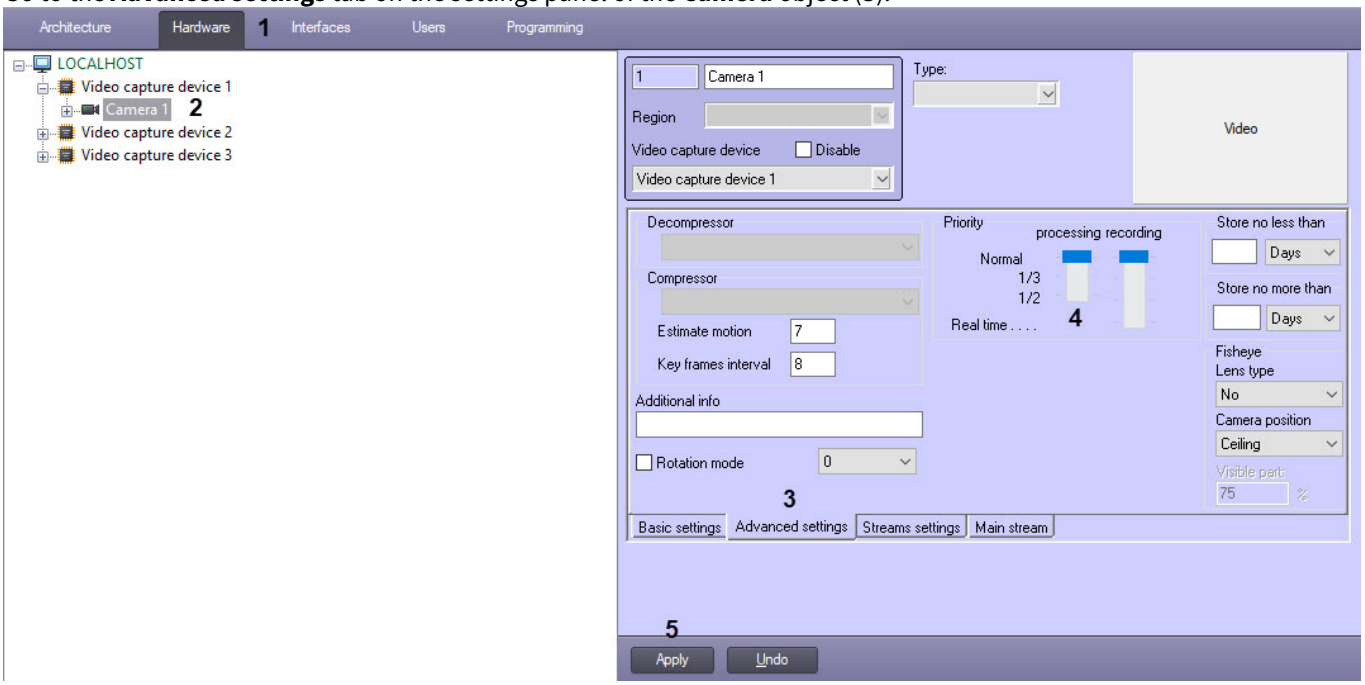
23.3.2.3.2.9 Setting video processing priority

While processing video before displaying it, ADC resources are reallocated between the cameras by queueing one of the cameras with 1/2 or 1/3 priority.

This setting is relevant only for the following video capture cards: FS5, FS6, FS8 and FS16.

To change the order of processing video from the selected camera, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).
2. Select the **Camera** object, created before, corresponding to the camera, ADC video processing queue of which is to be changed, in the **Hardware** tab in the objects tree (**2**). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Advanced settings** tab on the settings panel of the **Camera** object (**3**).



4. If it is necessary to queue the camera with 1/2 priority for ADC video processing, move the **Processing** slider in the **Priority** group to the **1/2** position (**4**).
5. If it is necessary to queue the camera with 1/3 priority for ADC video processing, move the **Processing** slider in the **Priority** group to the **1/3** position.
6. If it is necessary to return the camera into the normal queue for ADC video processing (set by default), move the **Processing** slider in the **Priority** group to the **Normal** position.
7. Click the **Apply** button (**5**).

Video processing priority is now set.

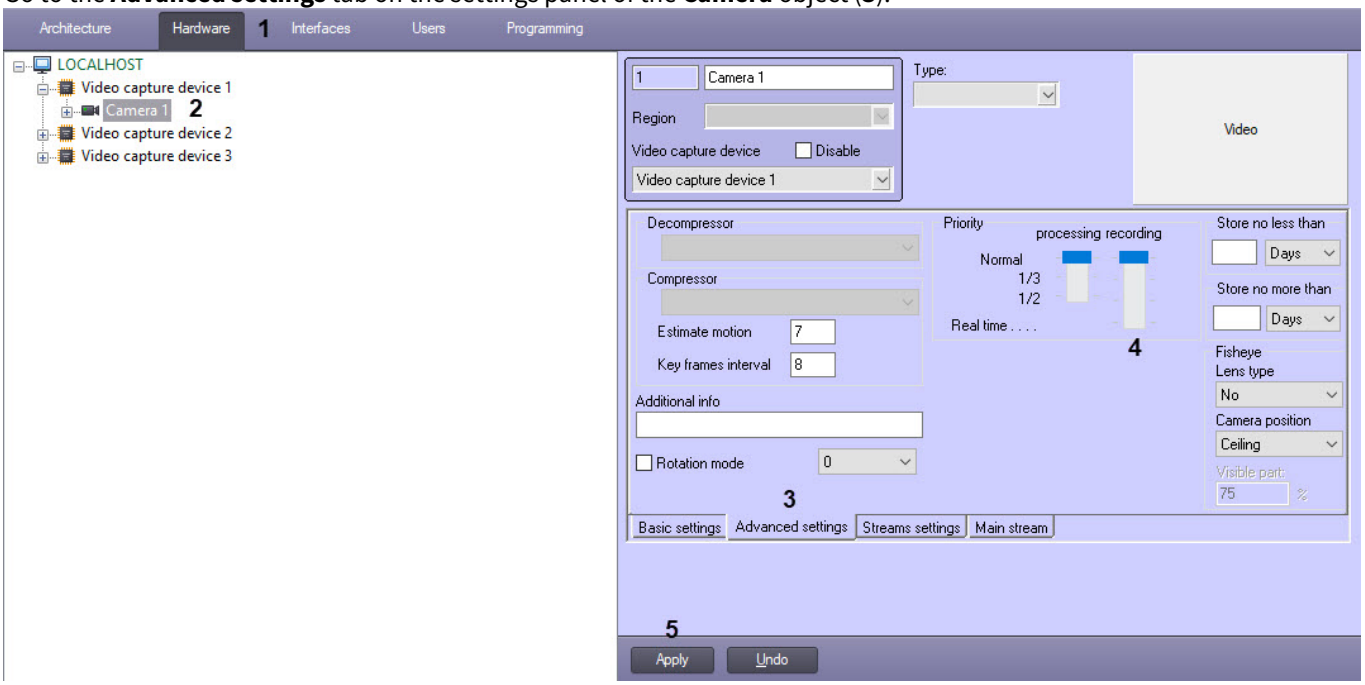
23.3.2.3.2.10 Setting video recording priority

While processing the video signal before recording it to the video server archive, ADC resources are reallocated between the cameras by queueing one of the cameras with 1/2, 1/3 or the Real time priority.

If the camera with Real time priority switches into the recording mode, it will be allocated with all ADC resources for its video processing. So, the frame rate on this camera becomes equal to the total frame rate of the considered ADC. No video from other cameras, allocated to a given ADC, is processed, displayed and recorded to the disk.

To change the processing queue of the video on the selected camera in the recording mode, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).
2. Select the **Camera** object, created before, corresponding to the camera, ADC video processing queue of which is to be changed, in the objects tree of the **Hardware** tab (**2**). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Advanced settings** tab on the settings panel of the **Camera** object (**3**).



4. If it is necessary to queue the camera with 1/2 priority for ADC video processing in the recording mode, move the **Recording** slider in the **Priority** group to the **1/2** position (**4**).
5. If it is necessary to queue the camera with 1/3 priority for ADC video processing in the recording mode, move the **Recording** slider in the **Priority** group to the **1/3** position.
6. If it is necessary to queue the camera with the Real time priority for ADC video processing in the recording mode, move the **Recording** slider in the **Priority** group to the **Real time** position.
7. If it is necessary to return the camera into the normal queue for ADC video processing in the recording mode (set by default), move the **Recording** slider in the **Priority** group to the **Normal** position.
8. Click the **Apply** button (**5**).

Video recording priority is now set.

23.3.2.3.3 Brightness, contrast, color depth and color rendition format settings

On the page:

- Brightness and contrast settings
- Color depth adjustment
- Selecting the color rendition format

23.3.2.3.3.1 Brightness and contrast settings

INTELLECT™ software provides facilities for video brightness and contrast adjustment in different modes depending on the demands of the video characteristics.

Brightness can be adjusted in the following modes:

1. Auto brightness and contrast adjustment. In this mode INTELLECT™ software automatically applies the internal algorithm of video brightness and contrast adjustment. In this mode manual brightness and contrast adjustment is unavailable. This mode is activated by default and it does not need any additional settings. This mode to adjust brightness and contrast is recommended for video with no special requirements to video characteristics.
2. Manual brightness and contrast adjustment. In this mode the administrator may change the **Brightness** and **Contrast** settings.
3. Manual brightness and contrast adjustment with auto optimization. In this mode the administrator manually presets the values of **Brightness** and **Contrast** parameters. After the preset is confirmed, INTELLECT™ software automatically launches the process of video image brightness and contrast optimization. This process involves step-by-step changing of video brightness and contrast.

Note.

The ManualBrightnessControl line parameter in the HKEY_LOCAL_MACHINE\SOFTWARE\ITV\INTELLECT\Video for 32-bit system (HKEY_LOCAL_MACHINE\Software\Wow6432Node\ITV\INTELLECT\Video for 64-bit system) registry is used to enable automatic adjustment of IP-cameras' brightness and contrast. If ManualBrightnessControl is equal to 1, then the manual brightness and contrast control of IP-cameras is enabled. If ManualBrightnessControl is equal to 0, then the mode of the manual brightness and contrast control of IP-cameras is set on the settings panel of the corresponding Camera object.

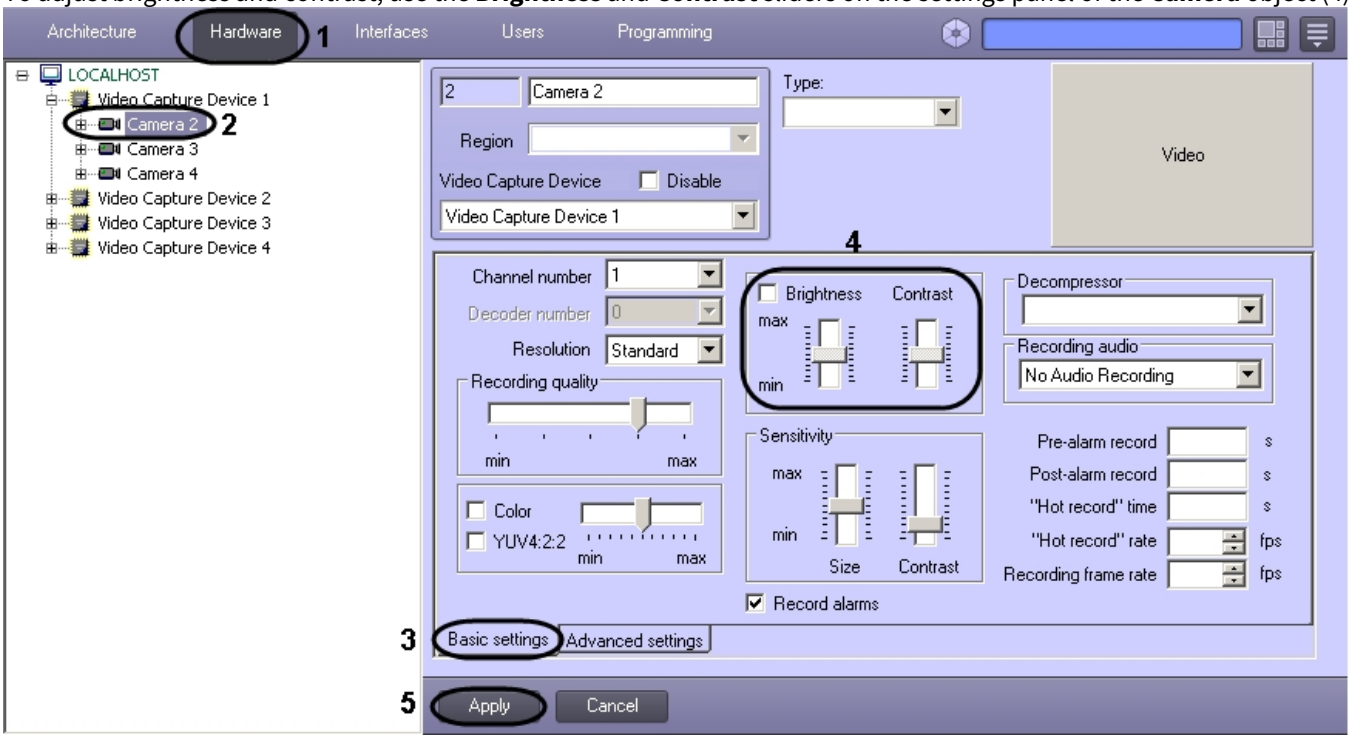
Note.

Manual Brightness and Contrast Control of IP-cameras is enabled by default.

Brightness and contrast are changed separately and independently for every camera.

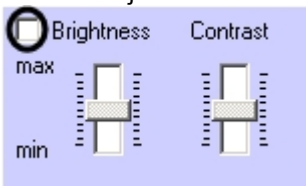
To adjust brightness and contrast, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object, created before, corresponding to the camera, brightness and contrast of which is to be adjusted, in the **Hardware** tab in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3).
   To adjust brightness and contrast, use the **Brightness** and **Contrast** sliders on the settings panel of the **Camera** object (4).



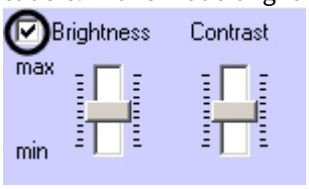
4. Auto brightness and contrast adjustment mode is activated by default. Active brightness and contrast auto adjustment mode is indicated by the absence of the check in the **Brightness** and **Contrast** boxes. In this mode manual brightness and

contrast adjustment is unavailable. So, the **Brightness** and **Contrast** sliders are deactivated.

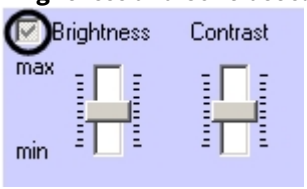


The mode is activated by default. To return to this mode, uncheck the checkbox next to the **Brightness** and **Contrast** sliders.

5. To go to the manual brightness and contrast adjustment mode, check the checkbox next to the **Brightness** and **Contrast** sliders. In this mode brightness and contrast settings are changed by moving the corresponding sliders.



6. To go to the manual brightness and contrast adjustment with auto optimization mode, check the checkbox next to the **Brightness** and **Contrast** sliders.



In this mode brightness and contrast settings are changed by moving the corresponding sliders. To launch the video brightness and contrast auto optimization, click the **Apply** button at the bottom of the **System settings** dialog box. The optimization sequence involves a step-by-step change of video brightness and contrast.

7. To activate the new brightness and contrast settings, click the **Apply** button (5).

Note.

The sight control of brightness and contrast settings is performed using the viewing field.

Brightness and contrast are now adjusted.

23.3.2.3.3.2 Color depth adjustment

Color depth (**Saturation** parameter in the HSL color spectrum model) defines the number of colors used to build an image, while digitizing it by the video capture card. Color depth in INTELLECT™ software corresponds to the **Color Depth** setting.

Color depth is set for each camera individually.

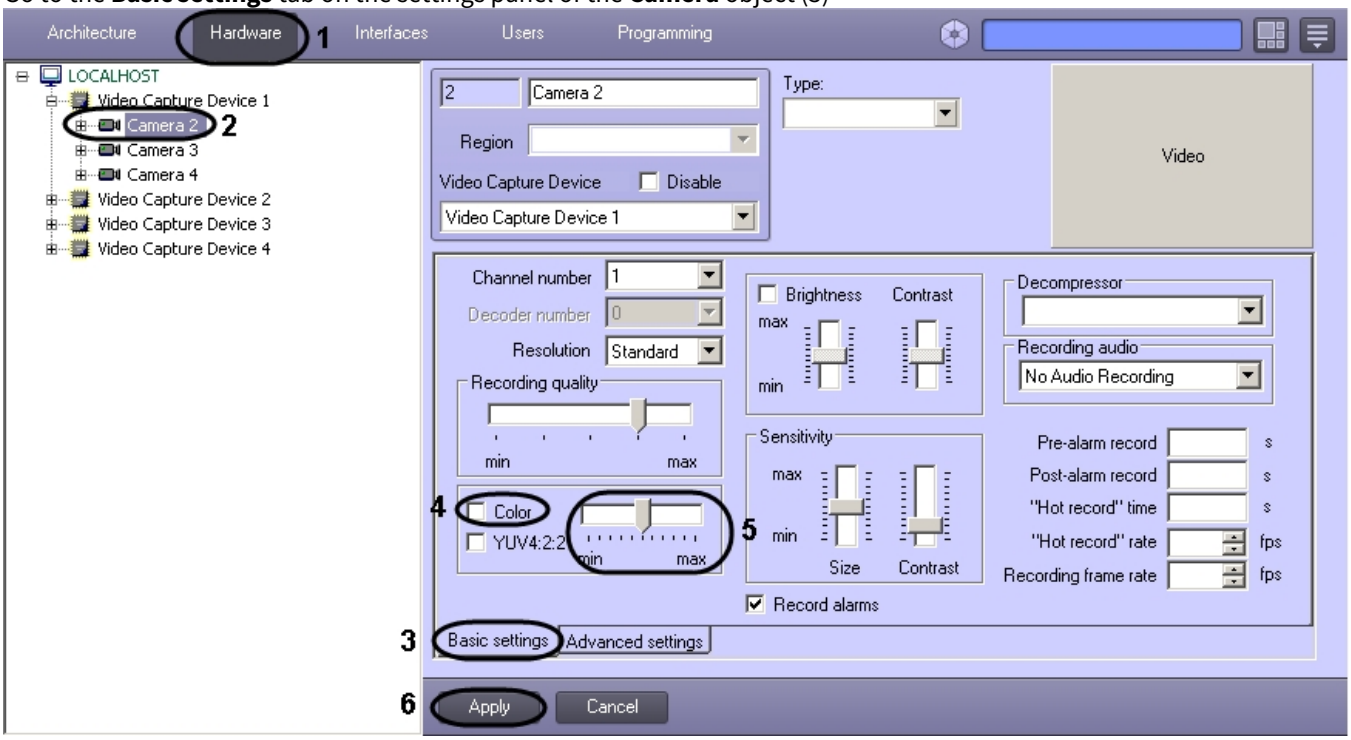
The color depth mean value is set by default.

While adjusting the color depth bear in mind that the image color depth is directly proportional to the frame size and thus to the video stream size. So, the digitized video stream with the greater color depth is bigger. The bigger the video stream, the bigger the HDD capacity to store it and the bigger the channel capacity to transmit it are required.

To change the image color depth, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object, created before, corresponding to the camera to be adjusted, in the **Hardware** tab in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.

3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3)



4. To reduce the image color depth to the black-and-white palette, uncheck the **Color** checkbox.
5. To change the color depth in other cases, move the **Color** slider on the right of the **Color** checkbox into the required position (5). The slider's **Max** position corresponds to the maximum color depth of the image, and the **Min** position - to its minimum color depth (black-and-white image). The sight control of color depth settings is performed using the viewing field.
6. Click the **Apply** button (6).

Color depth is now adjusted.

23.3.2.3.3.3 Selecting the color rendition format

Video image color rendition format fixes the number and the sequence of digitized video signal bits (or analog video signal frequencies), that contains its color depth data. So, the digitized video stream with the higher color depth is bigger. The bigger the video stream size, the bigger the HDD capacity to store it and the bigger the channel capacity to transmit it are required.

The TV systems use two formats of video color rendition: YUV 4:2:0 and YUV 4:2:2.

YUV 4:2:2 color rendition format is the standard format in TV systems. YUV 4:2:2 format provides high color depth and gives a large size of video stream. That is why video surveillance systems use to apply the YUV 4:2:0 format. In YUV 4:2:0 format, video signal color depth is slightly lower, than in YUV 4:2:2 format, and video stream size, digitized in YUV 4:2:0 format, is several times less than that in YUV 4:2:2 format.

INTELLECT™ software has digitization options in both formats: YUV 4:2:0 and YUV 4:2:2.

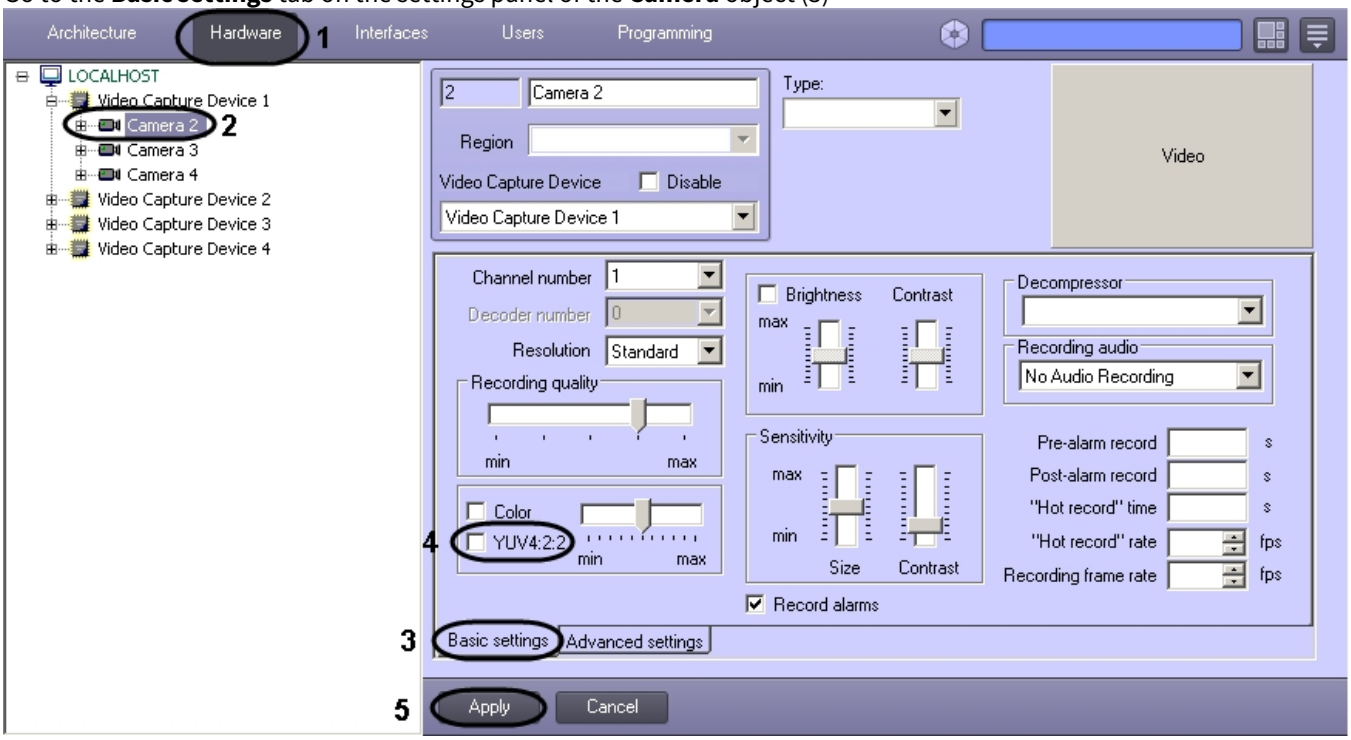
Video color rendition format is set for each camera individually.

Default encoding of video signals for all cameras is performed by the video capture card in YUV 4:2:0 color rendition format.

To configure the encoding of video signals in YUV 4:2:2 format, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object, created before, corresponding to the camera to be adjusted, in the **Hardware** tab in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.

3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3)



4. Set the **YUV 4:2:2** checkbox (4). The sight control of color rendition settings is performed using the viewing field.
5. Click the **Apply** button (5).

The color rendition format is now selected.

23.3.2.3.4 Configuring video compression

On the page:

- Compression rate settings
- Key frame rate settings
- Setting delta frame creation criterion

23.3.2.3.4.1 Compression rate settings

The image is compressed to reduce the size of video stream. Video is not compressed when it is displayed on the Monitor of the Server.

An increase in compression rate leads to video degradation. Intellect™ software compresses video right after its digitizing by the video capture card, prior to its recording and/or before transmitting it to the Remote Workstations.

Video compression rate is configured for each camera individually.

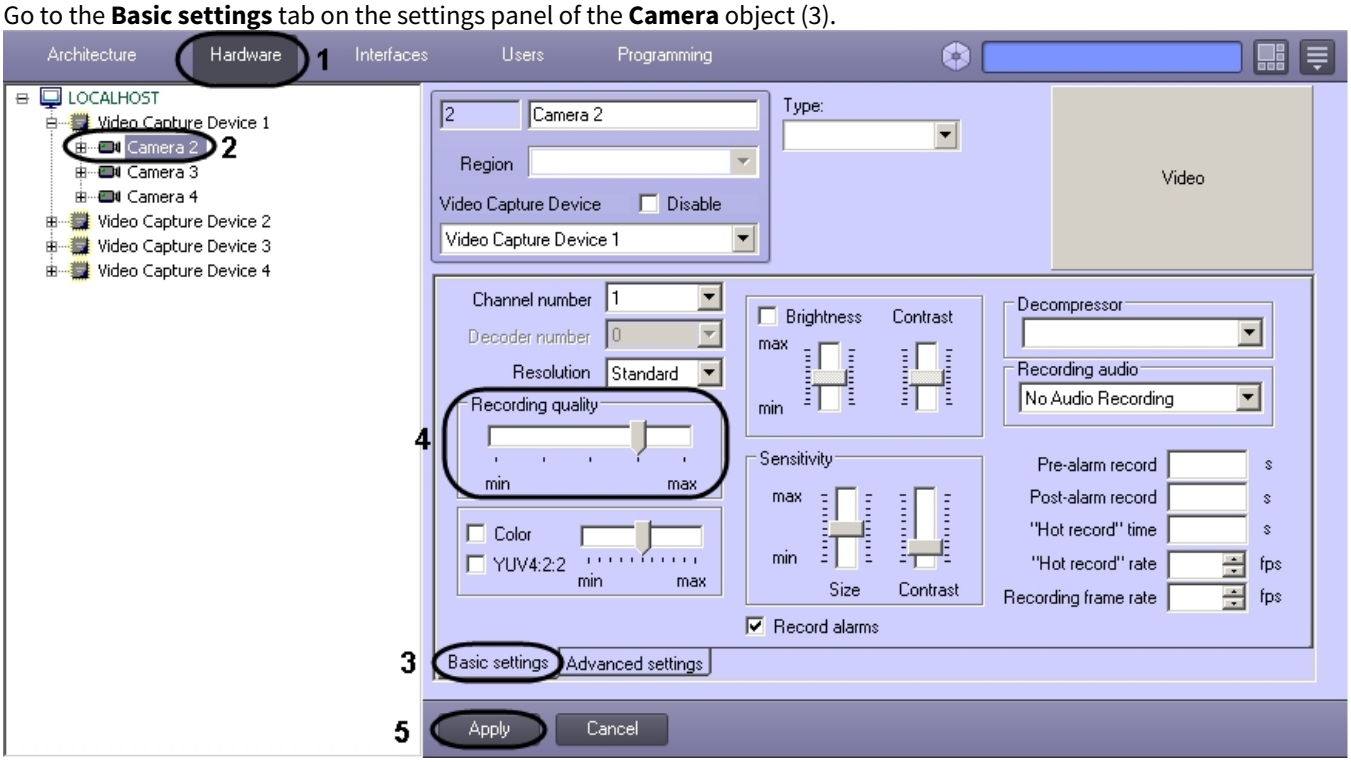
INTELLECT™ system uses the **Quality** setting for the compression rate parameter, which is reverse to the compression rate.

In most cases the default **Quality** setting is sufficient.

To change the video compression rate, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).

2. Select the **Camera** object, created before, corresponding to the camera to be adjusted, in the objects tree of the **Hardware** tab (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3).



4. If it is necessary to improve the video quality, move the **Quality** slider to the **Max** (4).
   If it is necessary to reduce the size of video stream from the camera, move the **Quality** slider to the **Min**.

> **Note.**
>
> Use the viewing field to estimate video enhancement or degradation.

5. Click the **Apply** button (5).

23.3.2.3.4.2 Key frame rate settings

INTELLECT™ software uses Motion Wavelet algorithm for video processing and compression. Processed by this algorithm, the video is the sequence of key - and delta frames. A key frame is a full frame of an image. A delta frame (differential frame) is an image containing only pixel blocks which differ from the previous key frame.

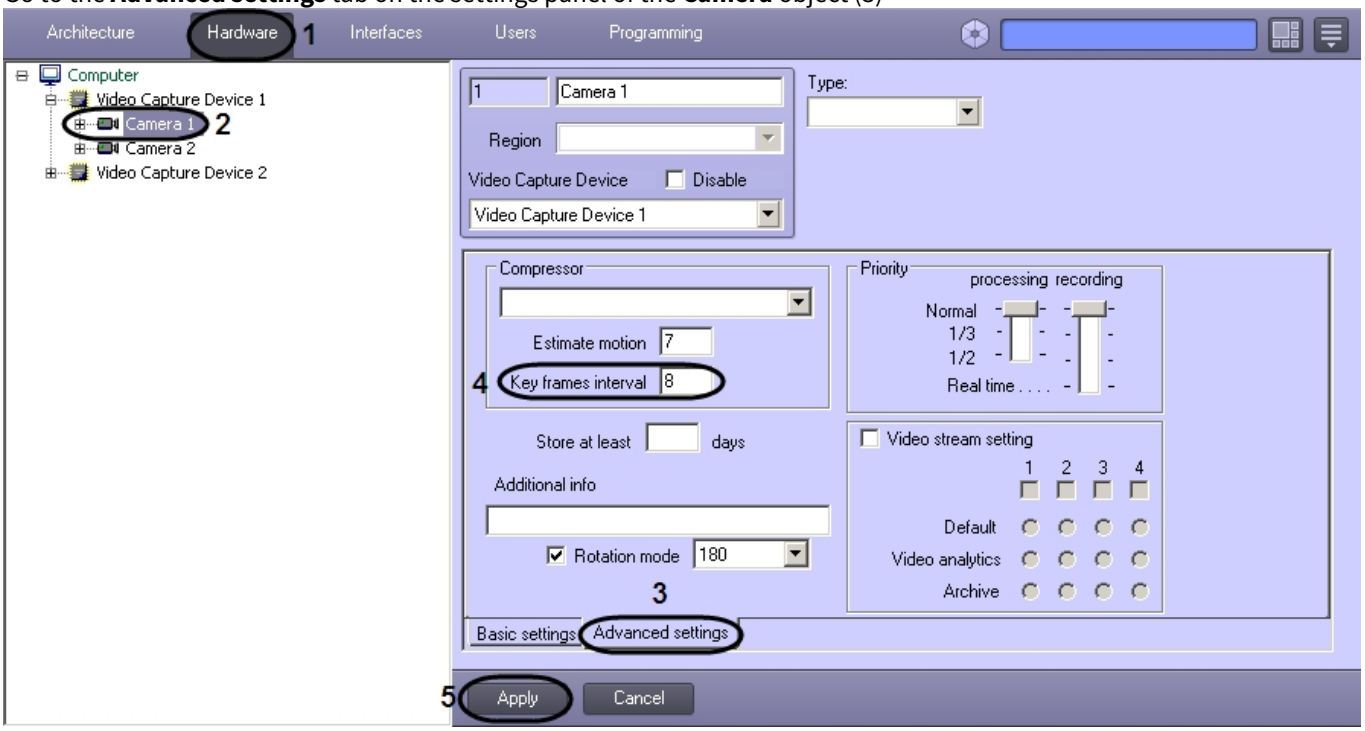
Motion Wavelet algorithm guarantees consistency of a frame regardless of key frame rate. With an increase of motion intensity in a frame, the size of delta frame is also increased and the quality of video does not change. With very intense motion (more than 70% of frame is engaged) the setting of key frame rate is ignored and every frame is processed as a key frame.

The best value of frame rate is set by default in INTELLECT™ software: every 8^{th} frame is processed as a key frame. If there are no special requirements to video size and quality, it is recommended to keep the default key frame rate.

To change the key frame rate, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object, created before, corresponding to the camera to be adjusted, in the objects tree of the **Hardware** tab (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.

3. Go to the **Advanced settings** tab on the settings panel of the **Camera** object (3)



4. Specify the required value of key frame rate in the **Key frames interval** field (4).
5. Click the **Apply** button (5).

Key frame rate is now configured.

23.3.2.3.4.3 Setting delta frame creation criterion

INTELLECT™ software uses Motion Wavelet algorithm for video processing and compression. Processed by this algorithm, the video is the sequence of key - and delta frames. A key frame is a full frame of an image. A delta frame (differential frame) is an image containing only pixel blocks which differ from the previous key frame. To compare the pixel blocks of a key frame to those of the frame next to the key frame, the average brightness of blocks is compared. If the difference in brightness exceeds a preset value, the block is considered to have fixed motion, and it becomes a part of a delta frame. Otherwise, the block is considered to have no motion, and it is not included into the delta frame.

Legitimate values of pixel block brightness lie within 0-225 range. The block becomes a part of the delta frame by default, if the difference between its average brightness in the current frame and in the previous key frame exceeds 7 units. If this value is increased, the size of the delta frame is decreased, and the video stream size is consequently decreased, as a delta frame now contains less pixel blocks. Note that the blocks with useful motion data now are more likely to be excluded from the processed video and consequently there is video degradation. So, by reducing the value of the parameter setting the criterion for blocks to be included into a delta frame, you may improve the image while building up its size.

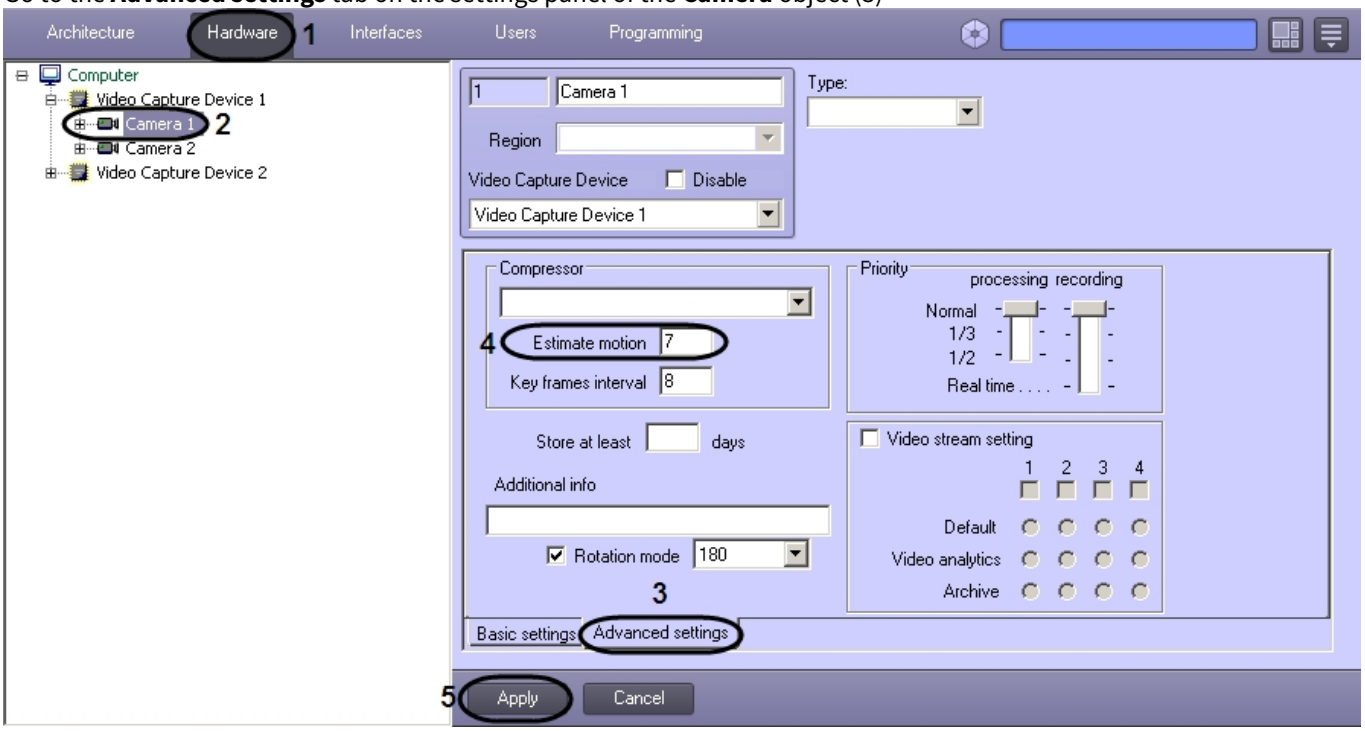
The best value of the parameter, which sets the criterion for blocks to be included into a delta frame, is defined by the brightness gradient of the video background and the moving objects in a frame: with a high gradient the parameter may be increased; with a low gradient the parameter value is to be decreased.

> **Note.**
>
> The **Estimate motion** parameter is ignored by the **Motion Wavelet 7.1** and **Motion Wavelet 7.1 Intr** compressors.

To change the value of the parameter, which sets the criterion for the block to be included into a delta frame, do the following:

1. Go to the Hardware tab in the **System settings** dialog box (1).
2. Select the **Camera** object, created before, corresponding to the camera to be adjusted, in the objects tree of the **Hardware** tab (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.

3. Go to the **Advanced settings** tab on the settings panel of the **Camera** object (3)



4. Specify the value of the parameter, which sets the criterion for the block to be included into the delta frame, into the **Estimate motion** field (4).
5. Click the **Apply** button (5).

Delta frames generation criterion is now set.

23.3.2.4 Creating and configuring a virtual Video Capture Device

On the page:

- General information about the virtual Video Capture Device
- Creating and configuring the virtual Video Capture Device
- Features of playing black the files in the virtual Video Capture Device

23.3.2.4.1 General information about the virtual Video Capture Device

Intellect implements a way to work with a virtual Video Capture Device. This way assumes that *Intellect* operates in a test mode and imitates the video stream feed to virtual Video Capture Device by playing back videos (video recordings). There are two types of virtual Video Capture Devices in *Intellect*:

1. **Virtual bench**. It plays back video recordings in mkv, mp4 and avi formats for which DirectShow codecs are installed on Windows OS.
2. **Virtual**. It plays back video recordings in internal *Intellect* format and files in .avi format.

Attention!

Video recordings with b-frames are not supported.

Virtual Video Capture Devices do not support multistreaming. To ensure the correct operation of a virtual Video Capture Device, including displaying the video archive and archiving, disable the multistreaming (see Configuration of multistream video).

It is not recommended to use LAV Splitter to playback video recordings in the Virtual Video Capture Device. The FFDSHOW mediadecoder is preferable.

Note

If only Windows Media Player 11 (or its older versions) is installed on Windows OS to view video recordings, then you should updated it to Windows Media Player 12 or use the DirectShow filters (codecs) of the third-party vendors.

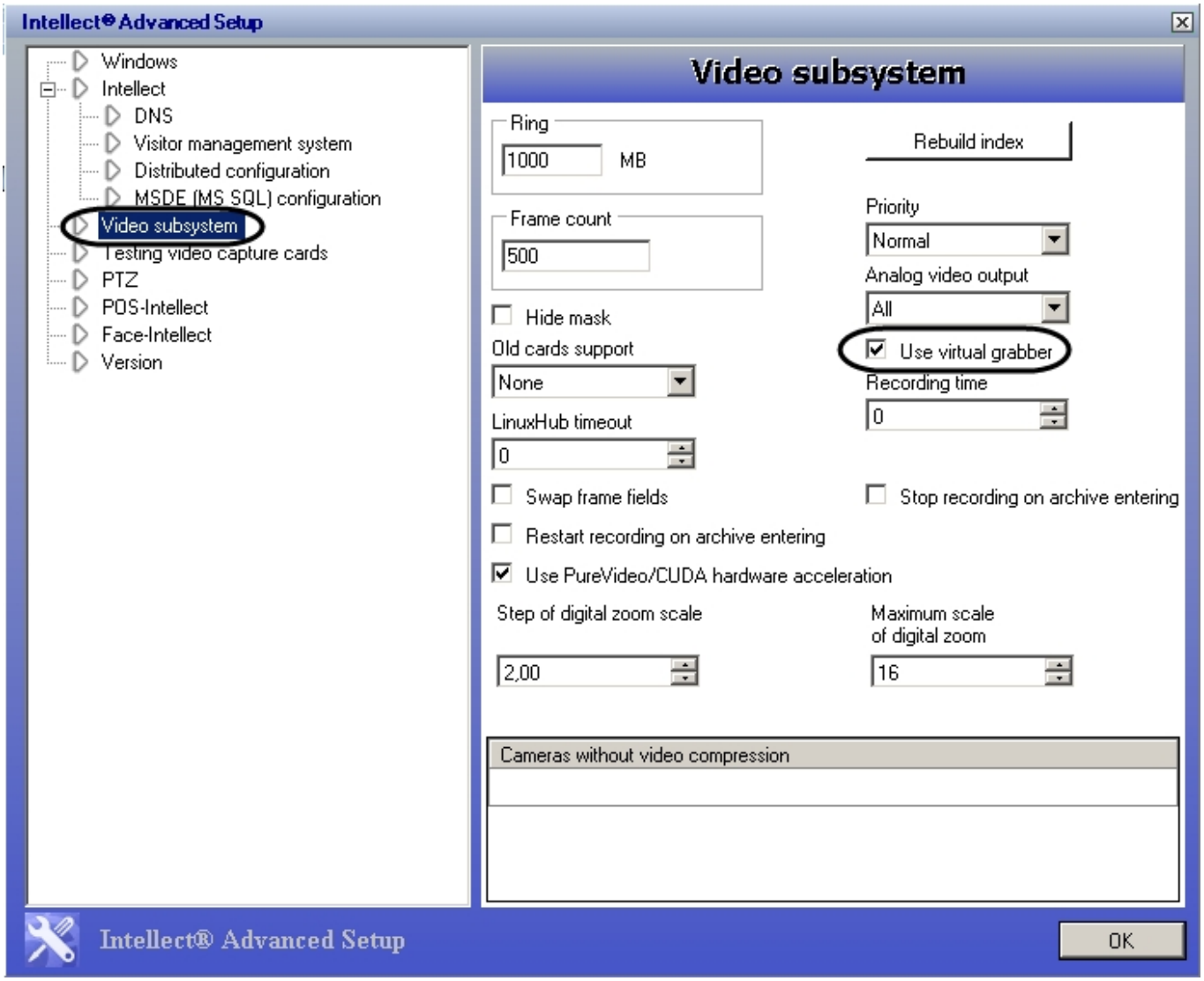
Note

Enable **Desktop Experience Feature** when using the virtual Video Capture Device on Server OS and the avi files.

23.3.2.4.2 Creating and configuring the virtual Video Capture Device

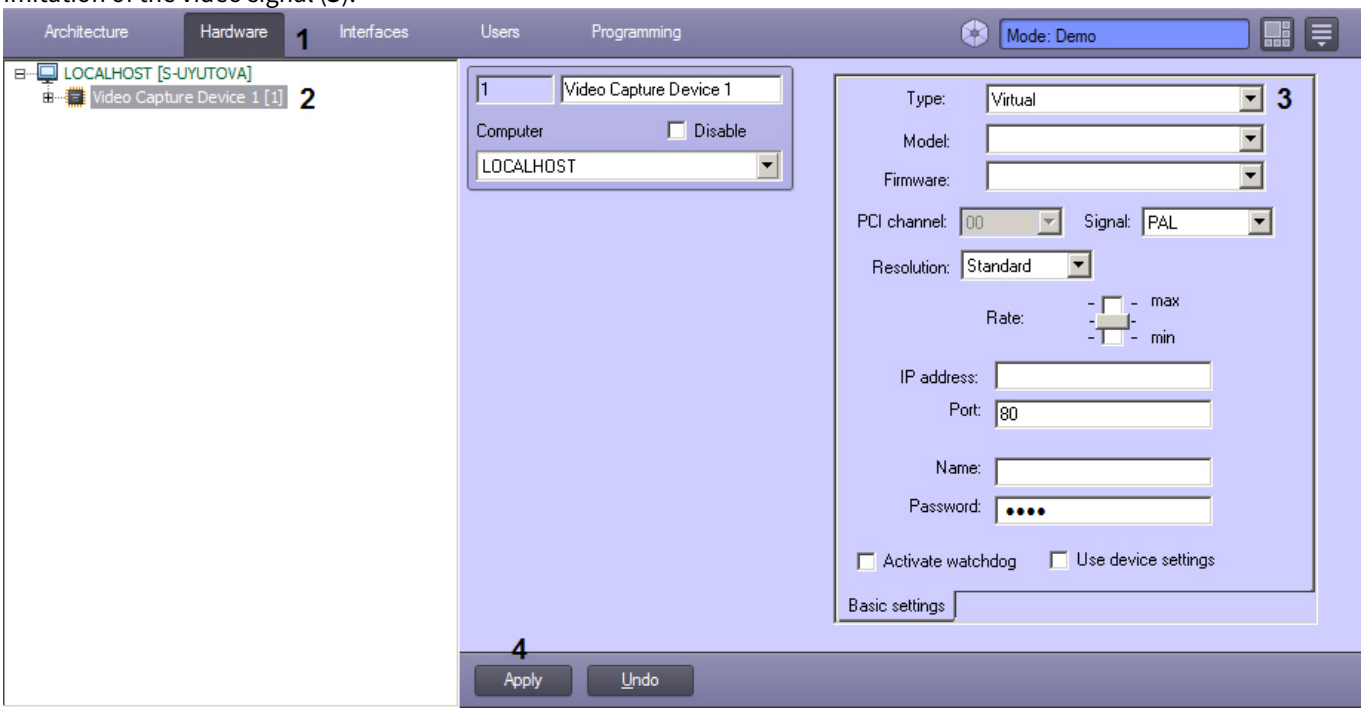
Create and configure the virtual Video Capture Device as follows:

1. Set the **Use virtual grabber** checkbox (The Settings panel of the Video subsystem section). Before that shut down *Intellect*.

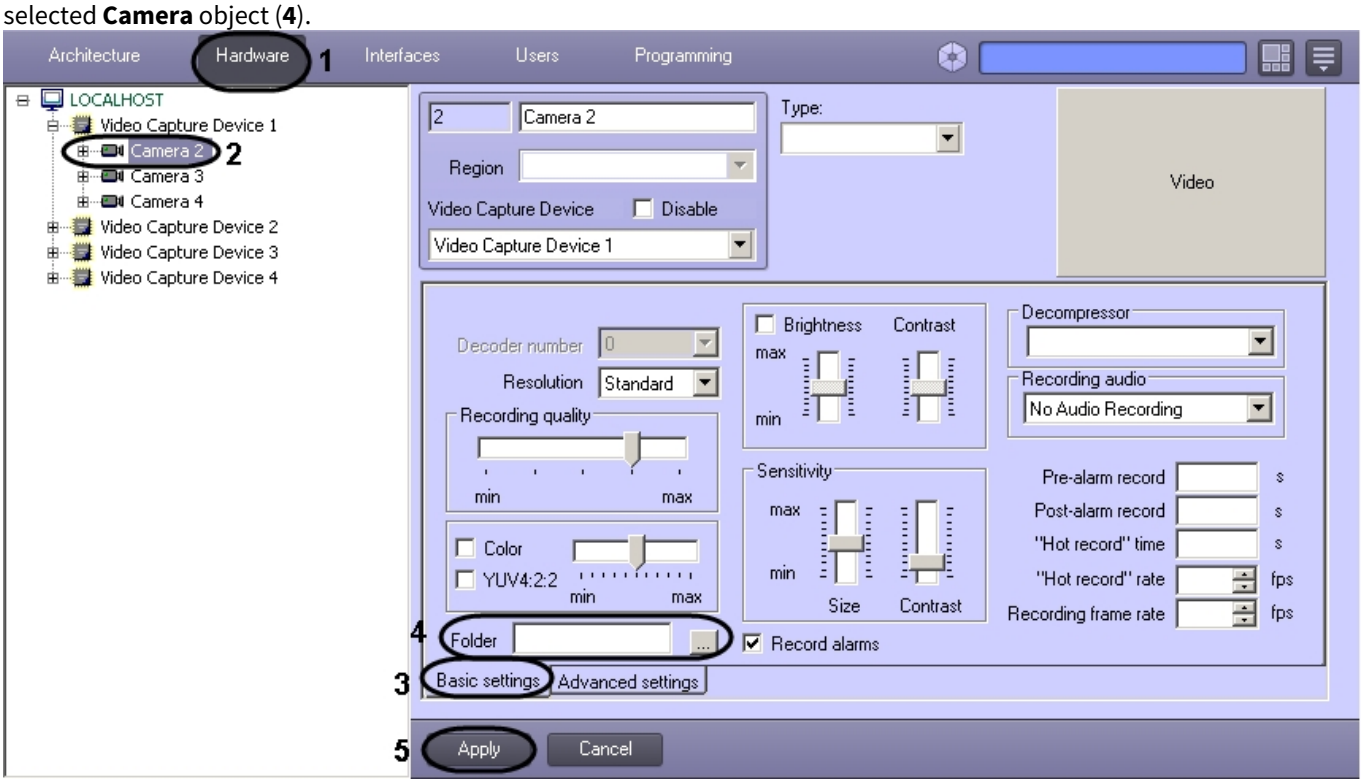


2. On the **Hardware** tab (**1**) create the **Video Capture Device** object (**2**).

3. Set the **Virtual** or **Virtual bench** type of the Video Capture Device depending on the type of the file that will be used for imitation of the video signal (**3**).



4. Click the **Apply** button (**4**).
5. Create the **Camera** child object for the Video Capture Device (**2**).
6. Specify the storage for the video recording that is used for the video signal imitation in the **Basic settings** tab (**3**) of the selected **Camera** object (**4**).



Note

It isn't recommended to use videos compressed by the Wavelet codec, as their use significantly increases the load on the Server.

7. Click the **Apply** button (**5**).
   If *Intellect* does not find files for playback within one minute after clicking the **Apply** button, the file search will be interrupted.

> **Attention!**
>
> The selected folder should not contain the video recordings of the internal *Intellect* format and AVI-files at the same time.
> It is recommended to use one video recording and specify the folder containing only the recording or the path to the file.
> If you need to use several video recordings, select the recordings with similar codec and resolution. This will help to avoid delays in *Intellect* work when switching between the recordings.

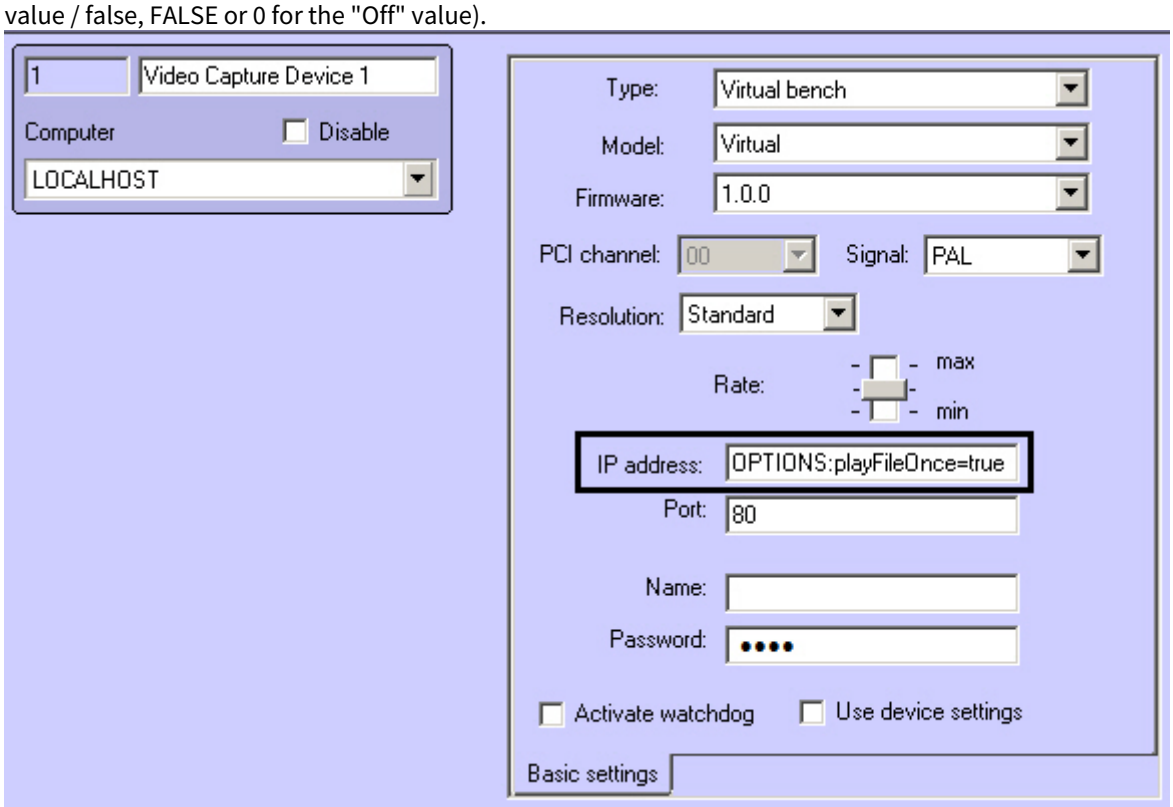
23.3.2.4.3 Features of playing black the files in the virtual Video Capture Device

As a result of the above settings, the video recording file from the selected folder will be played back in a loop.

If you set path to a separate file not a folder for a **Virtual** type, the file is played once without looping.

You can disable looping of a separate file for the **Virtual bench** type device in one of the following ways:

1. Enter "**OPTIONS:playFileOnce=true**" in the **IP address** field on the **Video Capture Device** settings panel:
   a. OPTIONS: enables the use of advanced options.
   b. playFileOnce corresponds to the "Single Play" option (the parameter name should be specified strictly case-sensitive).
   c. after the '=' symbol specify the value that should be applied (the correct values are true, TRUE, or 1 for the "On" value / false, FALSE or 0 for the "Off" value).



2. Set the playFileOnce = 1 registry key (see Registry keys reference guide).

If there are several files in the folder, they will be played back in the order set in the latest modification. Files can also be sorted by name and time of creation during playback. The sorting order is set by the VirtualGrabberSortMode registry parameter (see Registry keys reference guide).

When playing back the files, the system sends events to the Debug window displaying the playback status (see CAM Camera). There are also reactions for controlling video recordings playback in virtual Video Capture Device using the scripts (see GRABBER Video capture device).

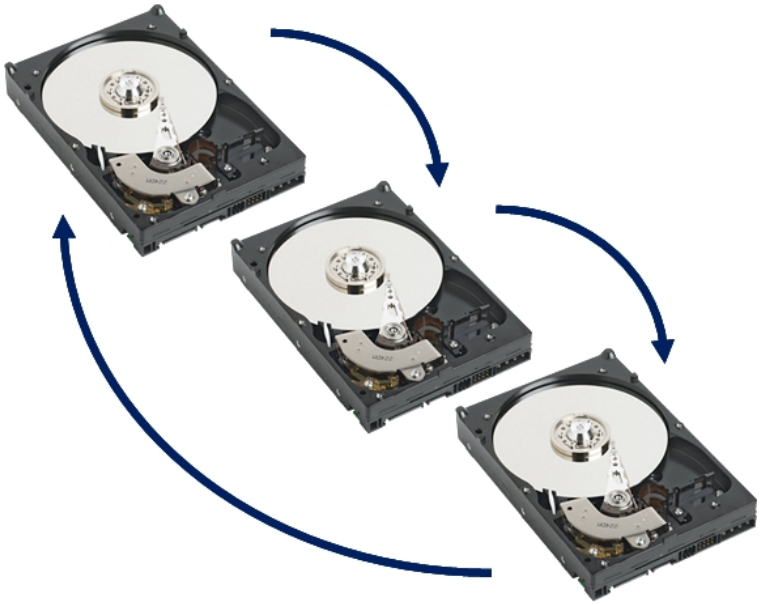
23.3.2.5 Configuring video archiving

23.3.2.5.1 General information on video archiving

Video archiving feature implemented in *Intellect* allows saving video according to the settings and analyze the parts of it that are of interest to the user.

The archive is saved on the Server storage device. Video is stored in the archive as one or more indexed files. To limit the size of the files, use the **Video Subsystem** tab in the tweaki utility.

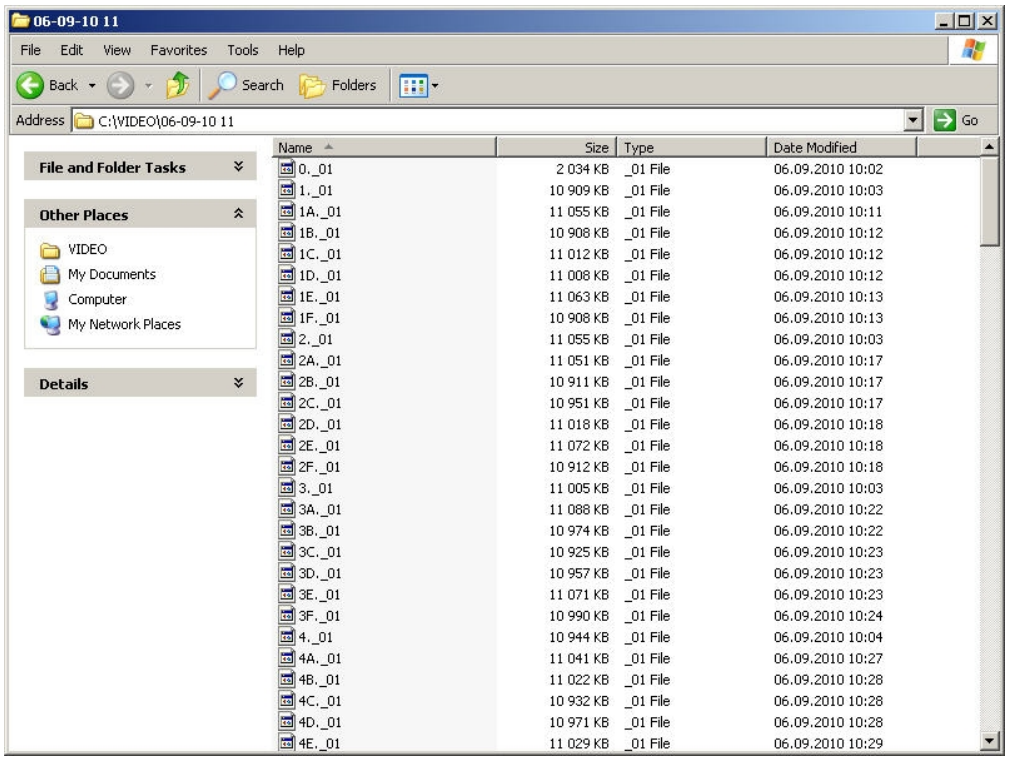
The archive is a storage of video recordings created in *Intellect*. Videos are recorded in a loop. When hard disks run out of the space allocated for storing the archive, the hard disks space is overwritten. The earliest recordings are deleted.



Video archive is stored in the VIDEO folder on the selected system disk. In the VIDEO folder, the subdirectories named in the DD-MM-YY HH (Date, Hour) format are stored. They contain the archive files for the current hour. Video file extension indicates the number of a video camera used to record the archive.

Attention!

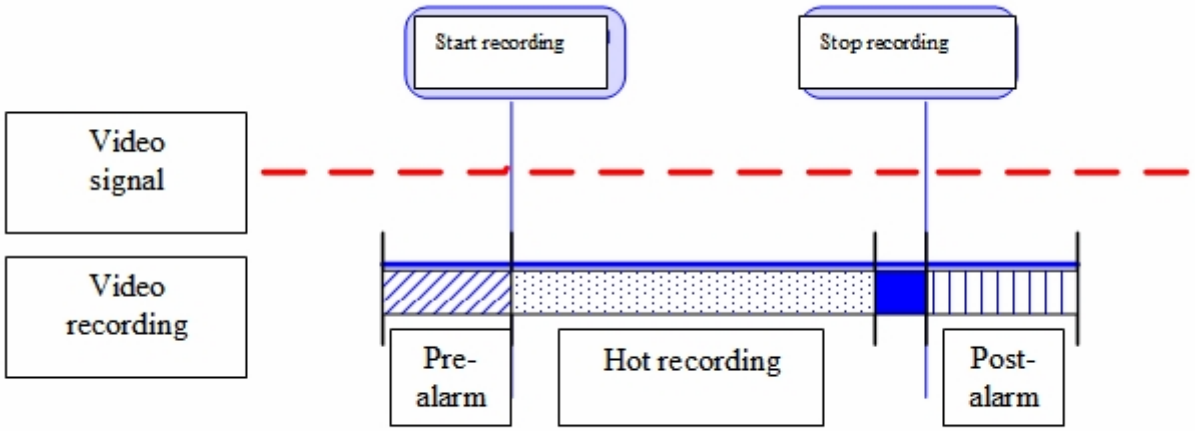
Intellect creates and stores video archive in its own format. You can view the archive files without converting in the Video surveillance window, using the converter.exe utility or using the AxxonPlayer utility when you select the required time period.
You can also export the video archive into other formats. For this, you can use the above instruments as well as the AviExport utility. See also Export and print out.
The codec in which the archive is recorded is by default determined by the codec of the original video signal — see Video signal compression and decompression. You can also record the archive in the MPEG4 format regardless of the codec of the original video signal. For this, create and configure the **MPEG4 Encoder** object.



There are three ways to start video recording:

1. Forced recording by the Operator command;
2. Automatic recording upon alarm registration;
3. Automatic recording upon a macro/script/program execution.

In order to improve the efficiency of analysis of causes and consequences of alarm events on the protected facilities, *Intellect* implements the expanded schemes for creating a video recording file. An example of a video recording expanded scheme is given in the figure below.



The scheme contains the following segments:

1. Pre-alarm event is recorded before the start time of the alarm event recording on the video camera. Pre-alarm event recording allows you to analyze the prehistory of the alarm event.

> **Attention!**

For the cameras without video compression that were added to the corresponding list in the **Video subsystem** section in the tweaki.exe utility (see The Settings panel of the Video subsystem section), video is not recorded in **Pre-alarm record** mode.

2. Post-alarm event is recorded after the end time of the alarm event recording on the video camera. Post-alarm event recording allows you to analyze the consequences of the alarm events.
3. Hot recording is a video recording segment with higher frame rate. Increased frame rate on the hot recording segment makes event analysis more effective. The hot recording segment always starts from the start time of the alarm event registration. The hot recording is finished at the recording end time (depending on the hot recording settings).

In *Intellect*, the restrictions are imposed on the use of additional sections when creating a video recording.

Video recording initialization mode	**Recording option**		
	pre-alarm	**hot recording**	**post-alarm**
By Operator command	No	Yes	No
On alarm event	Yes	Yes	Yes
On macro/script	Yes	Yes	Yes

Note

If the MPEG4 recording format is selected, a small fragment of the recording (about 0.5 seconds from the beginning) may be lost.

Free disk space (video archive size) required
Working with the archives

23.3.2.5.2 Video archiving procedure

Configuration of video archiving consists of the following steps:

1. Selecting the disks for video archive storage.
2. Switching off/on the auto alarm recording mode.
3. If a camera supports multistreaming, then select streams that are to be recorded to the archive upon alarm and those for continuous recording (see Configuration of multistream video).
4. Configuring video frame rate and other video stream parameters if the multistream mode is in use (see Configuration of multistream video).
5. Configuring video in the Hot recording mode.

   Note.

   If different streams are selected for recording upon alarm and for continuous recording (see Configuration of multistream video), then hot recording is not performed.

6. Configuring video in the Pre-alarm mode.
7. Configuring video in the Post-alarm mode.
8. Configuring audio and video synchro recording.

23.3.2.5.3 Selecting the disks for video archive storage

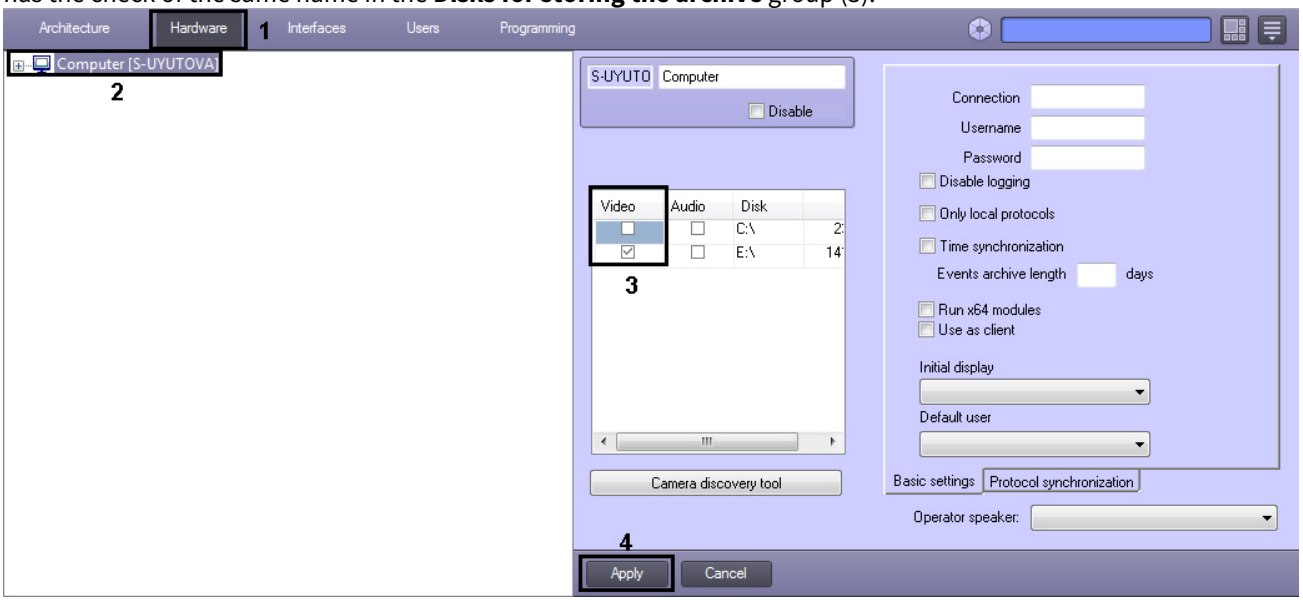
INTELLECT™ software performs video archiving to a storage device. When INTELLECT™ is installed, set the local disks to save the archive to in the **Hardware** tab of the **Computer** object.

Note.

Use disks with the NTFS file system for storing the archive. If the FAT32 file system is in use, then there can be problems caused by this system, for instance — it has no logging.

To select the disks for the archive, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Computer** object corresponding to the configured Server in the objects tree of the **Hardware** tab (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab. Each local disk available for archiving has the check of the same name in the **Disks for storing the archive** group (3).



3. Set the relevant check in the **Video** column next to the disk to be selected. Local, network and USB disks are available for storing (details on adding network disks are in Using network disks section).

   Note.

   For the reverse effect set the checkboxes corresponding to the disk unchecked in the **Video** column.

4. Click the **Apply** button (4).

The disks for video archive storage are now selected.

Note.

If no disk for storing the video is selected, then there is no storing to the archive.

Free disk space (video archive size) required
Working with the archives

23.3.2.5.4 Using network disks

To use network disks as an archive, set UNC paths to them in *Intellect*. Details of working with network disks in *Intellect* installed as a Service are given in Using network disks of INTELLECT™ installed as a Service section.

While working in Windows Vista and Windows 7 OS consider the following features:

1. For Windows Vista and Windows 7 OS with UAC enabled it is necessary to connect network disks via command prompt with Administrator's rights. The way of connecting is described in Connecting network disks in Windows Vista and Windows 7 OS section.

2. Access to network disks on computers with Windows Vista or Windows 7 OS can be forbidden when the user account control (UAC) is switched on. To enable access create the EnableLinkedConnections key of the DWORD type with 1 value in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System registry. Details of working with registry keys are in Working with Windows OS registry section.

Note

When connection with net disk fails, video is not recorded (for 30-60 seconds) and displayed. This is due to filesystem features.

Attention!

The archive from various Servers must not be recorded to one network storage as the archive index will be violated.

To add a network disk by specifying the UNC path, do the following:

1. Go to the last line in the disk list and click the down key.

2. Specify the path to a network disk in the appeared line in the **Disk** column. UNC path is set in **\\server_name\share_name** format where server_name is the name of file server and share_name is the network name of the general folder.

   Note

   If there are any problems with storing video/audio archive at network disks, then use the net use command of Windows command prompt:
   net use disk_name: \\server_name\share_name /delete
   net use disk_name: \\server_name\share_name /USER:user_name
   Where user_name is a user that has rights to store to selected network disk and on whose behalf the video module is launched;
   disk_name: is the name of the disk drive. This is to be performed after every Windows OS restart.
   Details about the net use command are in Microsoft official documentation (www.microsoft.com).

3. Set a checkbox for created disk in the **Video** column.
4. Click the **Apply** button.

A network disk by specifying the UNC path is now added.

Free disk space (video archive size) required
Selecting the disks for video archive storage
Working with the archives

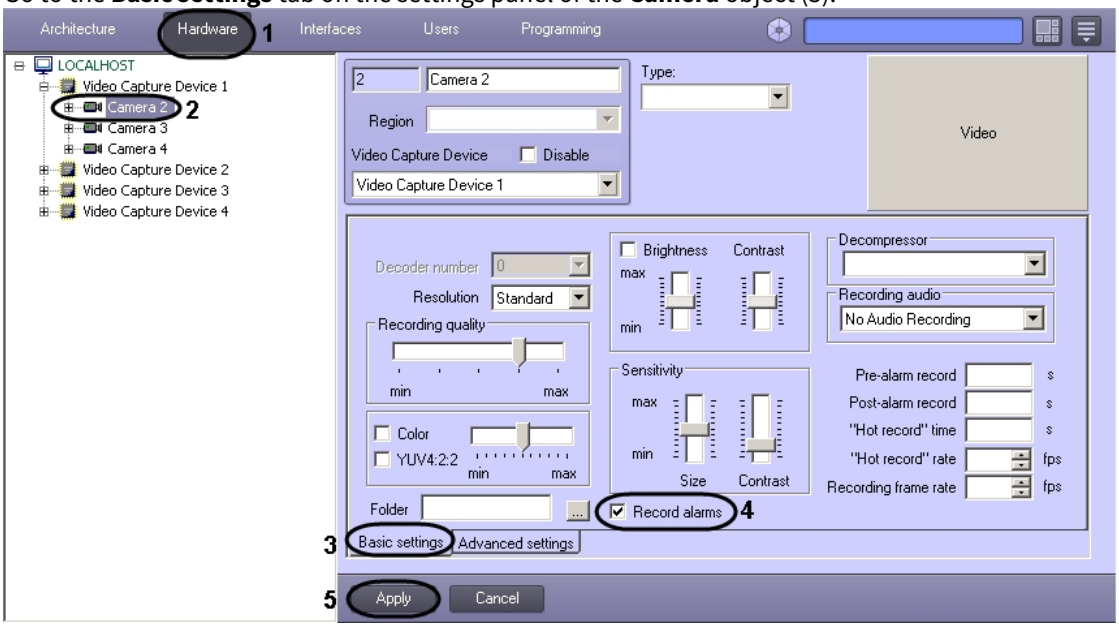
23.3.2.5.5 Disabling automatic recording upon alarm registration

INTELLECT™ software supports automatic video recording upon alarm registration for each **Camera** object individually. By default, the auto recording option is enabled for all cameras in the **Hardware** tab.

The auto recording option is disabled for each camera individually, as well.

To disable the auto recording upon alarm option for a selected camera, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object corresponding to the required camera in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3).



4. Set the **Record alarms** checkbox unchecked (4).
5. Click the **Apply** button (5).

Automatic recording upon alarm event registration is now disabled.

Note.

To re-enable the auto recording, repeat the above steps and set the **Record alarms** checkbox.

Events recording

23.3.2.5.6 Configuring video frame rate

By default, video is recorded to the archive with the same frame rate as the video capture card digitizes it. Thus, to reduce the archive size, the frame rate can be configured.

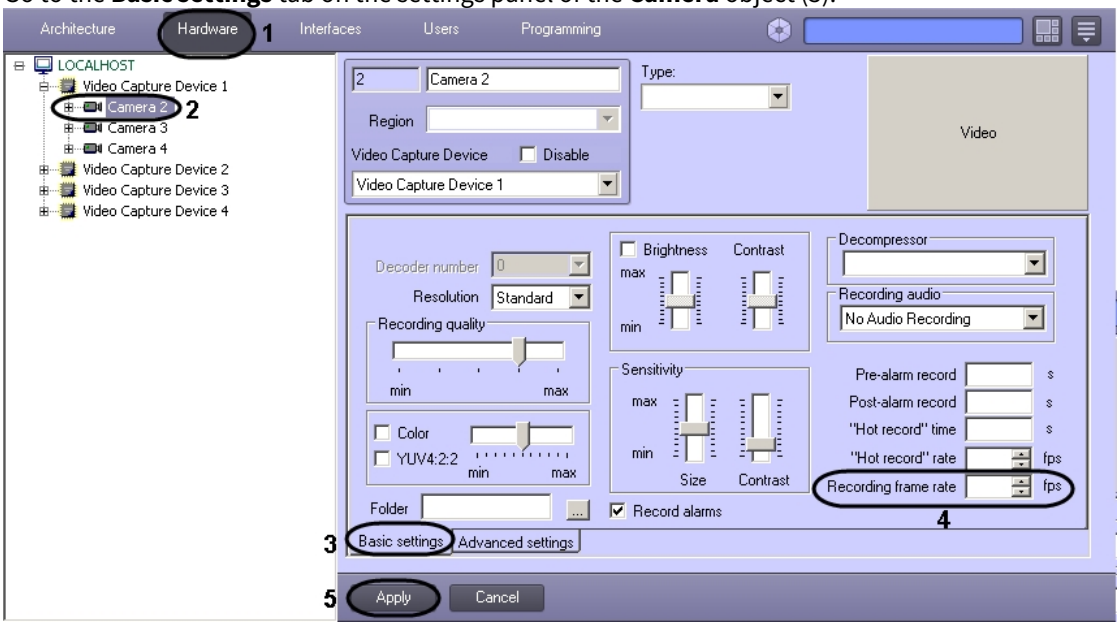
Note.

The reduction of the video recording frame rate does not affect the displaying of the video on the Server monitor and its transmission to the Remote Workstations by the network.

To change the recording frame rate, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object corresponding to the required camera in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.

3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3).



4. Specify the recording frame rate value in the **Recording frame rate** field (4). The value is not to exceed the digitization frame rate value. The value set for the **Recording frame rate** parameter allows calculating the interval (msec) in which a frame is to be captured to be stored in the archive. The calculation is made according to the formula:
Interval = 1000 / Value in the Recording frame rate field

> **Note.**
>
> Setting the value of the **Recording frame rate** parameter, take account of video digitizing rate and frame rate (fps), otherwise actual recording speed can differ from the set one.

5. Click the **Apply** button (5).

23.3.2.5.7 Configuring video in the Hot record mode

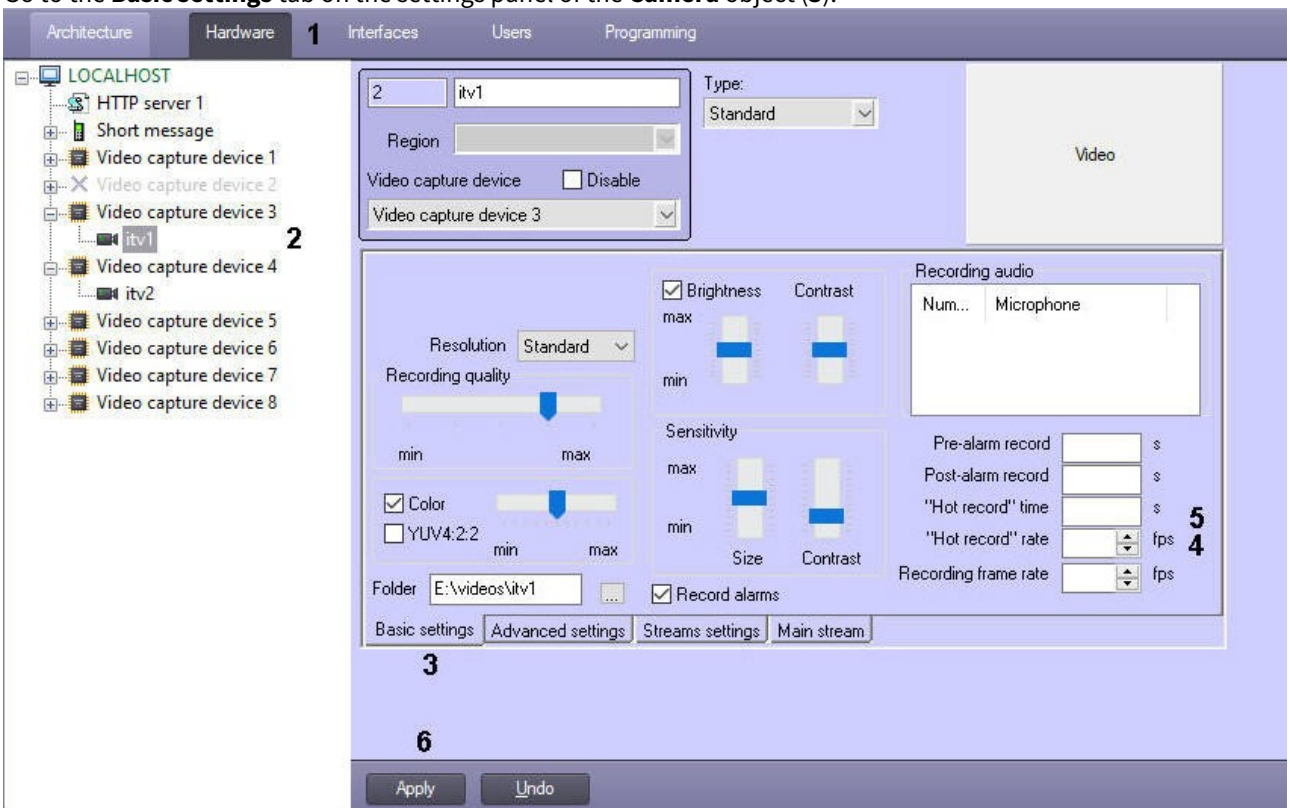
The **Hot record** mode is a video recording mode in which the frame rate of the video stream increases when an alarm is detected.

> **Note.**
>
> The **Hot record** mode settings are not applied when the **Camera** object is created under the **Video capture device** object using H264, MPEG4 or H265 codec.

By default, this mode is disabled: when an alarm is detected, the video is recorded at the frame rate specified in the **Recording frame rate** parameter (see Configuring video frame rate) or at the default rate if the **Recording frame rate parameter** is not specified. To enable the **Hot record** mode, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).
2. Select the **Camera** object corresponding to the required camera in the objects tree (**2**). The settings panel for the selected object is displayed on the right of the **Hardware** tab.

3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (**3**).



4. In the **"Hot record" rate** field (**4**) specify the frame rate for hot recording of the alarm event.
   The value specified in the **"Hot record" rate** parameter allows you to calculate the time interval (in milliseconds), after which it is necessary to capture a frame for recording into the archive. The calculation is made according to the formula:
   *Time interval = 1000 / The value specified in the **"Hot record" rate** field*
   The value of this parameter should not exceed the value of the frame rate with which the video signal is digitized.
5. In the **"Hot record" time** field (**5**) specify the interval in seconds from the moment of alarm registration or the start of recording, during which the video is recorded with the frame rate specified in the **"Hot record" rate** field.

   Note.

   If there is an end of alarm event while recording in the hot record mode, then recording to the archive will be with the same rate as hot record until the end of specified interval.

6. Click the **Apply** button (**6**).

Note.

If the **Recording frame rate** parameter is set to non-zero, regardless of its value of recording to the archive is performed only by anchor frames if H.264 codec is in use. If the **"Hot record" rate** parameter for H.264 codec is also in use, then the recording to the archive will be performed by anchor frames too. If the **Recording frame rate** parameter is set to 0 or not set, all frames are recorded to the archive.

23.3.2.5.8 Configuring video in the Pre-alarm record mode

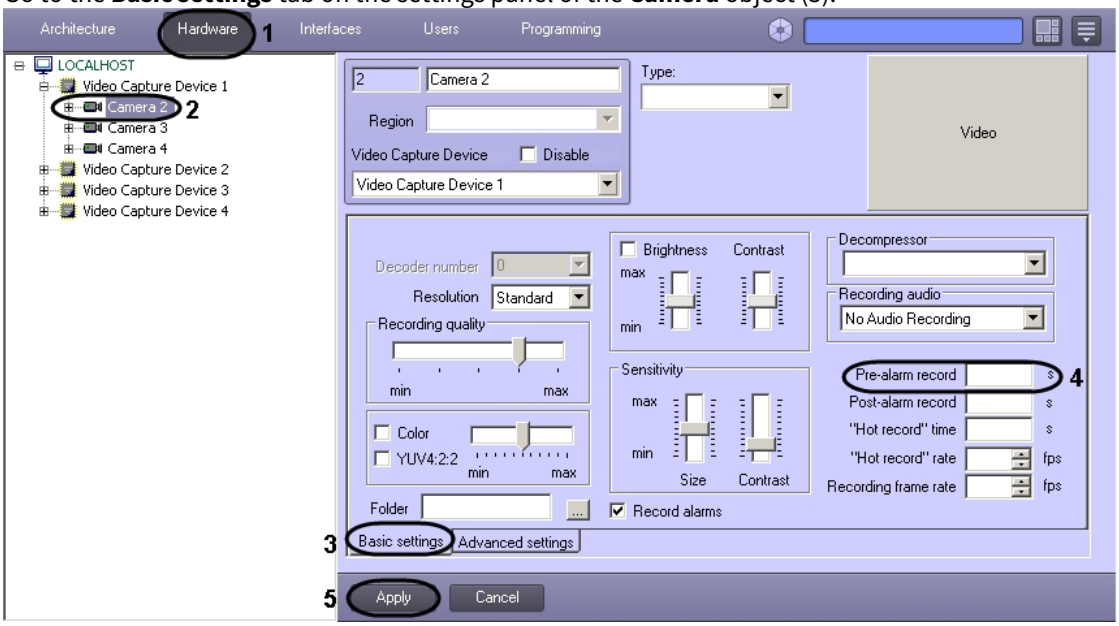
The **Pre-alarm record** mode is the record mode for recording pre-alarm events for a specified period before recording an alarm. Pre-alarm record is performed at the hot record rate. If the hot record rate is not specified, then at standard record rate.

Attention!

For cameras without video compression that have been added to the corresponding list in the **Video subsystem** section in the tweaki.exe utility (see The Settings panel of the Video subsystem section), video is not recorded in **Pre-alarm record** mode.

By default the recording in this mode is disabled. To enable the pre-alarm recording, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object corresponding to the required camera in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3).



4. In the **Pre-alarm record** field specify the required interval (sec) of pre-alarm events recording (4).
5. Click the **Apply** button (5).

Information on pre-alarm recording options is given in the table.

Camera state	Recording initiator	Recording
Armed	Macro	Without pre-alarm recording
Armed	Manually	Without pre-alarm recording
Armed	Alarm	With pre- alarm recording
Armed	Program	With pre-alarm recording
Disarmed	Macro	Without pre-alarm recording
Disarmed	Manually	Without pre-alarm recording
Disarmed	Alarm	-
Disarmed	Program	With pre-alarm recording

In INTELLECT™ one can make pre-alarm recording if camera is disarmed. One can do it with the help of DoReact("CAM","1","REC","rollback<1>") program; (see The Script object. Programming using the JScript language).

Specifying the long pre-record time can result in increasing the waste of running memory. Recommended pre-record time is not more than 20s.

To count the memory consumption ascertain the average size of video signal frame. To perform this, record the video fragment of 500 frames length to the archive (maximal size on default) and use the following formula:

Frame size = Fragment size / 500

The frame size is also depends on percent of motion in the frame.

It is possible to count the size of pre-record buffer for one camera it the frame size is known:

Size of pre-record buffer for one camera, MB=Pre-record time, sec * Frame frequency in the pre-record mode, fps * Frame size, MB.

General memory consumption in the pre-record mode is defined by sum of values for each camera.

It is possible to use the following formula in case of cameras perform pre-record with equal frame frequency:

Size of pre-record buffer for all cameras in system, MB = Number of cameras * Pre-record time, sec * Frame frequency in the pre-record mode, fps * Frame size, MB

Note

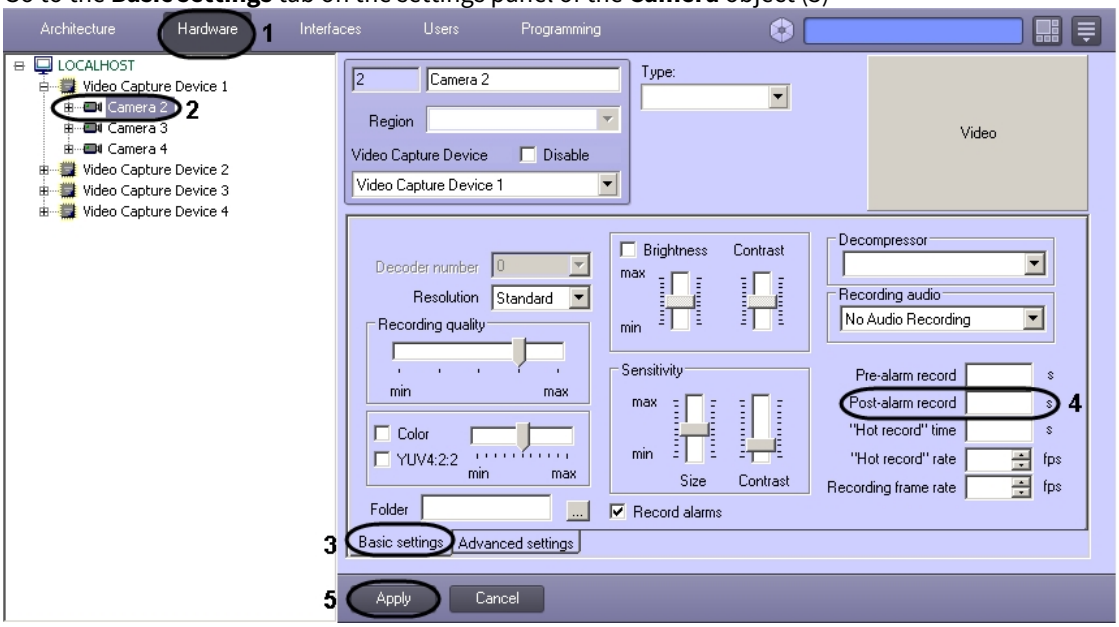
Example.
Camera performs pre-record for 15 seconds with the hot record speed 25 fps. Size of 500-frames fragment is 20 Mb. It is required to define size of pre-record buffer for such camera.
First, you it is necessary to define the average frame size:
Frame size = Fragment size / 500 = 20 MB/500 frames = 0.04 MB.
So, the size of pre-record buffer is:
The memory consumption in the pre-record mode for one camera, MB = Pre-record time, sec * Frame frequency in the pre-record mode, fps * Frame size, MB = 15 sec * 25 fps * 0.04 MB = 15 MB.

23.3.2.5.9 Configuring video in the Post-alarm record mode

The Post-alarm record mode is the record mode for recording post-alarm events for a specified period after recording an alarm.

By default, post-alarm recording is disabled. To enable the post-alarm recording, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object corresponding to the required camera in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3)



4. In the **Post-alarm record** field specify the required interval (sec) of post-alarm events recording (4).
5. Click the **Apply** button (5).

23.3.2.5.10 Configuring audio and video synchro recording

INTELLECT™ software provides audio and video synchro recording option.

Audio signal recording beginss at the recording start time and ends at recording end time. In synchro record mode, audio files are stored with video files in the Server archive in the "VIDEO" folders on the Server archive local disks.

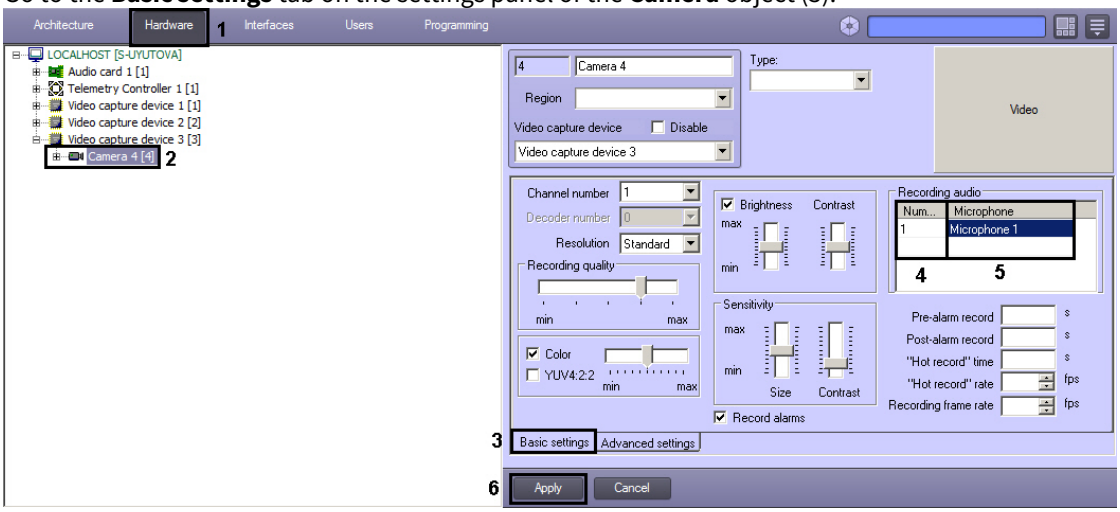
To use the synchro recording option, INTELLECT ™ software audio subsystem is to be properly configured. The audio subsystem configuration procedure in INTELLECT™ system is described in Configuring audio subsystem section.

Attention!

If camera and microphone configured for synchronous video- and audio record are created on the basis of different **Computer** objects (for example, **Server/RAW** and **Client**), than synchronous audio record will be performed only when disks for archive record on both computers have identical letters (see also Selecting the disks for audio archive storage and Selecting the disks for video archive storage).

If the audio subsystem is configured, do the following to configure synchro recording on the selected camera and microphone:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object corresponding to the required camera in the objects tree (2). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Basic settings** tab on the settings panel of the **Camera** object (3).



4. In the **Number** dropdown list of the **Recording audio** table select the ID of the microphone set for synchro recording when being registered in *Intellect* (4).
5. After the number is set, the name of any selected **Microphone** object is automatically displayed when clicking on any area of the **Microphone** column in the table (5).
6. If synchro audio recording from 2 microphones is to be performed, then repeat steps 4-5 for the second microphone.

   Note.

   Audio from two Microphones is recorded to one stream.

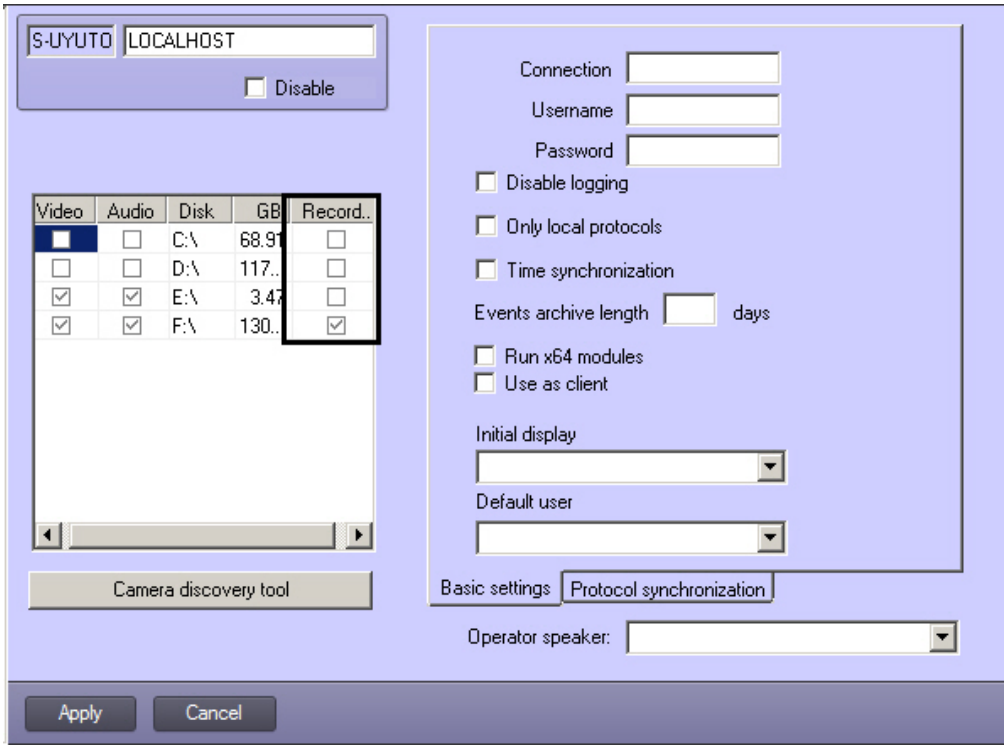
7. Click the **Apply** button (6).

Camera and microphone are now configured for audio and video synchro recording.

Synchronous playback of video and audio recordings
Audio and video synchronous recording

23.3.2.5.11 Selecting current disk for recording

The current disk on which the archive is stored is displayed in the **Recording** column of the **Computer** settings panel.



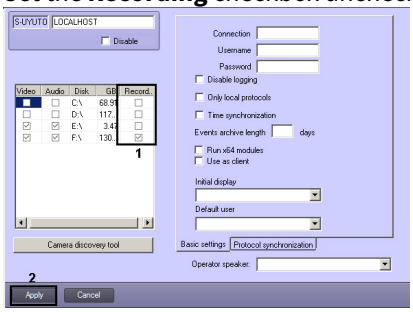
The *select current disk for recording* feature allows switching once to the disk from the list of active disks specified by the user (not to the following in the list) while loop recording in the list.

Example.

Recording of the archive is performed to 3 disks: A, B and C. When the archive is recorded in the standard mode, disks will be changed in the A->B->C->A->B->C.... order.
Let us assume that the recording is performed to disk B. Disk A (not C) is to be the following. Set the **Recording** checkbox checked for this disk, so disk C will be skipped and when disk B is full, archive will be recorded to disk A, then – to disk C, then – to disk A, etc.

Change the current disk for recording as follows:

1. Set the **Recording** checkbox unchecked next to a disk the recording is currently performed on.



2. Set the **Recording** checkbox checked next to a disk the recording is to be performed on.

   Note.

   A new disk is to be selected to store the archive (see Selecting the disks for video archive storage).

3. Click the **Apply** button.

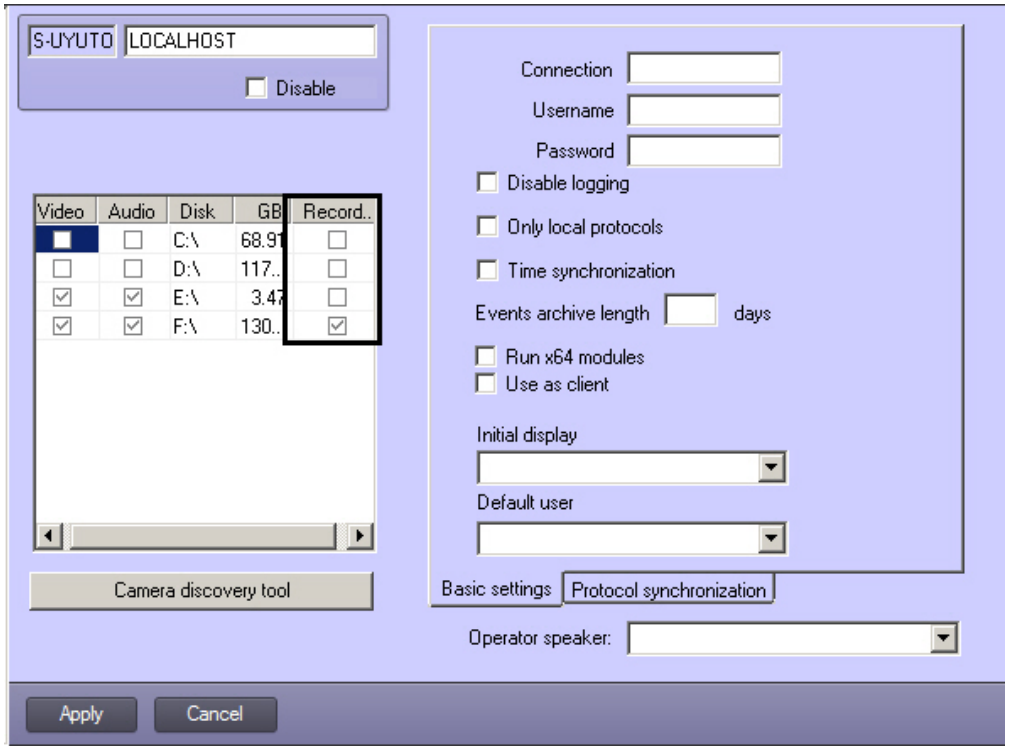
As a result the archive is stored on the selected disk. Further the loop recording continues (see General information on video archiving).

Note.

m_nCurVolume and m_dwTime registry parameters change when the current drive for recording is changed – see Registry keys reference guide.

23.3.2.5.12 Viewing current disk for recording

The current disk on which the archive is stored is displayed in the **Recording** column of the **Computer** settings panel.



23.3.2.5.13 Configuring video camera archive depth

It is possible to set the recommended period of keeping the video and audio archive (in case of synchro recording) on a camera in *Intellect.* This feature is implemented using the **Store no more than** and **Store no less than** parameters:

- The **Store no less than** parameter enables keeping the deeper archive on the selected camera by means of archives of other cameras. It is recommended to set the **Store no less than** parameter not more than on 30% of cameras on each server in the distributed system as this is advisory setting. If there is not enough space for keeping the archive, then the setting will be ignored and loop recording won't stop anyway (see General information on video archiving). The 'Ignoring "Keep no less than"' message is displayed in the Event viewer when the setting is ignored.
  If not less than 10 cameras are created on the server, then there will be the corresponding warning when clicking the **Apply** button while attempting to set this parameter for more than 30% of cameras on the server. It can be disabled using the NotifyAbout_arch_days registry key (see Registry keys reference guide).
- The **Store no more than** parameter enables specifying the time period over which the camera archive will be kept and at the expiring of which the archive will be deleted. The archive can be deleted earlier than specified time period if it is required by the loop recording. The check for files to be deleted is performed every 10 minutes system time (every 10 minutes after *Intellect* starting – since 4.10.5). If the deletion process takes more than 10 minutes, the next check starts in 10 minutes after the end of deletion.

Important!

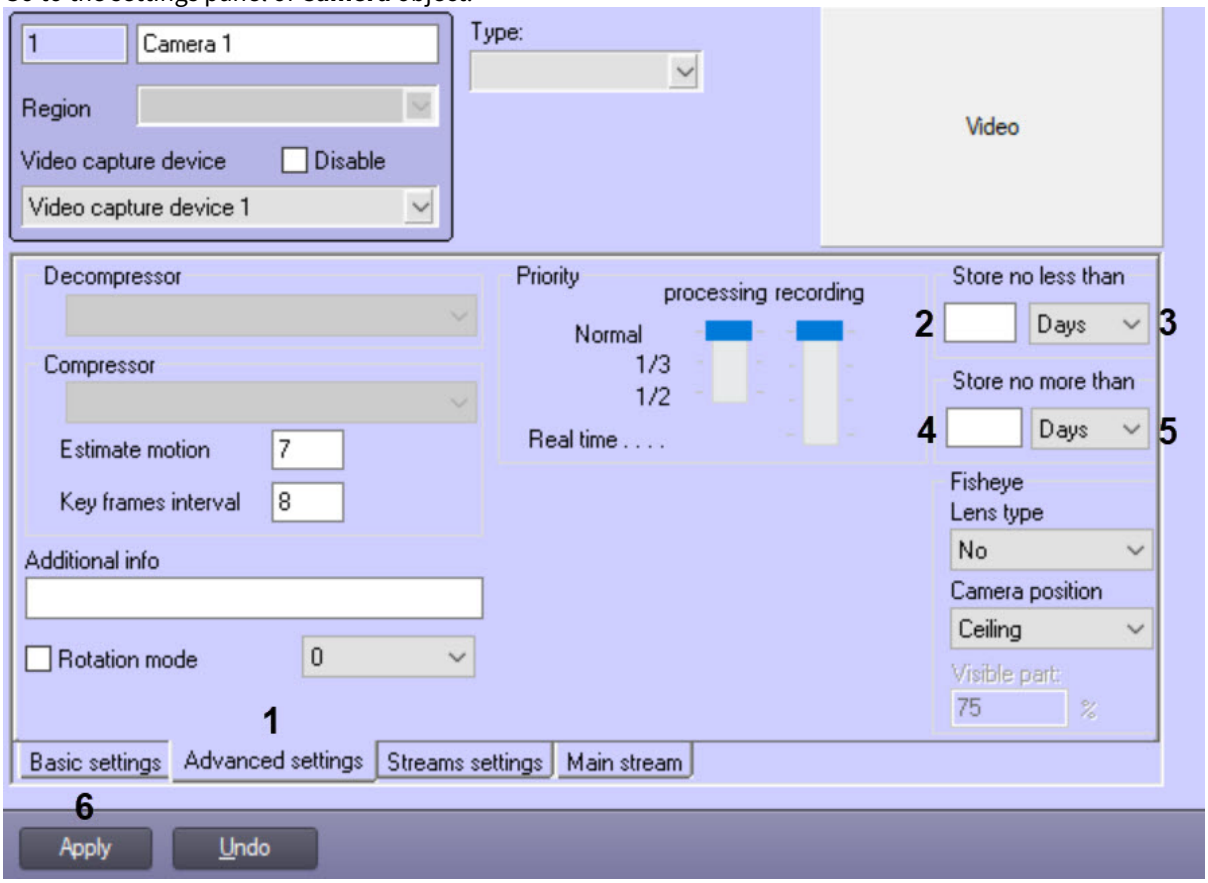
The parameter is to be used carefully – do not change it dramatically downward. For instance, if 1 TB archive is recorded and the archive depth is 360 days and the user sets 10 days value for the **Store no more than** parameter – it will result in one-time deletion of big data that will take a lot of time during which some frames can be skipped.

Note.

The **Store no less than** and **Store no more than** parameters refer to calendar time, e.g. if you set **Store no more than 2 days**, the archive files are deleted 2 days after being created regardless of the number of hours recorded.
Set the FileSystem.MinMaxHoursFromNow registry key to 0 in order to enable time counting from the last archive record timestamp (see Registry keys reference guide).

Configure the video camera archive depth as follows:

1. Go to the settings panel of **Camera** object.



2. Go to the **Advanced settings** tab (1).
3. In the **Store no less than** field specify the time period during which the video and audio archive (in case of synchro recording) is to be kept on the Server (2).
4. In the **Store no less than** dropdown list select the units used to set the time period in the **Store no less than** field: days or hours (3).
5. In the **Store no more than** field specify the time period over which the camera archive is to be kept and at the expiring of which the archive is to be deleted (4).
6. In the **Store no more than** dropdown list select the units used to set the time period in the **Store no more than** field: days or hours (5).
7. Click the **Apply** button (6).

The video camera archive depth is now configured.

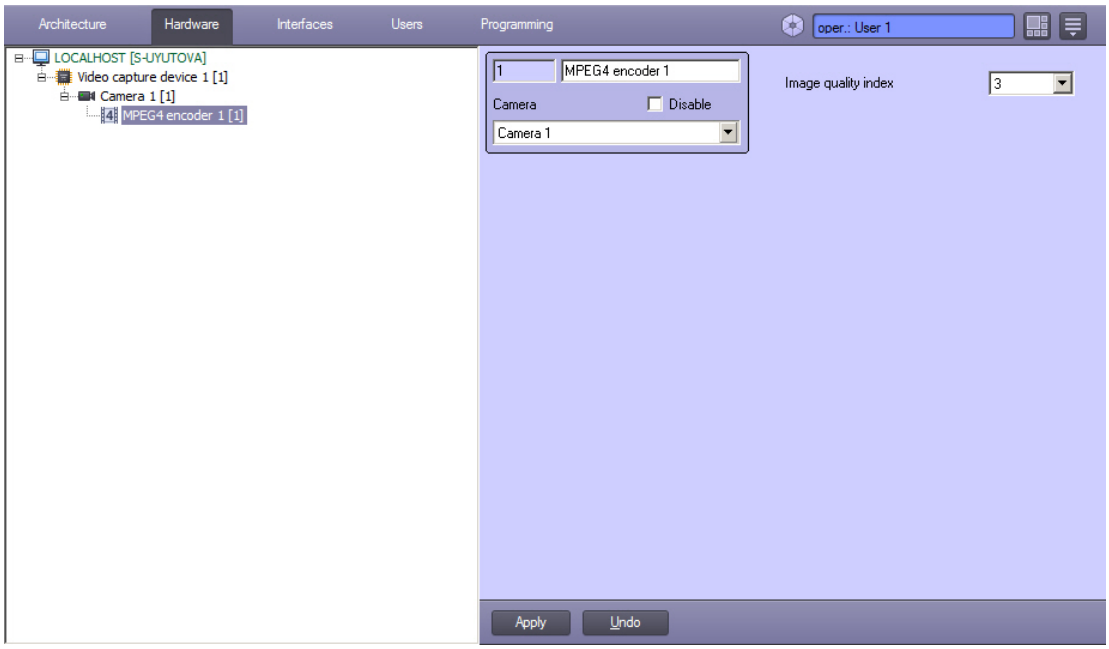
23.3.2.5.14 Video Archive Encryption

Encryption of the *Intellect* archive is performed by the Windows operating system means, namely using BitLocker Drive Encryption technology. Specific configuration on *Intellect* side is not required; just encrypt the disks of the Servers on which the archive is to be stored using BitLocker. The rest of the video archiving configuration is carried out in the same way as described in the sections above (see Configuring video archiving).

23.3.2.5.15 Creating and configuring the MPEG4 Encoder object

The **MPEG4 Encoder** object is intended for recording an archive in MPEG4 format. If the object is not created, then by default the archive is recorded in the same codec in which the video signal is received.

The **MPEG4 Encoder** object is created under the **Camera** object, the video archive of which must be stored in this codec.



Right after the **MPEG4 Encoder** object is created, the current archive fragment is finalized and the new fragment starts to be recorded in the MPEG4 codec.

Setting up the **MPEG4 Encoder** object consists in setting the **Image quality index** parameter: it affects the archive video bit rate and, therefore, the size of the resulting archive file. The larger the index, the higher the image quality and the larger the archive file size. The default value of 3 allows acceptable bit rate for various video resolutions.

See the tables below for the dependence of archive video characteristics on the value of the **Image quality index** parameter.

Codec H264, resolution 1920x1080

Image quality index	Size, Mb	Duration, sec.	Bitrate, kbps.	Quality, %
1	15	60	2048	17%
2	29,7	60	4055	33%
3	44,6	60	6089	50%
4	59,4	60	8110	67%
5	74,2	60	10130	83%
6	89,1	60	12165	100%

Codec H264, resolution 1280x720

Image quality index	Size, Mb	Duration, sec.	Bitrate, kbps.	Quality, %
1	6,68	60	912	23%
2	13,2	60	1802	46%
3	19,9	60	2717	69%
4	26,5	60	3618	91%
5	28,6	60	3904	99%
6	29	60	3959	100%

Codec H264, resolution 640x480

Image quality index	Size, Mb	Duration, sec.	Bitrate, kbps.	Quality, %
1	2,3	60	314	26%
2	4,7	60	641	53%
3	6,9	60	946	78%
4	8,7	60	1190	98%
5	8,8	60	1213	100%
6	8,9	60	1217	100%

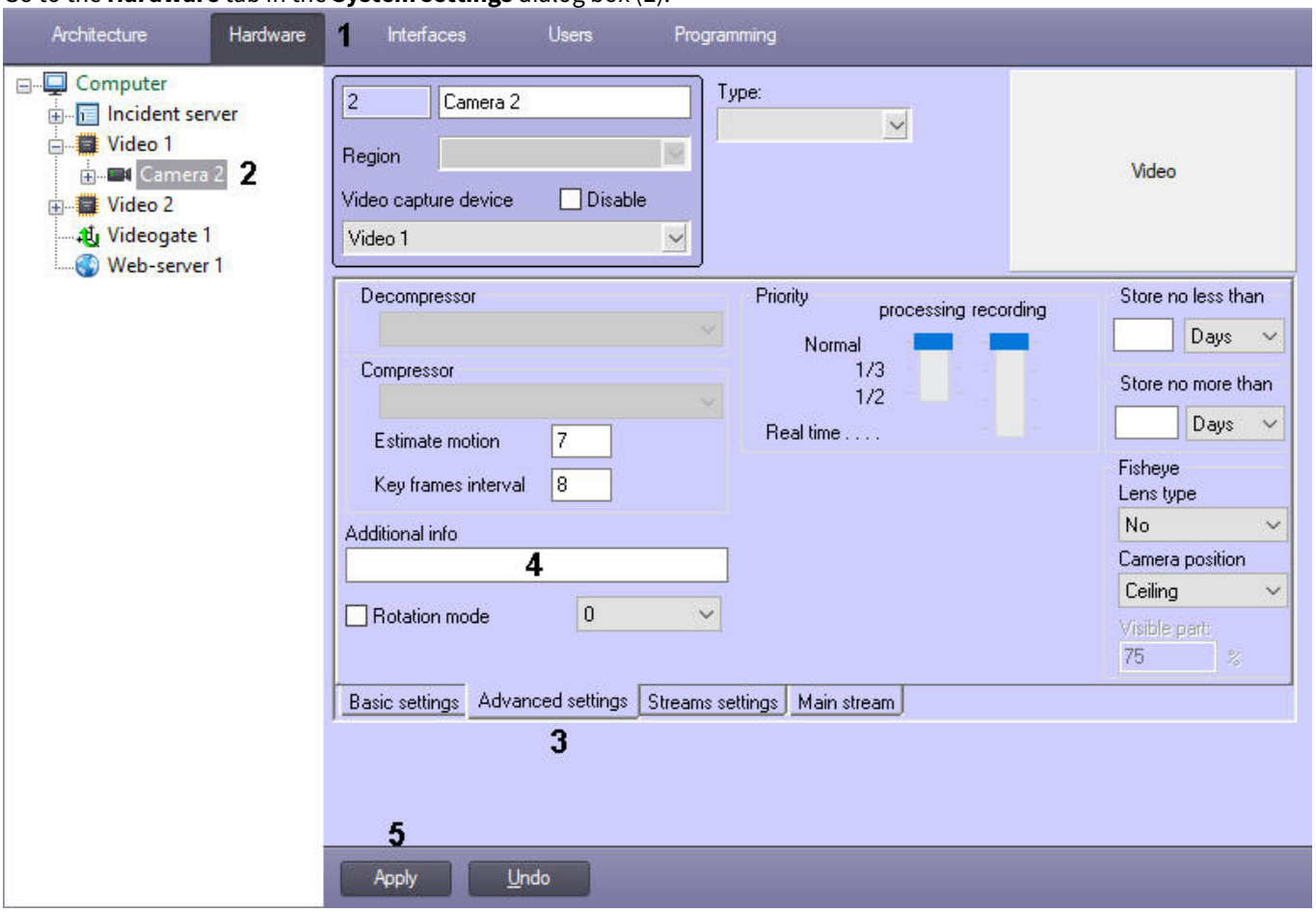
23.3.2.6 Additional information on camera

Additional information on the camera is:

1. Displayed on the video surveillance monitor over the camera name (disabled by default in order to reduce GPU load, see Setting the parameters of the Monitor interface box).
2. Added to the name of export file from interface monitor (AVI, BMP/JPEG) and for frame printing.
3. Displayed in the Event log window in the **Additional info** column.

To set additional information, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).



2. Select the **Camera** object, created before, corresponding to the camera to be adjusted, in the Hardware tab in the objects tree (**2**). The settings panel for the selected object is displayed on the right of the **Hardware** tab.
3. Go to the **Advanced settings** tab on the settings panel of the **Camera** object (**3**).
4. Type in additional information (not more than 100 characters) in the **Additional info** field (**4**).

> **Note**
>
> The color of additional information displayed on the Surveillance monitor changes according to the state of the Camera. For example, if the Camera is recording, the text will be red, otherwise it will be white. Using the **MonitorExtraTextColor** registry key, you can set an unchanging arbitrary color (for details, see Registry keys reference guide).

5. To save the changes, click the **Apply** button (**5**).

Additional information is now set.

> Event control via Event viewer
> Viewing video sequences from surveillance cameras
> Export and print out

23.3.2.7 Configuring video detection tools

23.3.2.7.1 General description of Intellect software detection tools

The following detection tools are available in the *Intellect* software:

1. Main motion detection tool and basic detection tools.
2. Smart video detection tools.

3. Embedded detection tools.
4. Face detection tool.

23.3.2.7.2 Enabling, configuring and disabling basic video detection tools

23.3.2.7.2.1 General information on basic detection tools

Basic video detection tools provide automatic video image analysis to recognize events occurring within the observed scene. Event recognition capabilities depend on the type of detection tool.

In INTELLECT™ software several types of basic detection tools are available:

1. main motion detection tool;
2. motion detection tool;
3. focusing detection tool;
4. video signal stability detection tool;
5. background change detection tool;
6. camera blinding detection tool;
7. camera covering detection tool;
8. infrared detection tool.

The following basic detection tools may be applied as sabotage detections: focusing, background change, camera blinding and/or camera covering.

By default, INTELLECT™ software uses solely the main motion detection tool, which detects the video surveillance camera alarms. The rest of detection tools are optionally activated in the course of INTELLECT™ software administration.

To configure basic detection tools, set up the program algorithms for them, enable auto recording on detection tool alarm option etc.

To activate Main detection tool, arm the corresponding camera (see Camera arming and disarming section of the Operator's Guide). To activate basic detection tools, arm the corresponding detection zone (see Use of video detection tools section of the Operator's Guide).

Important!

The basic detection tools process key frames only (for codecs with interframe compression). If detection tool configuration as described above does not result in the proper detection tool operation and the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video). For the MJPEG codec, the number of frames per second processed by the main motion detector is set using the DetectionFps registry key (see Registry Keys Reference Guide). This registry key also affects grooming for the H264 codec (key frames only).

Requirements to video parameters while working with detection tools and Tracker
Camera arming and disarming
Use of basic video detection tools

23.3.2.7.2.2 Requirements to video parameters while working with detection tools and Tracker

Requirements for the correct operation of video analytics are given in the table:

Camera	• Resolution:
	  • at least 640x480 but no more than 800x600 pixels for smart video detection tools
	  • at least 320x240 pixels for other video detection tools
	• FPS:
	  • at least 6 frames per second for smart video detection tools
	  • at least 1 frame per second for other video detection tools

	• Video analytics works with both black-and-white and color images • Camera shaking must not cause image shifting of more than 1% of the frame size
Lighting	• Moderate lighting. Insufficient or excessive lighting (night or bright sunlight) may impact the quality of video analytics • No abrupt changes in lighting
Scene and camera angle	• Moving objects are visually separable from each other • The background is mostly static and doesn't change abruptly. • Moving objects are minimally obscured by static objects in the scene (columns, industrial products, and so on) • Reflective surfaces and harsh shadows from moving objects can affect the quality of analytics • Long single-color objects may not be tracked properly
Object images for smart video detection tools	• An object must be visible on the image • There is no noise on the video image and there are no artifacts caused by the compression algorithm • The width and height of objects in the video should not be less than 1% of the frame size (at resolutions not less than 1920x1080 pixels) or 15 pixels (at lower resolutions) • The width and height of objects in the video should not be more than 75% of the frame size • It is recommended that the linear measurements of objects in the frame do not exceed 75% of the frame size • The speed of objects in the frame must be at least 1 pixel per second • The object is to be visible at not less than 8 frames • Within two adjacent frames the object cannot move in the movement direction for the distance that is longer than its size • Quantity of simultaneously tracked objects on a frame—no more than 25

23.3.2.7.2.3 Procedure for enabling and configuring basic detection tools

Generally the procedure of configuring basic detection tools includes the following steps (except for the main motion detection tool (camera alarm detection tool), configuration procedure of which is described in Configuring Main motion detection tool section):

1. Connecting basic detection tools. It is performed for each camera independently.
2. Setting detection tools parameters.
3. Testing video detection tool operation by using the video monitor.
4. If detection tool operates improperly, go back to step 2, change the settings and test it again.
5. If detection tool operates properly, the setup is completed.

23.3.2.7.2.4 Connecting basic detection tools

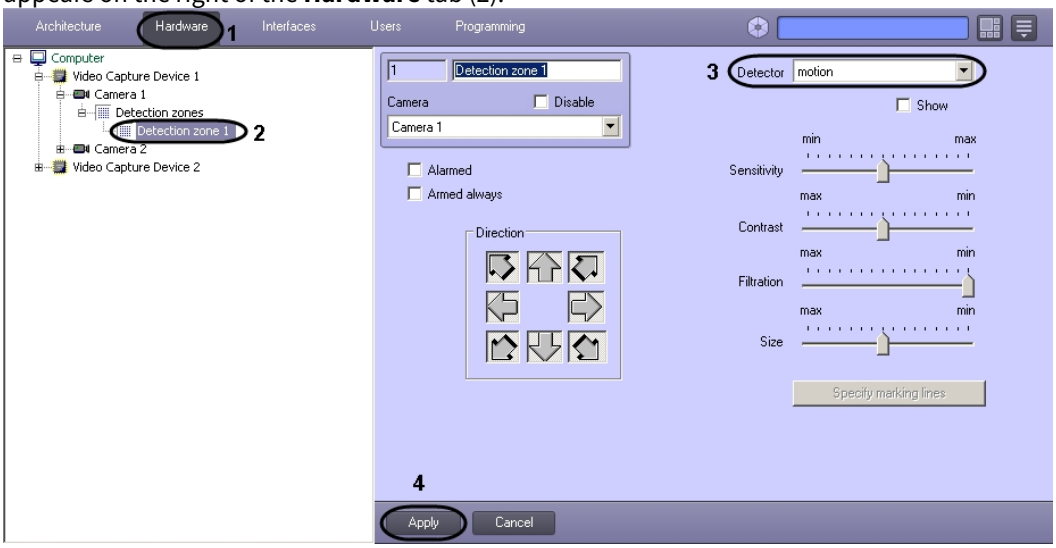
The list of video detection tools is created individually for each camera.

Initially only a Main motion detection tool is registered for each camera. No other detectors are registered by default.

To connect basic video detection tools (except the main motion detection tool), do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Camera** object, corresponding to the camera to process video from which a detection tool is connected and configured, in the objects tree of the **Hardware** tab.

3. Create the **Detection zone** object on the base of the **Camera** object. The settings panel for the **Detection zone** object appears on the right of the **Hardware** tab (2).



4. In the **Detector** list, select the required type of detection tool.
   When a detection tool is connected, the controls for configuring the selected detection tool are activated. Controls that are not required are disabled. With different types of detectors, the same graphics object may correspond to different settings.
   The setup procedure depends on the type of detection tool. Setup sequences for different types of detection tools are described in the relevant sections.
5. Click the **Apply** button (4).

A detection tool is now connected.

Requirements to video parameters while working with detection tools and Tracker
Camera arming and disarming
Use of basic video detection tools

23.3.2.7.2.5 Configuring basic detection tools

Configuring Main motion detection tool
The main motion detection tool is used to detect motion on the protected facility and to generate the system alarm events when the relevant camera is armed.

Main motion detection tool configuration is performed for each camera independently.

In most cases the default settings for Main motion detection tool are sufficient for it to function properly.

To configure Main motion detection tool, do the following:

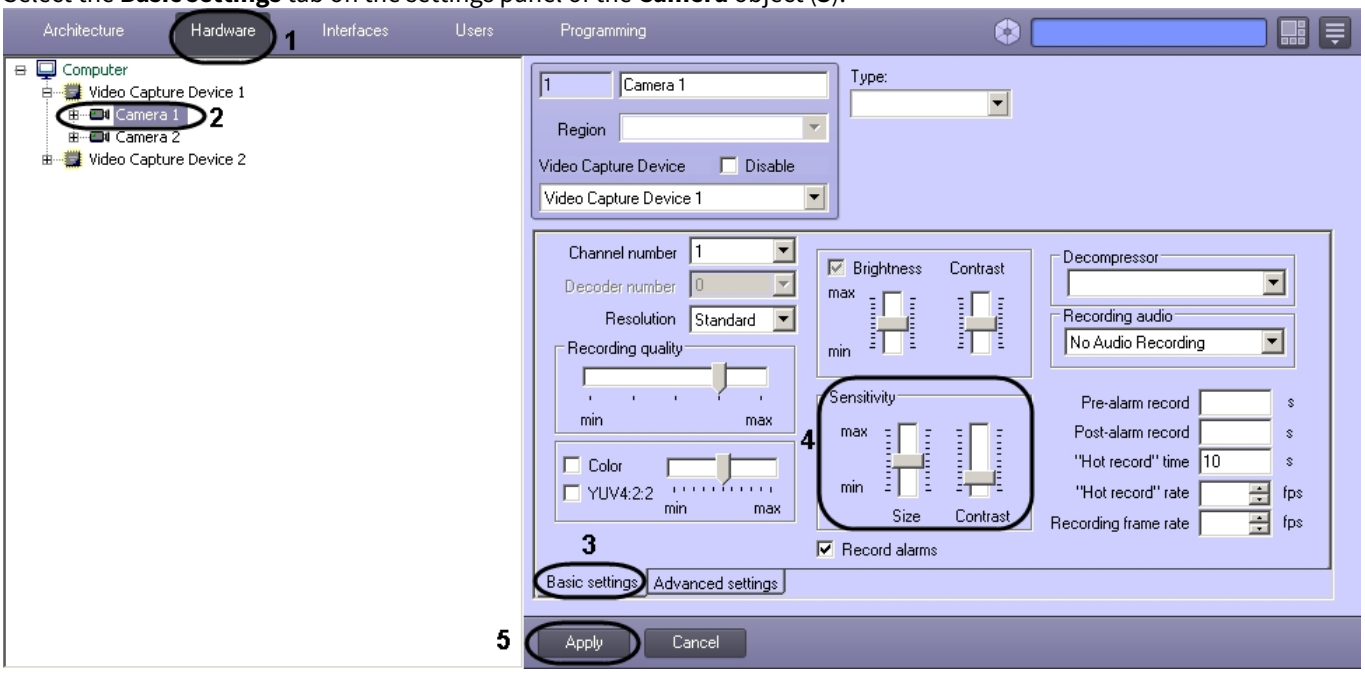
1. Display the video surveillance monitor on the screen and check if INTELLECT™ properly registers alarms on camera.
   If registration is proper, then additional settings may be skipped.

   Note

   If alarms on camera are registered improperly (for example, a detection tool is triggered by artificial or natural video signal noise (rain, snow, etc), a detection tool does not detect small object motion and high speed motion), a Main motion detection tool is to be configured. The proper setup of a Main motion detection tool allows significantly lowering the probability of unsatisfactory camera alarm detection.

2. Go to the **Hardware** tab in the **System settings** dialog box (**1**).
3. Select the **Camera** object corresponding to the camera on which a detection tool is configured, in the objects tree of the **Hardware** tab (**2**). The settings panel for the selected object appears on the right of the **Hardware** tab.

4. Select the **Basic settings** tab on the settings panel of the **Camera** object (**3**).



5. Set the **Size** value by moving the slider of the same name (**4**). The value of this setting corresponds to the part of the total frame square, occupied by the smallest detected object. When an object bigger than the preset one moves, the motion detection tool switches to the alarm status.
   The best valueof the **Size** parameter is defined by testing the triggering of a detection tool. With low values of the **Size** parameter, triggering by noise (including rain, snow) is more probable. With high values of the **Size** parameter, triggering by object motion is less probable.
   The value that is slightly lower than the average size of the moving objects in the frame is recommended to be set to the **Size** parameter. If a detection tool triggers upon video signal noise, then it is necessary to change the **Contrast** parameter.
6. Set the **Contrast** value by moving the slider of the same name (**4**). The value of this setting corresponds to the contrast of detected object.
   The best valueof the **Contrast** parameter is defined by testing the triggering of a detection tool. With low values of the **Contrast** parameter, triggering by moving objects, color spectrum of which is very similar to that of the background, is more probable. In most cases the default **Contrast** setting (the average value) is sufficient.
7. Click the **Apply** button (**5**).

Main motion detection tool is now configured.

Configuring Motion detection tool
The Motion detection tool discovers moving objects in the zone under control. When a moving object is detected, it is dynamically framed. The motion is detected by calculating the gradient between sequential frames to time.

Note.

The performance of this detector is much worse than performance of VMDA detector (see Motion in the Area detection tool configuration). When better recognition quality is required, VMDA detector is recommended to be used.

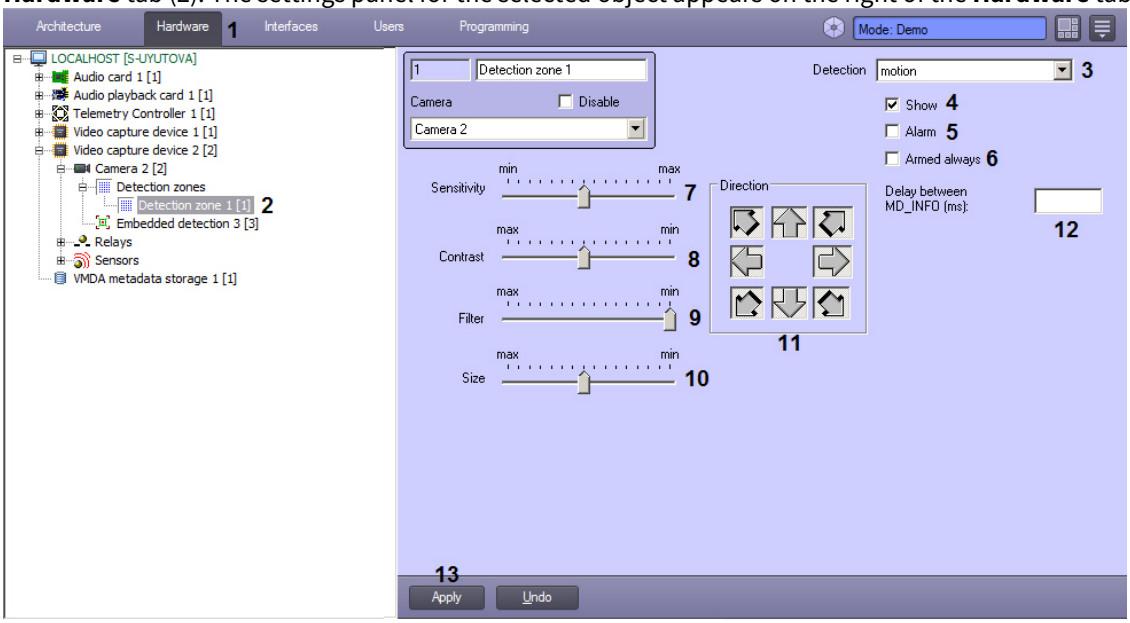
Note.

The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Motion detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).

2. Select the **Detection zone** object corresponding to the detection tool that is to be configured, in the objects tree of the **Hardware** tab (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the motion detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the motion detection tool registered earlier (3).
4. By default, the detected moving object is not dynamically framed. If the moving object need to be framed, set the **Show** checkbox (4).
5. To enable the auto recording option on a motion detection tool alarm and generate alarm for the corresponding camera, set the **Alarmed** checkbox (5).

> **Note.**
>
> If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed when the detection tool triggers.

> **Note.**
>
> If the **Alarmed** option is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

6. To disable disarming of the motion detection tool by any user (irrespectively of his rights), set the **Armed** always checkbox (6).

> **Note.**
>
> When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

7. Set the value of the **Sensitivity** parameter by moving the the slider of the same name. This setting corresponds to the minimum value of the average brightness of the moving object, with which the detection tool triggers by its motion only, and not by noise in a video signal (including rain, snow, etc.) (7).
   The best value of the **Sensitivity** parameter is defined by testing false triggering of detection tools. With low values of the **Sensitivity** parameter, false triggering by noise is more probable. With high values of the **Sensitivity** parameter, triggering by object motion is less probable.
   Set the value of the **Sensitivity** parameter after setting the **Size**, **Filtration** and **Contrast** parameters. It is recommended to select the value of the **Sensitivity** parameter that will exclude false triggering by noise.
8. Set the value of the **Contrast** parameter by moving the slider of the same name. This setting corresponds to the contrast of the detected object (8).

The best value of the **Contrast** parameter is defined by testing the triggering of detection tools. With low values of the **Contrast** parameter, triggering by moving objects, color spectrum of which is very similar to that of the background, is less probable. With high values of the **Contrast** parameter, false triggering of detection tools by noise is more probable. In most cases the default setting (the average value) is sufficient.

9. Set the value of the **Filtration** parameter by moving the the the slider of the same name (9). The value of this parameter corresponds to the threshold of color processing of objects, at which the detector should trigger.
   The best value of the **Filtration** parameter is defined by testing the triggering of detection tools. With low values of the **Filtration** parameter, triggering by noise (including rain and snow) is more probable. With high values of the **Filtration** parameter, triggering by object motion is less probable. If a detection tool triggers upon noise, then it is necessary to change the value of the **Sensitivity** parameter.
10. Set the value of the **Size** parameter by moving the slider of the same name (10). The value of this parameter corresponds to the minimum linear dimensions of the detection object as a percentage of the dimensions of the video. When an object that is bigger than the preset one moves, the motion detection tool switches to the alarm status.
    The best value of the **Size** parameter is defined by testing the triggering of detection tools. With low values of the **Size** parameter, triggering by noise (including rain and snow) is more probable. With high values of the **Size** parameter, triggering by object motion is less probable.
    It is recommended to set the value of the **Size** parameter that is slightly lower than the average size of objects moving in the frame. If a detection tool triggers upon video signal noise, then change the value of the **Sensitivity** parameter.
11. By default, a detection tool recognizes motion in any direction. To disable detection of motion in certain directions, click the relevant buttons in the **Direction** group. A detection tool detects motion in the directions of the pressed arrow buttons and does not detect it in the directions of pulled arrows (11).
12. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (12). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
13. Click the **Apply** button (13).

Motion detection tool is now configured.

Configuring Focus detection tool

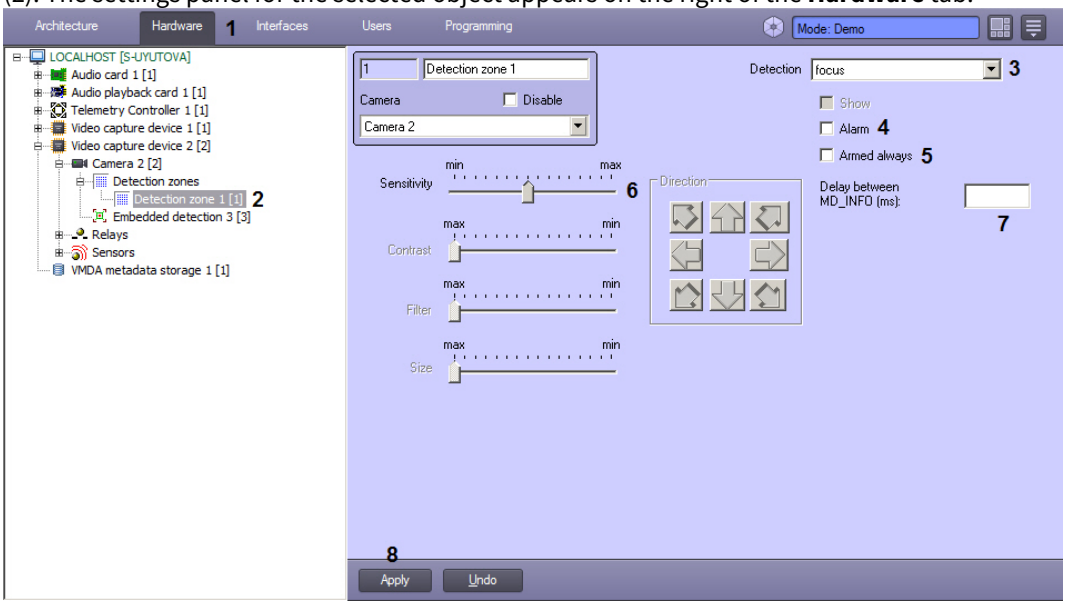
This detection tool notifies the Operator about camera tampering, resulting in focus loss or camera sensitivity degradation. The high frequency component of the video signal is analyzed to check for presence of distinct contours.

> **Note.**
>
> The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Focus detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).

2. Select the **Detection zone** object corresponding to the required detection tool, on the **Hardware** tab in the objects tree (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the focus detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the focusing detection tool registered earlier (3).
4. To enable the auto recording option on a focus detection tool alarm and generate alarm for the corresponding camera, set the **Alarmed** checkbox (4).

> **Note.**
>
> If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed after detection tool triggers.

> **Note.**
>
> If the **Alarmed** option is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

5. To disable disarming of the focus detection tool by any user (irrespectively of his rights), set the **Armed always** checkbox (5).

> **Note.**
>
> When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

6. Set the value of the **Sensitivity** parameter by moving the the slider of the same name (6). This setting corresponds to the minimum drop in image sharpness (that is the difference between the average number of contours and the number of contours in the current frame), with which the detection tool is to trigger.
   The best value of the **Sensitivity** parameter is defined by testing the triggering of detection tools. In most cases the default setting is sufficient.
7. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (7). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
8. Click the **Apply** button (8).

Focus detection tool is now configured.

Configuring Stability detection tool

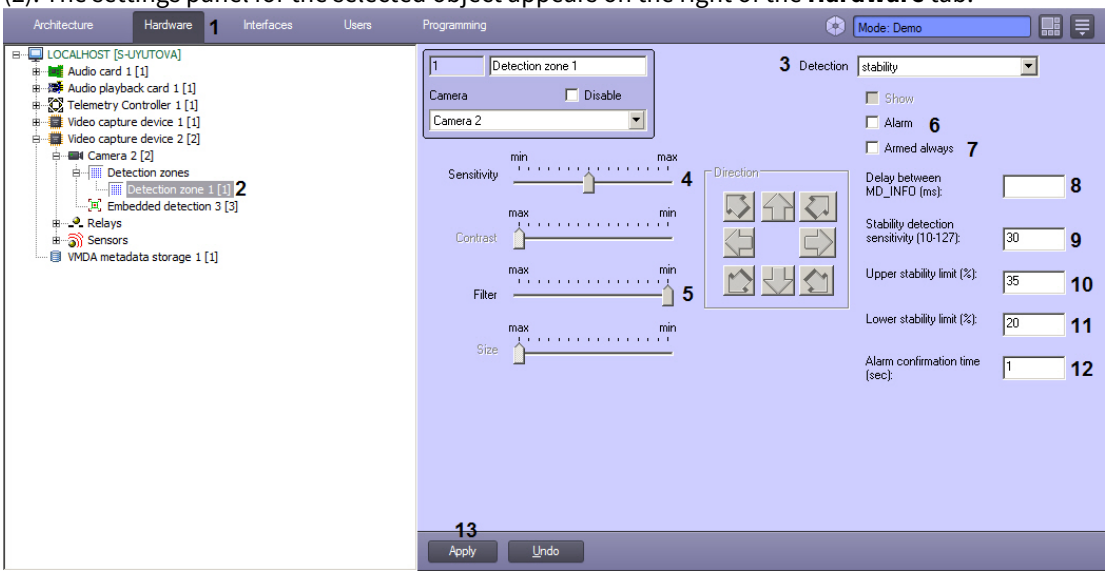
Stability detection tool reacts to any change in video camera position. Operation of the detection tool is based on the comparison between parameters of each frame and the average parameters (so called "background model"). Every frame is stabilized befor processing by correcting to the backgroung by least squares method. This allows eliminating alarms raising from camera blinding when the day/night mode is being enabled.

Note.

The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Stability detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Detection zone** object corresponding to the required detection tool, on the **Hardware** tab in the objects tree (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the stability detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the focusing detection tool registered earlier (3).
4. Set the value of the **Sensitivity** parameter by moving the the slider of the same name (4). This setting corresponds to the minimum drop in image sharpness (that is the difference between the average number of outlines and the number of outlines in the current frame), with which the detection tool is to trigger.
   The best value of the **Sensitivity** parameter is defined by testing the triggering of detection tools. In most cases the default setting is sufficient.
5. Set the value of the **Filtration** parameter by moving the the slider of the same name (5). The value of this parameter corresponds to the contrast threshold of the detected object.
   Decreasing the **Filter** parameter means that it is less probable that detection tool will trigger at objects the color gamut of which is close to the background color gamut. Increasing the **Filter** parameter means that it is more probable that the detection will trigger at the video signal noise. The best value of the **Filter** parameter is identified by testing the detection tool for triggering under the required conditions. In most cases, the default value is enough.
6. To enable the auto recording option on a stability detection tool alarm and generate alarm for the corresponding camera, set the **Alarm** checkbox (6).

   Note.

   If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed after detection tool triggers.

   Note.

If the **Alarmed** option is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

7. To disable disarming of the stability detection tool by any user (irrespectively of his rights), set the **Armed always** checkbox (7).

   Note.

   When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

8. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (8). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
9. In the **Stability detection sensitivity (10-127)** field, enter the threshold of the absolute difference between the brightness of the pixel in the current frame (taking into account the stabilization of brightness) and the background in the range of 10 to 127 (9). This parameter determines the percentage of pixels in the current stabilized frame differing from the background by more than the specified sensitivity value. The higher the value, the stronger the pixels of the frame should differ from the pixels of the background in order for the frame to be considered unstable (i.e. the scene should change in brightness).
10. In the **Upper stability limit (%)** field, enter the maximum permissible percentage of the stabilized frame pixels that differ from the background by more than the value in the **Stability detection sensitivity** (10). When this percerntage is ecxeeded, the alarm state starts to be verified. If the threshold continues to be exceeded during the **Alarm confirmation time**, the alarm is considered confirmed.
11. In the **Lower stability limit (%)** field, enter the maximum permissible percentage of the stabilized frame pixels that differ from the background by more than the value in the **Stability detection sensitivity** (11). The frame is considered stable until this threshold is not reached. The stable frame may be used for the background model. As soon as the lower stability limit is exceeded, the frame ceases to be used for the background model so that unstable frames do not interfere with the background model. The higher the value, the greater the number of pixels should differ from the background by the sensitivity value so that the frame to be considered unstable (i.e., the more global the change in the scene should be). The smaller the value, the more local the scene change may be for the frame to be considered unstable.
12. In the **Alarm confirmation time (sec.)** field, enter the time period in seconds during which the **Upper stability limit** must be exceeded to generate an alarm (12). The same time will be necessary to confirm the frame stabilization after the alarm is issued and before the background model begins to be accumulated again.
13. Click the **Apply** button (13).

Stability detection tool is now configured.

Configuring Background change detection tool

This detection tool reacts to changes in the scene background due to physical tampering of the CCTV camera. Operation of the detection tool is based on calculation of the standard deviation of integral frame intensity from its mean value.

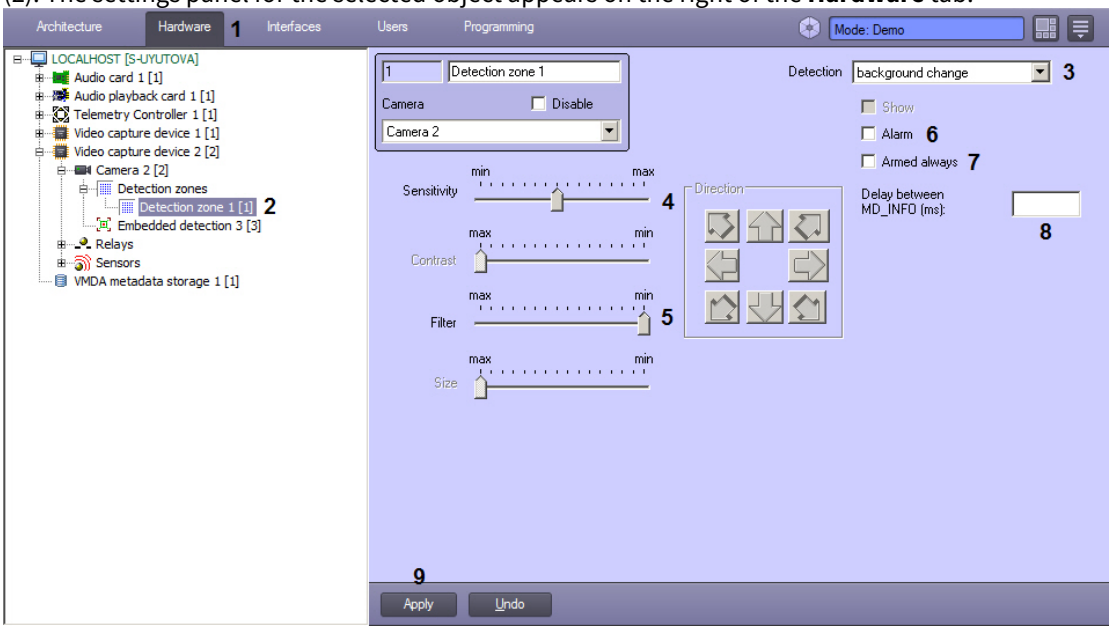
Note.

The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Background change detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).

2. Select the **Detection zone** object corresponding to the required detection tool, on the Hardware tab in the objects tree (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the background change detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the focusing detection tool registered earlier (3).
4. Set the value of the **Sensitivity** parameter by moving the the slider of the same name (4). This setting defines the deviation of the integral frame brightness from its mean value at which the detection tool is to trigger.
   The best value of the **Sensitivity** parameter is defined by testing the triggering of detection tools. In most cases the default setting is sufficient.
5. Set the value of the **Filtration** parameter by moving the slider of the same name (5). The value of this parameter corresponds to the contrast threshold of the detected object.
   Decreasing the **Filter** parameter means that it is less probable that detection tool will trigger at objects the color gamut of which is close to the background color gamut. Increasing the **Filter** parameter means that it is more probable that the detection will trigger at the video signal noise. The best value of the **Filter** parameter is identified by testing the detection tool for triggering under the required conditions. In most cases, the default value is enough.
6. To enable the auto recording option on a background change detection tool alarm and generate alarm for the corresponding camera, set the **Alarmed** checkbox (6).

> **Note.**
>
> If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed after detection tool triggers.

> **Note.**
>
> If the **Alarmed** option is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

7. To disable disarming of the background change detection tool by any user (irrespectively of his rights), set the **Armed always** checkbox (7).

> **Note.**
>
> When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

8. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (8). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
9. Click the **Apply** button (9).

Background change detection tool is now configured.

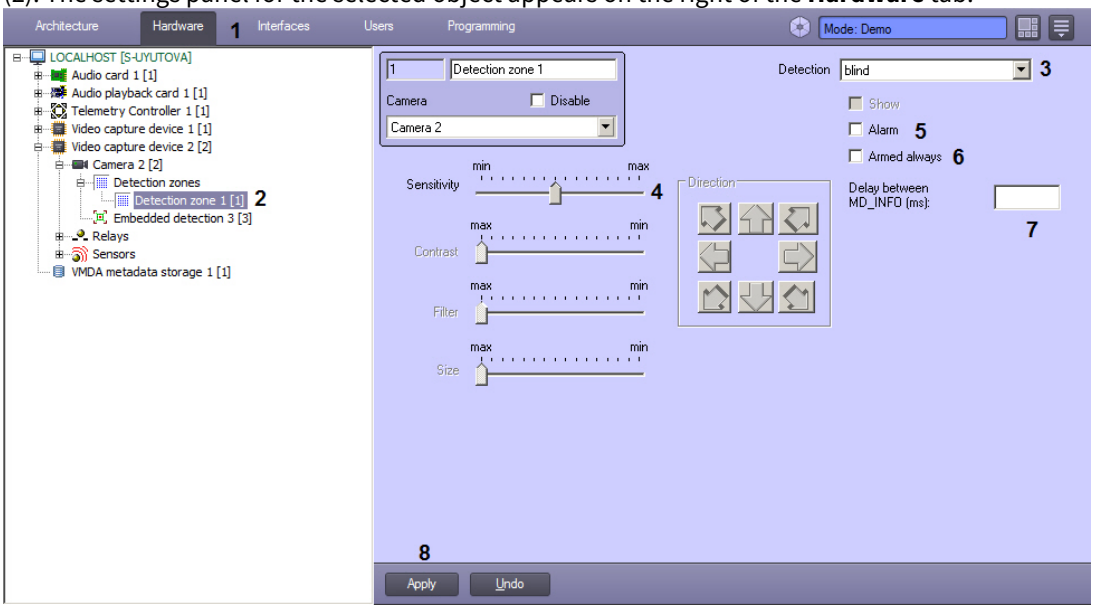
Configuring Blind detection tool
Blind detection tool detects camera blinding. Operation of the detection tool is based on comparison of the bitmap histogram of the current frame to that of the reference blinding frame (white).

Note.

The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Blind detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Detection zone** object corresponding to the required detection tool, on the **Hardware** tab in the objects tree (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the blind detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the focusing detection tool registered earlier (3).
4. Set the value of the **Sensitivity** parameter by moving the the slider of the same name (4). This setting defines the image blinding rate, expressed in the difference between the brightness histogram median position of the current and reference frames with which the detection tool is to trigger.
   The best value of the **Sensitivity** parameter is defined by testing the triggering of detection tools. In most cases, the default setting is sufficient.
5. To enable the auto recording option on a blind detection tool alarm and generate alarm for the corresponding camera, set the **Alarmed** checkbox (5).

Note.

If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed after detection tool triggers.

Note.

If the **Alarmed** option is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

6. To disable disarming of the blind detection tool by any user (irrespectively of his rights), set the **Armed always** checkbox (6).

Note.

When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

7. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (7). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
8. Click the **Apply** button (8).

Blind detection tool is now configured.

Configuring Cover detection tool

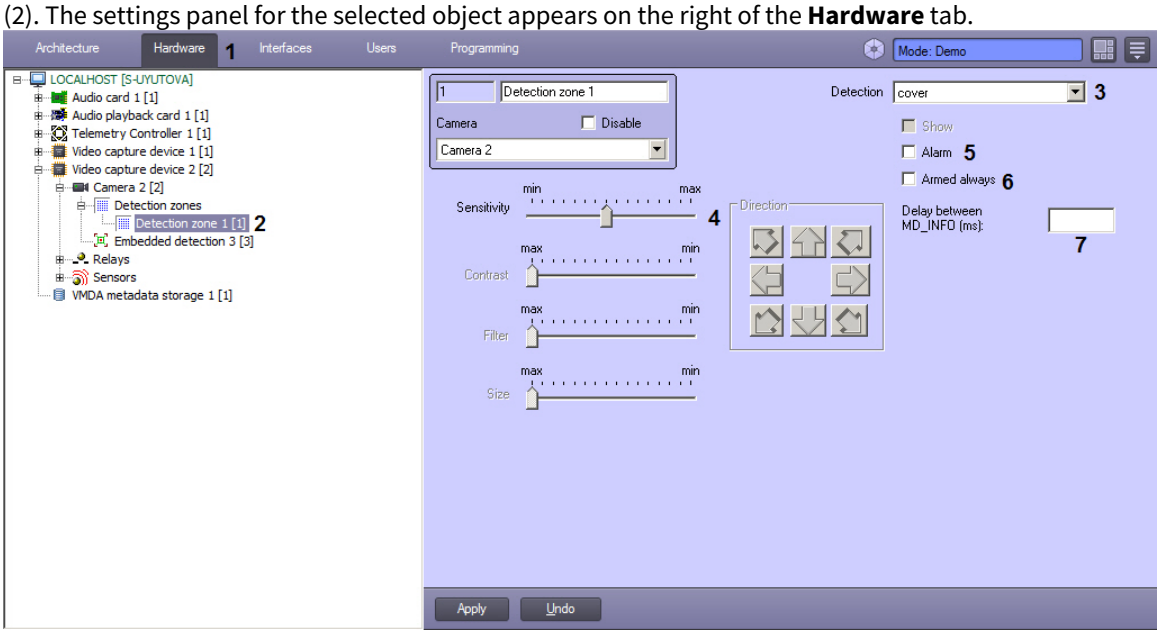
Cover detection tool detects camera covering. Operation of the detection tool is based on analysis of the broadening of the frame histogram, relative to the histogram median of the reference covering frame (grey).

Note.

The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Cover detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).
2. Select the **Detection zone** object corresponding to the required detection tool, on the **Hardware** tab in the objects tree (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the cover detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the focusing detection tool registered earlier (3).
4. Set the value of the **Sensitivity** parameter by moving the the slider of the same name (4). This setting corresponds to the contraction rate of the frame brightness histogram, i.e. estimation of grey filling ratio with which the detection tool is to trigger.

The best value of the **Sensitivity** parameter is defined by testing the triggering of detection tools. In most cases the default setting is sufficient.

5. To enable the auto recording option on a cover detection tool alarm and generate alarm for the corresponding camera, set the **Alarmed** checkbox (5).

> **Note.**
>
> If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed after detection tool triggers.

> **Note.**
>
> If the **Alarmed option** is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

6. To disable disarming of the cover detection tool by any user (irrespectively of his rights), set the **Armed always** checkbox (6).

> **Note.**
>
> When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

7. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (7). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
8. Click the **Apply** button (8).

Cover detection tool is now configured.

Configuring Infrared detection tool

Infrared detection tool is used for thermal imagers – infrared cameras. Infrared detection tool detects moving objects within the controlled scene. Detected moving objects are dynamically framed. The motion is detected by calculating gradients between consequent frames.

> **Note.**
>
> The thermal imager is a device, that allows both day and night, to control the situation in any kind of weather, functioning in the thermal, invisible spectral range. It enables to see things that are invisible for night vision devices and TV cameras. Heavy snow, fog, the absence of lighting at night strongly reduce the effectiveness of standard video surveillance facilities. The thermal imager, unlike the common highly sensitive camera or infrared camera, functions properly without regard to the weather and illumination: moonless night, heavy clouds, mist, smoke or, vice versa, very bright sunlight do not affect its functioning. The sensitive element of the thermal imager operates in the invisible spectral range and in fact is not affected by the environmental changes. The thermal imager provides instant temperature measurement at thousands of object points.

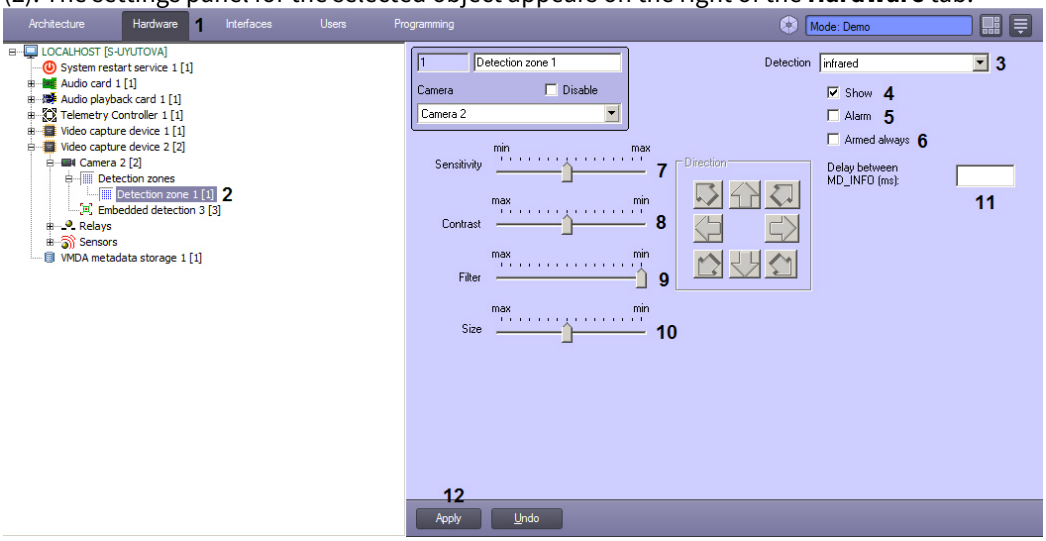
> **Note.**
>
> The video signal from the thermal imager is treated as a standard video signal, but the size of a detected object may be very small (as small as 3 pixels), so the detection tool needs fine tuning.

> **Note.**

The detection is performed by key frames. If detection tool configuration process described below does not result in a proper detection quality, i.e. the detection tool does not trigger or triggers with a delay, it is recommended to reduce key frame rate for video camera (see Configuring video compression) or video analytics stream if the camera has multiple streams (see Configuration of multistream video).

To configure Infrared detection tool, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1)
2. Select the **Detection zone** object corresponding to the required detection tool, on the **Hardware** tab in the objects tree (2). The settings panel for the selected object appears on the right of the **Hardware** tab.



3. Enable the infrared detection tool (see the Enabling, configuring and disabling basic video detection tools section) or select the infrared detection tool registered earlier (3).
4. By default, detected moving objects are dynamically framed. If a moving object is not to be framed, set the **Show** checkbox unchecked (4).
5. To enable the auto recording option on an infrared detection tool alarm and generate alarm for the corresponding camera, set the **Alarmed** checkbox (5).

> **Note.**
>
> If the **Recording alarms** option is disabled in the **Camera** object settings, then no video recording is performed after detection tool triggers.

> **Note.**
>
> If the **Alarmed** option is disabled in the detection tool settings, then detection tool arming is ineffective, though the line with the name of this detection tool is highlighted with a yellow square in the feature menu of the video surveillance window. This means that detection tool alarms are displayed in the Event Viewer but not shown in Video Surveillance Monitor or Map in any way.

6. To disable disarming of the abandoned objects detection tool by any user (irrespectively of his rights), set the **Armed always** checkbox (6).

> **Note.**
>
> When the **Armed always** checkbox is set, the line with with the name of the detection tool is not displayed in the feature menu of the video surveillance window.

7. Set the **Sensitivity** slider to the position corresponding to the minimal value of the average brightness of the moving object which triggers the detection tool by its motion (7).

> **Note.**

The best value of the **Sensitivity** parameter is defined by testing the false triggering of detection tools. With low values of the **Sensitivity** parameter, false triggering of detection tools by thermal noise is more probable. With high values of the **Sensitivity** parameter, detection of motion in the frame is less probable.
Set the **Sensitivity** parameter when the **Size**, **Filtration** and **Contrast** parameters are set. It is recommended to set the value of the **Sensitivity** parameter which does not lead to false triggering by noise in video signal.

8. Set the **Contrast** slider to the position corresponding to the minimal value of the contrast which triggers the detection tool by its motion (8).

   Note.

   The best value of the **Contrast** parameter is defined by testing the triggering of detection tools. With low values of the **Contrast** parameter the detection tool triggering by motion of objects colors of which are close to the color of the background is less probable. With high values of the **Contrast** parameter triggering of detection tools by noise in a video signal is more probable.
   In most cases, the default setting (mean value) is sufficient.

9. Set the **Filter** slider to the position corresponding to the minimum color threshold of the detected object at which the detector will trigger (9).

   Note.

   The best value of the **Filtration** parameter is defined by testing the triggering of detection tools. With low values of the **Filtration** parameter triggering of detection tools by noise (including snow and rain) in a video signal is more probable. With high values of the **Filtration** parameter triggering of detection tools by motion in the frame is less probable. If a detection tool triggers upon noise in a video signal, then change the value of the **Sensitivity** parameter.

10. Set the **Size** slider to the position corresponding to minimal size of the object, which triggers the detection tool (10). The size of the object is expressed in fractions relative to the size of the frame. When there is motion of the object which size exceeds the given value, motion detection tool switches to the alarm status.

    Note.

    The best value of the Size parameter is defined by testing the triggering of detection tools. With low values of the **Size** parameter triggering of detection tools by noise (including snow and rain) in a video signal is more probable. With high values of the **Size** parameter triggering of detection tools by motion in the frame is less probable.
    It is recommended to set the value to the **Size** parameter that is slightly lower than the mean size of objects moving in the frame. It is recommended to set the value of the **Size** parameter that is a little less than the mean size of objects moving in the frame. If a detection tool triggers upon noise in a video signal, then change the value of the **Sensitivity** parameter.

11. In the **Delay between MD_INFO (ms)** field, enter the time period in milliseconds to pass between MD_INFO events (11). This parameter may be set to avoid overloading the Event Viewer with excessive amount of the events that may occur when the MD_INFO event of the CAM_ZONE object is enabled in .ddi file – see The Events tab.
12. Click the **Apply** button (12).

Infrared detection tool is now configured.

23.3.2.7.3 Configuring smart video detection tools

23.3.2.7.3.1 General information on forensic search

The forensic search in the archive is the search for video records in the archive using the video image metadata. The forensic search of video recordings in the archive is performed by the parameters of an object that appeared in the video camera field of view (FOV), e.g. its direction of movement.

Note.

Since the metadata is recorded to the VMDA metadata storage at the same time as the archive is being recorded, the forensic search in the archive imported from edge storage can not be performed. The process of the archive importing from edge storage is described in the Configuring the access to the archive in edge storage section.

Such criteria as **Line crossing** and **Motion in the area**, which are are available in the video surveillance window, are used for the forensic search. For more information about these search criteria, see Search by line crossing and Search by motion in the area.

To perform the forensic search in *Intellect*, it is necessary to create and configure the following objects:

1. The **VMDA metadata storage** (see Creating and configuring VMDA metadata storage);
2. The **Tracker** (see Creating and configuring the Tracker object).
3. Optional: the **Neurotracker** object being part of the *Detector Pack* subsystem for forensic search by metadata received from the *Neurotracker*. See the *Detector Pack. User Guide* in AxxonSoft documentation repository for details on configuration and operation of this module.

One VMDA metadata storage can be used with several Intellect Servers with Trackers. However, this depends on resource capabilities available on metadata storage Server. Please refer to AxxonSoft Platform Calculator for more specific calculation of Server quantity.

It is possible to create the VMDA detection tools on the basis of the **Tracker** object (see Creating and configuring the VMDA detection). If the VMDA detection tools are configured, their triggering can initiate the video recording to the archive. When recording is enabled, the **Tracker** object records all trajectories of detected objects, regardless of whether the VMDA detection tools are created on its basis or not.

The **Tracker** object and the **VMDA detection tools** also allow extended object classification and object classification using the neural filters. In the extended object classification, the following object types are supported:

- a human;
- a group of humans (with a possibility to count number of people in a group);
- a vehicle;
- noise;
- an object carried into the area;
- an object carried out of the area;
- other.

Configuration and use of this classification method is performed using the scripts and registry keys. For details, see the CAM_VMDA_DETECTOR VMDA detection section of the *Programming Guide*.

The use of neural filters allows to classify any types of objects and cut off false alarms of detectors more accurately. Neural filters are configured individually for each use case (for details, see Configuring the neural filter).

Requirements to video parameters while working with detection tools and Tracker
Video requirements to be met for abandoned object detection tool of the Tracker object operation
Requirements for video parameters to perform the forensic search in the archive
Define required disk space (VMDA metadata storage)
Search by line crossing
Search by motion in the area
Search by colour

23.3.2.7.3.2 Requirements for video parameters to perform the forensic search in the archive

Video parameters are to be met the same requirements as while detection working when the forensic search in the archive is used (see the Requirements to video parameters while working with detection tools and Tracker section).

Also, there is dependence between minimal and maximal available speed of objects motion on the video image from the camera frames:

1. Maximal speed depends on the object size. Dependence of maximally available speed from the frame frequency for typical objects – person and car is given in the table:

Frame frequency	Maximally available speed of a person	Maximally available speed of a car

6 fps	5 km/h	40 km/h
12 fps	10 km/h	85 km/h
25 fps	20 km/h	170 km/h

So, for example, if it is required to recognize people moving with speed till 10 km/h, the frequency 12 fps is enough.

2. The minimal speed of object motion is to be such as the displacement of object image will be less than 1 pixel per frame.

23.3.2.7.3.3 Hardware requirements for the Tracker with neural filter operation

When using the neural filter for the **Tracker** object, the following hardware requirements should be met:

1. The neural filter supports the following processors: CPU, GPU (discrete GPU NVIDIA, built-in Intel GPU), VPU (Intel NCS, Intel HDDL).

   Note.

   In order to connect the Intel NCS, plug in the device to the USB port and make sure that Windows shows it with one of the following names: Movidius, Myriad X, VSC Loopback Device.
   Intel NCS can be utilized with any computer compliant to the *Intellect* hardware requirements (see Requirements for base PCs).

   Important!

   It is not recommended to use more than one Intel NCS device on the same Server.

2. If CPU or Intel GPU is in use for the neural filter operation, keep in mind that the following processors are supported: Intel Core generation 6 and later, Intel Xeon and Intel Pentium® processors N4200/5, N3350/5 or N3450/5 with Intel® HD Graphics https://software.intel.com/en-us/openvino-toolkit/hardware.
3. NVIDIA GeForce 1050 Ti GPU or newer. GPU requirements:
   a. at least 2 GB of memory;
   b. Compute Capability 3.0 or higher.

   Note.

   Please check the GPU's Compute Capability version on the manufacturer's web site.

   Important!

   Install the latest NVIDIA driver from the NVIDIA official web site.

A single neural network consumes 500 MB of video memory. Each neural network is distributed between several object trackers within the GPU. For example: to apply the neural fire detector and the neural smoke detector to any number of channels, you should use a 1 GB graphics card or higher. You can use multiple video cards in your system.

Note.

Make sure that video image requirements are met in order to provide the correct neural tracker operation – see Requirements to video parameters while working with detection tools and Tracker

Requirements for video materials for neural networks preparation and further training
To use neural network analytics (a neural filter as part of the base *Intellect* software, and a neural tracker, a posture detection tool as part of the Detector Pack subsystem), you need to collect and submit to AxxonSoft the images and video recordings from your actual video cameras with the same resolution, expected weather conditions and time of day as in your future application.

For example, if your neural network is intended to operate in the outdoor environment, then your video recordings should contain all range of weather conditions (sun, rain, snow, fog, etc.) at different times of the day (morning, afternoon, evening, night).

Additional requirements for the images and video recordings for each neural analytic tool are listed in the following table:

Neural Filter	No less than 1000 frames containing the objects of interest in the given scene conditions, and the same number of frames without the required objects in the frame (background footage)
Neural Tracker	3-5 minutes of video recordings containing the objects of interest in the given scene conditions
Posture detection tools	No less than 100 different unique persons in the given scene conditions. ***Attention!*** *Different conditions also mean all kinds of positions of a person in the scene (tilts, different positions of body parts, etc.)*

23.3.2.7.3.4 Video requirements to be met for abandoned object detection tool of the Tracker object operation

1. Camera requirements:

1. Resolution must be not less than 640x480 pixels.
2. 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.

- Abandoned object images requirements:

1. An abandoned object must be visible on the image.
2. There must be no noise on the video image and there must be no artifacts caused by the compression algorithm.
3. Object dimensions on the video image must not be less than 1% of the frame size.
4. The width and height of objects in the video should not be less than 1% of the frame size (at resolutions not less than 1920x1080 pixels) or 15 pixels (at lower resolutions).
5. The width and height of objects in the video should not be more than 25% of the frame size.

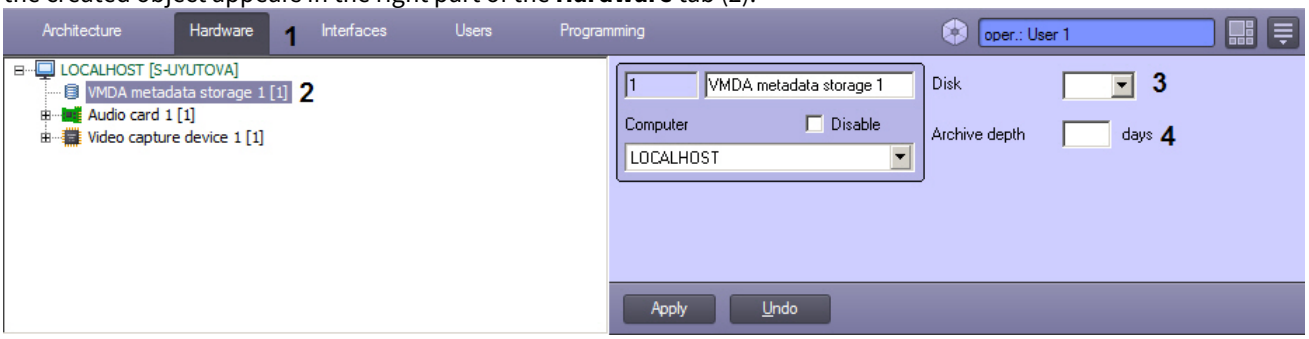
23.3.2.7.3.5 Creating and configuring VMDA metadata storage

VMDA metadata storage stores object trajectories covered by a camera. Information that is stored in the VMDA metadata storage is used for the forensic search in an archive.

To configure the VMDA metadata storage, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (1).

2. Create the **VMDA metadata storage** object on the base of the **Computer** object in the objects tree. The settings panel for the created object appears in the right part of the **Hardware** tab (2).



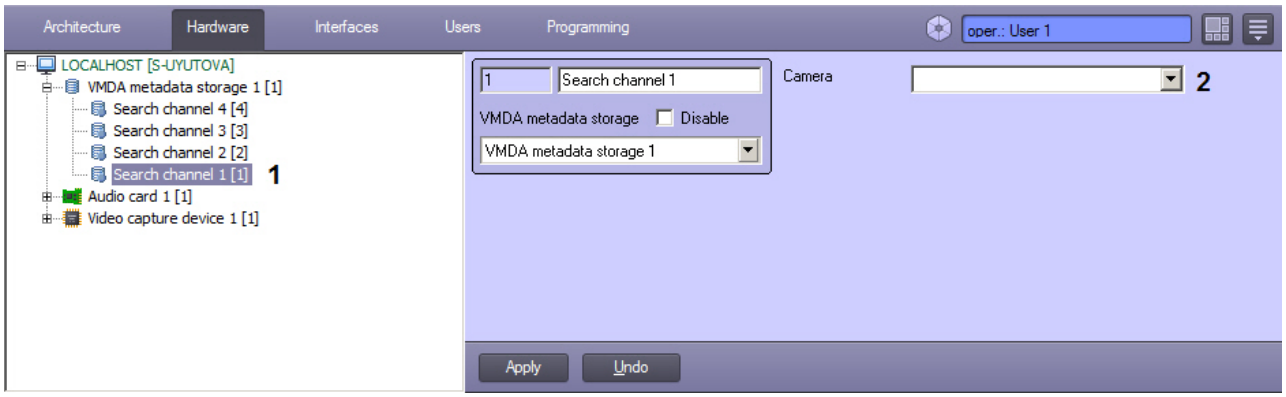
3. In the **Disk** drop-down list, select the disk for saving the archive (3).

> **Note.**
>
> The archive will be saved on the selected disk in the VMDA folder.

> **Attention!**
>
> Storing the data to the VMDA metadata storage may be very computer-intensive. The following actions are to be performed for proper system operation:
> 1.Create the **VMDA metadata storage** object on a separate Server.
> 2.Enable disk caching by means of redundant array of independent disks or OS.

4. In the **Archive depth** field, set the time period (in days) of storing the archive (4).
5. Select cameras metadata from which is to be saved in a created storage. To do this, follow these steps:
   a. Create a **Search channel** object under the **VMDA metadata storage** object (1). The number of available search channels is determined by the number of cameras in the license key.

> **Note.**
>
> If the license key was received earlier than December 2020, the **VMDA metadata storage** object should be configured as described in the documentation for Intellect 4.10.4, i.e. without creating **Search channel** objects. After updating the license key, please create and configure the **Search channel** objects as described below.



   b. From the **Camera** drop-down list, select the **Camera** object (2).
6. To save the changes, click the **Apply** button (7).

The VMDA metadata storage is now created and configured.

23.3.2.7.3.6 Recommendations on configuring smart video detection tools

Before configuring the smart video detection tools (see Creating and configuring the Tracker object), consider the following recommendations that could help to reduce the number of false positives:

1. Configure the **Tracker** object iteratively and check its operation quality at each iteration.
2. The parameters that affect the **Tracker** object operation quality the most are: **Minimum size**, **Maximum size**, and **Sensitivity**.
3. It is recommended to set the **Sensitivity** parameter to zero (left end position of the slider). This will enable automatic sensitivity ranging to ensure reasonable operation quality of the tracker in changing lighting conditions.
4. If lighting is stable, it could be reasonable to adjust the **Sensitivity** parameter manually. To detect the low contrast objects, set the **Sensitivity** value at about 35, for the high contrast ones—at about 15.
5. Minimum size of an object must be selected so that it is slightly smaller than the size of a typical object on the image.
6. Maximum size of an object must be selected so that it is slightly larger than the size of a typical object on the image, considering that the object can be joined with its shadow.
7. Lowering the **Waiting for loss** parameter will allow you to exclude triggering on false static objects. Increasing the parameter will allow you, in some cases, not to break off overlapping or temporarily disappearing objects.
8. To increase the VMDA detection tools accuracy, use an advanced object classifier, which is configured using the scripts and registry keys—see CAM_VMDA_DETECTOR VMDA detection.
9. To increase the VMDA detection tools accuracy, the neural filter can be used. It is trained individually for each use case and provides the high accuracy of the objects classification—up to 99% (see Configuring the neural filter).
10. To increase the operation stability of *Intellect,* you can separate the VMDA trackers operation into a separate **detector_ext.run** process using the **VMDAEXT** key (see Intellect Enterprise base version). However, keep in mind that allocating trackers to a separate process increases the CPU and memory resources used.

23.3.2.7.3.7 Creating and configuring the Tracker object

On the page:

- Basic settings
- Tracker mask
- Detected object sizes

The **Tracker** object registers the object tracks in the camera FOV during recording and saves them into the VMDA metadata storage.

To configure the **Tracker** object, do the following:

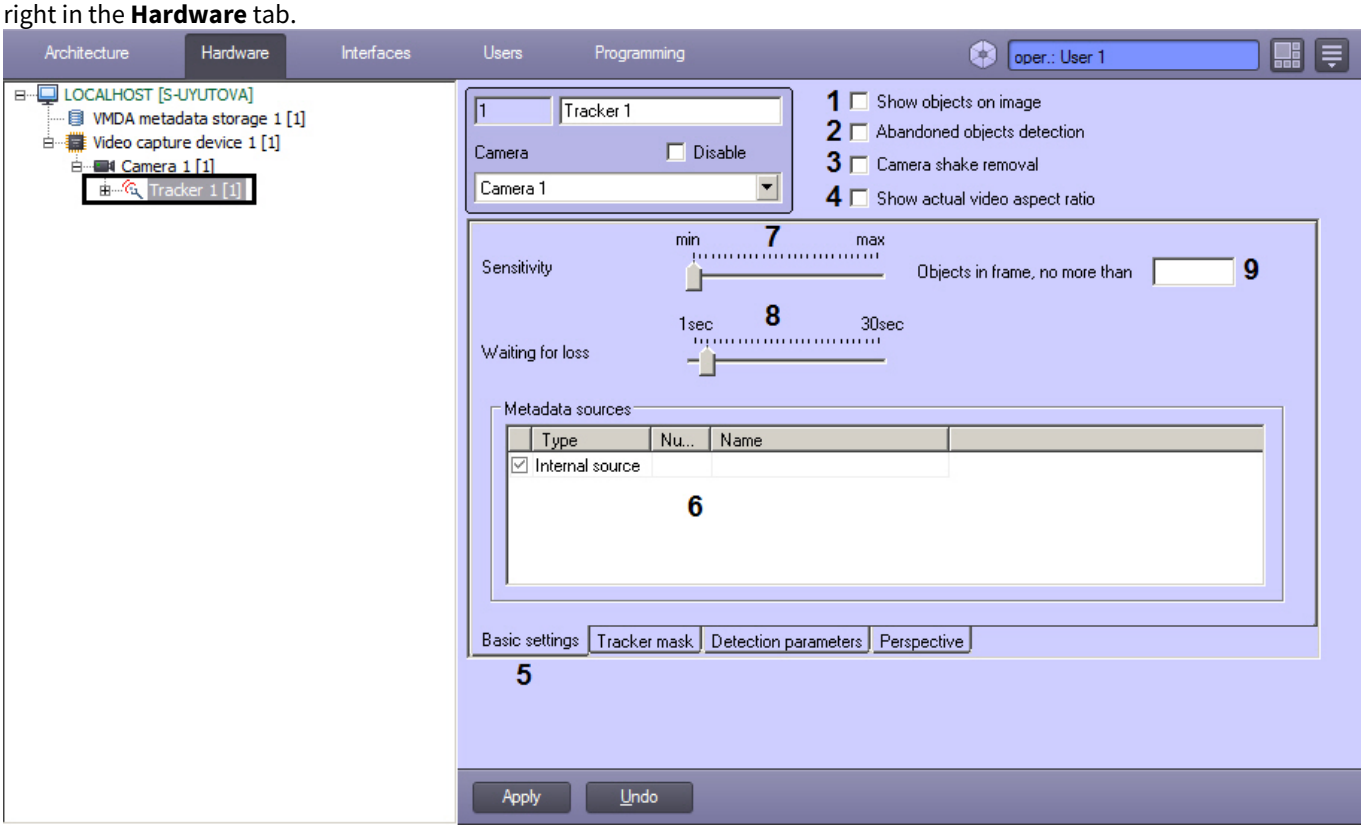
1. Adjust the basic settings.
2. Optional: add mask to disable analysis in any part(s) of the camera FOV.
3. Optional: set detected object sizes or configure the perspective settings (see Configuring perspective).

Basic settings

To configure the **Tracker** object, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box.
2. In the objects tree in the **Hardware** tab, select the **Camera** object, corresponding to the camera, the video image from which you want to analyze.

3. Create the **Tracker** object on the base of the **Camera** object. The settings panel for the **Tracker** object appears on the right in the **Hardware** tab.



4. Set the **Show objects on image** checkbox (**1**), if it is necessary to frame the objects in the surveillance window. The frames are displayed on live video only, e.g. in Video surveillance monitor.

> **Note**
>
> To display the objects tracker ID, set **1** value for the **DrawDetectorNumbers** line parameter in the HKEY_LOCAL_MACHINE\SOFTWARE\AxxonSoft\INTELLECT\Video (HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\AxxonSoft\INTELLECT\Video for 64-bit system) registry. Frame color is adjusted by the **DrawDetectorColors** parameter in the same registry:
> - When value is **1**, the frame color is the average color in the area
> - When value is **0**, the frame color is white.

5. To allow the VMDA detectors monitor the objects abandoned in the camera FOV, set the **Abandoned objects detection** checkbox (**2**). The video requirements for this feature to operate are described in Video requirements to be met for abandoned object detection tool of the Tracker object operation, and the settings for VMDA detection tools are described in Creating and configuring the VMDA detection. Customization specifics:
   a. To ensure the operation of the **Abandoned objects detection**, it is necessary to additionally configure the **Abandoned object** detector type (see Motion in the Area detection tool configuration).
   b. By default, if the **Abandoned objects detection** option is enabled, when viewing the live video and archive video, only the abandoned objects and disappeared objects will be framed on a video image. In order for the VMDA detector to detect only the disappeared objects, or only the abandoned objects, it is necessary to change the value of the **VMDA.filterGivenOrTaken** and **VMDA.determineGivenTaken** registry keys (for details, see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).
   c. The function of framing the abandoned and disappeared objects on the video image is available for the standard and the converted fisheye video.

> **Note**
>
> If there is no need to monitor the objects abandoned in the camera FOV, disable the **Abandoned objects detection** option to reduce Server load. When you disable this option, you also disable the detectors configured to monitor the abandoned objects.

6. If the camera is installed on the moving object, set the **Camera shake removal** checkbox (**3**) to stabilize the image and reduce the error in the detector operation.

   Attention!

   When the **Camera shake removal** option is active, the Server load increases.

7. If the video in the preview window is too distorted on the **Tracker mask**, **Detection parameters**, and **Perspective** tabs, set the **Show actual video aspect ratio** checkbox (**4**). In this case, the video may not occupy the entire area of the preview window.
8. Go to the **Basic settings** tab (**5**).
9. In the **Metadata sources** table, set the checkboxes next to the objects used for metadata creation (**6**):
   a. **Internal source**. The resources of the **Tracker** object are used as metadata source.
   b. **Embedded detector**. Metadata comes from the detectors embedded in the camera (see Embedded detectors).

      Note

      Tracks recording from the embedded detectors must be supported by the device. Furthermore, this functionality has to be integrated in *Intellect*.

   c. **VideoIntellect detector**. Metadata comes from *VideoIntellect* (see Configuring the integration with VideoIntellect software).
10. Set the value of the **Sensitivity** parameter by moving the slider to the required position (**7**). The value of this parameter corresponds to the minimum value of the moving object averaged brightness on which the detector will trigger only to its motion, not to the video signal noise (including snow, rain, etc.).

    Note

    If the slider is in the left end position, then the value of the **Sensitivity** parameter is selected automatically.

11. Set the **Waiting for loss** slider into position corresponding to time when the object stops moving and is considered to be active and the detector is still tracking it (**8**). If the object is motionless for a longer period than the set value, then the object is considered to be lost.

    Note

    If the lost object starts moving it is considered as a new object.

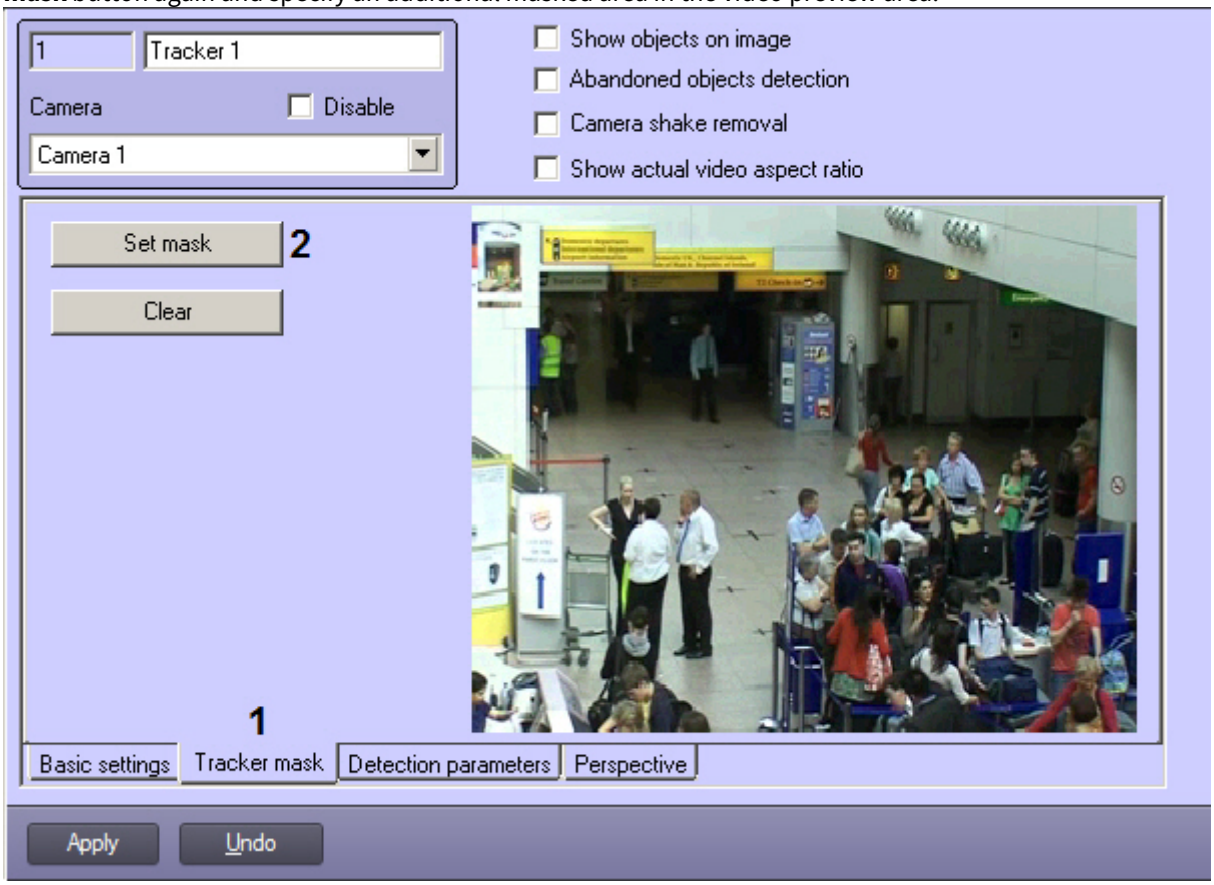
    Note

Fine-tuning of the abandoned objects detection tool is performed using the registry keys (see Registry keys reference guide).

12. In the **Objects in frame, no more than** field, specify the maximum number of objects in the frame that are detected (**9**). If the number of objects is equal to or exceeds the specified value, then the MD_LIMIT event is generated (see CAM Camera section of Guide for creating scripts (programming)). If the parameter is not set or equal to 0, this event is not generated.

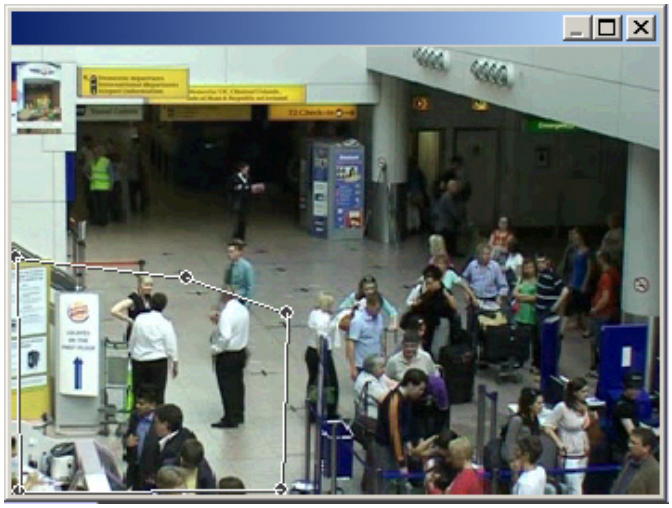
Tracker mask

To disable analysis in the camera FOV, in the **Tracker mask** tab (**1**), click the **Set mask** button (**2**) and specify the area in the video preview area. It is possible to disable analysis in several areas, i.e. to set several masks. To set an additional mask, click the **Set mask** button again and specify an additional masked area in the video preview area.



To zoom in on the video preview area for a more precise selection of the masked area, right-click the video preview area while holding down the Shift key on the keyboard after clicking the **Set mask** button. The video opens in a separate window, which can be resized by dragging its borders. After setting the mask in this window, close it by clicking the ✕ button in the upper right

corner.

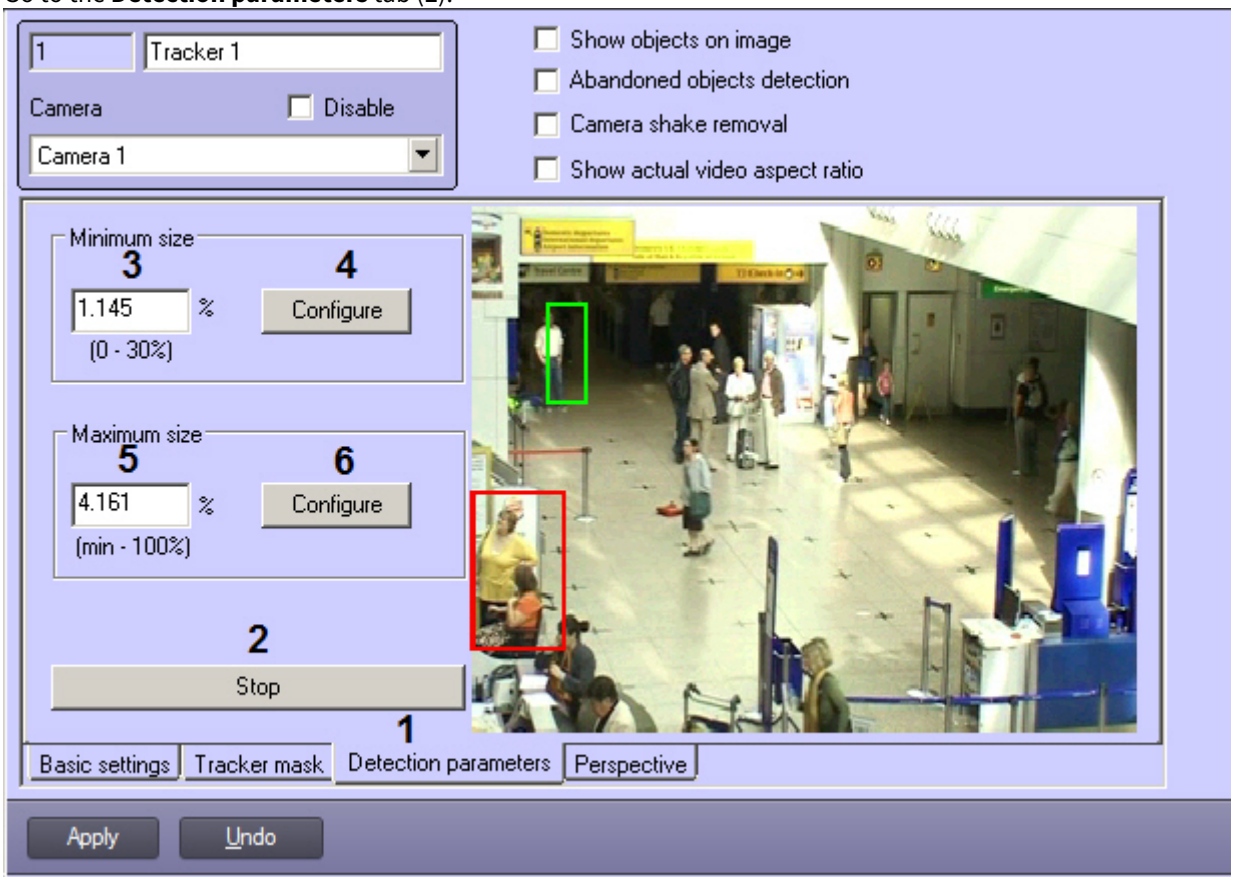


Detected object sizes

To set the minimum and maximum sizes of the detected object, do the following:

> **Note**
>
> If the perspective configuration is enabled, the parameters for the maximum and minimum object size for detection are ignored. **Width, m** and **Height, m** parameters in the **Perspective tab** (see Configuring perspective) are considered instead.

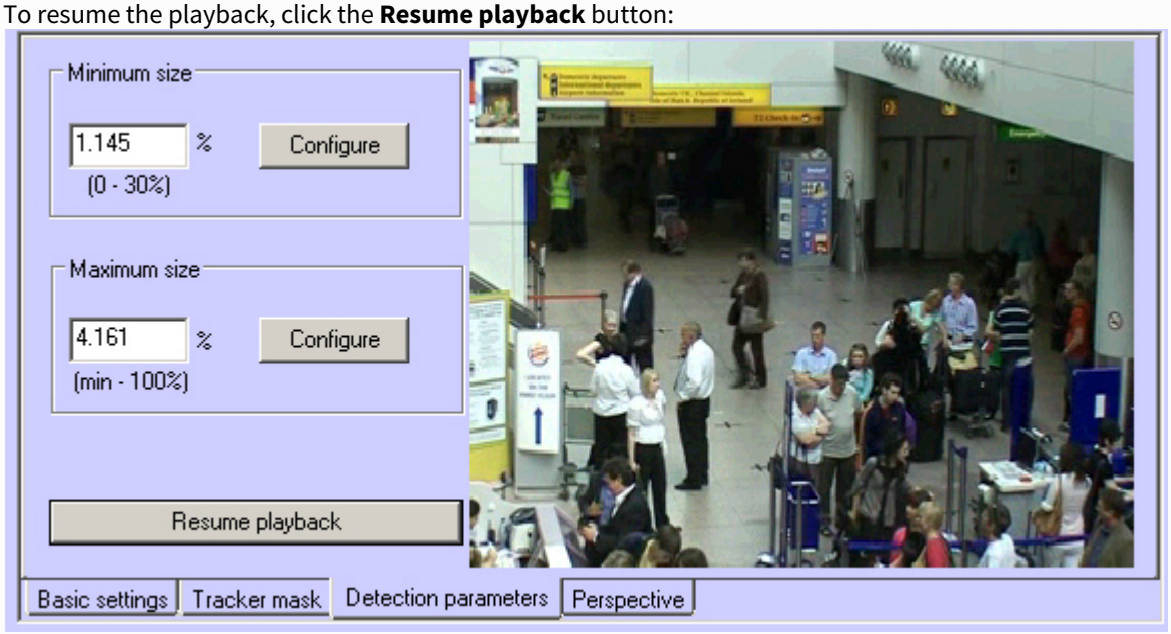
1. Go to the **Detection parameters** tab (**1**).



2. To stop the playback in the video preview area, click the **Stop** button (**2**).

Note

To resume the playback, click the **Resume playback** button:



3. In the **Minimum size** group, specify the minimum size of the detected object as a percentage of total image area (**3**) or click the **Configure** button and specify the size in the video preview area (**4**).

   Note

   The range of values of the **Minimum size** parameter varies from 0 to 30% relatively to the frame size.

4. In the **Maximum size** group, specify the maximum size of the detected object as a percentage of total image area (**5**) or click the **Configure** button and specify the size in the video preview area (**6**).

   Note

   Maximum size should be greater than the minimum size and not greater than 100%. If the maximum size is equal to the minimum size, no detection is performed.

Note

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

Smart video detection tools operation

Configuring perspective

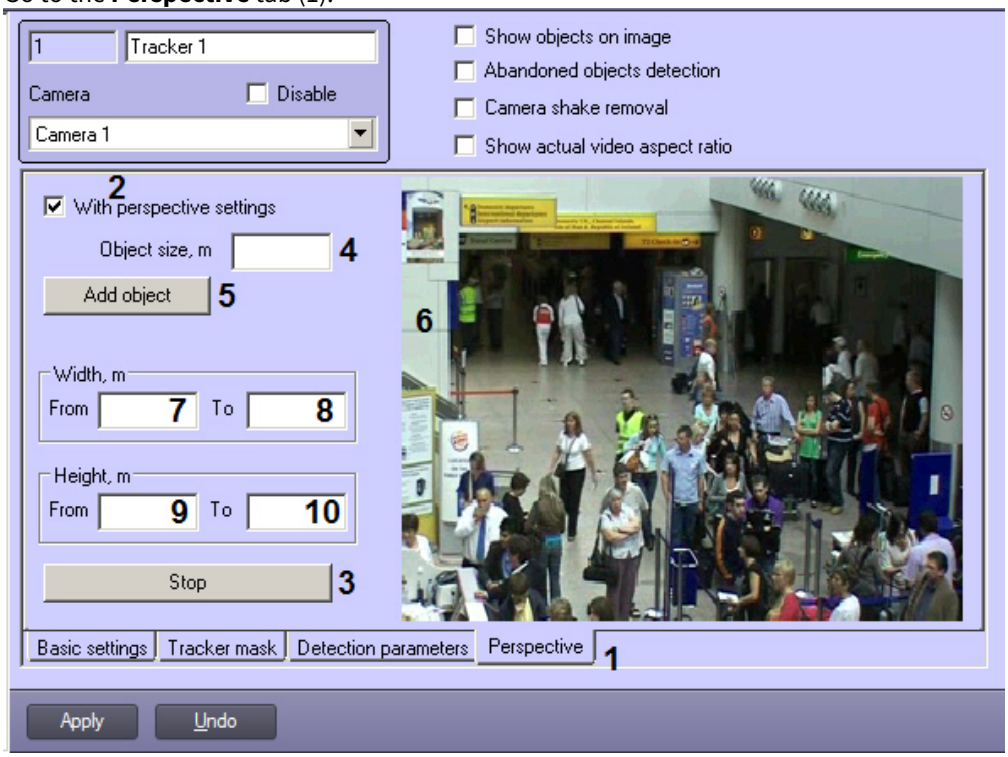
Perspective in the **Tracker** object is configured in order to set maximum and minimum object size (in meters) for these sizes to be considered correctly regardless of the fact that small objects can look bigger than big objects in the background. Perspective calibration allow better performance of the **Tracker** object.

If the perspective setting is active in the **Tracker** object then sizes specified in the **Detection parameters** tab are not taken into account. The **Width, m** and **Height, m** parameters are used instead.

To set perspective there are to be at least three objects of the same size in the scene that is in the camera's field of view. The perspective will be calibrated by these cameras. Poles, people, etc. can be calibration objects. Calibration objects are not to be on the same line. For higher accuracy they are to be positioned in all frame grounds: foreground, medium shot and background. Though, in some cases this is not obligatory: for instance, if there is no need to detect objects in the background and objects in the foreground are to be detected, then calibration objects are to be positioned in the foreground. The more there are calibration objects, the higher the accuracy of parameters restoration is.

If the perspective is to be considered when setting maximum and minimum object size do the following:

1. Go to the **Perspective** tab (1).



2. Set the **With perspective settings** checkbox checked (2).
3. Click the **Stop** button to stop playback in the viewing tile (3).
4. Specify the size of calibration object (in meters) in the **Object size, m** field (4).
5. Set the position of calibration objects on the video image in the viewing tile as follows:

> **Note.**
>
> Zoom in on the video preview field for more precise positioning of calibration objects. To do that, right-click the video preview while holding the Shift key on the keyboard. The video opens in a separate window, which can be resized by dragging its borders. Close this window after adding all required objects.

1. Click the **Add object** button (5).
2. Position the object over the calibration object on the video image (6).
3. Correct the object size by dragging its edges using left mouse button.

> **Note.**
>
> To delete an object click the button next to it.

4. Repeat steps a-c for all calibration objects in the scene.

- In the **Width, m** group set the maximum and minimum width of detected object (in meters) in the **From** (7) and **To** (8) fields (8).
- In the **Height, m** group set the maximum and minimum height of detected object (in meters) in the **From** (9) and **To** (10) fields.
- To save the changes, click the **Apply** button.

The perspective in the **Tracker** object is now configured.

23.3.2.7.3.8 Configuring object classification

There are three types of object classification by the smart detection tools in *Intellect*.

1. **Standard**. The following objects can be classified: a human, a vehicle, and other object (see Cross line detector configuration and Motion in the Area detector configuration). The method is based on determining the ratio of width to height of an object: if the width is greater than the height—a vehicle, if the width is less than the height—a human.
2. **Advanced**. The following objects can be classified with higher accuracy due to fine-tuning: a human, a group of humans, a vehicle, noise, an object carried into the area, an object carried out of the area, other object (see CAM_VMDA_DETECTOR VMDA detection).
3. **Neural filter** is a neural network-based classification. Any objects can be classified to a high precision. The neural network is trained individually for each use case. See Configuring the neural filter.

Configuring the neural filter
The neural filter allows classification of any objects to a high precision.

> **Note**
>
> The neural filter only works with tracks that have already been received from the **Tracker** object, allowing you to remove the excess (noise) and leave the necessary data (human, vehicle, etc.). Since the tracker records the trajectories of objects in the camera field of view, the neural filter receives the tracks only from the moving objects (or from the objects that stopped moving).

In most cases, one neural networks model is enough for the standard objects classification (e.g. a human / a vehicle). However, for the non-standard tasks with multiple object classes, more than one model may be required:

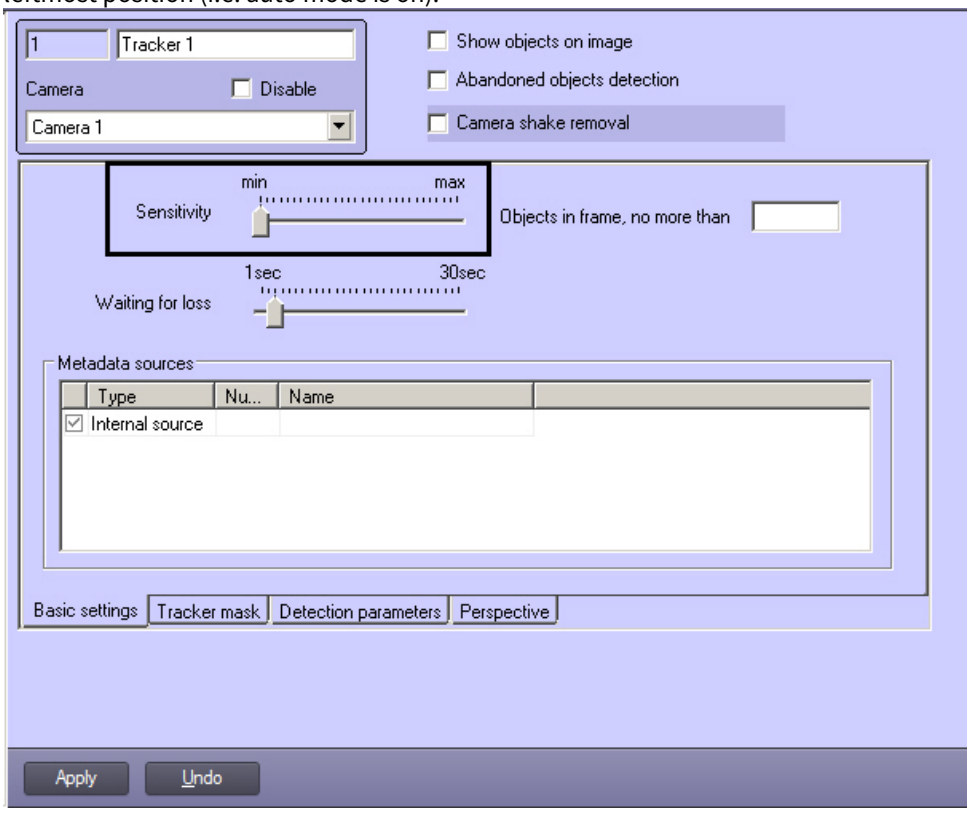
- if there are different classification tasks: for example, for some cameras the human/vehicle object classification is required, and for other cameras, the vehicle type (passenger car/freight vehicle) classification is required;
- if different conditions apply to different cameras, and the tracker will work better if each neural network is trained to work under different conditions: for example, the task is to protect the factory perimeter (only the human and vehicle detection is required) and the factory workshop (only the people in special work clothes detection is required).

Prior to configuring the neural filter, it is necessary to contact the AxxonSoft technical support and request the model files of the trained neural networks. Technical support specialists will request the data necessary for the preparation of models, and then provide you with the ***.ann** files for each model of the neural network. These files should be distributed among all the servers where the neural filter will be used.

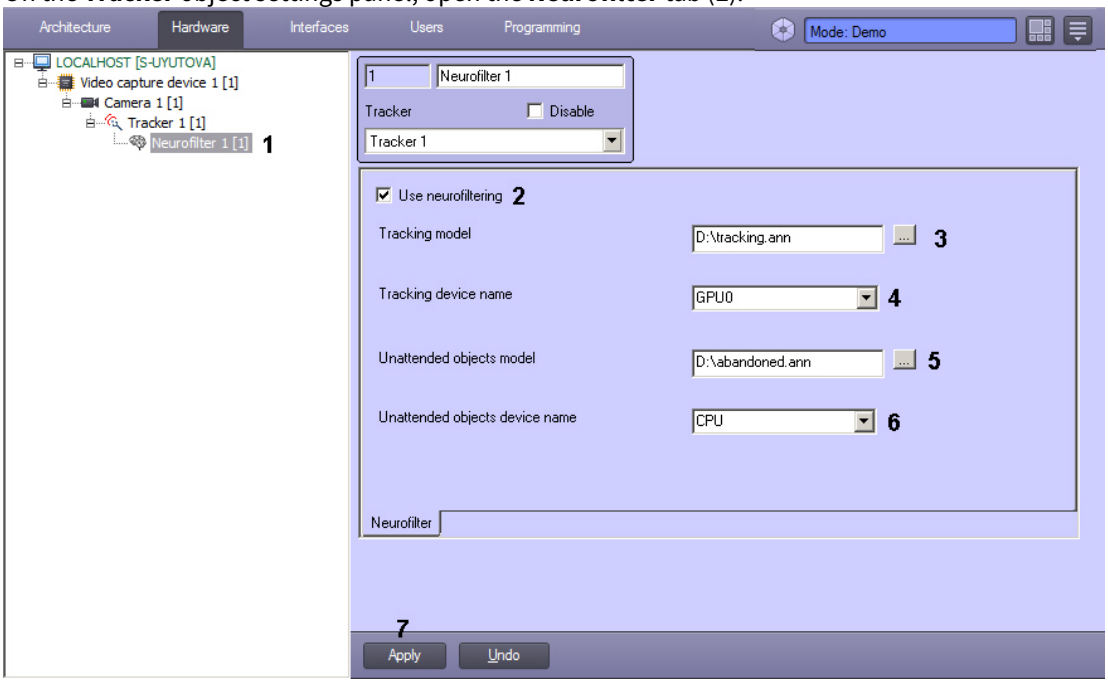
The neural filter is configured in the following way:

1. Install the *Detector Pack* subsystem (if not already installed). The *Detector Pack* subsystem installation guide is available in the corresponding documentation section, the most current version of the documentation is in the AxxonSoft documentation repository.
2. Make sure that the value of **1** is set for the the VMDAEXT key (for details on the key, see Registry keys reference guide). This key is automatically created with the value of 1 when the *Detector Pack* subsystem is installed.
3. Make sure that the value greater than **2000** but less than 5000 is set for the the VMDAEXT.RAM key. It is recommended to specify **4000**, depending on the computer hardware resources. This key is automatically created with the value of 2000 when the *Detector Pack* subsystem is installed.

4. Go to the **Basic settings** tab on the **Tracker** object settings panel and make sure that the **Sensitivity** slider is in the leftmost position (i.e. auto mode is on).



5. On the **Tracker** object settings panel, open the **Neurofilter** tab (**1**).

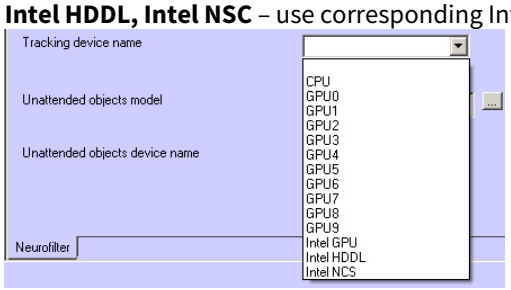


6. Set the **Use neurofiltering** (**2**) checkbox.
7. In the **Tracking model** field (**3**), enter the full path to the tracker model file received from the AxxonSoft technical support, or click the **...** button and select the file in the standard Windows dialog box.
8. From the **Tracking device name** drop-down list (**4**), select the name of the device that should be used by the tracker for the objects classification:
    a. **CPU** — use the CPU.

b. **GPU0**, **GPU1**, **GPU2** ... — use the NVIDIA GPU. Usually GPUs are recognized in the system in the order of their physical installation: the first (usually the upper one) GPU is number 0, the middle one is number 1, and the last (usually the lower one) is number 2.

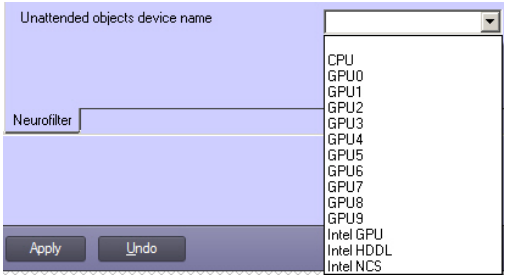
> **Note**
>
> If there are NVIDIA GPUs in the system, it is recommended to use them. If there are no NVIDIA GPUs in the system, the CPU resources should be used. GPUs from other manufacturers are not supported.

c. **Intel GPU** – use Intel GPU.
d. **Intel HDDL, Intel NSC** – use corresponding Intel VPU (vision processing unit).



9. In the **Unattended objects model** field (**5**), enter the full path to the abandoned objects detection model file received from the AxxonSoft technical support, or click the **...** button and select the file in the standard Windows dialog box.
10. From the **Unattended objects device name** drop-down list (**6**), select the name of the device that should be used by the tracker for the abandoned objects classification.

> **Note**
>
> For the unattended objects neural filter operation, it is necessary that the unattended objects detector of the **Tracker** object is enabled, and the VMDA detectors are configured appropriately (see Creating and Configuring the Tracker Object and Creating and Configuring VMDA Detection).



11. Click the **Apply** button (**7**).

> **Attention!**
>
> Each tracker with configured neural filter uses about 900 MB of video memory. If you are using several neurotrackers which in total consume more video memory than is available in the system, an error will occur. In cases when there is not enough video memory, it is recommended to use several video cards in one system.

The neural filter is configured.

Creating and configuring the VMDA detection
The VMDA detection tools react to object movement. When they trigger, an alarm is generated. On the basis of this alarm, you can perform actions in the system.

If you want to initiate an alarm on a camera when the VMDA detection tool triggers, set the **Generate alarm on camera** checkbox.

> **Note**
>
> You can set the alarm generation mode for any type of VMDA detection tools using the VMDA.oneAlarmPerTrack registry key (see Registry keys reference guide).

You can arm and disarm the VMDA detection tools using macros or scripts, which must be created manually (for the detailed information about macros, see Creating and using macros). By default, the detection tool is armed after creation.

The table below describes possible reactions on detection tool triggering (for example, on line crossing or motion in the area).

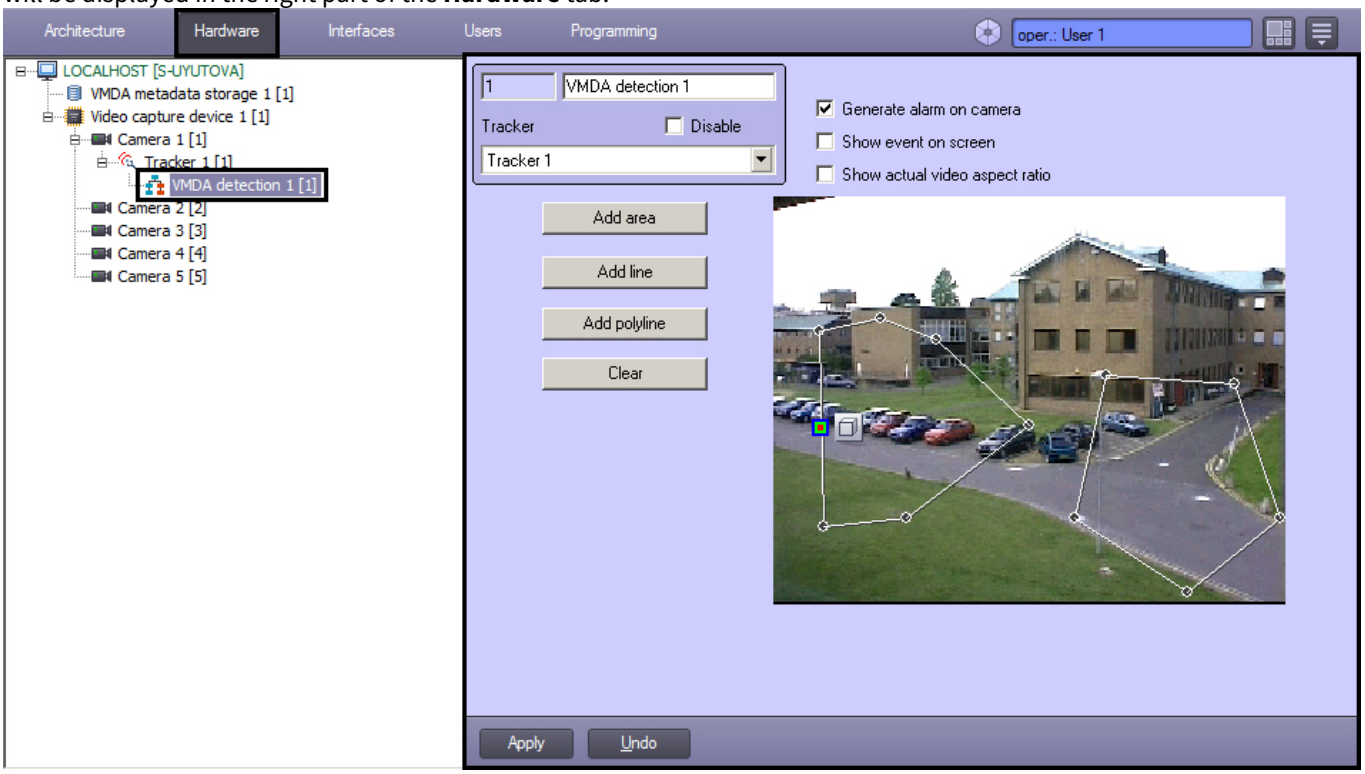
	VMDA detection tool is armed	**VMDA detection tool is disarmed**
The **Generate alarm on camera** checkbox is set	Alarm on camera + alarm on detection tool	Nothing happens
The **Generate alarm on camera** checkbox is clear	Alarm on detection tool	Nothing happens

Note

The **Disappearance in area** detection tool triggers **immediately** after an object in the area disappears. By default, the alarm is reset 15 seconds after the alarm triggers. You can change the alarm reset time using the DisappearedAlarmDuration registry key (see Registry keys reference guide).

To create a VMDA detection, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box.
2. Select the **Tracker** object in the objects tree on the **Hardware** tab.
3. Create the **VMDA detection** object on the basis of the **Tracker** object. The settings panel of the **VMDA detection** object will be displayed in the right part of the **Hardware** tab.



Note

Video from the camera on the basis of which the **VMDA detection** object is created is displayed in the **Video** field.

The VMDA detection is now created.

Next, you must select and configure the motion variant to which the detection tool will trigger:

- Moving from one area to another detection tool configuration;
- Motion in the Area detection tool configuration;
- Cross line detection tool configuration.

Attention!

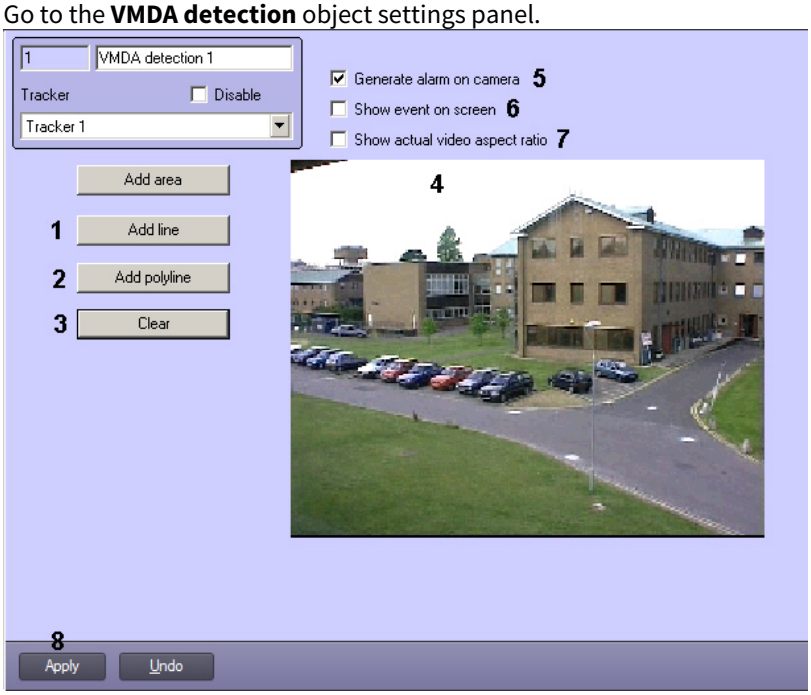
When you create VMDA detection on IP cameras, you must consider the information in Requirements for IP devices.

Cross line detection tool configuration

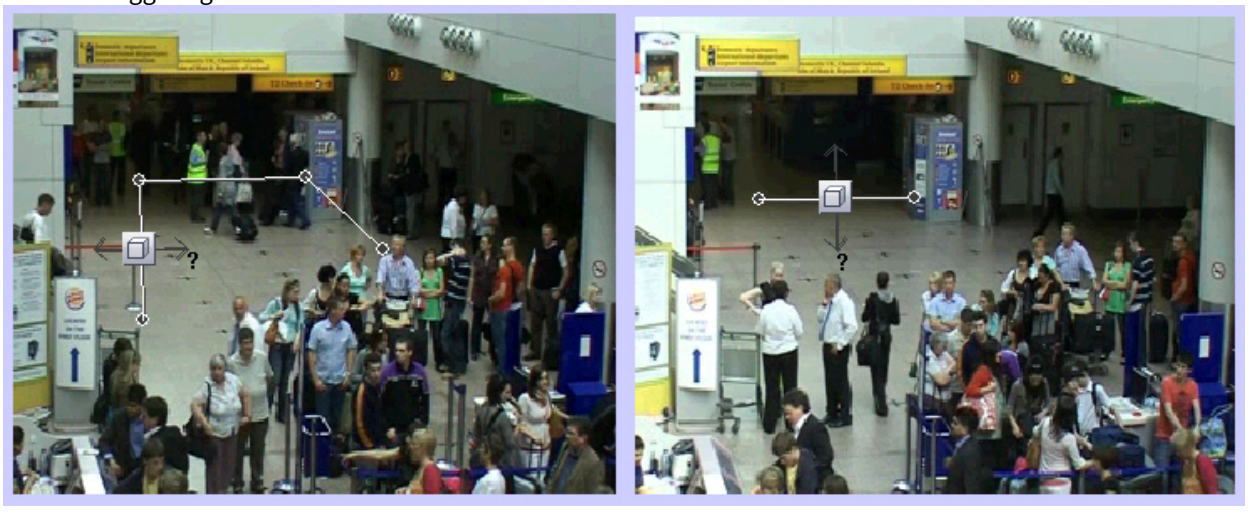
A cross line detection tool is a VMDA detection tool that triggers when the object trajectory in the camera FOV crosses a virtual line.

To configure a cross line detector, do the following:

1. Go to the **VMDA detection** object settings panel.



2. Select a line type (straight or polyline) the crossing of which leads to a detector triggering. Only one line can be added. The first line will be deleted if there is an attempt to add a second one.
   a. If a detector is to trigger while crossing a straight line, click the **Add line** button (**1**).
   b. If a detector is to trigger while crossing a polyline, click the **Add polyline** button (**2**).
3. In the **Video preview** field (**4**), set the end points of the line, by clicking left mouse button, which crossing leads to a detector triggering.



4. Make the necessary operations with a line. The operations are shown in the table.

Operation	Result
Left mouse click in the video surveillance window	Creation of a line's end point
Hover to an end point and holding the left button pressed move the mouse	Shift of a line's end point
Hover to an end point and click the right mouse button	A line's deletion

5. To select object type for which the detector will be enabled, click the symbol. Available object types are:
   a. Any object. Detector triggers when the line is crossed by any object
   b. A human. Detector triggers when the line is crossed by an object which width is less than height.
   c. Vehicle. Detector triggers when the line is crossed by an object which width is greater than height.

   Note.

   Detection of the following object types can be configured using scripts and registry keys: a human, a group of humans (with a possibility to count the number of people in a group), a vehicle, noise, an object carried into the area, an object carried out of the area, other objects. See also CAM_VMDA_DETECTOR VMDA detection section of the Guide for creating scripts (programming).
   More precise objects classification can be performed using the neural filter (see Configuring the neural filter).

6. To set the object color to be triggered by the detector, click the icon. The color picker palette will open. Circle the required color range with the left mouse button.

   To reset the selected color range to the default value, right-click in the palette area.
7. By default, the detection tool triggers on line crossing in both directions. Click the left mouse button upon one of the arrows to ignore crossing in one of the directions. The arrow will be colored gray.

   Note

   When just added, the arrow has minimum length.

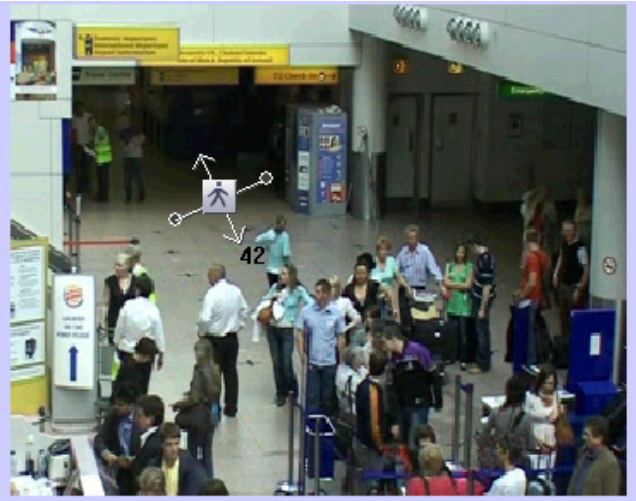
   The approximate speed of detected objects as a percentage of the frame per second is displayed near the arrow. Change the speed by moving the arrow head with pressed left mouse button and changing the arrow length. The detection tool is triggered when an object crosses the line in the selected direction with a speed that is approximately the same as the specified speed. At minimum and maximum value of speed the "?" sign will display and the fact of line crossing will be detected regardless of the speed.
   In order for the detection tool to be triggered when object speed is less than the specified speed, specify the id of the detection tool in the **VMDA.useSpeedLimitTypeLessThan** parameter (for details on the key, see Registry keys reference guide).
   In order for the detection tool to be triggered when object speed is greater than the specified speed, specify the id of the detection tool in the **VMDA.useSpeedLimitTypeMoreThan** parameter (for details on the key, see Registry keys reference guide).

   Note

For more information about working with the registry, see Working with Windows OS registry.

Important!

The same VMDA detector id can only be specified for either the **VMDA.useSpeedLimitTypeLessThan** or the **VMDA.useSpeedLimitTypeMoreThan** parameters. The simultaneous operation of both these parameters for the same VMDA detector is not allowed.



Note

It is necessary to set at least one object direction across the line.

Note

If both directions are set, the detector will trigger at line crossing by an object in any direction.

8. Set the **Generate alarm on camera** checkbox (**5**), if the camera alarm should be generated when the detector triggers.
9. To display the tracks of objects detected by the cross line detection tool regardless of whether the corresponding setting of the **Tracker** object is enabled, set the **Show event on screen** checkbox (**6**).
10. If the video in the preview window is too distorted, set the **Show actual video aspect ratio** checkbox (**7**). In this case, the video may not occupy the entire area of the preview window.
11. To save the changes, click the **Apply** button (**8**).

Note

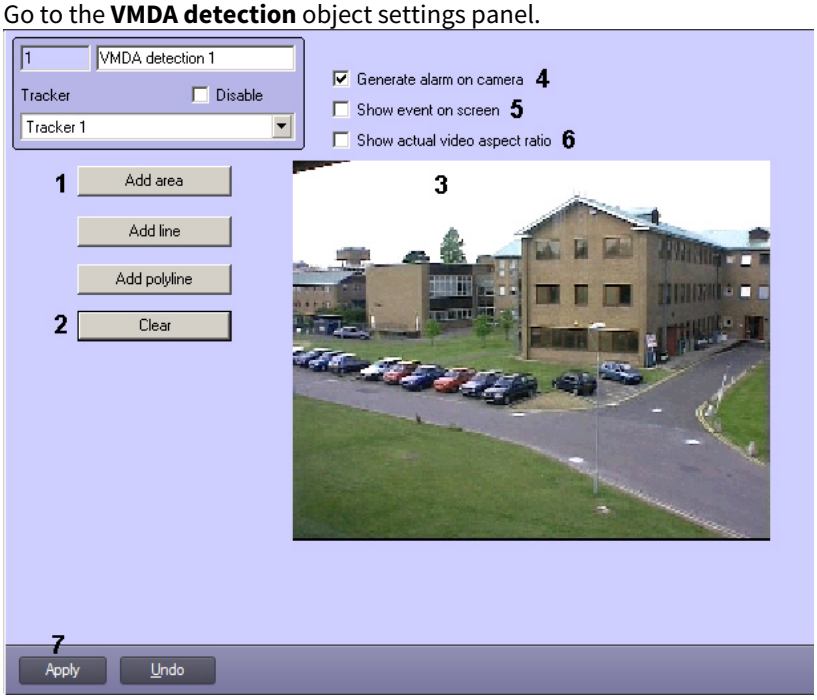
To clear the preview field from a visual element (a line), click the **Clear** button (**3**).

A cross line detector is configured.

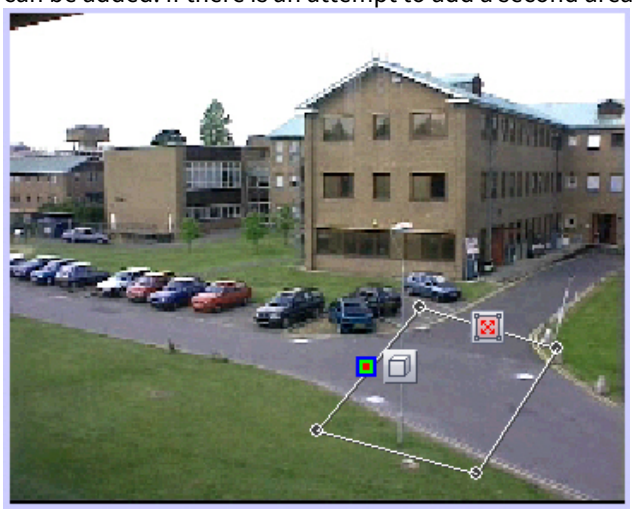
Motion in the Area detection tool configuration
A motion in the area detector is a VMDA detection tool that triggers when the object (objects) makes some actions in a virtual area that is in the camera FOV.

To configure a motion in the area detector, do the following:

1. Go to the **VMDA detection** object settings panel.



2. Click the **Add area** button (**1**).
3. In the **Video preview** field (**3**), set the nodal points of the area one by one by clicking the left mouse button. Only one area can be added. If there is an attempt to add a second area, the first one will be deleted.



4. Make the necessary operations with an area:

Operation	Result
Left mouse click in the video surveillance window	Area's nodal point addition
Hover to a nodal point and holding the left button pressed move the mouse	Area's nodal point shift
Hover to a nodal point and press right mouse button	Line deletion. If there are three nodal points the whole area will be deleted

5. To select an object type for which the detector will trigger, click the symbol. Available object types are:
   a. Any object. Detector triggers on any object.
   b. A human. Detector triggers on an object which width is less than height.

c. A vehicle. Detector triggers on an object which width is greater than height.

> **Note**
>
> Detection of the following object types can be configured using scripts and registry keys: a human, a vehicle, noise, an object carried into the area, an object carried out of the area, other objects. See also CAM_VMDA_DETECTOR section of the Programming Guide.
> More precise objects classification can be performed using the neural filter (see Configuring the neural filter).

6. To select a detector type, click the symbol. Available detector types are:
   a. Any movement in the area. Detector triggers due to any motion in the area.
   b. Entering the area. Detector triggers due to object's entrance into the area.
   c. Exiting the area. Detector triggers due to the exit of object from the area.
   d. Appearance in the area. Detector triggers due to the object's appearance in the area.
   e. Disappearance in the area. Detector triggers due to the object's disappearance from the area.
   f. Stop in the area. Detector triggers due to the object's stop in the area.
   g. Staying in the area for more than 10 sec (i.e. loitering detection). Detector triggers due to the object's presence in the area for more than 10 sec. This period can be configured with LongInZoneTimeout registry key (see Registry keys reference guide).
   h. Abandoned object. Detector triggers due to the item abandoned in the area.

> **Note**
>
> To ensure the Abandoned object detector type to work, the **Abandoned objects detection** checkbox must be set in the **Tracker** settings (see Creating and configuring the Tracker object).

7. To set the object color to be triggered by the detector, click the icon. The color picker palette will open. Circle the required color range with the left mouse button.

   To reset the selected color range to the default value, right-click in the palette area.
8. Set the **Generate alarm on camera** checkbox (**4**), if the camera alarm should be generated when the detector triggers.
9. To display the tracks of objects detected by the cross line detection tool regardless of whether the corresponding setting of the **Tracker** object is enabled, set the **Show event on screen** checkbox (**5**).
10. If the video in the preview window is too distorted, set the **Show actual video aspect ratio** checkbox (**6**). In this case, the video may not occupy the entire area of the preview window.
11. To save the changes, click the **Apply** button (**7**).

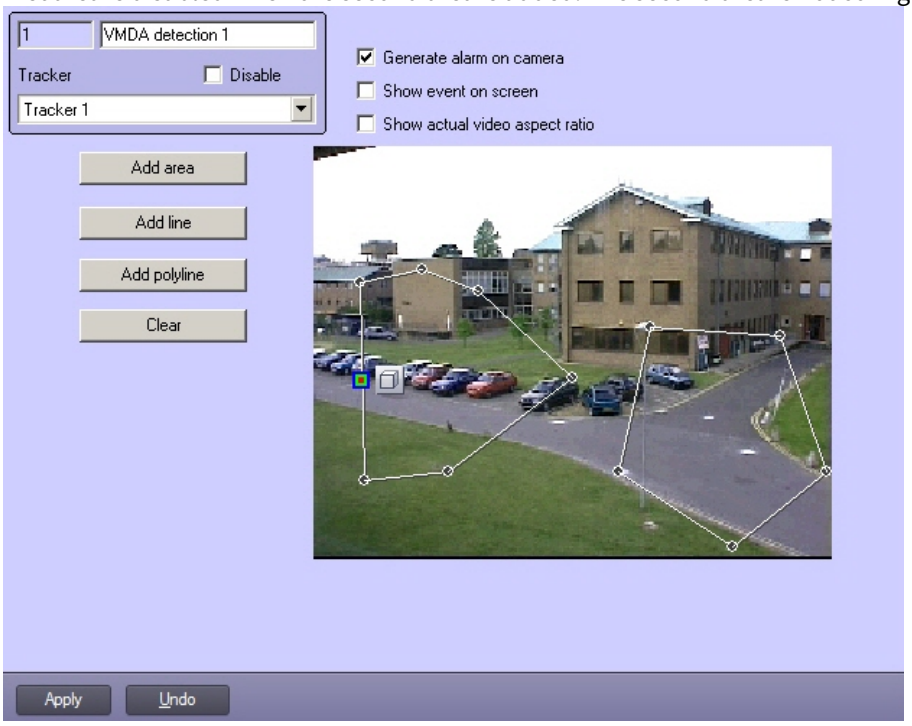
> **Note**
>
> To clear the preview field from a visual element (an area), click the **Clear** button (**2**).

A motion in the area detector is configured.

Moving from one area to another detection tool configuration
The **Moving from one area to another** detection tool is a VMDA detection tool that triggers when the object of a specified type moves from one area to another.

To configure **Moving from one area to another** detection, do the following:

1. Configure the **Motion in the Area** detection by setting the type of object. Do not select the detection tool type (see Motion in the Area detection tool configuration).
2. Add a second area similar to the first one. The possibility of selecting the type of **Motion in the Area** detection tool for the first area is disabled when the second area is added. The second area is not configurable.



> **Note**
>
> Only two areas can be added. If two areas are added, when you try to add a third area (by clicking the **Add area** button), the previous two areas will be deleted.

3. Click the **Apply** button.

The **Moving from one area to another** detection tool will trigger on transition of any object of the selected type from the first area to the second one.

The configuration of the **Moving from one area to another** detection tool is now complete.

23.3.2.7.4 Embedded detectors

At the moment of writing the documentation the embedded analytics of various cameras and Stretch cards (if it is supported-see reference manual concerning these devices) has been integrated into the *Intellect* software complex.

> **Note.**
>
> To clarify whether the embedded analytics is integrated for a particular video camera, please refer to the documentation for the relevant version of Drivers Pack - see page Documentation Drivers Pack.

Moreover, ACAP app for Axis devices is supported by *Intellect* – AxxonSoft Object Tracker for Axis cameras. This app allows using AxxonSoft analytics in Axis devices. Information on how to add the app to Axis device as well as how to configure and use it in *Intellect* can be found in the AxxonSoft Tracker in Axis devices section. The app can be downloaded here.

This section contains an example of embedded detectors auto setup. One should consult with reference manual while setting up embedded detectors of special devices manually.

Note.

If there is no time synchronization for some IP devices, the events of the onboard detection tools may work incorrectly in *Intellect*. In this case it is recommended to enable the synchronization of time and time zone between the Server and the IP device in the web-interface of the latter.

23.3.2.7.4.1 Creating embedded detectors

To create build-in detectors do the following:

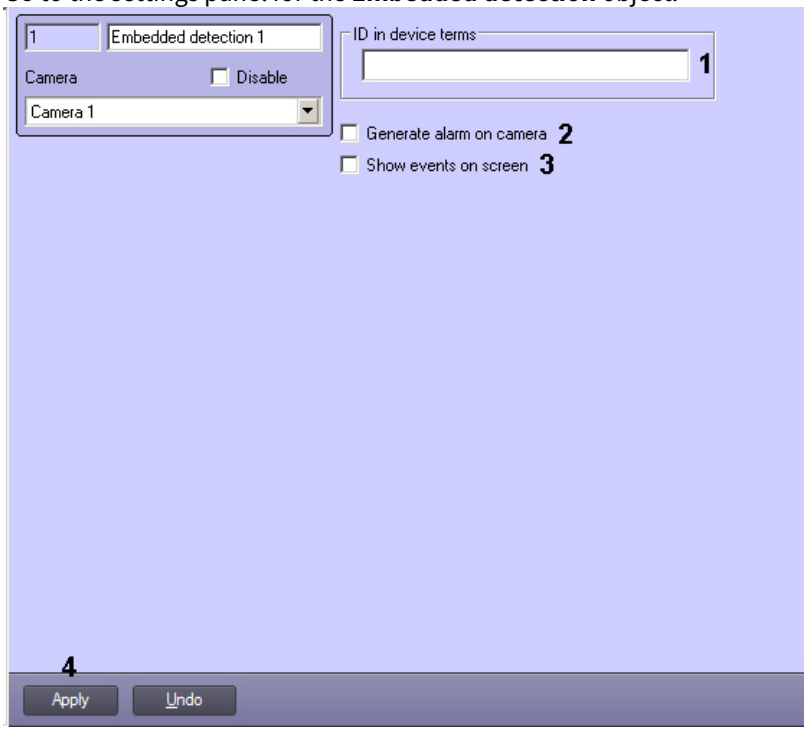
1. With the help of *Camera discovery tool* create IP devices that support build-in analytics.
2. In result the created objects will be displayed in the objects tree together with build-in detectors.

Build-in detectors creation is completed.

23.3.2.7.4.2 Configuring embedded detection

To configure embedded detection tools, do the following:

1. Go to the settings panel for the **Embedded detection** object.



2. In the **ID in device terms** field, the detector code in the device is specified (camera, card) (1). It is recommended to leave this field unchanged for proper operation of the detection tool.
3. Set the **Generate alarm on camera** checkbox if the alarm is to be generated on the camera by detector's response (2).

Note

The alarm triggers on the embedded detection tool instead of the camera when the camera is disarmed. Furthermore, the alarm triggers neither on camera nor embedded detection for metadata events intended for the *Tracker* (see Creating and configuring the Tracker object).

4. Set the **Show events on screen** checkbox if it is necessary to display tracks from the built-in detection tool regardless of the corresponding settings of the **Tracker** object and metadata source selected in it (3). For example, this setting can be applied for embedded detection tools that are in use for AxxonSoft Tracker in Axis devices.

   Note

   See also Creating and configuring the Tracker object.
   You can change the time during which the trigger frame is displayed in **Video surveillance monitor** when the Embedded detection tool is triggered. For this, use the **EmbededDetectorsLifetime** key (see Registry keys reference guide).

5. Click the **Apply** button to save the changes (4).

Embedded detectors are now configured.

Thermal camera operation
CAM_IP_DETECTOR Embedded detection

23.3.2.7.4.3 AxxonSoft Tracker in Axis devices

Attention!

Tracker isn't supported since DriverPack 3.76 (see Documentation Drivers Pack).

You can use analytics from AxxonSoft (Smart video detection tools) on Axis devices.

Note

This option is available for all devices based on Axis MIPS architecture (ARTPEC-4 or ARTPEC-5 processor) or ARMv7 architecture (ARTPEC-6 or ARTPEC-7 processor). The settings are given in the AxxonSoft Tracker Help.

All CPU heavy analytics and metadata generation tasks are delegated to the camera in this case reducing Server load.

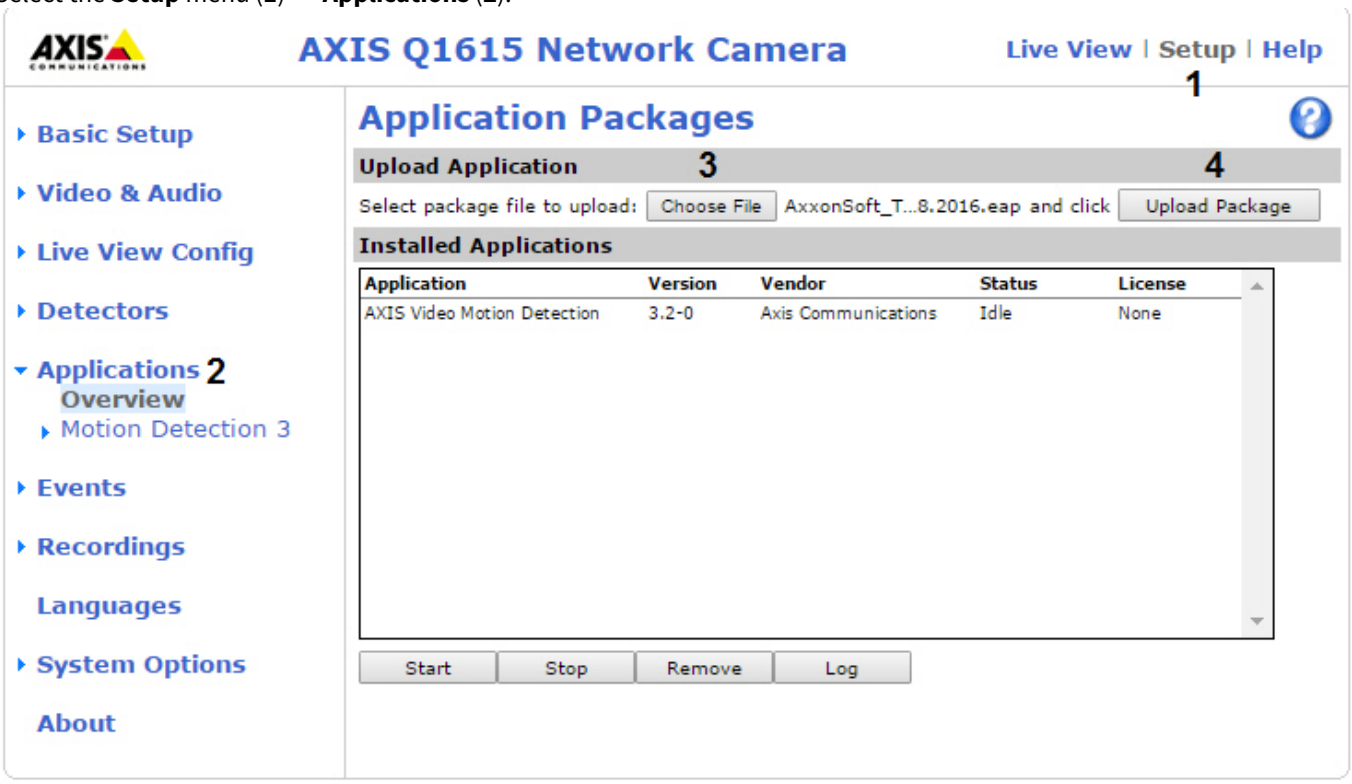
Attention!

In order to perform forensic search in the archive when using Axis devices for metadata generation, create and configure the **VMDA metadata storage** and **Tracker** objects and select the created above detection tool as metadata source for the **Tracker**. See also Creating and configuring the Tracker object and Creating and configuring VMDA metadata storage. It is not necessary to create the **VMDA metadata storage** and **Tracker** objects only to receive the detection tool triggerings.

To do this, do the following:

1. Go to the device's web interface.

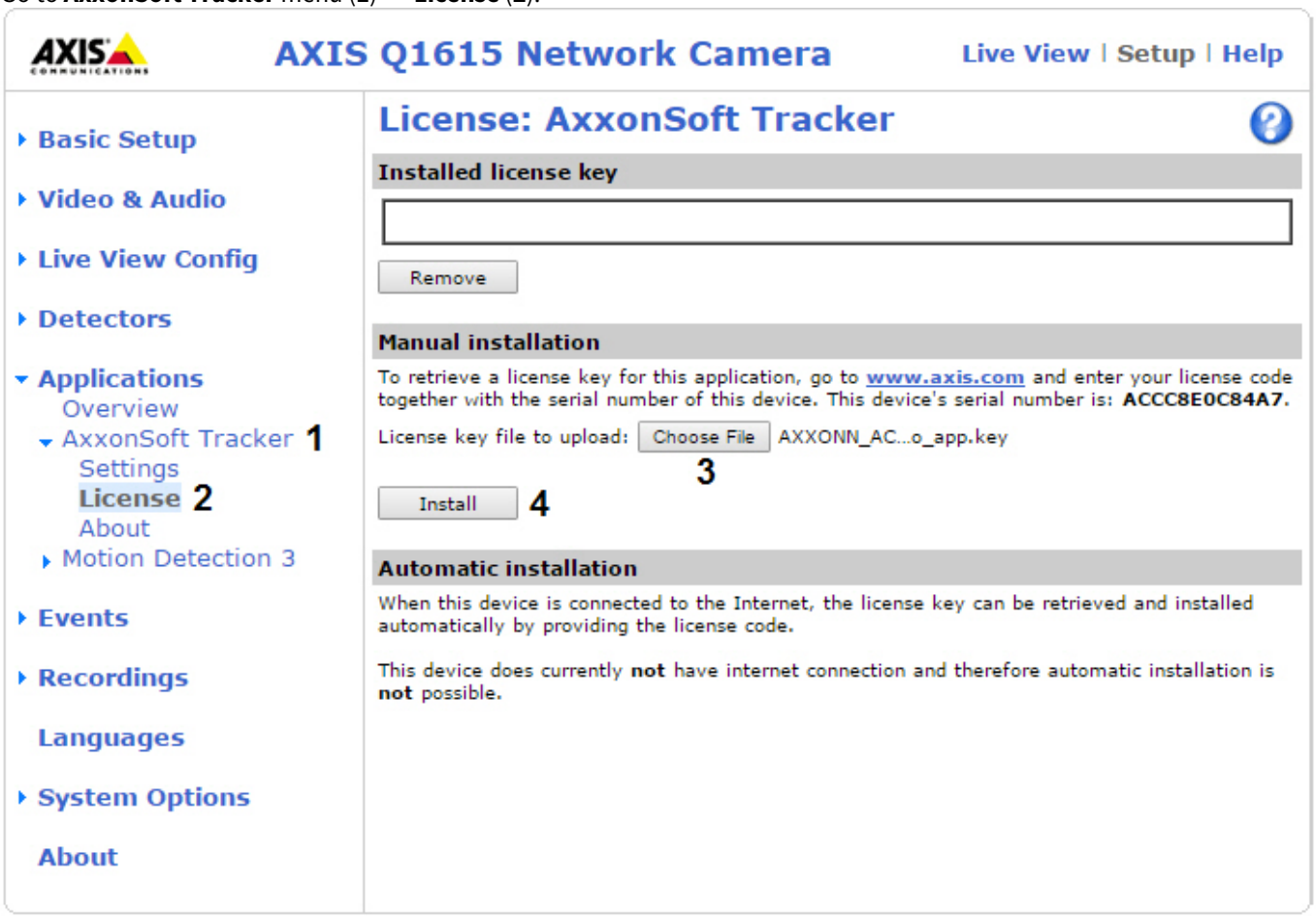
2. Select the **Setup** menu (**1**) → **Applications** (**2**).



3. Select the ACAP application (**3**) and click the **Upload Package** button (**4**).

> **Note**
>
> You can download the app from AxxonSoft website here.

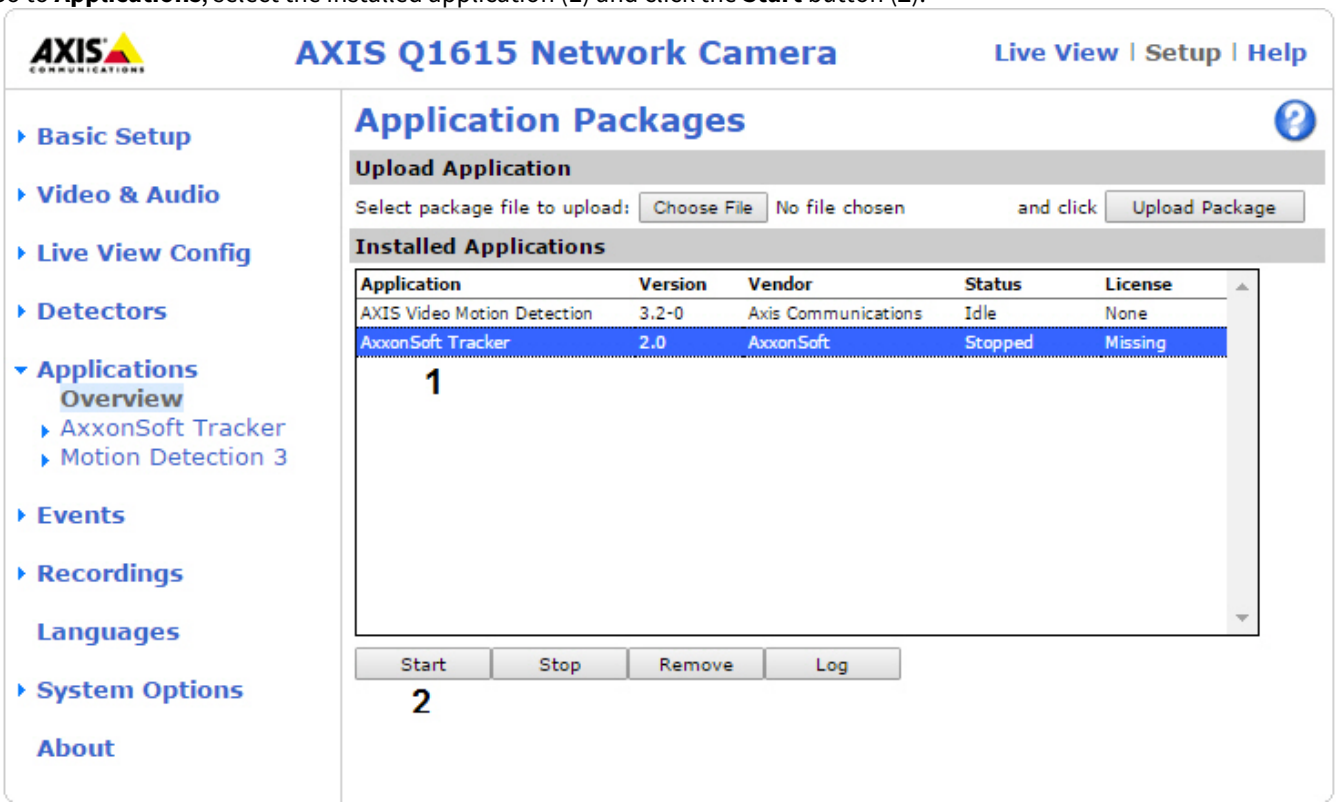
4. Go to **AxxonSoft Tracker** menu (**1**) → **License** (**2**).



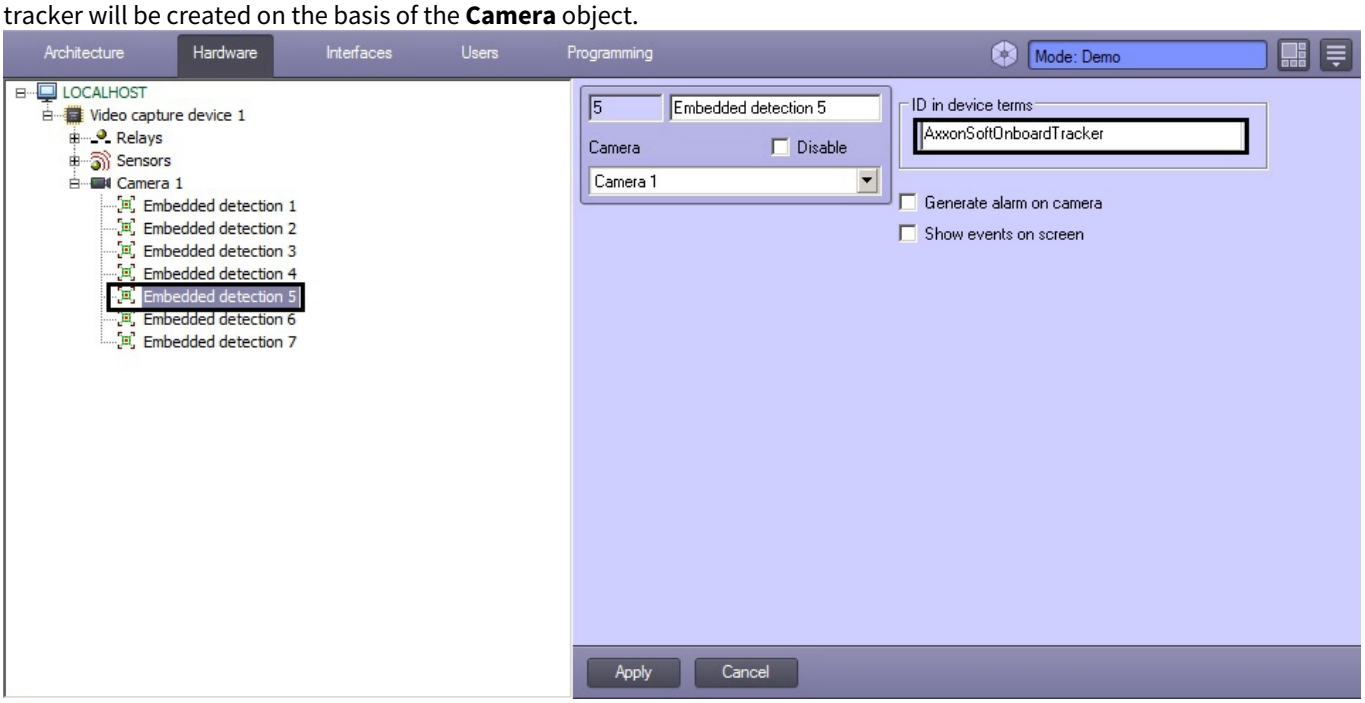
5. Select the license file (**3**) and click the **Install** button (**4**).

> **Note**
>
> Register a license code along with camera's MAC address on Axis website in order to get the license file. Contact AxxonSoft help-desk to get the license code.

6. Go to **Applications**, select the installed application (**1**) and click the **Start** button (**2**).



7. Add the Axis device to *Intellect* using the Camera discovery tool. An **Embedded detection tool** object corresponding to the tracker will be created on the basis of the **Camera** object.



8. Configure this object in *Intellect* according to Configuring embedded detection.

> **Note**
>
> You can configure the tracker parameters in the **Setup** → **Applications** → **AxxonSoft Tracker** → **Settings** section of the Axis device web-interface similar to the **Tracker** object in *Intellect* (see Creating and configuring the Tracker object).

AxxonSoft Tracker is now configured to be used in Axis devices.

23.3.2.7.4.4 Example of setting up and using the embedded detectors on Bosch FLEXIDOME IP dynamic 7000 VR IP camera

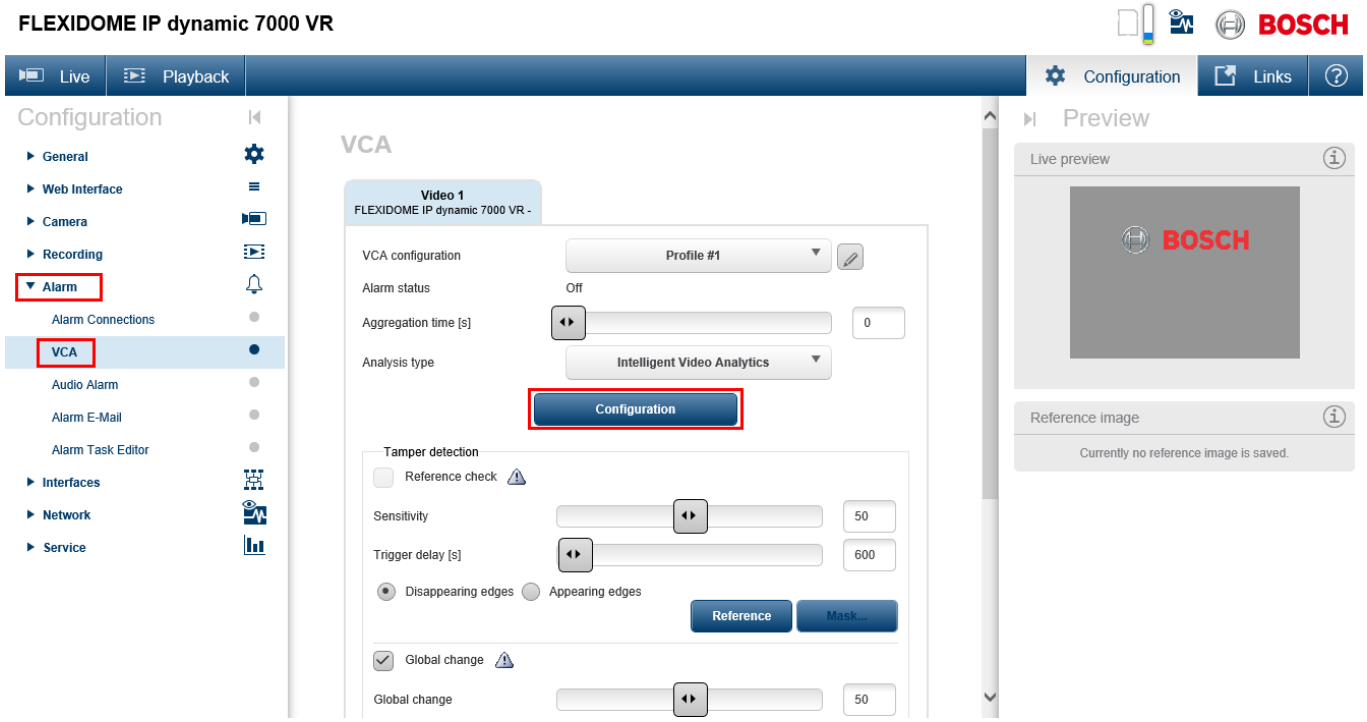
On the page:

- Configuring the visitors counter using the camera web interface
- Configuring Intellect to receive the events from the Bosch camera's visitors counter
- Using the Bosch camera visitors counter in Intellect

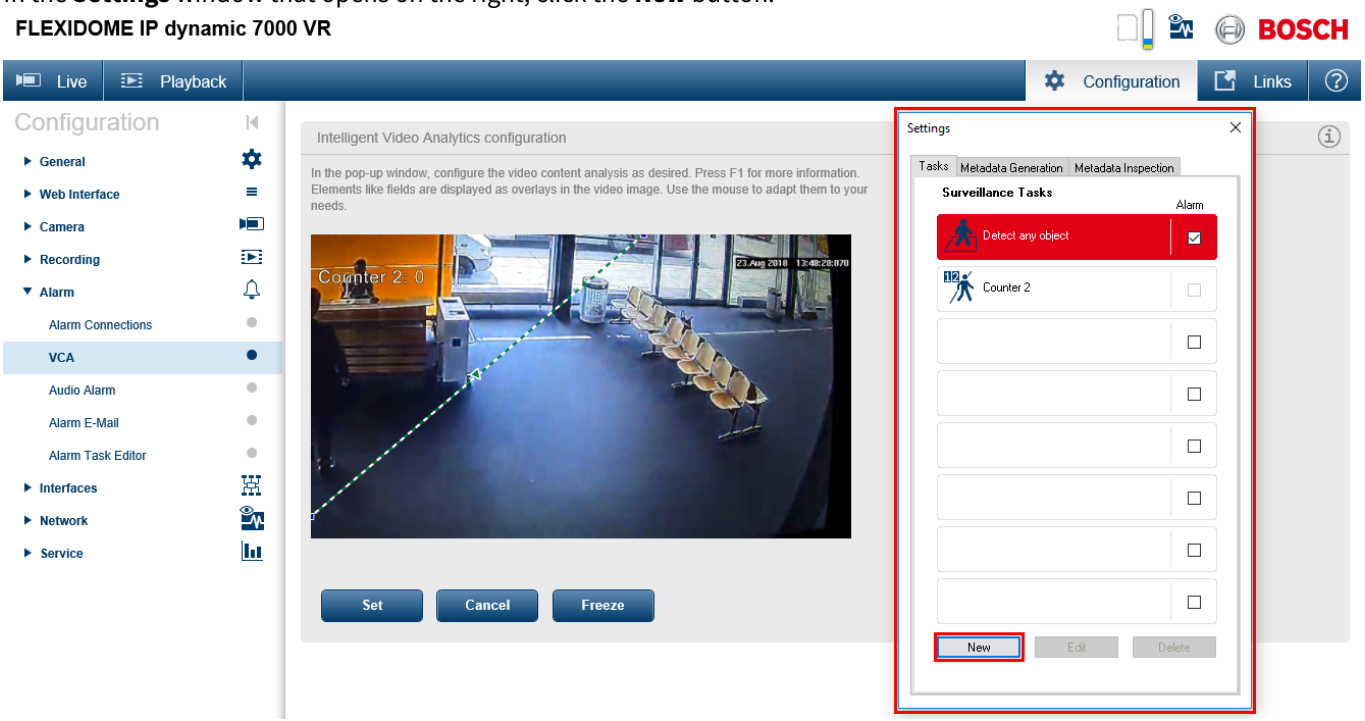
Configuring the visitors counter using the camera web interface

To configure the visitors counter using the camera web interface, do the following:

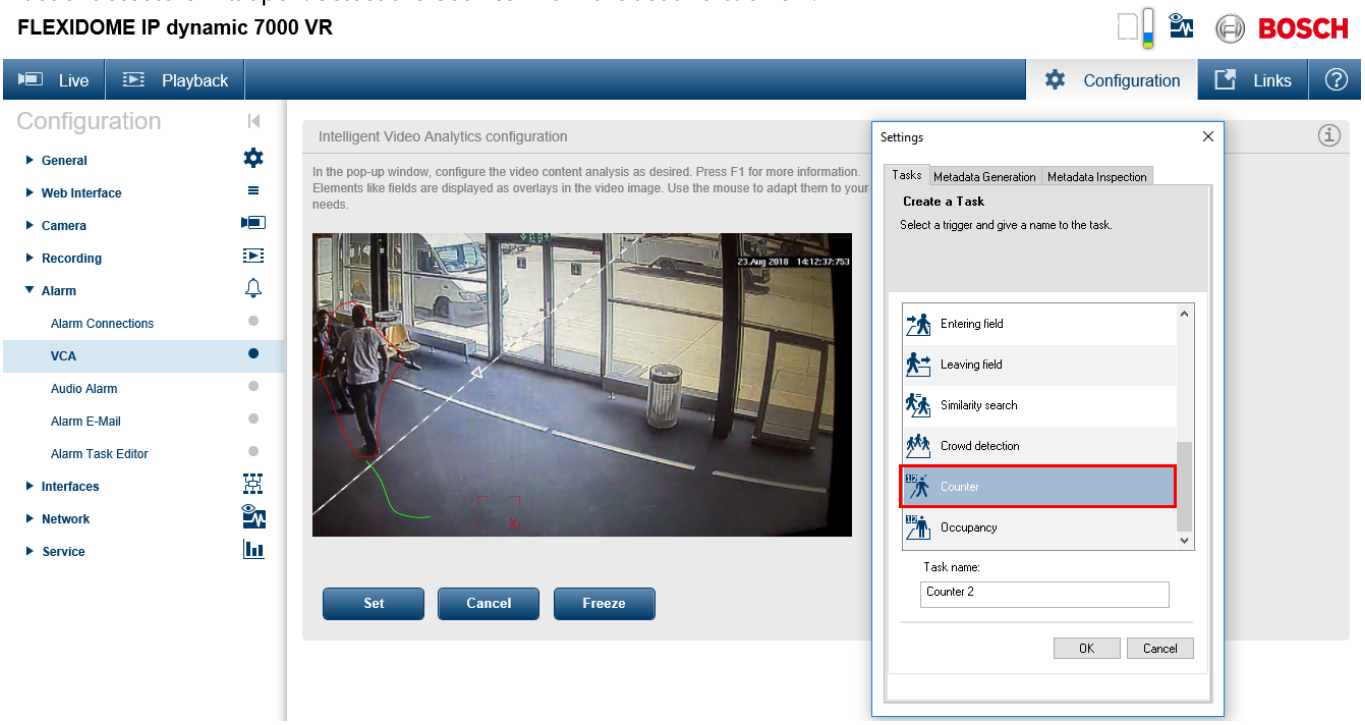
1. Open the camera web interface in the browser (see How to call the Web Server home page of IP device).
2. Go to **Settings** → **Alarm** → **VCA**, and then click on the **Configuration** button.



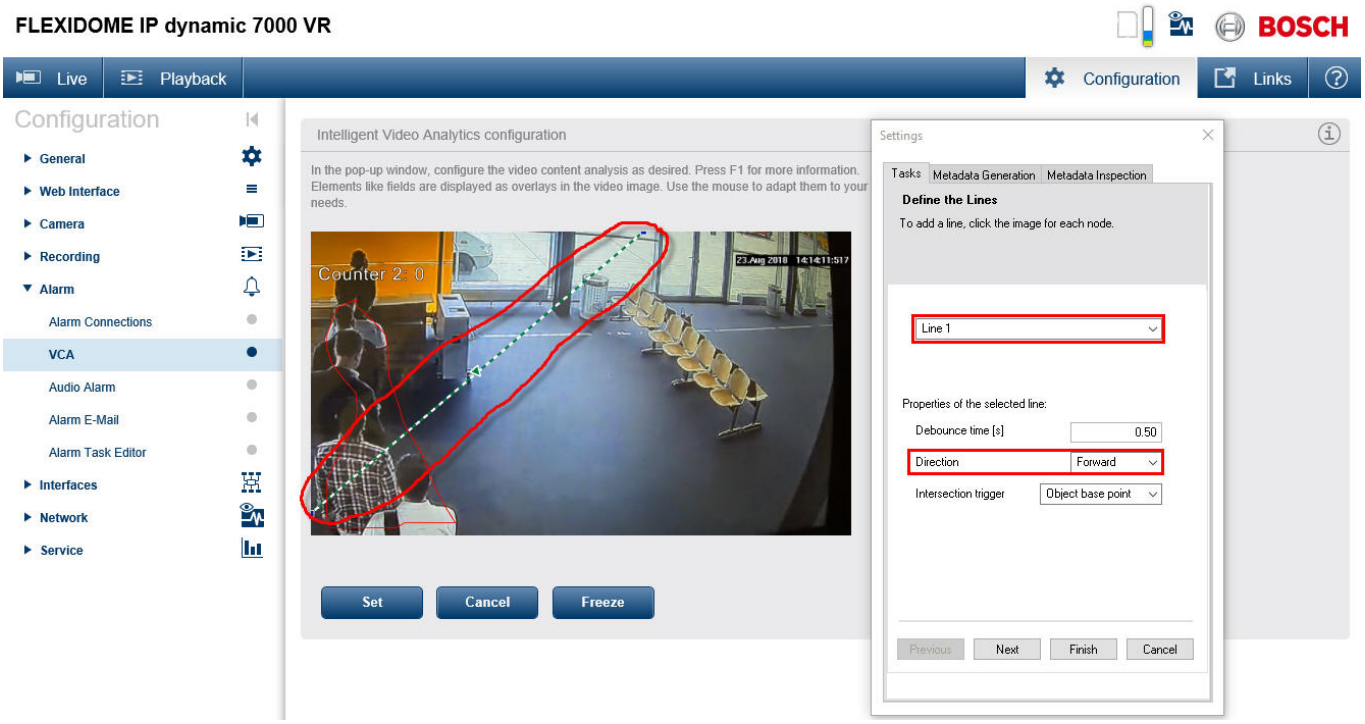
3. In the **Settings** window that opens on the right, click the **New** button.



4. A list of detectors will open. Select the **Counter** from the list and click **OK**.



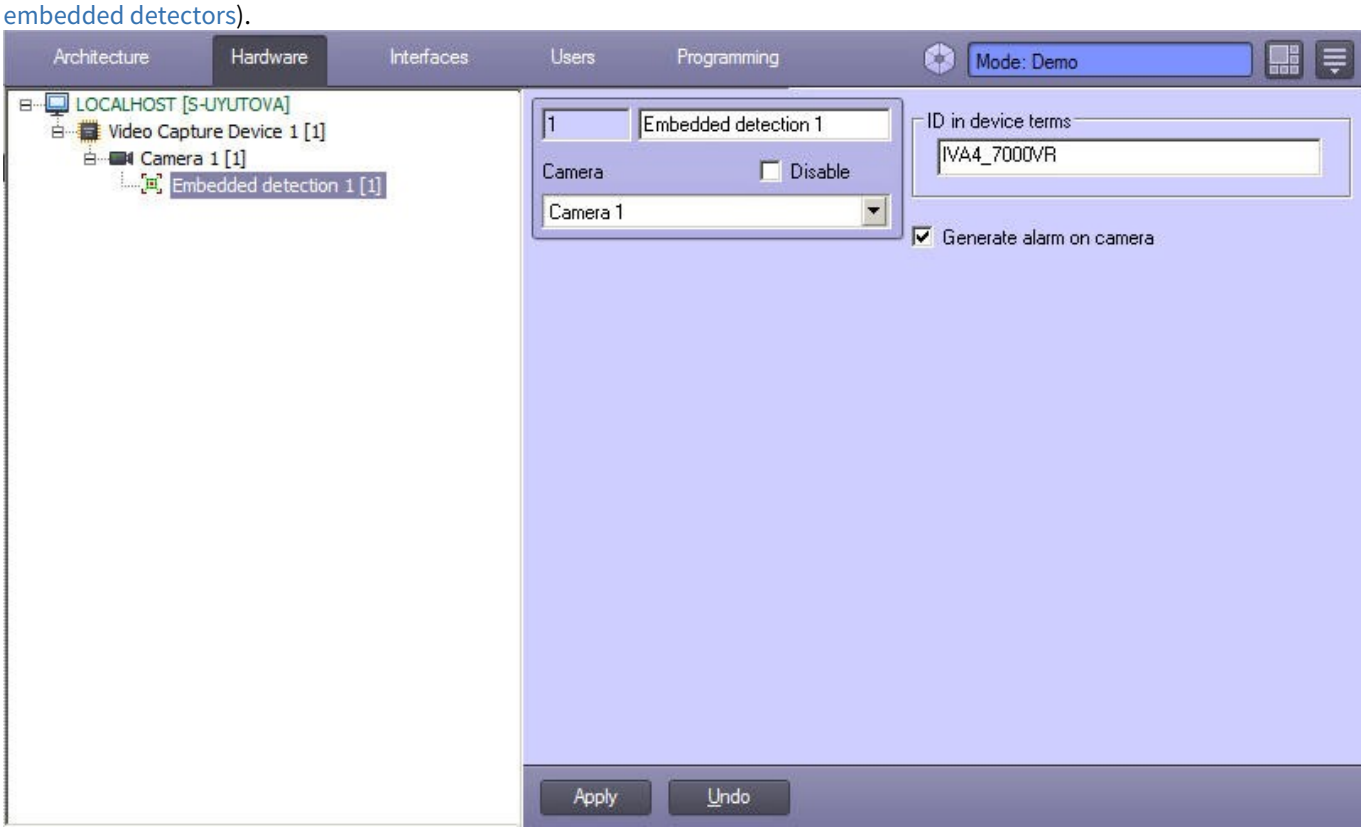
5. Draw a line. The visitors who cross that line will be counted. Select the direction of movement, and then click **Finish**.



Configuring the visitors counter using the camera web interface is complete.

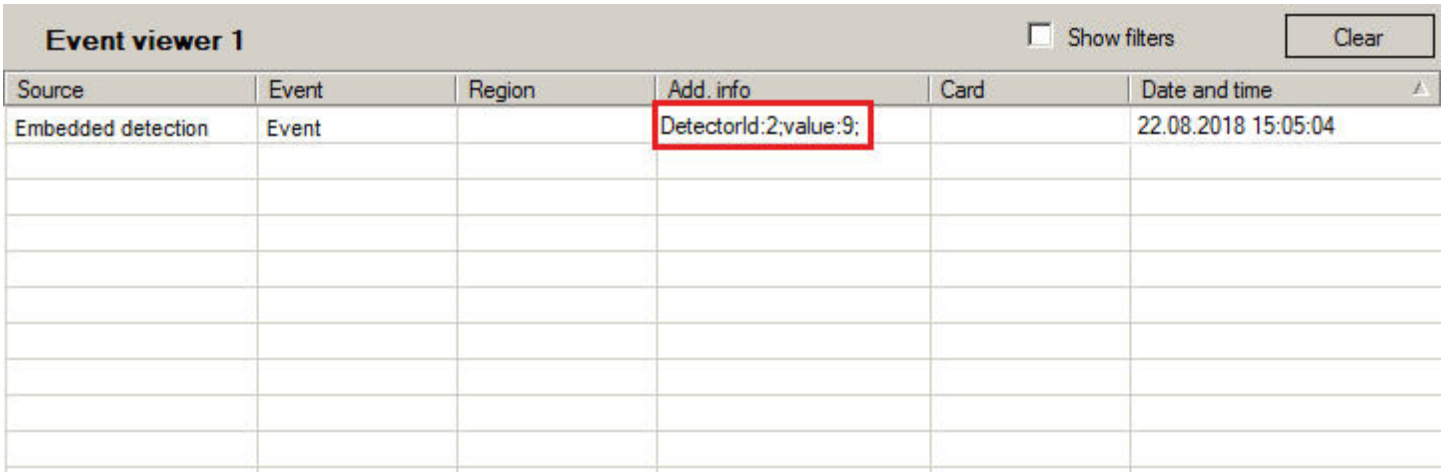
Configuring Intellect to receive the events from the Bosch camera's visitors counter
To configure the *Intellect* to receive the events from the Bosch camera's visitors counter, do the following:

1. Create and configure the **Embedded detection** object based on the **Camera** object which corresponds to the Bosch FLEXIDOME IP dynamic 7000 VR IP camera. If you use the Camera discovery tool, this object will be created automatically. If you create this object manually, it is necessary to configure it (see Creating embedded detectors and Configuring embedded detectors).

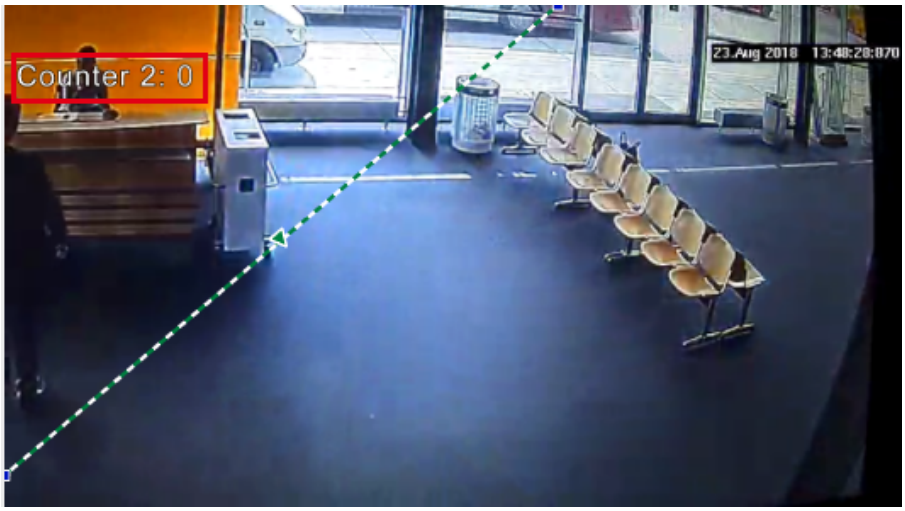


2. Create and configure the **Event viewer** object based on the **Display** object on the **Hardware** tab of the **System settings** dialog box (see Configuring the Event Viewer interface object).

Using the Bosch camera visitors counter in Intellect
The *Intellect* **Event viewer** interface window displays the **Event** (DETECTED) events from the **Embedded detection** (CAM_IP_DETECTOR, see CAM_IP_DETECTOR Embedded detection) object. The **Add. info** field (param0 parameter) displays the detection tool identifier and the counter value, for example, “DetectorId:2;value:9”, where DetectorId:2 is the detection tool identifier, and value:9 is the number of objects counted.



The detection tool identifier is displayed in the camera web interface in the video preview area.



The events from the Bosch camera's visitors counter can be used in macros, programs, and scripts — see Examples of scripts in JScript language.

23.3.2.7.5 Face detection tool

23.3.2.7.5.1 General information on face detection tool

Face detection tool recognizes «faces» objects in the controlled zone. While detecting the «faces» in the frame the following can be observed:

1. A face is dynamically framed on the frame;
2. If Face Intellect is installed, then there is possibility to record a frame with a face to the file of .bmp format to the folder «<Face-Intellect>\ Bmp\ person\».

Note.

The **External capture** and **Maximum performance** options are only used with *Face-Intellect* installed. For more details please refer to Face intellect. Administrator's Guide. The most relevant version of this document is available in the AxxonSoft documentation repository.

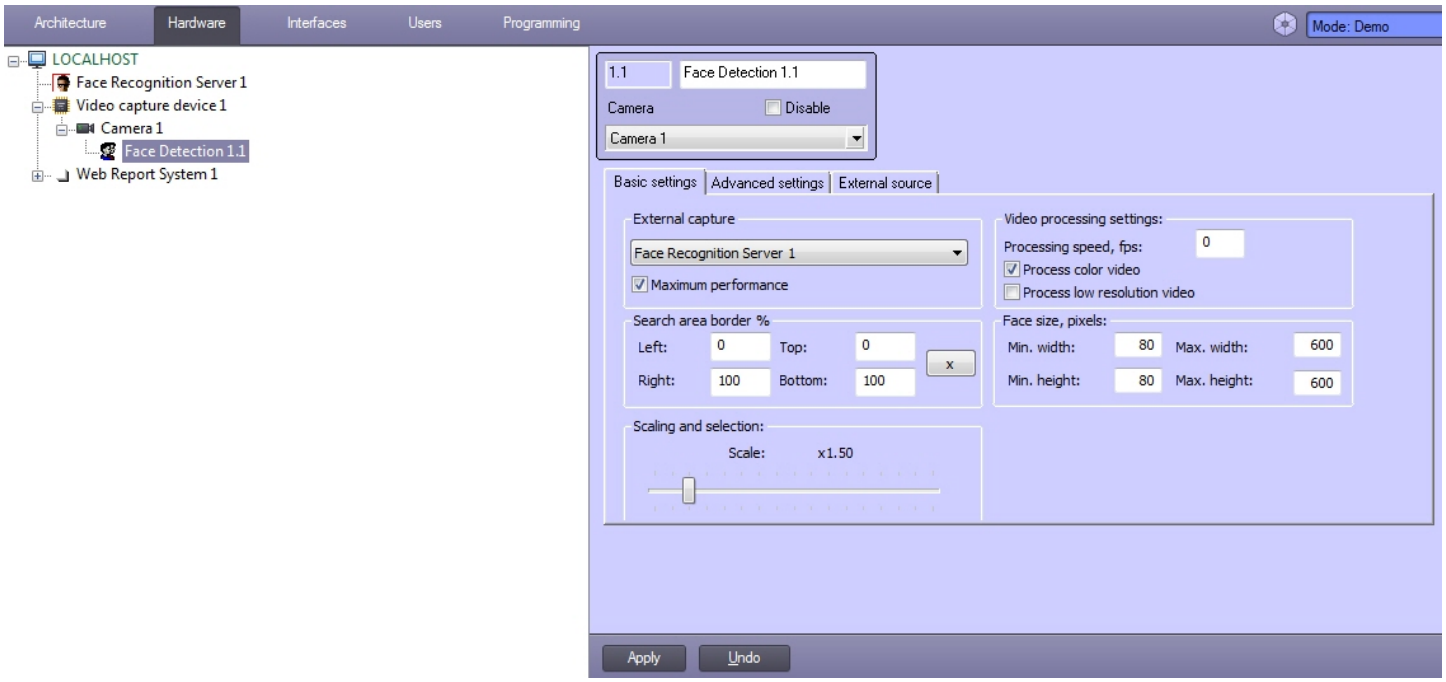
23.3.2.7.5.2 Requirements to video parameters while using face detection tool

When a face detection tool is in use, the following requirements must be met:

1. Minimum linear dimensions of a face to be detected are 24 pixels.
2. Maximum speed of a face to be detected is not to be more than a half of linear dimensions in pixels per frame (i.e. face overlapping between two adjacent frames must be not less than half-width and half-height of face).
3. A detection tool needs 8 frames to confirm face detection – otherwise, a face detection message won't be sent.

23.3.2.7.5.3 Configuring Face detection tool

The **Face Detection** object is created on the basis of the **Camera** object in the **Hardware** tab of **System settings** dialog box.

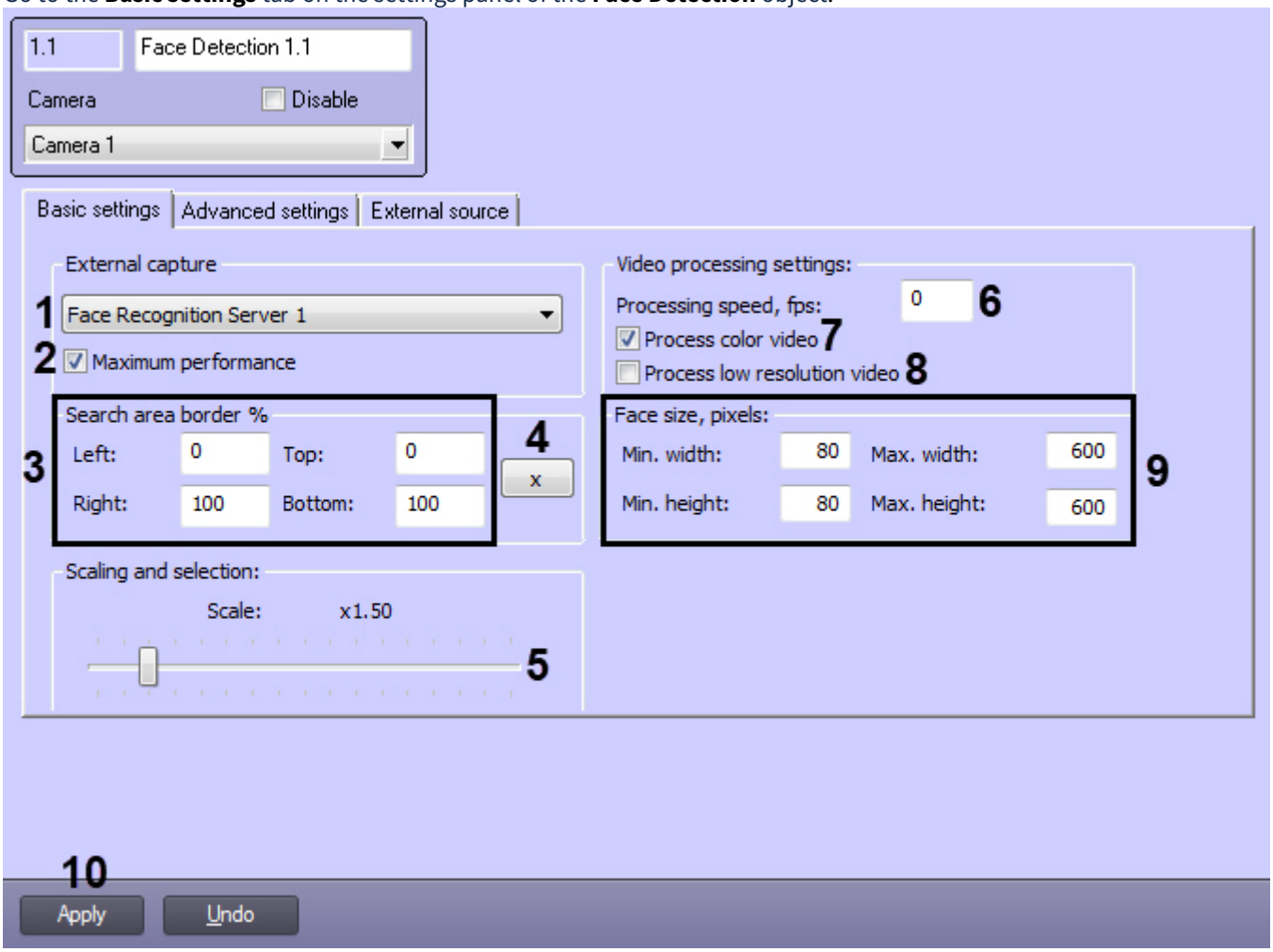


Note

The video image resolution received by the **Face Detection** from the camera can be changed using the **ResizeWidth** registry key (for details, see Registry keys reference guide).

Face Detection tool basic settings
Configure the basic settings of the *Face Detection* module as follows:

1. Go to the **Basic settings** tab on the settings panel of the **Face Detection** object.



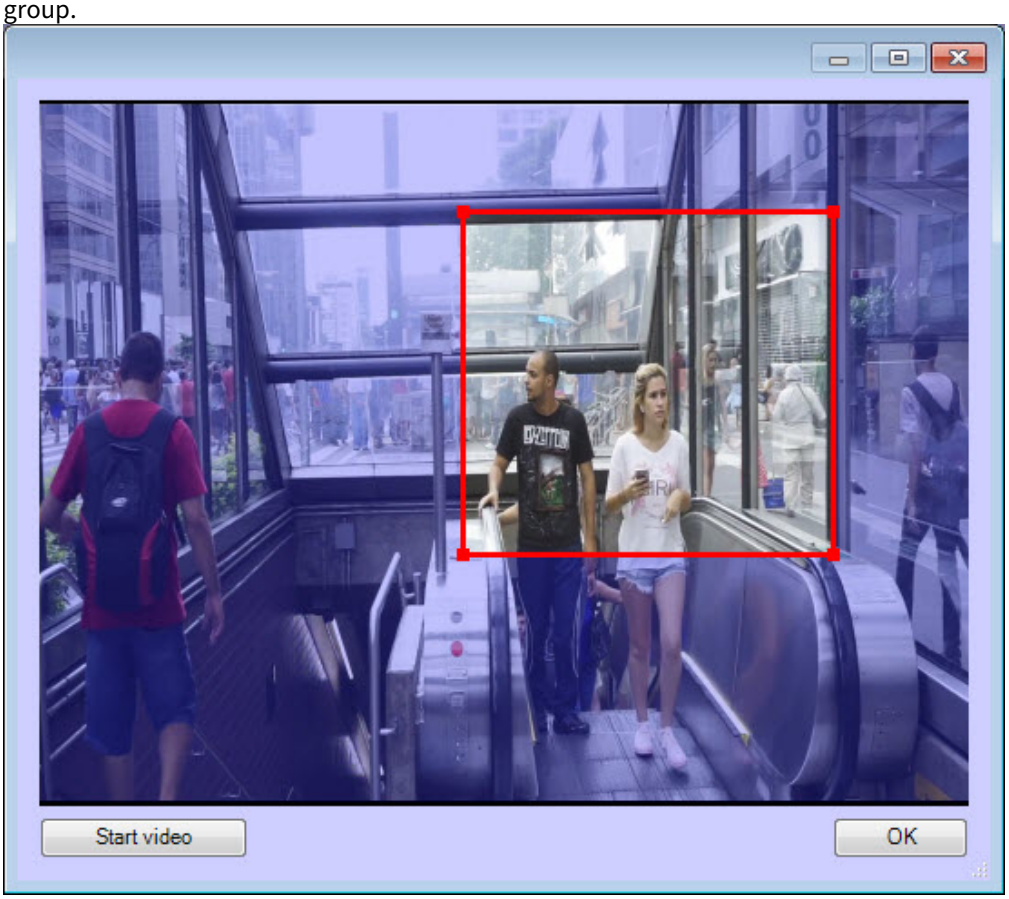
2. There are several variations of the face detection operation depending on the setting of the external capture and Face Recognition Server (**1**):
   a. External capture is NOT selected and the detection is NOT added to any of the Face Recognition Server channels. In this case, only capturing of photos of faces detected by Intellect software capturing is performed, and generation of vectors is not performed. This option is not for *Face Intellect*.
   b. External capture is NOT selected but the detection is added to any of the the Face Recognition Server channels. In this case, capturing and saving of photos of faces detected by Intellect software capturing, generation of vectors and recording them to database are performed. This option does not allow face recognition (while search and visitor counting are available).
   c. External capture is selected but the detection is NOT added to any of the Face Recognition Server channels. In this case, the photos of faces captured by the face recognition modules (see Structure of the Face Intellect software package), are captured and saved, and the vectors are generated, but the vectors are not saved in the database. This option is only suitable for use in scripts.
   d. External capture is selected and the detection is added to any of the Face Recognition Server channels. In this case, the photos of faces captured by the face recognition modules (see Structure of the Face Intellect software package), are captured and saved, and the vectors are generated and recorded to the database

   The external capture is recommended for use. From the **External capture** drop-down list select the Face Recognition Server with the help of which the face capturing with the subsequent generation of a vector (if the **Create FIR in detection unit** checkbox is set on the settings panel of the corresponding Face Recognition Server object – see Configuring the Face Recognition Server object) and saving of photos will be performed.

Note.

Proper configuring of the face recognition server selected as external capture is performed with the help of the Cfgedit.exe utility (detailed information about this utility see in the Cfgedit.exe utility for configuring the Cognitec face recognizer section).

3. The **Maximum performance** mode is enabled by default (**2**). This mode allows improving the quality of face capture and recognition by using all available processor cores and increasing the RAM consumption. When this mode is disabled, the memory consumption will decrease, but faces can be missed at capturing.
4. Set the face search area border on the video image by specifying the required values in percent in the corresponding fields (**3**), or by clicking the button (**4**) and using the interactive interface. After you click the button, the window with the corresponding video camera image will open. To set the face search area border, click the **Stop video** button at the required time, select the required area using the left mouse button, and then click **OK**. The specified face search area border values will be automatically entered in the **Left**, **Right**, **Upper** and **Lower** fields of the **Search area border %** group.



Attention!

Setting the face search area border is available only if the *VA* or *VideoIntellect 1.1* face recognition modules are used.

5. Set the **Scaling and selection** slider (**5**) to the position corresponding to the required scale of the captured face in the frame for recording and highlighting the face with a dynamic frame. The current scale value is displayed in the field above the slider and ranges from 1 (only the captured face is recorded) to 5 (the whole frame is recorded).

Note

This setting is relevant only if *Face Intellect* is installed.

6. In the **Processing speed, fps** field (**6**), specify how many fps from the video stream are processed by the Face detection program module. This parameter is necessary for reducing the load on the Server.
7. If it is necessary to convert the color video image to black and white image to generate the vectors by the black-and-white frames, then uncheck the **Process color video** checkbox (**7**).

Important!

Generation of vectors by black-and-white frames is supported by *VA* and *VideoIntellect 1.1* face recognition modules only. It reduces the CPU load, insignificantly affecting the face capture and recognition quality.

8. By default the Face detection tool processes a video with the resolution set for the **Camera** parent object. To process a video with 320x240 pixels resolution, set the **Process video in low resolution** checkbox (**8**).

Note.

Enabling this option reduces the load of the Server's processor, but the probability of face capture also reduces.

Attention!

The **Process video in low resolution** setting is not relevant in case, when a high resolution is set for a **Camera** parent object. Also this settings is not in use if the *VA* or *VideoIntellect 1.1* module is applied for face capture.

9. Set the minimum and maximum width and height of the face on the video image in pixels in the corresponding fields of the **Face size, pixels** group (**9**).

Note.

If the specified minimum dimensions differ significantly from the actual ones, then the faces will not be captured. For example, if the video contains large faces (15-30%), then if you set the minimum size to 5%, and the maximum size to 80%, then the faces will not be detected. However, if you specify a minimum size of 12% and a maximum size of 80%, the faces will be captured.
Thus, if the detection tool is configured to capture small faces, then it cannot detect large ones, and vice versa.

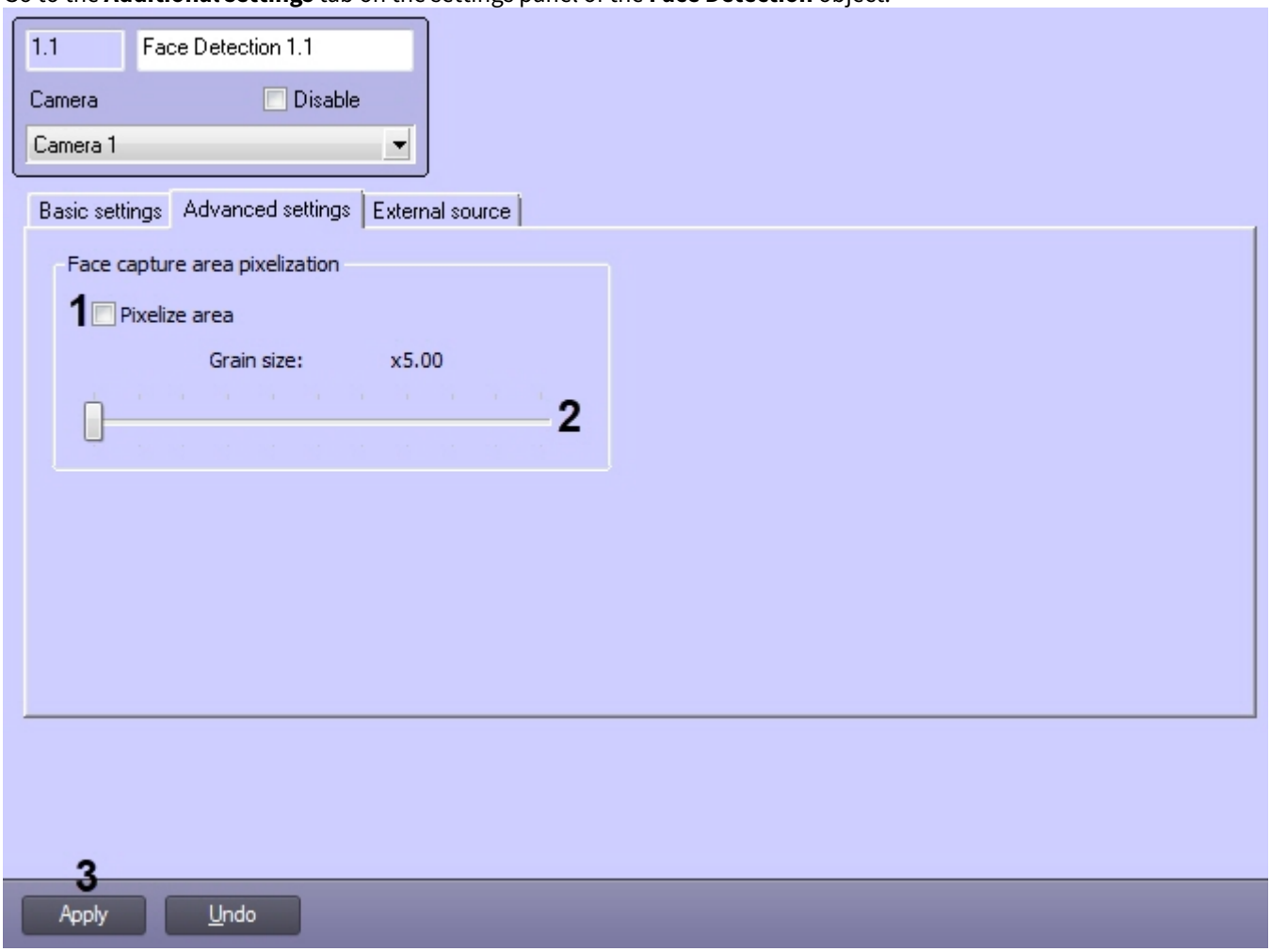
Note.

If all face sizes are set to 0, the Face Detection tool uses similar parameters set on the **Face Recognition Server** object settings panel (see Configuring the captured face size for recognition).

10. To save the changes click the **Apply** button (**10**).

Face Detection tool advanced settings
Configure the advanced settings of the *Face Detection* module as follows:

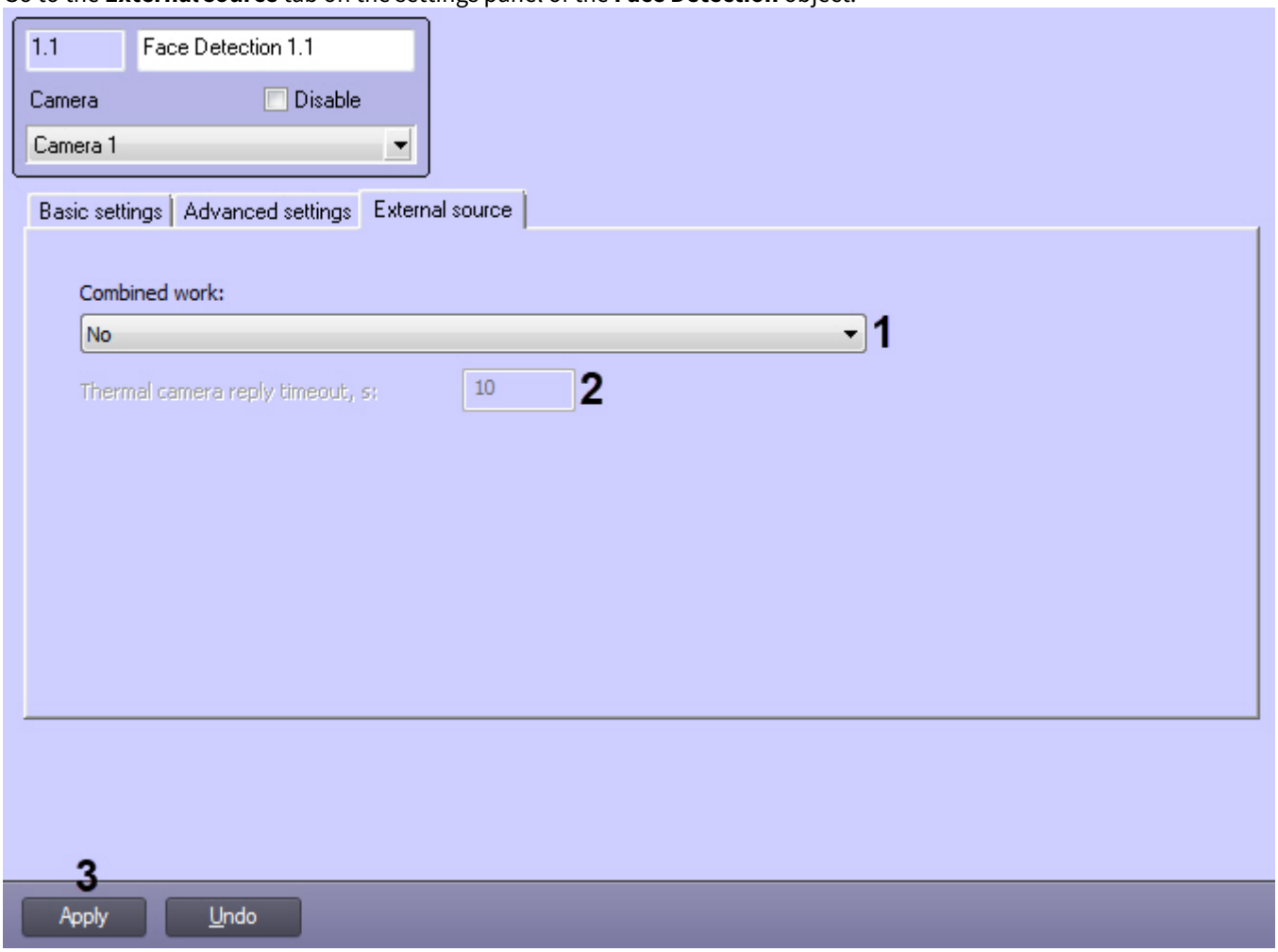
1. Go to the **Additional settings** tab on the settings panel of the **Face Detection** object.



2. To pixelate the part of video image in which the face was recognized, set the **Pixelize area** checkbox (**1**).
3. Set the **Grain size** cursor in position corresponding to the pixelation grain size in pixels (**2**).
4. To save the changes click the **Apply** button (**3**).

Configuring the Face detection tool combined work with thermal camera or external system
Configure the *Face detection* module operation with a thermal camera or an external system as follows:

1. Go to the **External source** tab on the settings panel of the **Face Detection** object.



2. From the **Combined work** drop-down list (**1**) select the combined operation mode:
   - **No** - combined operation mode is not used.
   - **Combine with thermal camera temperature** - receiving the temperature and coordinates of a captured face frame from the thermal camera. A photograph of a captured face will be obtained from the capturing camera. If this mode is selected, the following setting become available:
     - **Thermal camera reply timeout, s** (**2**) - sets the timeout in seconds for receiving data from the thermal camera.

       Note

       The FIND_PERSON event will be generated only when the temperature is received from the thermal camera or after the time specified in the **Thermal camera reply timeout, s** parameter.
   - **Get photo from thermal camera** - receiving the temperature and photos of a captured face from the thermal camera.
   - **Get photo and metadata from external system** - receiving the temperature and photos of a captured face from a thermal camera or *Axxon Next*.
3. Click **Apply** (**3**) to save the changes.

23.3.2.8 Configuration of multistream video

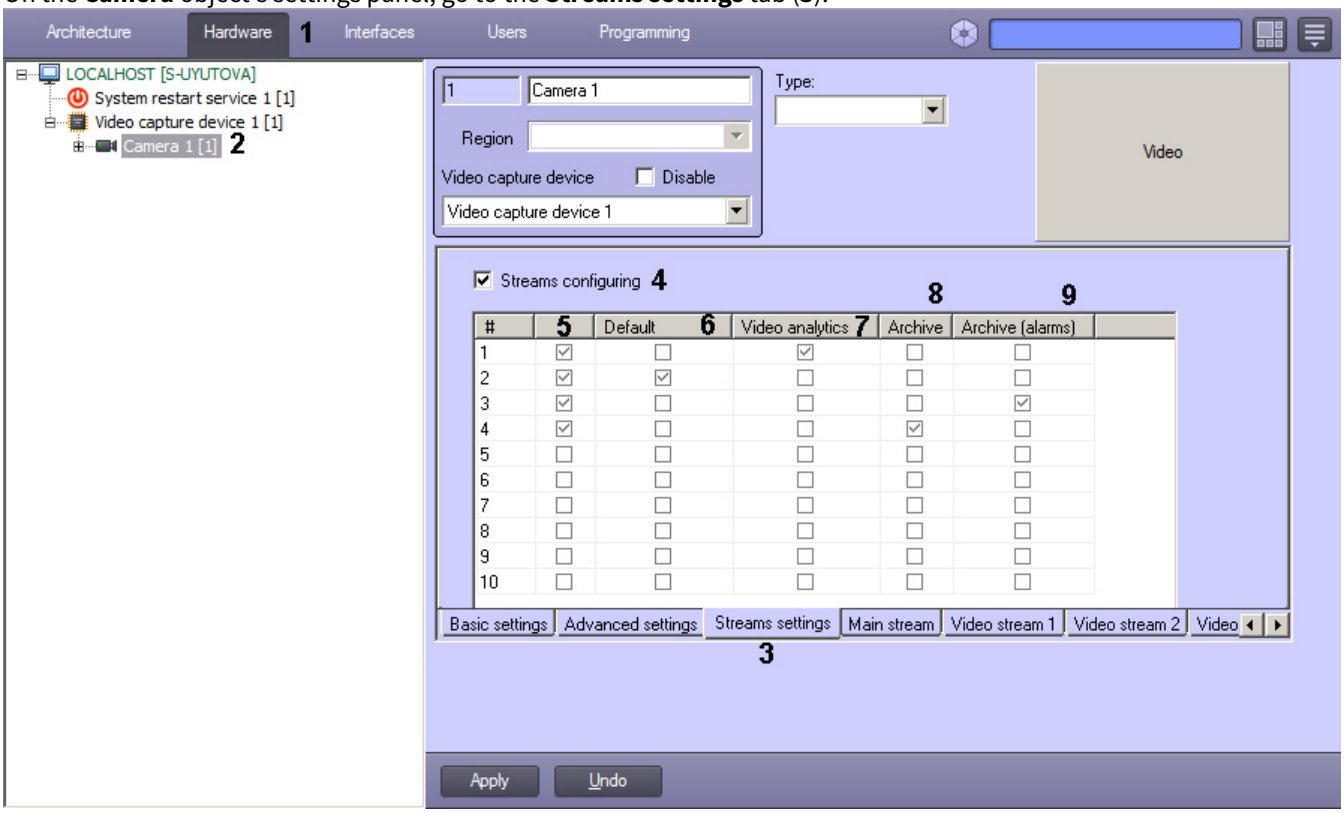
The *Intellect* Software System supports the use of different streams from a video camera for display on the Video Surveillance Monitor, archiving, and video analytics. For example, this feature lets you display a low-quality video signal on the monitor while writing a high-quality signal to the archive, reducing the load on the Client.

To use multistreaming over the ONVIF protocol, select ONVIF 2.X brand and 1-channel-multistream model when creating an ONVIF device (using Camera discovery tool, see Installing and configuring security system components guide). Two streams will be available.

> **Note.**
>
> There are instances in multistream mode where changes to some video stream parameters may affect others–without any user notification. This is related to the video camera's model and firmware, because certain cameras do not support user selection of the resolution, codec, etc.

To configure multistream settings, do the following:

1. Go the **Hardware** tab (**1**) in the **System Settings** dialog window.
2. In the object tree on the **Hardware** tab, select the previously created **Camera** object (**2**) that corresponds to the video camera for which multistream mode is to be configured. The right part of the **Hardware** tab shows the settings panel for the selected object.
3. On the **Camera** object's settings panel, go to the **Streams settings** tab (**3**).



4. To enable multistream mode, check the **Streams configuring** box (**4**).
5. Check the boxes next to the video streams to enable them (**5**).
6. Check the box in the **Default** column (**6**) in the line of the stream number that should be used in the following cases:
   a. To display video both locally and on remote clients;
   b. To send to remote clients, including the Videogate, that can record this video stream;

   > **Note.**
   >
   > If a specific video stream is requested via Video gate, then the requested stream is send to Video gate, not the **Default** stream.

   c. When a video stream is not specified for the video request.

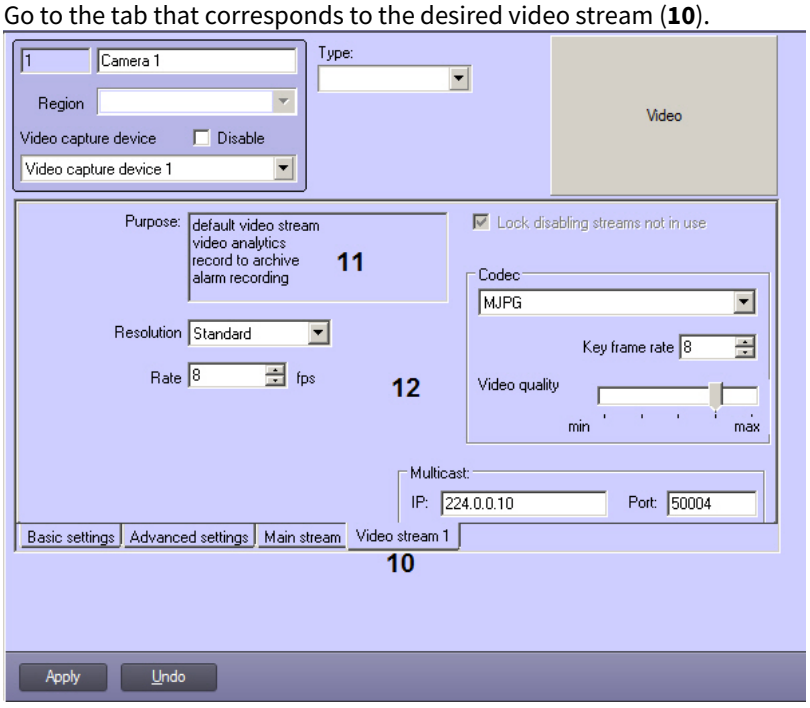
   > **Note.**
   >
   > This stream is used, for example, to display video on the Video Surveillance Monitor if a default stream has been selected for the camera or for displaying video on the Video Surveillance Monitor of the web server.

7. Check the box in the **Video analytics** column (**7**) in the line of the stream number that should be used for the LPR channel, the main motion detection tool, zone detection tools, tracking detection tool and face detection tool (if an external recognizer is not used).
8. Check the box in the **Archive** column (**8**) in the line of the number of stream that is to be recorded to the archive not upon alarm – the continuous recording is performed.
9. Check the box in the **Archive (alarms)** column (**9**) in the line of the number of stream that is to be recorded to the archive upon alarm.
   This stream is also used for Backup archive.

> **Note.**
>
> If different streams are selected for recording to the archive upon alarms and continuous recording, recording is performed non-stop and detection tools are enabled, then upon alarm recording of the current archive fragment is stopped in the continuous recording stream and recording of a new fragment starts in the alarm recording stream. When the alarm ends and after pre-alarm recording the continuous recording with the corresponding stream resumes.
> If the same stream is selected for recording to the archive upon alarms and continuous recording, then recording of current fragment is not stopped upon alarm.

> **Note.**
>
> If pre-alarm recording is configured, then when different streams are selected for recording to the archive and continuous recording, some archive recordings overlay as the following video fragment starts before the previous ends.

10. Configure the video streams as follows:
    a. Go to the tab that corresponds to the desired video stream (**10**).



    b. The **Purpose** field (**11**) displays a description of how the video stream is used.
    c. Specify the video stream's parameters (**12**) (see The Settings panel of the Camera object).

> **Attention!**
>
> Following video streams are available for Axis cameras:
> 1. Receiving of H264/MJPEG/MPEG4 video. It is available to specify settings of video stream using the *Intellect* software package facilities. Settings are specified in the **Video stream 1** tab.

2-4. Stream corresponding to “Quality”, “Balanced” and “”Bandwidth” profiles. These profiles configure in the camera web-interface. **Video stream 2** corresponds to the “Quality” video stream, **Video stream 3** corresponds to the “Balanced” video stream, **Video stream 4** corresponds to the “Bandwidth” video stream.

d. Repeat steps a-d for the remaining video streams.

11. Click the **Apply** button.

This completes the process of configuring multistream mode.

23.3.2.9 Video record from computer monitor

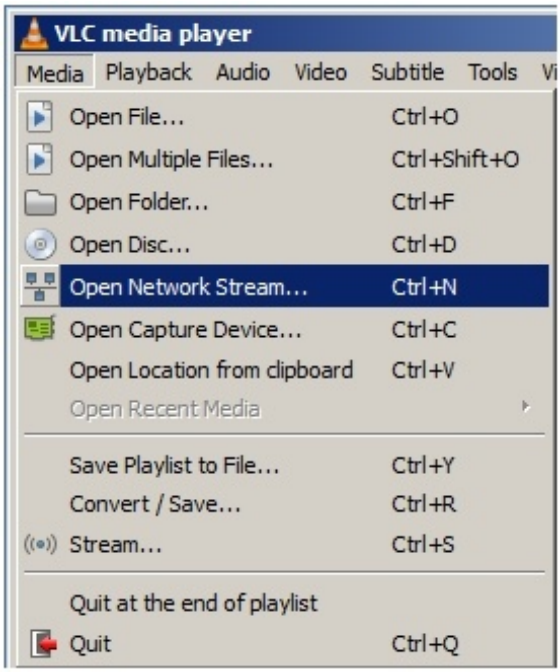
Record of video from computer monitor is performed to control operator actions. Video from computer monitor can be transmitted to the Intellect software package by general protocols using external programs, for example:

1. By RTSP protocol using the VLC Media Player which is available to download from the http://www.videolan.org/vlc/ web-site.
2. By ONVIF protocol using the ScreenOnvif program which can be got in the http://screenonvif.com/en web-site.

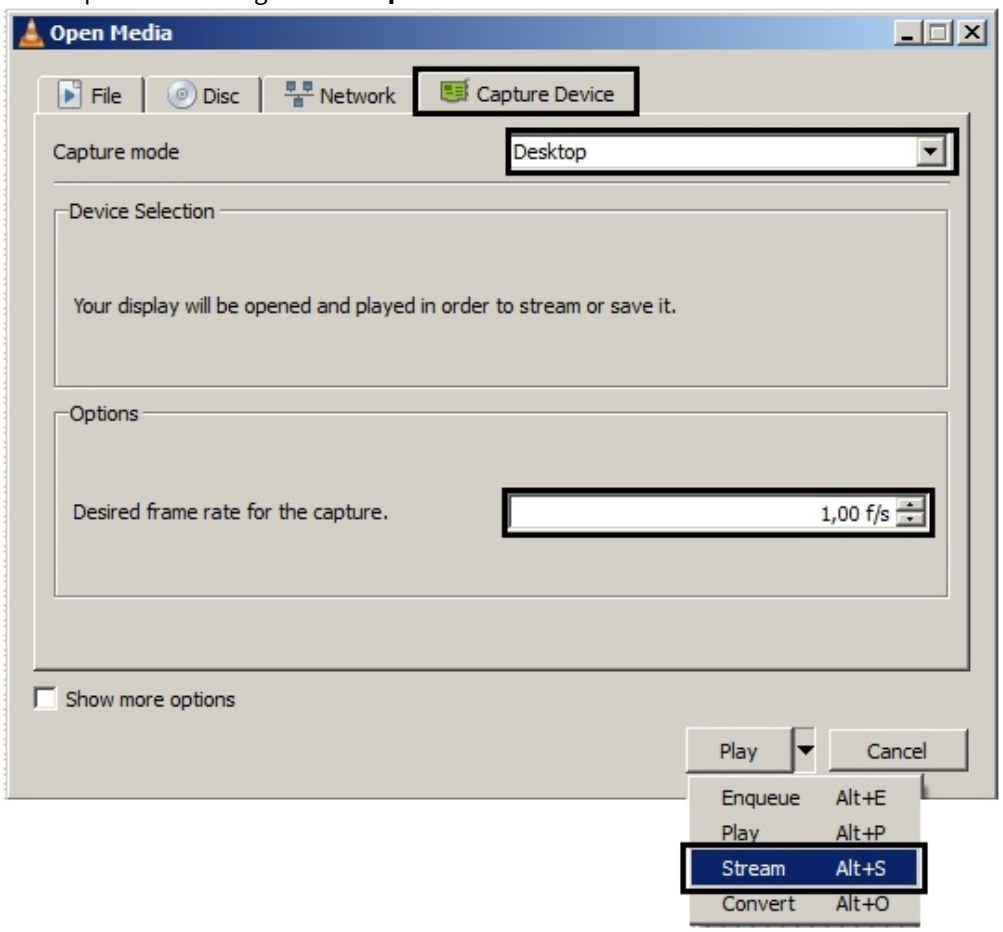
Example of the VLC Media Player configuring for transmitting video from computer monitor to the *Intellect* by the RTSP protocol is presented in this section. Configuring of the Intellect software package to receive and record this video stream is performed by standard means as described in the Configuring rtsp Server module and Selecting the disks for video archive storage sections.

Configuring the VLC Media Player for transmitting video from computer monitor to the Intellect software package by the RTSP protocol is performed the following way:

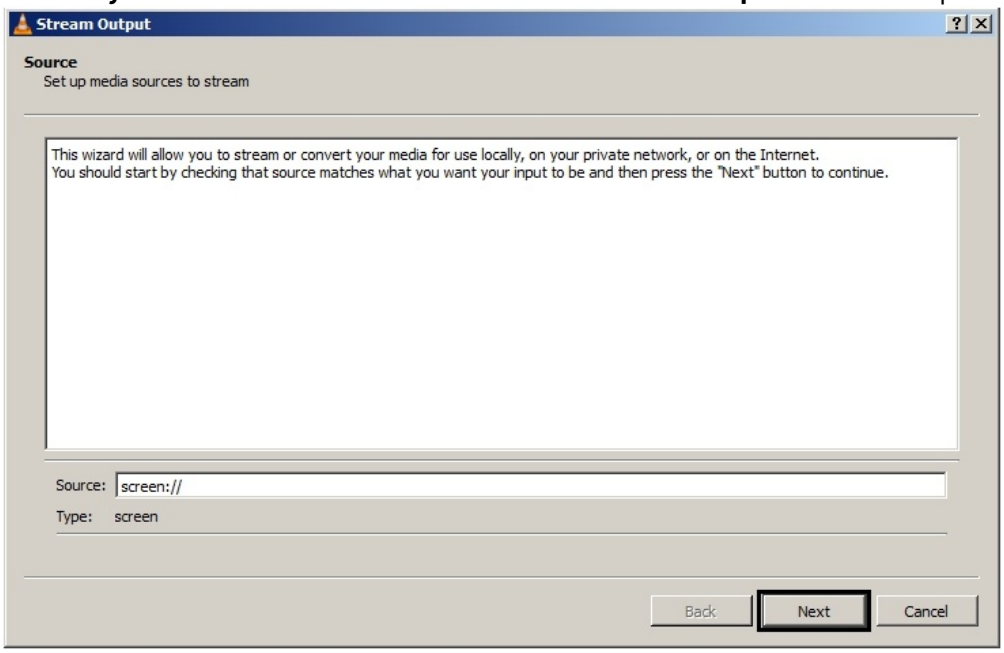
1. Run the VLC Media Player.
2. Select the **Open Network Stream item...** in the **Media** menu.



3. In the opened window go to the **Capture Device** tab.

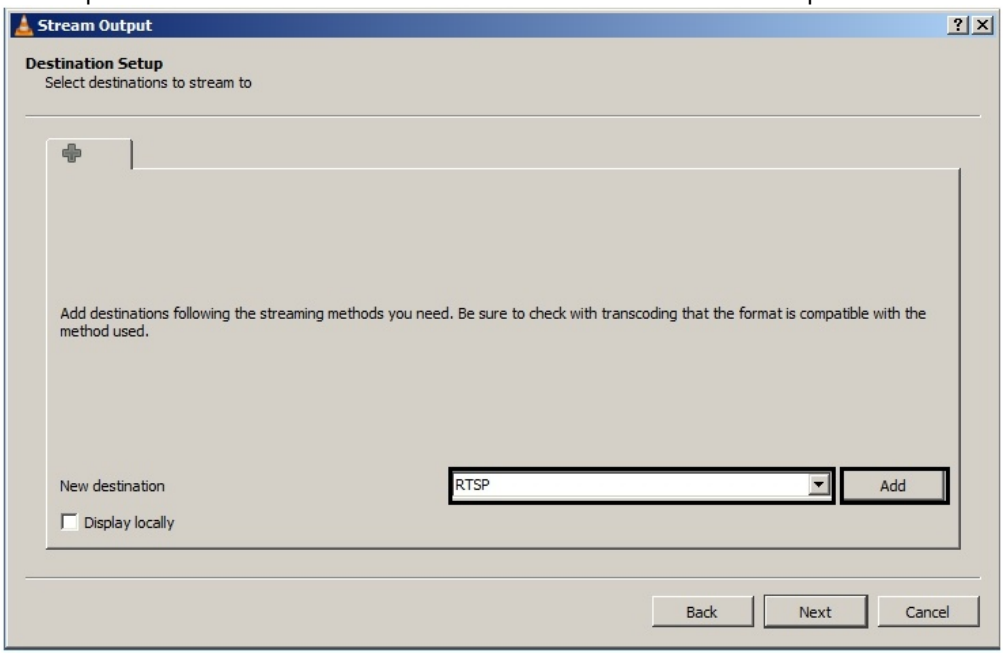


4. In the **Capture mode** drop-down list select the **Desktop** value.
5. Set the desired frame rate for the capture in the corresponding field.
6. In the **Play** list select the **Stream** value. As a result the **Stream Output** window will open.

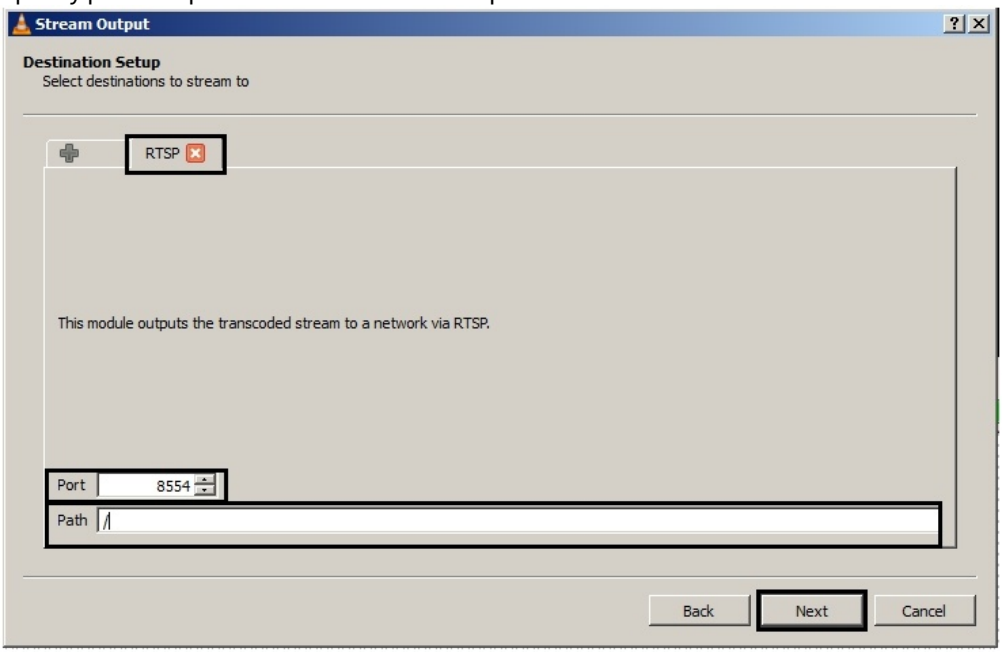


7. Click the **Next** button.

8. In the opened window select the **RTSP** value in the **New destination** drop-down list and click **Add** button.

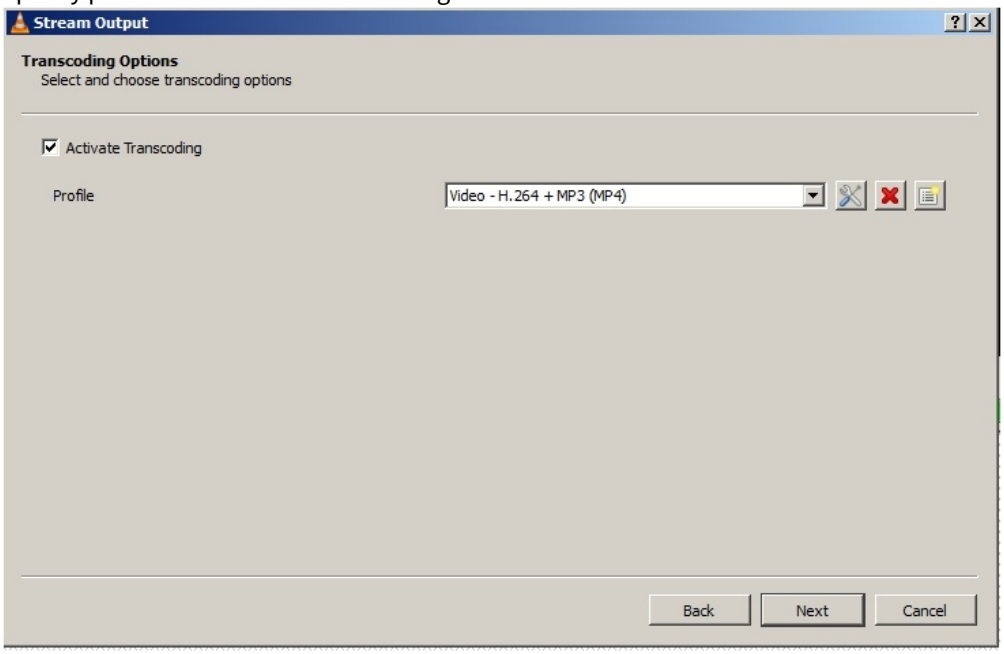


9. Go to the **RTSP** tab.
10. Specify port and path to the stream if it's required.

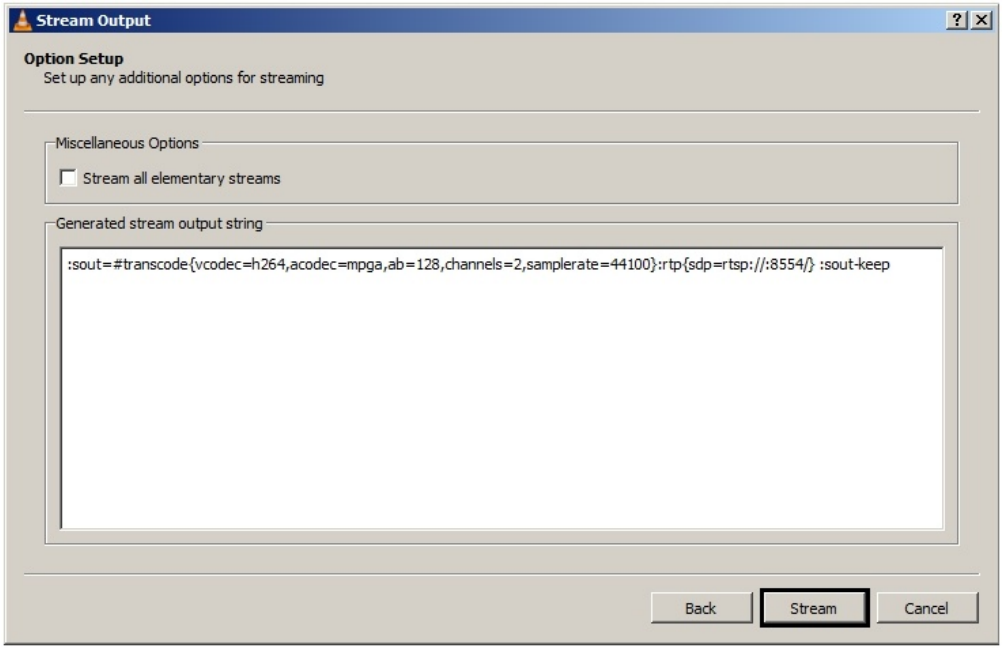


11. Click **Next** button.

12. Specify parameters of video transcoding and click **Next** button.



13. Click **Stream** button in the opened window.



After that configure receiving of the RTSP stream and its record to the archive in the Intellect software package – see Configuring multimedia receipt using RTSP protocol and Selecting the disks for video archive storage sections.

Configuring of the VLC Media Player for transmitting video from computer monitor by the RTSP protocol to the Intellect software package is completed.

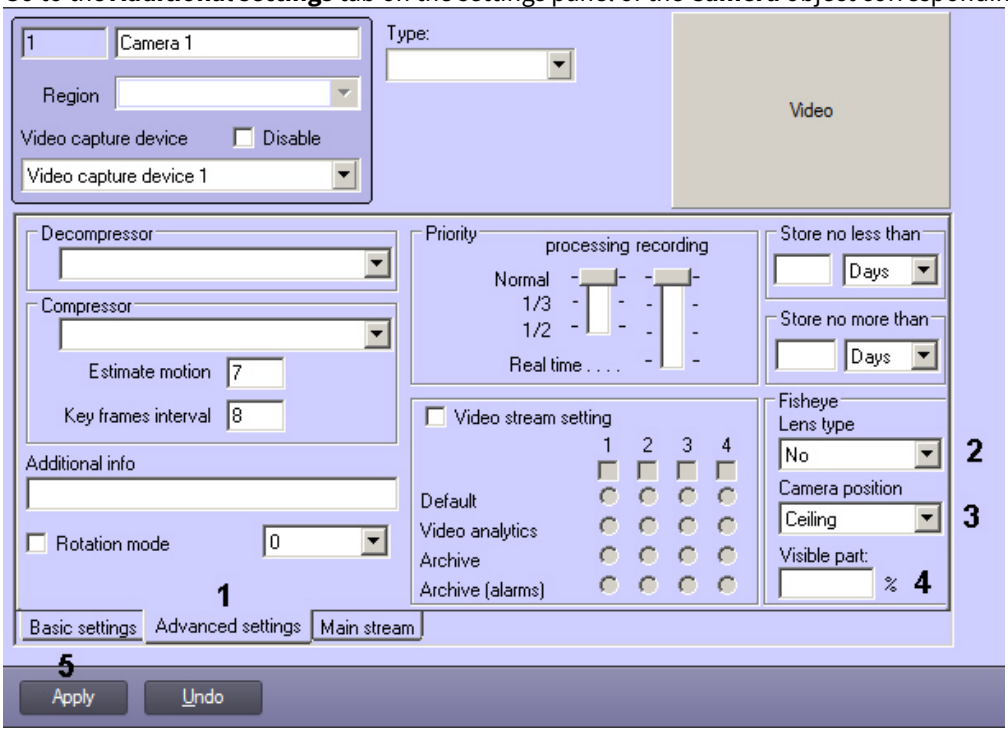
23.3.2.10 Configuring fisheye cameras

In the Intellect PSIM, you can correct (dewarp) video from fishey cameras in the Video Surveillance Monitor as well as in all camera windows opened through other interfaces, for instance,

- through the Event Log (refer to Event control via Event viewer),
- during search by captions (refer to Search in the captions database), etc.

Conversion of video from fisheye cameras when displaying it on the video surveillance monitor is possible in *Intellect.* The conversion type is selected when adding a camera to the Monitor (see Selecting and configuring video cameras). To use this feature specify the lens type and fish eye camera location when configuring it in *Intellect*:

1. Go to the **Additional settings** tab on the settings panel of the **Camera** object corresponding to the fisheye camera (**1**).



2. Select the **Standard fisheye lens** value in the **Lens type** dropdown list if this is a fish eye camera (**2**). If a camera with anamorphic lens is in use, then select its type in this dropdown list.
   With some settings there can be some artifacts at the top of video for a standard fisheye lens. If there are such artifacts , then select the **Autocalibration** in this dropdown list.

   > **Important!**
   >
   > Video will be calibrated every time the settings are applied.

3. In the **Camera location** dropdown list select the value corresponding to the camera (**3**).
4. Frame edge areas can degrade or loss information as a result of dewarping. By default, such degraded edges are cut off, i.e. not displayed on the Video Surveillance Monitor. Default visible frame part is 75% for the **Ceiling** position and 66% for the **Wall** position. To increase or decrease the displayed frame area, change the value of the **Visible part** (**4**) parameter correspondingly. The value of this parameter is chosen experimentally, depending on the camera.
5. Click the **Apply** button (**5**).

The fisheye camera is now configured.

23.3.3 Configuring audio subsystem

23.3.3.1 General information on configuring audio subsystem

In the video surveillance systems, based on INTELLECT™ software, the audio subsystem contains software modules and hardware devices, used to receive and transmit audio (i.e. support for bidirectional audio), as well as digitize, process, record and play back audio signals from video surveillance and audio monitoring system microphones.

Audio subsystem hardware includes optionally:

1. video capture cards;
2. standard soundcards;
3. multi-channel soundcards;
4. audio capture IP-devices;

5. microphones;
6. loudspeakers and headphones.

Audio subsystem software includes:

1. components for configuring the audio signal digitizing devices;
2. components for recording digital audio signals;
3. components for transmitting digital audio signals to Remote Workplaces and remote servers;
4. components for digital audio signals playback.

Requirements for audio input units
Audio player operation

23.3.3.1.1 Audio digitizing devices

On the page:

- Video capture cards
- Standard soundcards, microphones, loudspeakers and headphones
- Multichannel audio capture devices
- IP-devices

Audio capture and digitizing devices are used to receive and process analog audio signals from connected microphones.

To enter and digitize an audio signal, the servers, created in the INTELLECT™ software, use:

1. video capture cards;
2. standard soundcards;
3. multi-channel soundcards;
4. IP-devices.

23.3.3.1.1.1 Video capture cards

Video capture cards, used as audio capture devices, support reception and digitization of audio signals. Video capture cards don't support audio signal output to headphones and loudspeakers.

Video capture cards digitize audio signals in conjunction with processing and digitization of video signals. Audio and video signals are processed independently.

The facility to receive and digitize audio signals depends on the server hard- and software configuration, on the type of video capture cards and the key file parameters.

23.3.3.1.1.2 Standard soundcards, microphones, loudspeakers and headphones

Standard soundcards are used for audio capture and audio output devices. They receive and digitize audio signals, reconvert digitized audio signals and feed them to the loudspeakers and headphones.

INTELLECT™ software system supports the audio signal sample rate range, corresponding to the standard soundcard and restricted to a 48 kHz frequency.

Usually up to 2 microphones and 1 headphone are used with a standard soundcard.

23.3.3.1.1.3 Multichannel audio capture devices

Multichannel audio capture devices are PCI cards (for example, MidiMan Delta, Comart Hera, Olkha 9P) or outer hardware and software modules (for example, Echolot USB-32), used for digitization and processing of 2 or more audio signals. For the list and features of INTELLECT™ software compatible multichannel audio capture devices, see the Integration section on the site of AxxonSoft company: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.

Multichannel audio capture devices reproduce sound and digitize audio signals in parallel, or sound is reproduced by the standard sound cards. The Audio signal sample rate range depends on the audio capture device type. The INTELLECT™ software system sample rate range, available to the installed card, is restricted to a 48 kHz maximum value.

23.3.3.1.1.4 IP-devices

The INTELLECT™ software system supports audio signals reception, digitization, processing and playback using audio capture IP-devices. IP-cameras and IP-servers' built-in microphones or the external analog microphones, connected to IP-devices, may be used for receipt, digitization and processing of audio signals. Outer loudspeakers or headphones, connected to IP-servers may be IP-devices used for playback of audio signals. For the list of INTELLECT™ software compatible IP-devices for audio signals reception, digitization, processing and playback see the Integration section on the site of AxxonSoft company: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.

The audio signal sample rate range depends on the IP-device type, which is used as the audio capture device. The sample rate range, available to the installed card, is restricted to a 48 kHz maximum value.

Registration of audio cards and microphones in INTELLECT™ software

23.3.3.1.2 Configuring the digitization devices for audio signals

Audio capture and digitizing devices are configured via the **System Setup** dialog box.

Audio capture and digitizing devices are configured by setting the audio signal sample rate and sound volume.

The sample rate is the same for all audio signals, processed by a common device; it can't be individually set for every audio signal.

Until *Intellect* 4.10.1 audio playback and video recording were performed in the PCM format with digitization rate not more than 8000 Hz. Since *Intellect* 4.10.2 the number of hertz depends on the selected rate on the settings panel of the **Audio card** object and playback of audio from IP device is performed using any codec selected on the camera and supported by this device in the Drivers Pack. See Requirements for audio input units for the list of supported codecs.

Volume is adjusted after the audio signal has been digitized by the audio capture device. With INTELLECT™ software you can restrict volume to a certain value or switch on the automatic gain control (AGC). This levels out the sound volume across the range to a constant level.

Configuring audio signals digitization and processing

23.3.3.1.3 Digitized audio signal recording

Audio signals archiving provides post-event analysis of evidence footage.

Audio recording can be performed:

1. As an audio and video synchro recording;
2. Independently, by Operator command.
3. As a sound activated audio recording.

In synchro recording mode, audio recordings are combined with video recordings; they are stored in the videoserver archive.

When audio signals are recorded by Operator command or by sound activation, audio recordings are separately stored in the audio archive.

Once the archive disk(s) is full, the archive is overwritten.

Configuring audio signals recording

23.3.3.1.4 Digital audio signal transmission to Remote Workstations and servers

INTELLECT™ software enables to transmit audio signals to Remote Workstations on IBM PC's, connected to the videoserver via local TCP/IP net, to remote servers and to mobile clients on the basis of iOS or Android.

Both real-time and archive audio signals may be transmitted to Remote Workstations.

23.3.3.1.5 Audio signal playback

Audio signal playback is performed on Remote Workplaces with the use of the **Video surveillance monitor** or **Audio player** interface objects.

Realtime audio monitoring and synchro audio and video playback is performed by the video monitor. Nonsynchronous audio recording cannot be replayed by the video monitor.

The Audio player allows to playback audio signals from microphones, and to replay audio recordings. Audio recordings, synchronous to video recordings, cannot be replayed by the Audio player.

A standard soundcard installed on a Remote Workstation or remote server and configured by INTELLECT software, with microphones or loudspeakers attached to its output, is necessary to play back audio signals.

Configuring audio playback

23.3.3.2 Registration of audio cards and microphones in INTELLECT™ software

Audio capture cards are registered in the INTELLECT™ software by creating and setting up **Audio card** objects. **Audio card** objects are created on the **Hardware** tab on the base of the **Computer** objects (see Installing and configuring security system components guide, the Audio subsystem configuration section).

Listening to the audio signal through microphones

23.3.3.3 Configuring audio signals digitization and processing

23.3.3.3.1 Audio signals sample rate settings

The signal sample rate affects the quality of the audio signal and audio recording size. The higher the audio signal sample rate, the higher the signal quality and, hence, the efficiency of real-time and post-event analysis. When the audio signal sample rate increases, the size of the audio stream, transmitted by the network to Remote Workplaces and recorded to the disk, increases. These factors should be considered while choosing the sample rate of the audio signals.

If audio is to be received from IP devices, then the digitization rate is set on the settings panel of the **Microphone** object in the driver parameters (see Configuring audio acquisition from IP devices section in Installing and configuring security system components guide). The rate set on the settings panel of the **Audio card** object is ignored.

In other cases the digitization rate is set on the settings panel of the Audio card object (see Creating and configuring the Audio card object section in Installing and configuring security system components guide). By default, the audio signals sample rate is set to the minimum value. The sample rate is set for each audio capture device individually and covers any microphone, connected to it. Different sample rate settings for different microphones, connected to the same audio capture device, are unavailable.

23.3.3.3.2 Setting up the audio signal volume amplification

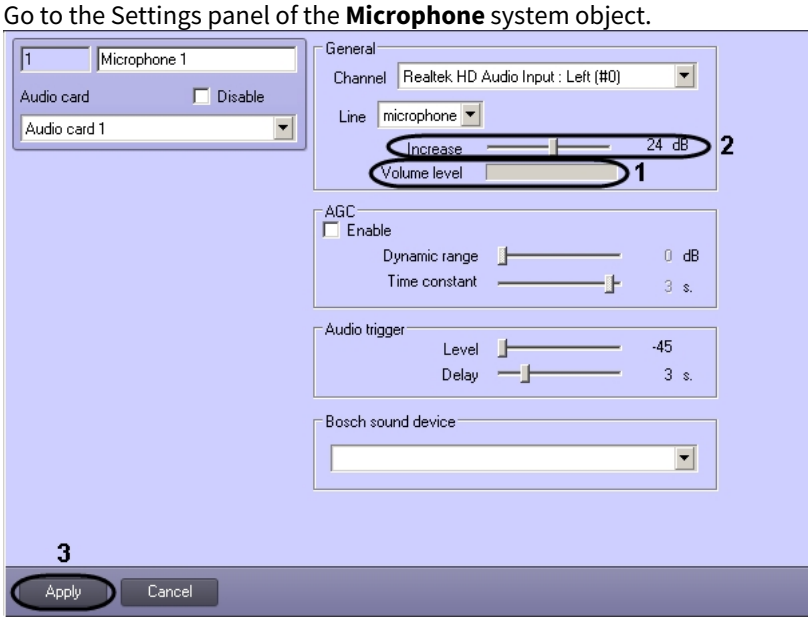
It is possible to amplify incoming audio signals with the help of software.

Note.

If the signal power varies during the audio session, it is necessary to increase the audio signal power by a constant value and to use Automatic Gain Control (AGC).

To amplify audio signal do the following:

1. Go to the Settings panel of the **Microphone** system object.



2. Feed the audio signal with to the microphone. Power level of incoming signal will be displayed on the indicator Level (1).
3. When necessary set the slider **Volume** to the position, corresponding to the required value of amplification (2).The current value in dB is shown in the right field next to the slider.
4. Repeat steps 2 and 3 for the required power level of audio signal.
5. Press **Apply** button to save all the changes (3).

Set of audio signal volume amplification is completed.

23.3.3.3.3 Setting up the Automatic Gain Control for sound cards of Olha line

Automatic Gain Control (AGC) is designed to make the audio signal volume constant. AGC mechanism should be set only with the use of sound cards of Olha line : Olha-9P, Olha-10LP, Olha-12U, Olha-14.

It is recommended to use AGC when input audio signal power is unsteady or when the power of the sound signals, coming from different sources and forming the joint audio signal, differs significantly. AGC levels out the power levels of audio signal components from different sources.

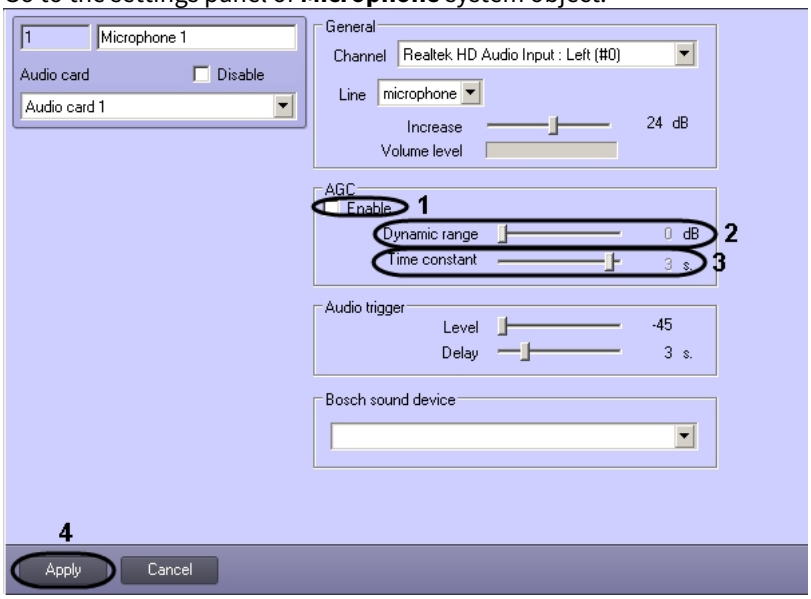
INTELLECT™ software has an AGC adjust option. AGC has two adjustable parameters: a target power level, to which AGC brings different audio signals, and the adjustment time of bringing the signal to the target power level. The second parameter has certain restrictions: the less time it takes to bring the signal to a certain power level, the lower the quality of AGC operation, which may result in greater power level jumps in the processed signal. However a longer adjustment time lengthens the areas where the power of the processed audio signal builds up and decreases. So, processing may bring sizable distortions into the audio signal. Hence, AGC settings depend substantially on the conditions of audio signal formation, and when these conditions have been changed, new AGC settings should be set.

AGC is independently applied to any audio signal from any microphone of the video surveillance and audio monitoring system.

By default, AGC is disabled. The AGC option is enabled for each microphone independently.

To set up the AGC follow the steps:

1. Go to the settings panel of **Microphone** system object.



2. Set the **Enable** checkmark in the **AGC** group.
3. As a result, sliders in the **AGC** group **Dinamic range** and **Time constant** are activated (3).
4. Set the **Dynamic range** slider to the position, corresponding to the desired level of video signal's output power. The current power value, measured in decibels, is shown in the field on the right of the slider .
5. Set the **Time constant** slider to the position that corresponds to the time of bringing the signal to the defined power level. The value of the time constantin seconds, set by the slider, is displayed on the right of it.
6. Click the **Apply** button to save all the changes.
7. It is recommended to check AGC correctness after the settings were made. To do so, use one of the audio playback devices of the INTELLECT ™ software, for example, Audio player object. Audio player should be preset for audio signals playback.
8. If audio signal power is too high, move the **Dynamic range** slider some points to the left. If audio signal power is too low, move the **Dynamic range** slider some points to the right.
9. If increasing and decreasing of audio signal power is perceptible, move the **Time constant** slider some points to the left. If significant jumps in audio signal power are perceptible, move the **Time constant** slider some points to the right.
10. When necessary repeat 7-10 steps. If AGCis set up correctly, finish AGC setting up procedure.

AGC setting up is completed.

23.3.3.4 Configuring audio signals recording

23.3.3.4.1 Audio signals recording modes

Audio recording can be performed:

1. As audio and video synchro recording;
2. By sound activation, i.e. when input audio signal power exceeds a certain value.
3. Independently, by Operator command.

In synchro recording mode audio and video signals' recording is initialized simultaneously (by Operator's command or by alarm).

Audio and video signals' recording is stopped simultaneously. Audio recording shutdown may be caused by:

1. Video recording shutdown (by Operator command or by the end of alarm recording);
2. Post-alarm recording shutdown (if the relevant camera is configured to perform post-alarm recording).

In synchro recording mode, audio recordings are combined with video recordings; they are stored in the videoserver archive.

In sound activated recording mode, audio recording is initialized at the moment, when signal power exceeds a preset (threshold) value. Audio signal recording is shutdown at the moment, when signal power becomes lower than a preset value, that has been previously exceeded.

An audio recording file, created in sound activated recording mode or by Operator command, includes an audio signal segment from the start till the end of the recording. In sound activated recording mode, as well as at recordind by Operator command, audio recording files are stored in a separate server archive (audio archive).

Note.

In the sound activated audio recording mode the disk space, reaching which the recordings are deleted for loop recording, is 100 MB.

Audio recording of events
Free disk space (video archive size) required
Configuration of audio

23.3.3.4.2 Selecting the disks for audio archive storage

INTELLECT™ software performs audio signal archiving to the local server disks, net disks and USB disks.

In synchro recording mode, audio recording files are stored together with video recordings in the "Video" folder(s). So, selecting the disks for audio recording storage in synchro recording mode is equivalent to selecting the disks for video recording storage. For description of the procedure, see the relevant section of this Guide. In sound activated recording mode, audio recording files are stored in the "AUDIO" folder separately from the video archive.

By default, no HDD is listed for the sound activated audio recording storage, hence, sound activated recording is unavailable. To enable the sound activated recording, select one or more disks.

Important!

If audio recording is activated by sound – not performed in synchro record mode – then disks different from those for recording video are to be selected.

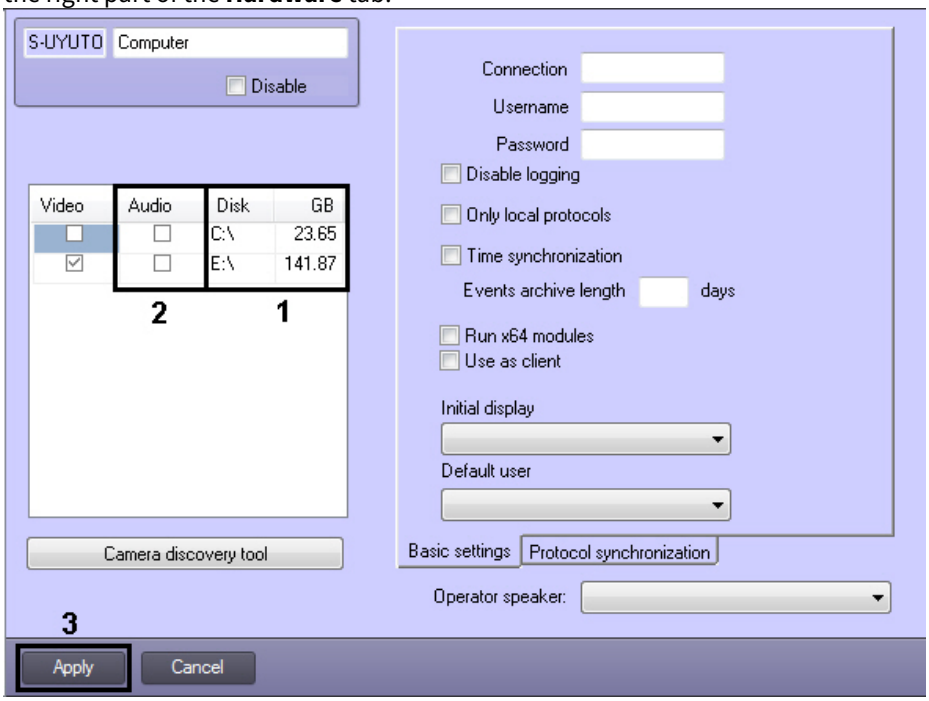
Note.

Use disks with the NTFS file system for storing the archive. If the FAT32 file system is in use, then there can be problems caused by this system, for instance — it has no logging.

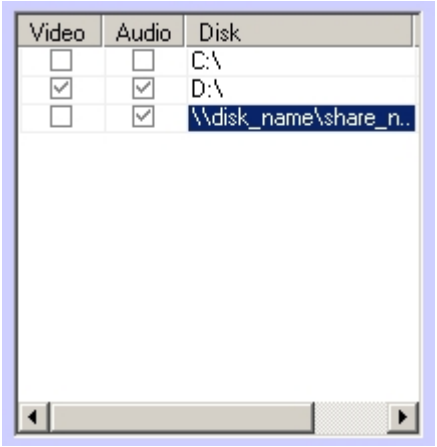
Disk(s) selection is done in one of the following ways:

1. Estimate the disk capacity, necessary for audio archive storage in the sound activated mode. The estimation technique is similar to the one used for the video archive (see Free disk space (video archive size) required).
2. Go to the **Computer** object settings panel.

3. Select the **Computer** object on the **Hardware** tab in the objects tree. The settings panel of the selected object appears in the right part of the **Hardware** tab.



4. The local disk names, available for audio archiving, are presented in the **Disk** column of the **Archive storage disks** table (1). The **GB** column contains the relevant disks capacities in gigabytes (GB). Select the disks for audio archiving and make sure that the total selected disk capacity is sufficient.
5. Set the checkmarks in the **Audio** column for the selected disks names (2). Local, net and USB disks are available for storing.
6. To add a net disk via UNC paths do the following:
   a. Go to the last line in the disk list and click the down key.



   b. Enter the path to a net disk in the appeared line. UNC path is set in the format «\\server_name\share_name», where «server_name» is the name of file server and «share_name» is the net name of general folder.
   c. Set a checkbox in the **Audio** column for created disk.
7. Click the **Apply** button (3).

Selecting the disks for audio archive storage is completed.

23.3.3.4.3 Setting up the sound activated recording

The sound activated audio recording mode is the mode, in which audio signal recording starts at the moment, when signal power exceeds a preset level and is shutdown at the moment, when signal power becomes lower than the preset level that has been previously exceeded.

To set up the sound activated recording, INTELLECT™ software uses the settings:

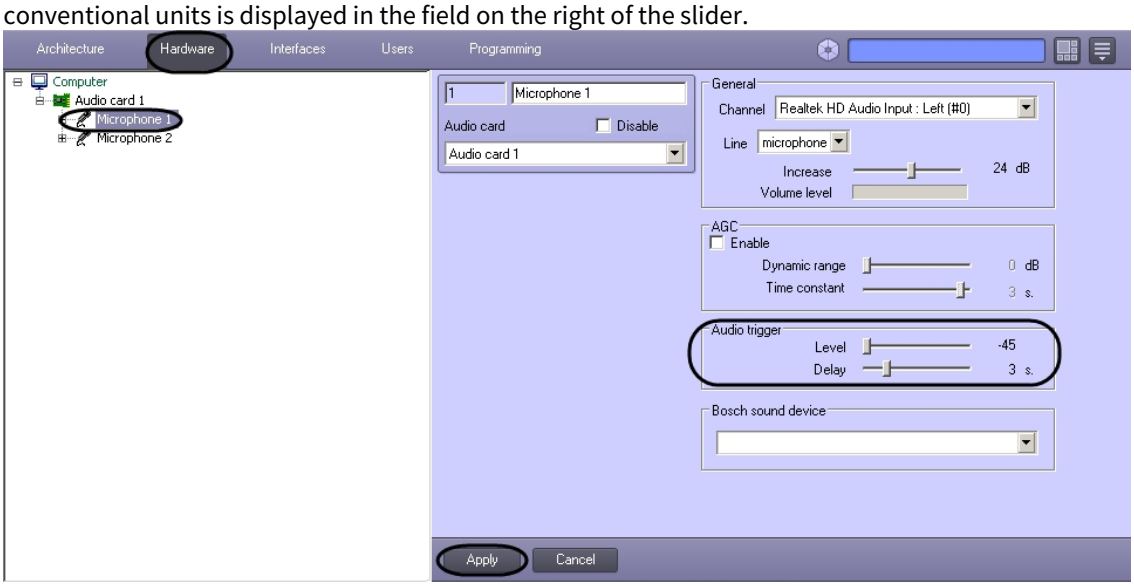
1. **Level** - When audio signal power exceeds a threshold value (Level setting) during a preset interval (Delay), audio signal recording starts automatically(alarm's registration).
2. The **Delay** setting defines the time interval, during which audio signal is prerecorded after the end of alarm.

Sound activated recording is adjusted separately and independently for any microphone. It is recommended to select the optimal settings by trial and error to avoid malfunction.

By default, sound activated audio signal recording is disabled.

Enabling and setting up the sound activated recording option for a selected microphone is done in the following way:

1. Select the disk(s) to store audio recordings in the sound activated mode (see. Selecting the disks for audio archive storage).
2. Set the **Audio player** object to operate with the selected microphones.
3. Go to the **Microphone** system object settings panel.
4. Set the slider **Audio trigger** to the position, corresponding to the required level of video signal.The current level in conventional units is displayed in the field on the right of the slider.



5. Set the **Audio trigger** slider to the position, corresponding to the required delay time of audio signal after the end of alarm. The current delay time in sec is displayed in the field on the right of the slider.
6. Click the **Apply** button to save all the changes.
7. With the help of **Audio player** object check if the sound activated recording is initialized, when the sound signal of the required volume is fed to the microphone. If not, reduce the value of Level by moving the **Level** slider some points to the left (see 4-5 steps).
8. With the help of **Audio player** object check, if the sound activated recording is initialized, when the sound signal of lower volume, is fed to the microphone. If yes, move the **Level** slider some points to the right (see 4-5 steps) to increase the setting value.
9. Repeat steps 7-9. If the sound activated recording is properly set up, complete the set up procedure.

Setup of sound activated recording of audio signal is completed.

Recordings by acoustic start

23.3.3.4.4 Setting up the audio and video synchro recording

Audio and video synchro recording is applied to enable post-event analysis of evidence footage, retrieved simultaneously from video surveillance system microphones and cameras. In this mode audio is recorded by start and end video recording times.

Audio and video synchro recording is configured by coupling cameras, registered in INTELLECT™, with microphones. Any single camera can be coupled with one or two microphones. If simultaneous recording is performed from two Microphones, audio is recorded to one stream.

The procedure of audio and video synchro recording configuration is described in Configuring audio and video synchro recording section.

Synchronous audio and video recordings

23.3.3.5 Configuring audio playback

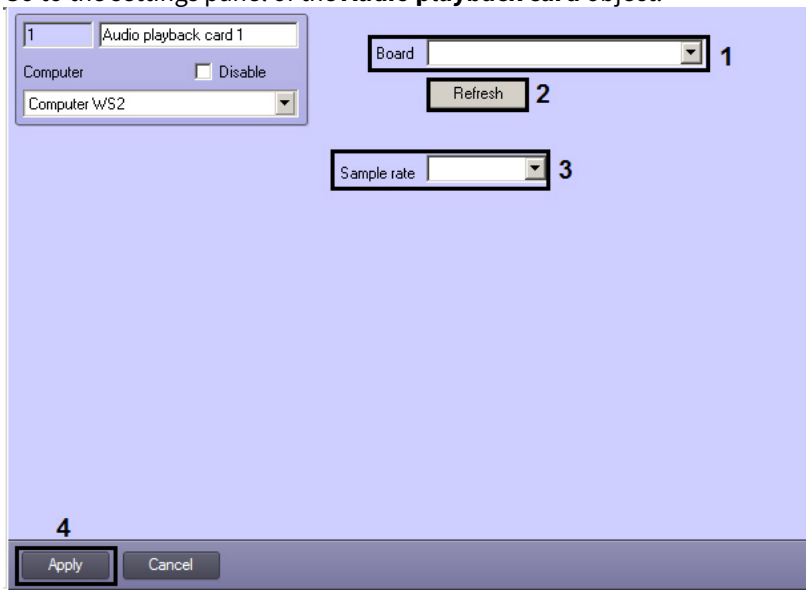
INTELLECT™ software provides an audio playback using the **Audio playback card** object. The **Audio playback card** object combines speakers objects in case the playing card has several channels. You can direct sound from the microphone to the dynamic using audio switch (see Setting up the sound switch section), macro or script.

23.3.3.5.1 Creating and configuring the Audio playback card object

The **Playback card** object is registered on the basis of the **Computer** object in the **Hardware** tab of the **System settings** dialog box.

To configure the **Audio playback card** object, do the following:

1. Go to the settings panel of the **Audio playback card** object.



2. Select the type of audio digitization device in the **Board** dropdown list (1).

Note.

SoundBlaster, ADC video card, audio digitization USB devices, IP cameras digitization devices are used as audio digitization devices.

3. Select the rate of audio digitization in the **Sample rate** dropdown list (3).
4. To save the changes, click the **Apply** button (4).

Note.

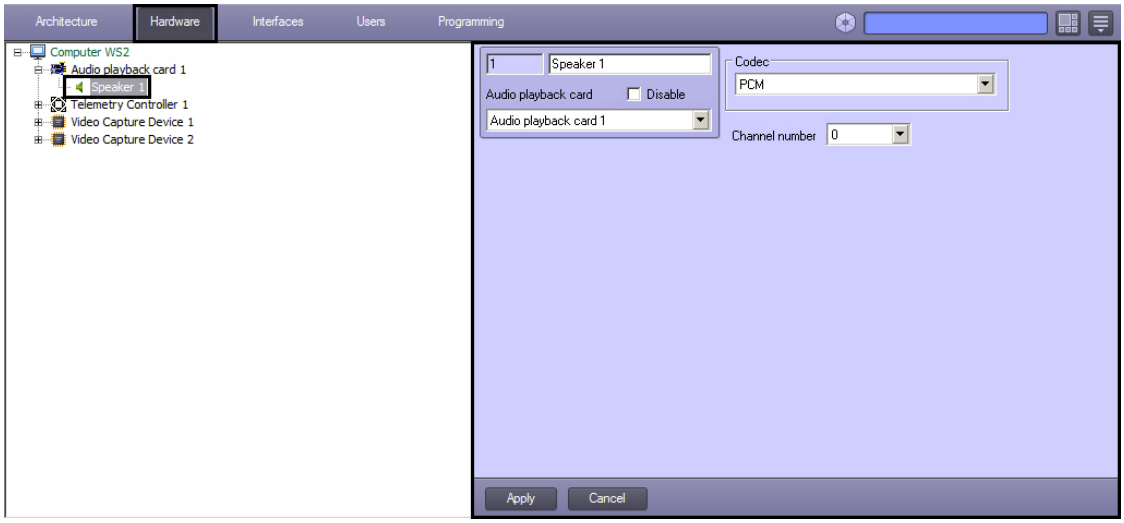
The **Refresh** button is for returning to previous settings of audio digitization device if new settings were not saved (2).

The **Audio playback card** object is now configured.

23.3.3.5.2 Creating and configuring the Speaker object

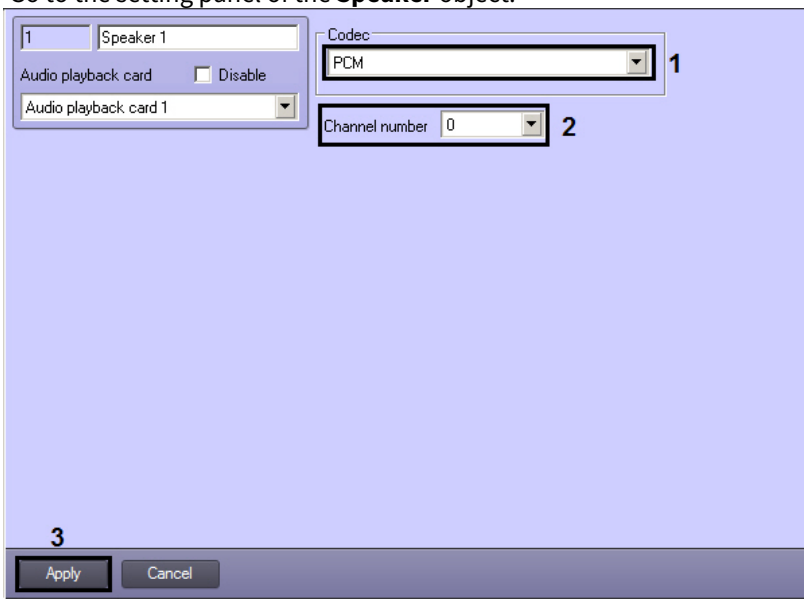
The **Speaker** object is an audio playback device.

The **Speaker** object is registered under the **Audio playback card** object in the **Hardware** tab in the **System settings** dialog box.



To configure the **Speaker** object, do the following:

1. Go to the setting panel of the **Speaker** object.



2. Select the coding format of reproductible audio signal in the **Codec** dropdown list (1). The following codecs are supported:
   a. PCM

b. G.711
c. G711_alaw
d. G721
e. G.723
f. G726_16
g. G726_32
h. IMA_ADPCM
i. G726_SUN16
j. G726_FFMPEG_16
k. G726_FFMPEG_32
l. G726_40
m. G726_SUN24
n. G726_FFMPEG_24
o. G726_FFMPEG_40
p. PCM_8
q. VNDR.0.9

3. Select channel number of speaker connection in sound card from the list of the same name (2).
4. To save the changes click the **Apply** button (3).
5. Select the created object in the **Speaker** drop-down list on the **Operator** tab of the **Computer** object settings panel – see Selecting speaker, microphone and camera for SIP-operator.

> **Note.**
>
> Several **Speaker** objects can be configured in the system. When the speaker is changed over using the **Speaker** list on the **Computer** object settings panel, then *Intellect* is to be restarted on the computer where it is in use.

6. Click the **Apply** button.

The **Speaker** object is now configured.

23.3.3.6 Features of standard sound card use

23.3.3.6.1 General information on standard sound cards

Standard sound cards are PCI cards or motherboard integrated modules, and are used to play back digital audio signals (2, 4, 6 or 8 sound channels) and/or to digitize analog video signals.

Usually standard sound cards have 1 output for connecting loudspeakers or headphones (modifications exist with 2 and 3 outputs for multi-channel sound realization and some others) and 1 input for connection of microphones.

> **Note.**
>
> Sound cards have one plug for 2 channels to connect microphones to. To connect 2 microphones, resolder the connector or use the mini jack 2xRCA adapter.

Standard sound cards perform sound playback and audio signals digitization in parallel.

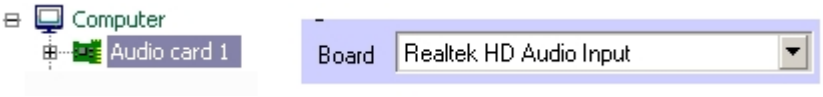
The audio signal sampling rate range depends on the audio card type. The INTELLECT™ software system sampling rate range, available to the installed card, is bounded by the 48 kHz maximum value.

23.3.3.6.2 Features of standard sound card setup

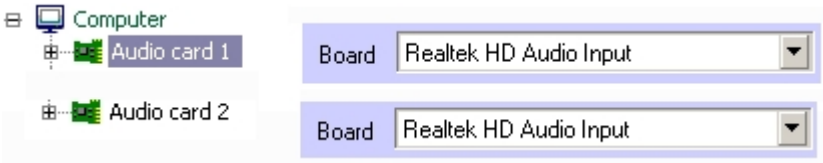
As a rule a standard sound card digitizes no more than 2 audio signals.

Each standard sound card is registered in the INTELLECT™ software by creating and setting up **Audio card** objects. **Audio card** objects are created on the **Hardware** tab on the base of the **Computer** object. During creation of the **Audio card** object for each standard sound card, the different values in the numbering sequence should be assigned to the **Board** parameter: for the first **Audio card** object the FS 6 (0) value should be selected, for the second one - FS 6 (1) and so on.

Example of **Board** settings for Realtek standard sound cards:



A.at single standard sound card registration



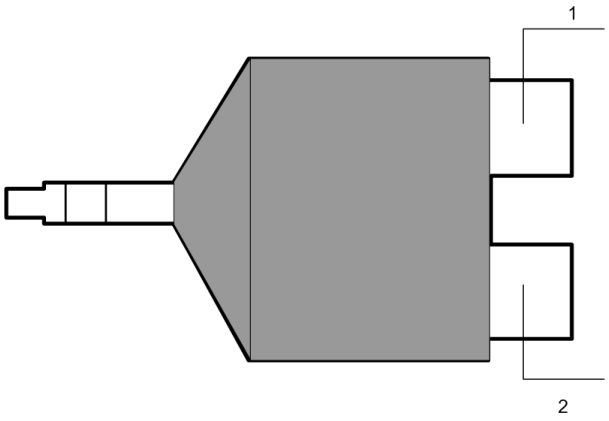
B. at registration of two standard sound cards of the same type

To register the microphones, connected to the standard sound card input audio channels, create **Microphone** objects on the base of the **Audio card** object. Up to 2 **Microphone** objects may be placedn the base of a single **Audio card** object. The relevant hardware tree segment during the registration of the standard sound card and 2 microphones is shown in the figure.

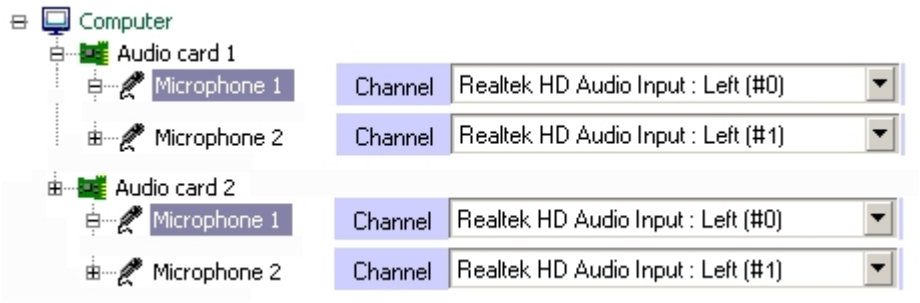
After the sound card registration in the INTELLECT™ system, the values should be assigned to the **Channel** settings of the **Microphone** objects, according to the channel numbers of the microphone connections to a standard sound card.

To connect more than one microphone to a standard sound card, the mini jack 2xRCA adapter is used. The mini jack 2xRCA adapter numbering layout is shown in Figure 8.8-31. Examples of **Microphone** object settings with one and two FS-5 video capture cards, registered in the INTELLECT™ system, are shown in Figure A and Figure B correspondingly.

Mini jack 2xRCA adapter numbering layout:



A.for a single standard sound card



B. for two standard sound cards

23.3.3.7 Using multi-channel audio capture devices

23.3.3.7.1 General information on multi-channel audio capture devices

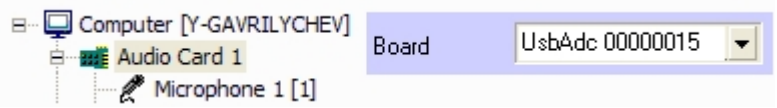
Multi-channel audio capture devices are PCI cards (for example, MidiMan Delta, Comart Hera, Olha9P) or external hardware and software modules (for example, Echolot USB-32), used for digitization and processing of 2 or more audio signals. For the list and features of INTELLECT™ software compatible multi-channel audio capture devices, see the Integration section on the site of AxxonSoft company: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.

Multi-channel audio capture devices reproduce sound and digitize audio signals in parallel, or sound is reproduced by the standard sound cards. The audio signal sampling rate range depends on the audio capture device type. The INTELLECT™ software system sampling rate range, available to the installed card, is limited to the 48 kHz maximum value.

23.3.3.7.2 Setting up multi-channel audio capture devices

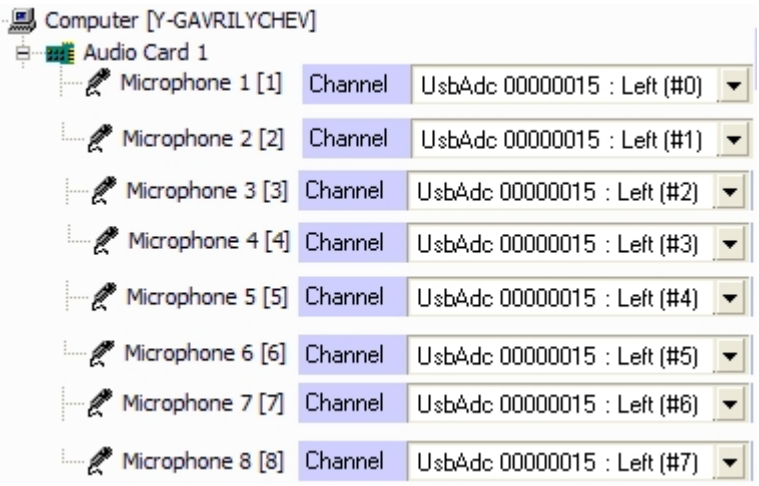
Usually multi-channel audio capture devices digitize 2 or more audio signals, de on the device type.

Each multi-channel audio capture device is registered in the INTELLECT™ software by creating and setting up **Audio card** objects. **Audio card** objects are created on the **Hardware** tab on the base of the **Computer** object. During creation of the **Audio card** object for each multi-channel audio capture device the value, corresponding to its name, should be assigned to the **Board** parameter.



To register the microphones, connected to the multi-channel audio capture device input audio channels, create **Microphone** objects on the base of the **Audio card** object. The number of **Microphone** objects, allocated on the base of a single **Audio card** object, is defined by the number of audio input channels and restricted by the License key file. The relevant hardware tree segment during the registration of the standard sound card and 8 microphones is shown in the figure.

The hardware tree segment at registration of an Eholot USB-32 multi-channel audio capture device and 8 microphones:



After registration in the INTELLECT™ system, the values should be assigned to the **Channel** settings of the **Microphone** objects according to the channel numbers of the microphone connections to the audio capture device. An example of **Microphone** object settings is shown in the figure above.

23.3.3.8 Using IP-devices

23.3.3.8.1 General information on IP-devices

INTELLECT™ software system supports audio signals reception, digitization, processing and playback options, using audio capture IP-devices. IP-cameras and IP-servers built-in microphones or the external analog microphones, connected to IP-devices, may be used for audio signals receipt, digitization and processing. External IP-loudspeakers or headphones, connected to IP-servers or IP-cameras may be used for audio signals playback. For the list of INTELLECT™ software compatible IP-devices for audio signal reception, digitization, processing and playback, see the Integration section on the site of AxxonSoft company: http://www.axxonsoft.com/products/axxon_enterprise/core_functionality/integration.php.

The audio signal sampling rate range depends on the IP-device type, used as an audio capture device. The INTELLECT™ software system sampling rate range, available for the installed card, is limited to the 48 kHz maximum value.

Note.

*Intellec*t supports IP devices with dynamic IP address using DynDNS or other services. In these cases specify the address (hostname) given by DynDNS service instead of IP address when configuring IP devices.

23.3.3.8.2 Setting up the transmission of audio signals to IP devices

Intellect has the possibility of transmitting the audio signals from microphones to IP devices and playing back the audio signals with loudspeakers or headphones connected to IP devices.

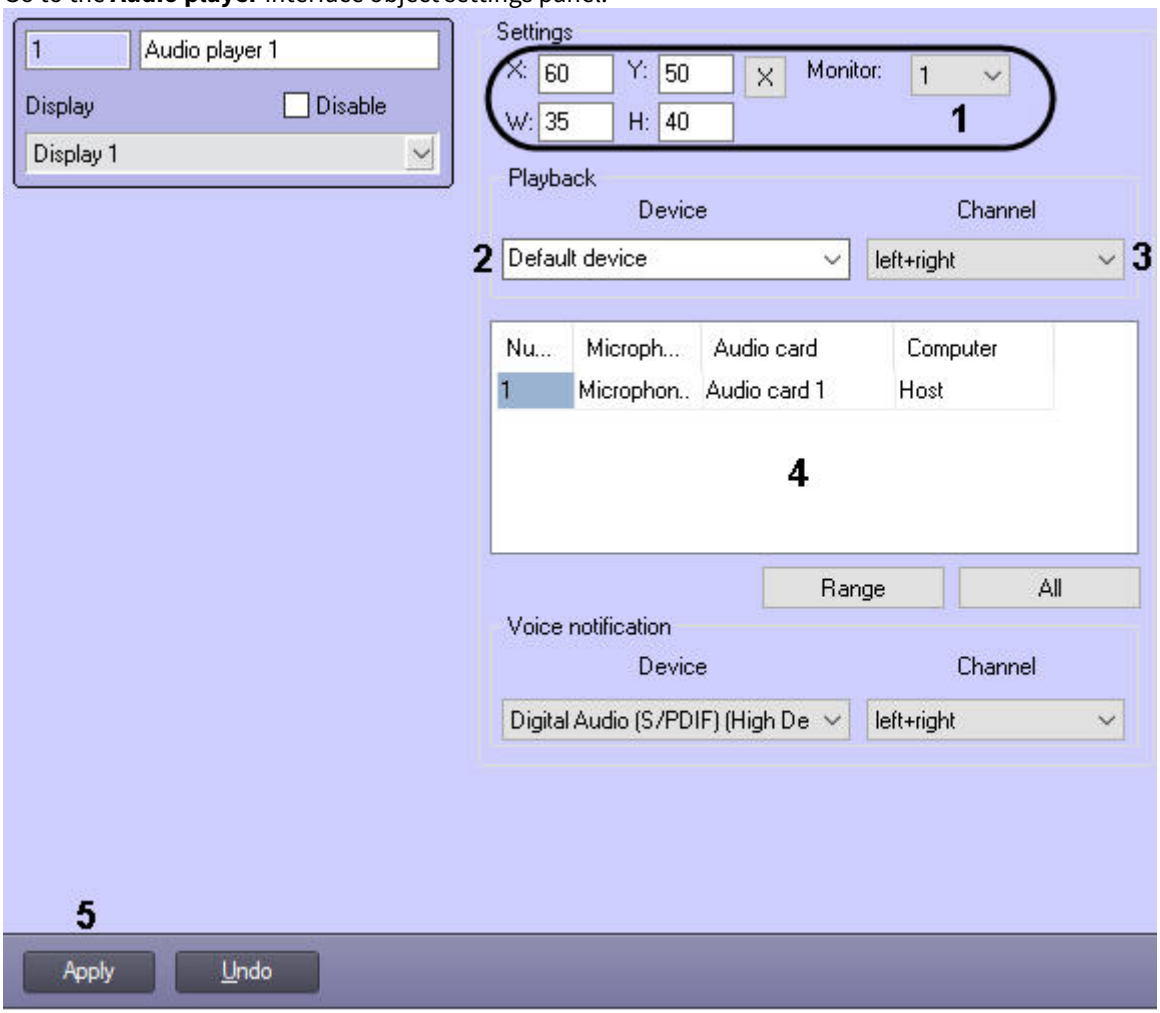
There are two ways audio signals can be transmitted to IP devices in *Intellect*:

1. using the **Audio player** interface object;
2. using the **Voice notification service** system object.

The **Audio player** object is used to transmit audio signals from the selected microphones to the supported IP devices.

To set up the transmission of audio signals using the **Audio player** object, do the following:

1. Go to the **Audio player** interface object settings panel.



2. Set the coordinates and the size of the **Audio player** interface window, as well as the number of the physical monitor on which the window will be displayed (**1**).
3. From the **Device** drop-down list, select the required IP device (**2**).
4. From the **Channel** drop-down list, select the required audio signals playback channel (**3**).
5. From the drop-down list in the **Number** column, select the **Microphone** object number, from which the audio signal has to be transmitted to the selected IP device (**4**). Other columns of the table will be filled in automatically.
6. Repeat step 5 for each required **Microphone** objects.
7. Click the **Apply** button to save the changes (**5**).

Setting up the transmission of the audio signals using the **Audio player** object is completed.

Note

To enable audio signals transmission from the microphone to the IP device, click the button (Interception from microphone) in the **Audio player** interface window.

The **Voice notification service** object is used to transmit audio files in the WAV format to the supported IP devices. Setting up of the **Voice notification service** object is described in Setting up the voice notification.

Note

When using **Audio player** and **Voice notification service** together, note that the sampling rate of the audio signals transmitted from the microphones via the **Audio player** (the **Sample rate** setting of the **Audio card** object) and the sampling rate of the audio files transmitted with the help of the **Voice notification service** should be the same.

23.3.3.8.3 Setting up the transmission of duplex audio signals to IP-devices

Transmission of duplex audio signals to IP-devices is configured by coupling speakers, registered in INTELLECT™ software, with microphones.

> **Note.**
>
> The feature of transmitting audio to an IP-device must be supported by the IP-device and be integrated into the Intellect™ software – see Drivers Pack documentation.

To configure transmission of duplex audio signals to IP-device, do the following:

1. Create and configure the **Camera** object on the base of the **Video Capture Device** object.
2. To work with a microphone of an IP-camera, create and configure the **Audio card** and **Microphone** objects (see Registration of audio cards and microphones in INTELLECT™ software section).
3. To work with a speaker of a camera, create and configure the **Playing card** and **Speaker** objects (see Configuring audio playback section).
4. To redirect a signal from a microphone to a speaker of a camera, create and configure the **Live sound switch** object (see Creating and configuring the Live sound switch object section).

As a result, one can direct audio to a speaker of a camera while working with the **Live sound switch** object (see Using the Live sound switch object section).

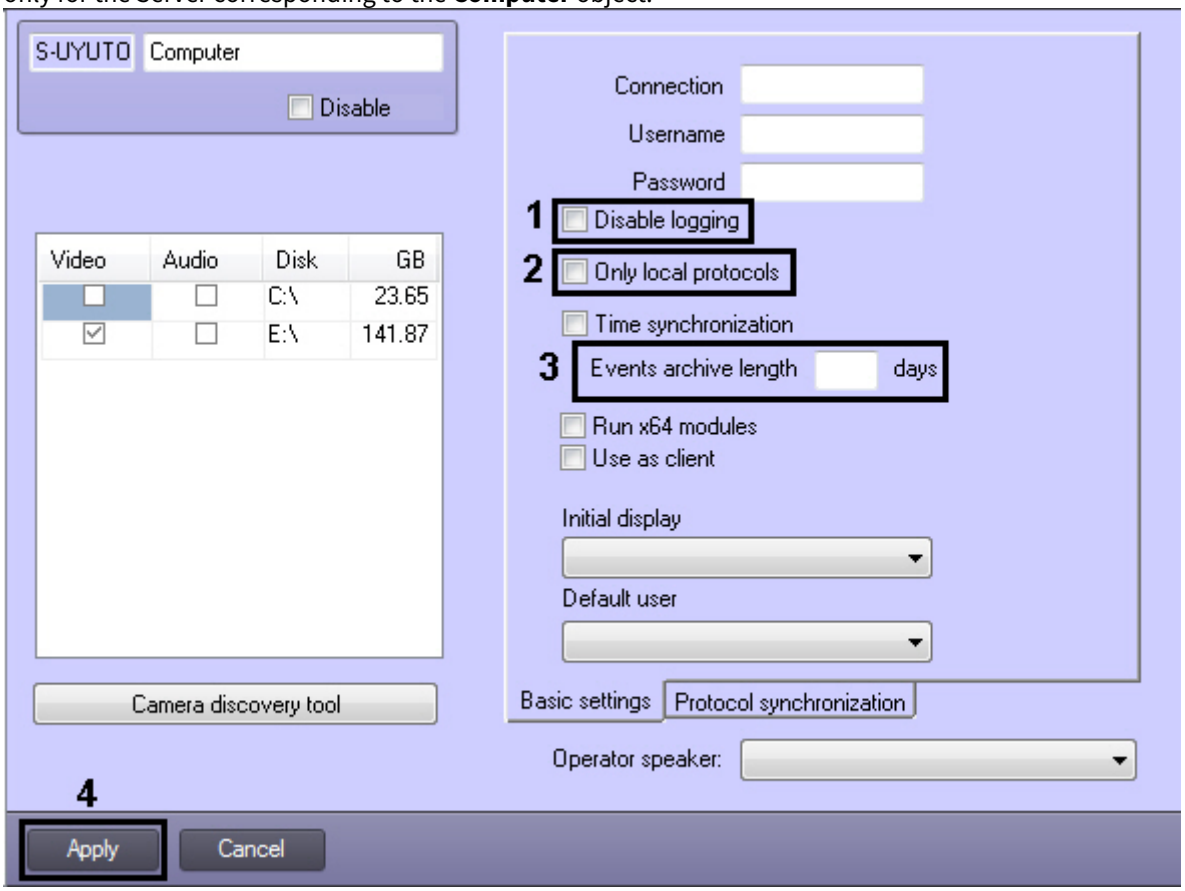
23.3.4 Configuring events logging

The data about events registered in the system is stored in the Protocol table in *Intellect* (by default) or in the Protocol table of an individual database (see Extracting event protocol into an individual database).

The Event Viewer database is configured by means of the settings panel of the **Computer** system object.

Configure the Event Viewer database as follows:

1. To disable events recording to the Event Viewer database, set the **Disable logging** checkbox (**1**). This setting is relevant only for the Server corresponding to the **Computer** object.



2. If you want to log to the Event Viewer database only the events registered on this computer, set the **Only local protocols** checkbox (**2**). This setting is relevant only for the Server corresponding to the **Computer** object.
   If this checkbox is set, then the Event Viewer database synchronization has to be started manually using the SyncProtocol.exe utility or a macro (see The SyncProtocol.exe utility to synchronize event log database and Example of macro to start the Event Viewer databases synchronization).
3. In the **Events archive length** field, specify the time period in days for storing the event archive in the Event Viewer database (**3**). This setting is relevant only for the Server corresponding to the **Computer** object. To specify the time period for storing the event archive for all Servers in the distributed system, use the common settings in the **Programming** tab (see The Settings panel of the Security zone object). The value of the **Events archive length** parameter on the settings panel of the **Computer** object has the higher priority. If no value is specified in the **Events archive length** field on the settings panel of the **Computer** object, the value specified in the settings panel of the **Security zone** object is used.

   Note

   The specified **Events archive length** is also applied to the events received by the **Incident server**, which are stored in the PROTOCOL_INC_SERVER table of the *Intellect* database.

   Note

   The process of clearing the database of the events older than the specified storage period is started by default every three minutes and deletes 100,000 events starting with the oldest ones.

4. Click the **Apply** button to save the changes (**4**).

The events logging to database is now configured.

Note

You can also use the tweaki.exe utility to configure events logging (see the The Settings panel of the Intellect section).

Define required disk space (size of event log database)
Configuring the Operator protocol interface object
Configuring the Event Viewer interface object
Event control via Event viewer
Event processing using the Operator protocol
Configuring Incident server and Incident handler
Events control and processing using the Incident manager

23.3.5 Configuring the Event Viewer databases synchronization

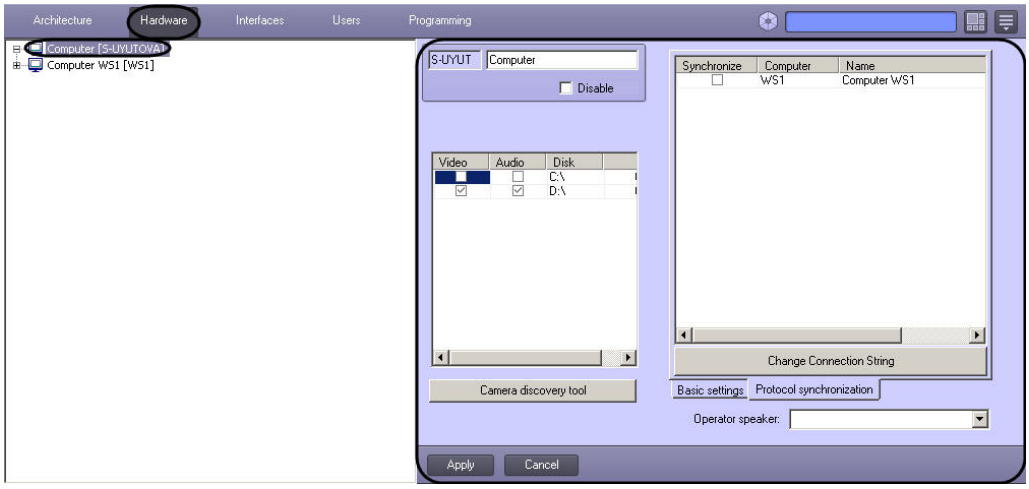
23.3.5.1 General information on the Event Viewer databases synchronization

In *Intellect* information on the events registered in the system is stored in the Event Viewer database. The local copy of the distributed database is stored on each Server. The synchronization of local copies of the Event Viewer databases is to be configured for data replication.

By default the synchronization of the Event Viewer databases is performed automatically. If the **Only local protocols** checkbox is set checked on the **Computer** settings panel, then the Event Viewer database synchronization is started via programming resources, for example, using macros or the SyncProtocol.exe utility.

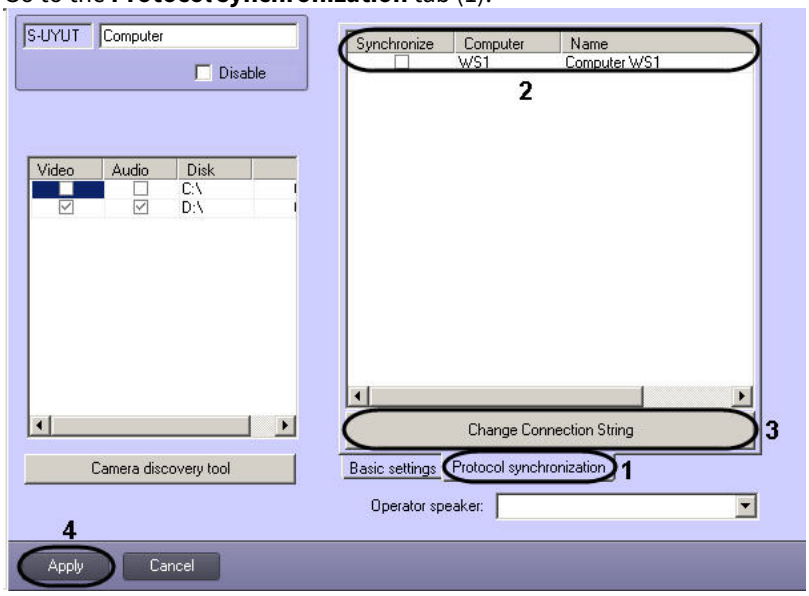
23.3.5.2 Configuring the Event Viewer database synchronization

Synchronization of the Event Viewer databases is configured on the settings panel of the **Computer** object in the **Protocol synchronization** tab.



To configure the synchronization, do the following:

1. Go to the **Protocol synchronization** tab (1).



2. In the **Synchronize** column set checkboxes next to those computers with which the synchronization of the Event Viewer databases is to be performed on the Server (2).
3. Set the connection string in the Event Viewer database on remote computers:
   a. Select the cell corresponding to the required computer in the line of the table.
   b. Click the **Change Connection String** button (3).
   c. In the opened **Data communication channel** box configure the connection to the Event Viewer database located on the selected computer.
   Connection configuration is performed via Windows standard tools and is described on the Microsoft reference web-site (http://msdn.microsoft.com/).
   d. Repeat 3.1 – 3.3 steps for all required computers.
4. Click the **Apply** button to save the settings (4).

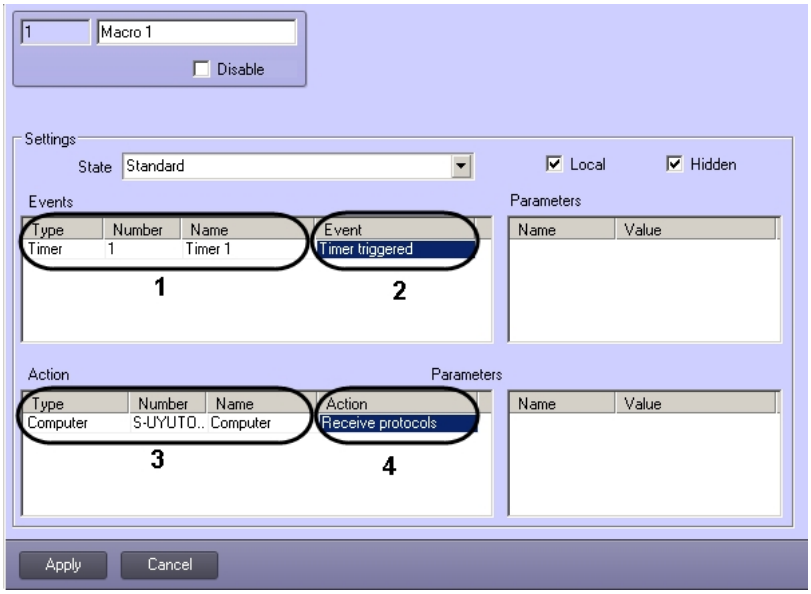
Synchronization of the Event Viewer databases is now configured.

23.3.5.3 Example of macro to start the Event Viewer databases synchronization

On the WS3 computer the synchronization of the Event Viewer databases is to be performed when Timer 1 is triggered.

Set the macro parameters using one of the following ways (see figure and table):

Event		**Action**	
Object	**Event**	**Object**	**Action**
Timer 1 (1)	Timer triggered (2)	Computer (3)	Receive protocol (4)



23.3.6 Configuring telemetry

In digital video surveillance system PTZ devices are used for extension of video surveillance area by mechanical rotation of the camera. Detailed description of connection and configuration of PTZ devices is given in the Installing and configuring security system components guide manual.

Requirements for PTZ and control panels
Telemetry control

23.3.7 Configuring operation of distributed architecture in the failover mode

23.3.7.1 General information about Failover mode

On the page:

- Purpose and features of the Failover mode
- Examples of Failover system organization
  - 1 main Server + standby Server
  - N main Servers + standby server
  - Two Servers being standby for each other
- Limitations of the Failover mode

23.3.7.1.1 Purpose and features of the Failover mode

Distributed architecture can operate in the failover mode. If the connection with one of distributed system Servers fails, then this mode enables transferring the configuration created under the Server to a Standby Server. A Standby Server temporarily becomes a video server and records archive in accordance with the settings of the **Computer** object that corresponds to a Standby Server (see Selecting the disks for video archive storage). When the connection is restored, the configuration is restored on the main Server.

Note

Video image update on Client Video Surveillance Monitors can take several seconds after configuration transfer, as the update is performed sequentially every 3 seconds. Video is displayed as usual after the update. If more than 64 cameras are added to the monitor, the update does not occur while the **System Settings** dialog box is open. The update period can be decreased by the monitor_refresh_delay registry key – see Registry Keys Reference Guide.

Note

When moving configuration to the backup Server and getting it back to the main Server the **Failover service** object generates START and STOP events. These events can be used in scripts for flexible system configuration. For examples, see Examples of scripts in the JScript language section of The Script object. Programming using the JScript language.

The configuration transfer time after losing connection with the main Server depends on many factors including but not limited to the following:

1. Computer capacity.
2. Data storage system speed.
3. The value of the FastIndex key in the registry (see Registry keys reference guide). It is recommended to set the key value to 1.
4. The system objects tree (the more subsystems and modules there are, the slower the configuration transfer).

Example

The following migration time is confirmed in both directions (i.e. from the main Server to the standby Server and vice versa):

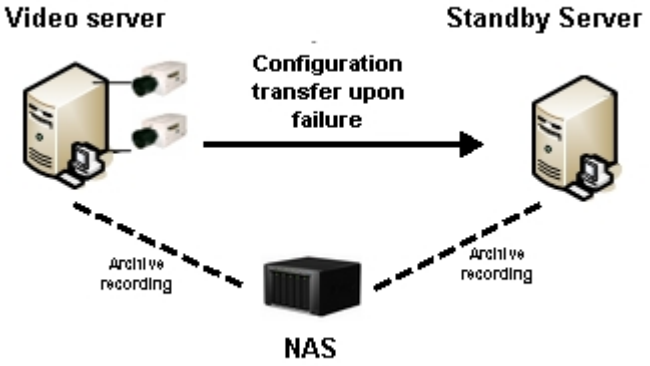
1. 100 cameras are transferred in less than 20 seconds;
2. 200 cameras are transferred in less than 30 seconds.

The archive size tested was more than 5 TB and the Servers hardware as follows:
Main Server: Intel Core i5-8500, 16 GB RAM.
Standby Server: Intel Core i5-8400, 16 GB RAM.

23.3.7.1.2 Examples of Failover system organization

23.3.7.1.2.1 1 main Server + standby Server

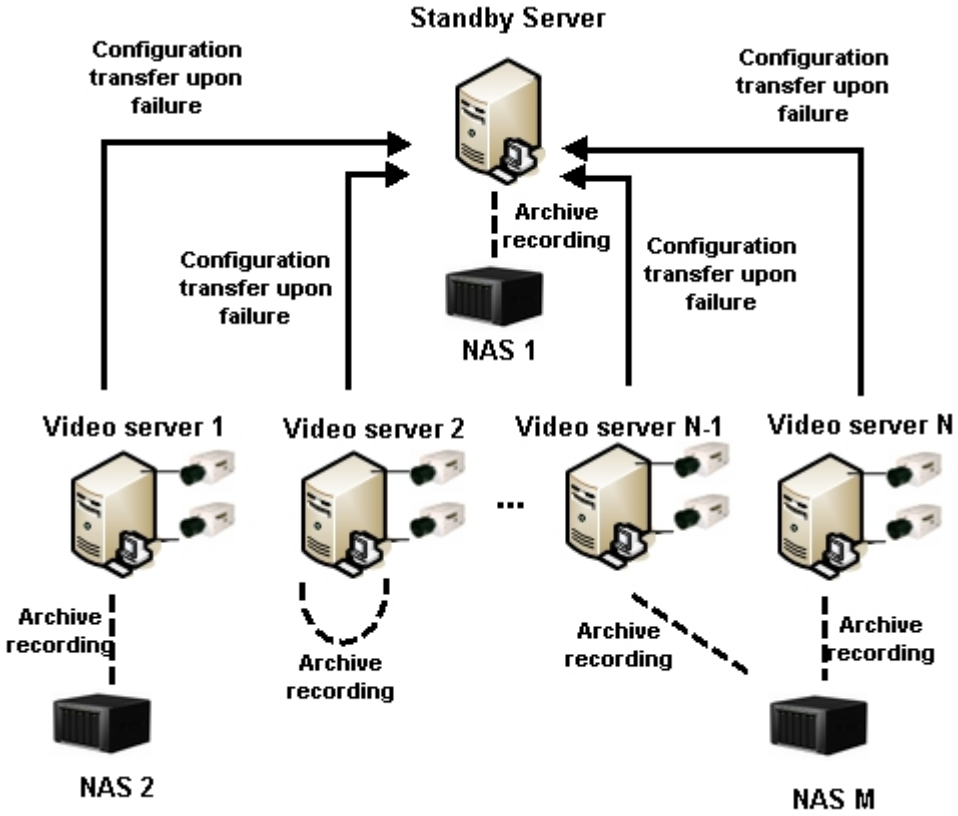
If the main Server + standby Server operation scheme is in use (see the figure below), it is possible to configure both main and standby Servers for recording on the same network resource or several resources (see Using network disks). In this case, the archive is always available no matter which Server operates with cameras.

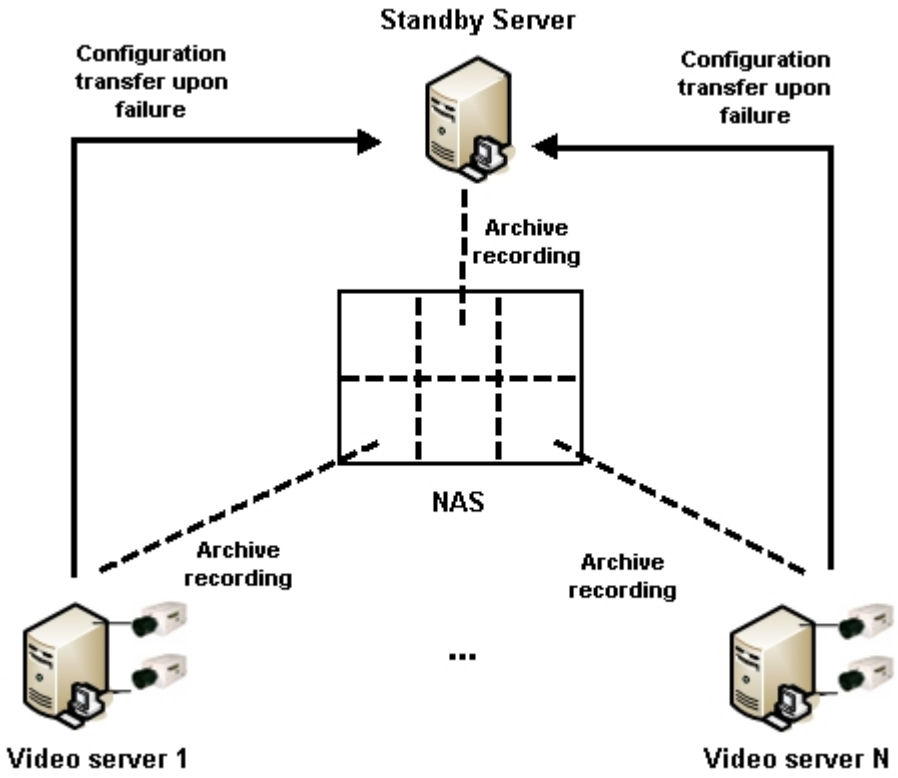


23.3.7.1.2.2 N main Servers + standby server

If the N main Servers + standby server operation scheme is in use (see the figures below), it is impossible to create a unified archive. In this case the main Servers perform recording on different logical drives (sections, partitions), local or network. If these drives are specified for archive recording on the standby Server, then the archives from different main Servers will mix.

The *AxxonPlayer.exe* utility can be used to access the archive created by the standby Server on NAS or local drive (see The Axxon Player utility for viewing and converting the video archive). Alternatively, the main and the backup Server archives can be synchronized through the *Backup archive* module (see Configuring archive synchronization of main and backup Servers).

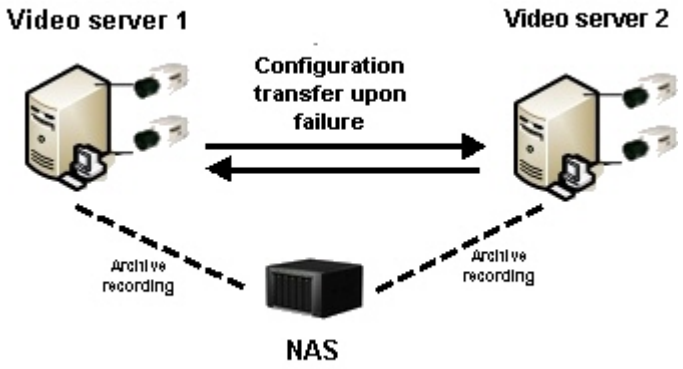




If configuration from several main Servers is transferred to a single standby Server, you should foresee a situation where all main Servers fail and ensure that standby Server has sufficient CPU, RAM and LAN resources.

23.3.7.1.2.3 Two Servers being standby for each other

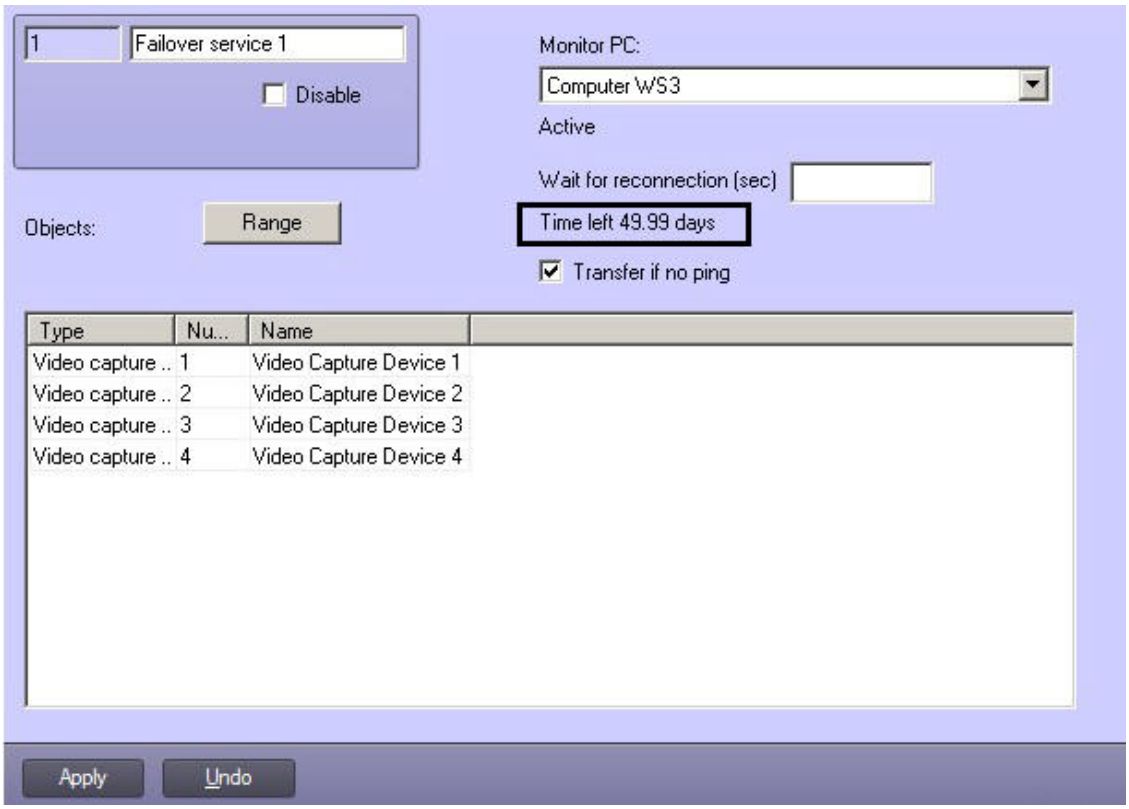
Any Server can act both as a main and as a standby at the same time given that the performance of the Server platform allows it. Therefore, a Failover system can be organized with two video servers that are standby in relation to each other.
As in the cases described above, if both Servers record the archive to the network storage, access to the archive is available when the configuration is transferred. If the Servers record a local archive or use different network storages, the *AxxonPlayer.exe* utility (see The Axxon Player utility for viewing and converting the video archive) or synchronization through the *Backup archive* module (see Configuring archive synchronization of main and backup Servers) can be used to access the archive created by the standby Server on NAS or on local drive.



23.3.7.1.3 Limitations of the Failover mode

The Failover mode is configured using the **Failover service** objects created on the basis of the **Computer** objects corresponding to backup servers in the **Hardware** tab of the **System settings** dialog box.

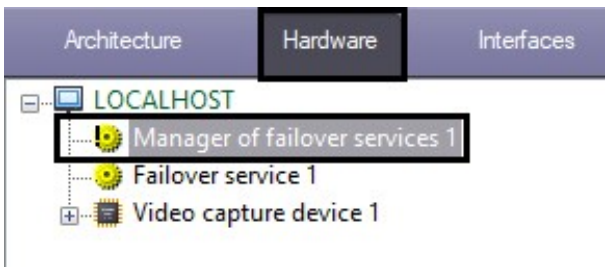
If the quantity of cameras is bound to specific Servers in the security key, then the license becomes invalid when cameras are moved to the backup Server. In this case the system gives 50 days to restore the failed Server in order to move the cameras back and the license to become valid again. Otherwise, *Intellect* will unload on the backup Server because the hardware limit is exceeded (see Features of the Intellect software operation when the object limit is exceeded). The time (in days) remaining for restoring the main Server is displayed on the settings panel of the **Failover service** object:



If *Intellect* is normally shut down on the main Server, the configuration is not transferred to the standby Server.

In case of manual shutdown of the main Server, the configuration is also not transferred to the standby Server.

The number of failover services running on each computer simultaneously can be limited. The **Manager of failover services** object is used for this. It is created on the basis of the **Computer** object that is not the Client (see Role-assignment in distributed system).

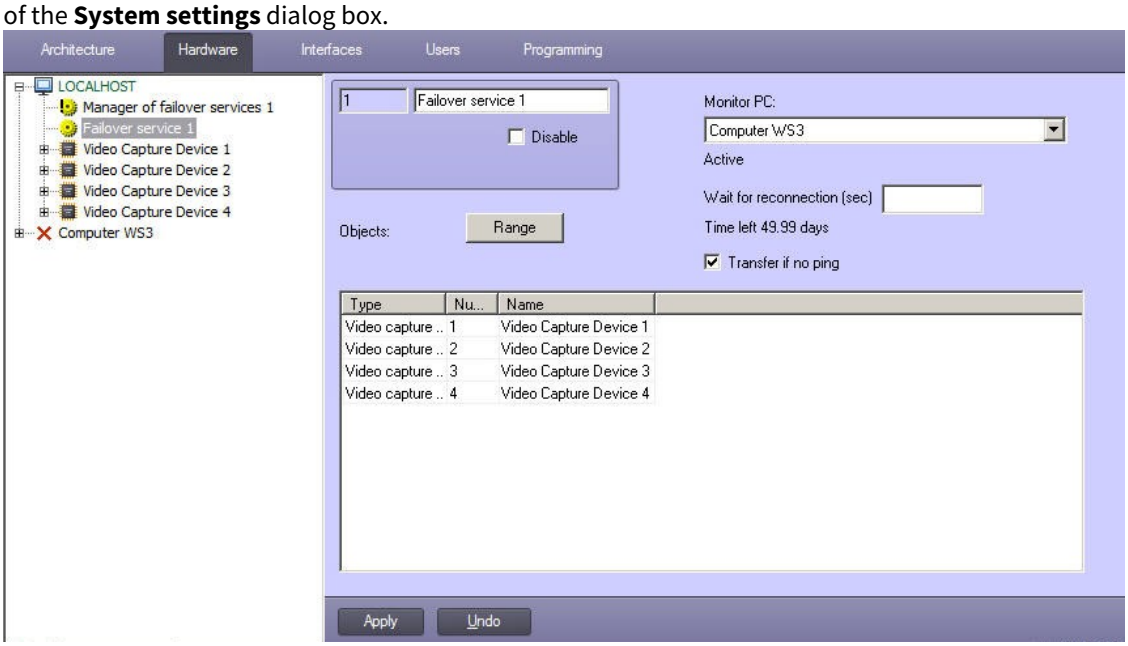


If the number of failed Servers exceeds the specified limit, the configuration from the new failed Servers will be transferred to the corresponding backup Server as the previously failed Servers become operational.

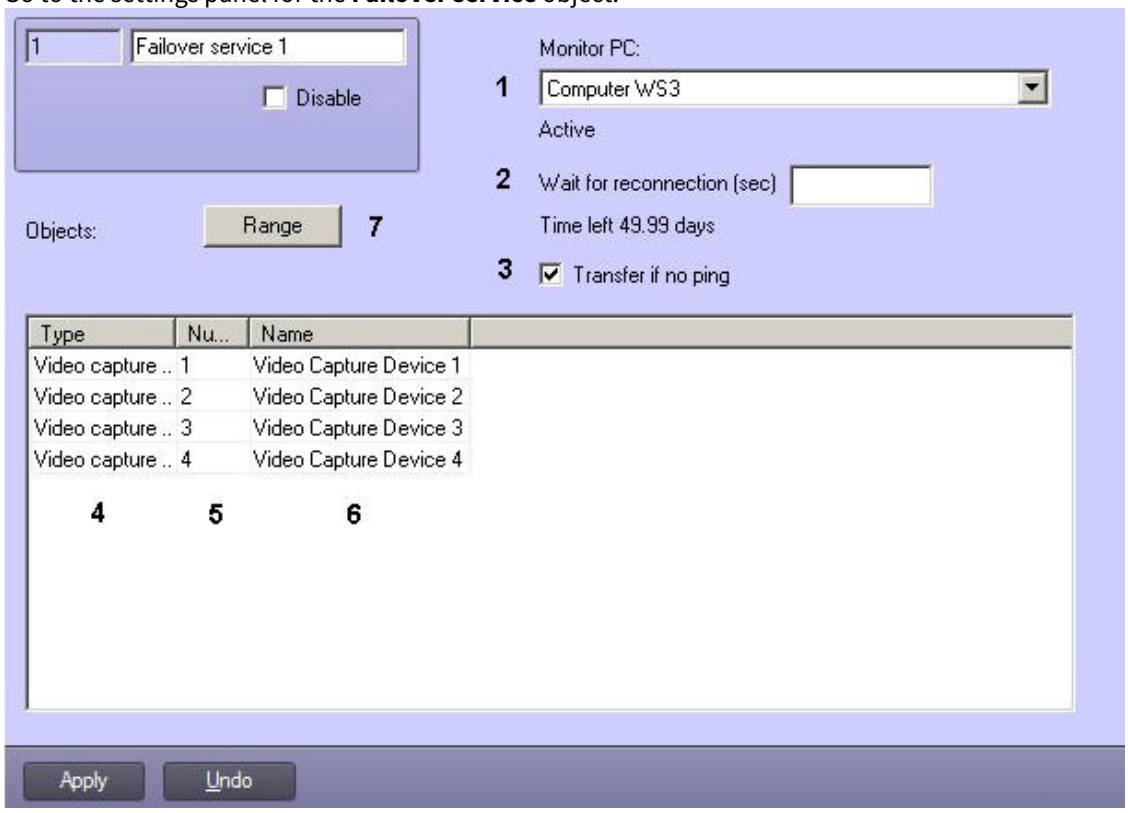
23.3.7.2 Configuring Failover service

To configure the failover service, configure a standby Server as follows:

1. Create the **Failover service** object under the **Computer** object corresponding to the standby Server in the **Hardware** tab of the **System settings** dialog box.



2. Go to the settings panel for the **Failover service** object.



3. In the **Monitor PC** drop-down list, select the name of the **Computer** object that is to be under control (**1**).
4. In the **Wait for reconnection (sec)** field, specify the time period (in seconds) at the end of which configuration is transferred to a standby Server when the Server connection fails (**2**).

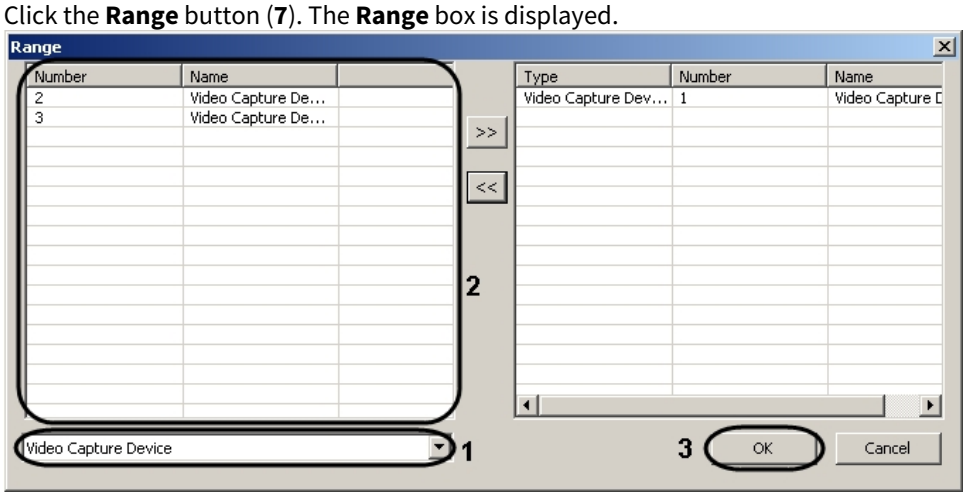
5. If it is necessary to transfer the configuration without the ping from the main Server, set the **Transfer if no ping** checkbox (**3**).
6. In the **Objects** table, specify the list of configuration objects (that are to be transferred to a standby Server if connection fails) of the main Server:
    a. Manually one by one:
        i. In the **Type** drop-down list, select the object type (**4**).

> **Note**
>
> The **Manager of failover services** type is not available. Such objects are not transferred to the backup Servers as each backup Server has to have its own **Manager of failover services**.

        ii. In the **Number** drop-down list, select the object ID (**5**).
        iii. The **Name** field is automatically filled in with the name of a corresponding object (**6**).
        iv. Repeat steps i—iii for all objects (that are to be transferred to a standby Server if connection fails) in the objects tree of a Server under control.

> **Note**
>
> To add a new line in the table, click the downwards arrow on the keyboard.

        v. Click the **Apply** button.
    b. As a group:
        i. Click the **Range** button (**7**). The **Range** box is displayed.



        ii. In the drop-down list, select the object type (**1**).

> **Note**
>
> The **Manager of failover services** type is not available. Such objects are not transferred to the backup Servers as each backup Server has to have its own **Manager of failover services**.

        iii. In the table, mark the required objects of this type (**2**). To mark several objects, hold the Ctrl key on the keyboard.
        iv. Click the >> button to transfer selected objects to the list of the objects under control. The list is on the right of the **Range** box.

> **Note**
>
> The << button is used to transfer the object back from the list of objects under control to the list of available objects.

        v. Repeat steps ii—iv for all required objects.
        vi. Click the **OK** button (**3**).
        vii. Click the **Apply** button.

7. Repeat steps 1—5 for all main Servers under control of a configured standby Server in the distributed system.

The failover service is now configured.

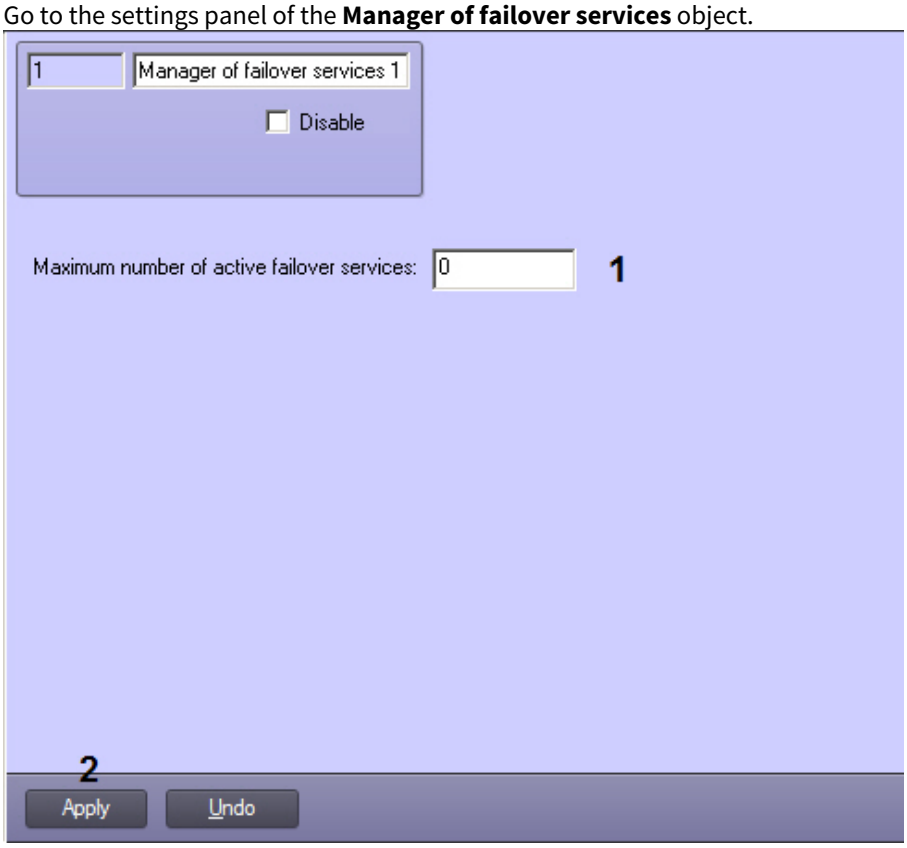
> **Attention!**
>
> For a **SIP-terminal**, it is necessary to additionally specify the IP address of the backup server in the **sip_terminal.config** file (see Configuring a SIP-terminal for Failover service).

23.3.7.3 Limiting number of failovers running simultaneously

Create one **Manager of failover services** object on each backup Server. Managers of failover services are not transferred from one backup Server to another.

Limit the number of failovers running simultaneously as follows:

1. Go to the settings panel of the **Manager of failover services** object.



2. In the **Maximum number of active failover services** field specify the maximum number of dead servers – when this limit is reached the configuration transferring is to be stopped until one of failovers becomes vacant (1).
3. Click the **Apply** button (2).

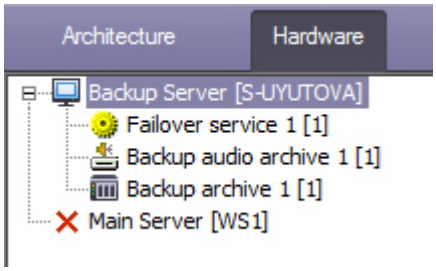
Limit to the number of failovers running simultaneously is now set.

23.3.7.4 Configuring archive synchronization of main and backup Servers

In *Intellect* one can configure the synchronization of the video archive of the main and backup Servers. In this case, after restoring the main Server, the video archive will be transferred from the backup Server using the *Backup archive* module.

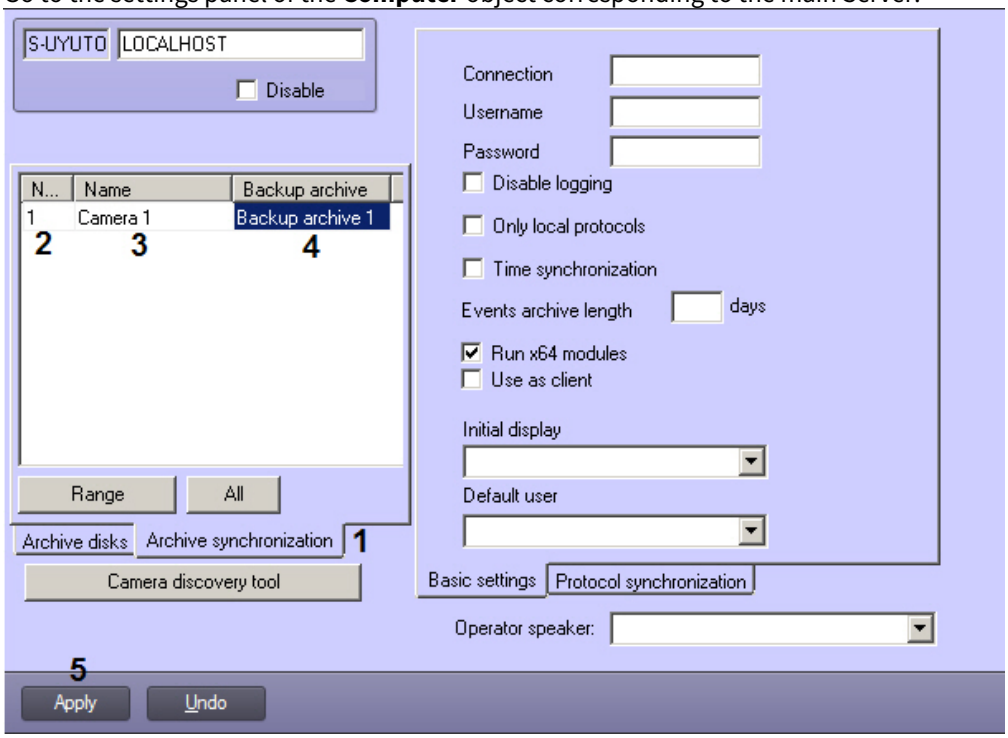
> **Important!**
>
> Only video records without sound are moved from backup Server to main Server at synchronization. If synchronous recording of video and audio is configured, sound will be eliminated at transmission files from backup Server to main Server, and only video files will get to the main Server.

To use the archive synchronization mechanism create a Backup archive object under the same **Computer** object as the **Failover service** object.



Cooperation with the Failover service is to be enabled on the settings panel of the Backup archive (see Enabling cooperation of Backup archive with Failover service).
Configure synchronization on the main Server as follows:

1. Go to the settings panel of the **Computer** object corresponding to the main Server.



2. Go to the **Archive synchronization** tab (1).
3. Configure the list of cameras the archive of which is be synchronized when restoring the main Server:
   a. Select the camera ID in the **Number** dropdown list (2).
   b. Select the camera name in the **Name** dropdown list (3).
   c. In the **Backup archive** dropdown list select the name of the **Backup archive** object configured to cooperate with the Failover service and located on the backup Server where the selected camera is transferred to when the main Server fails (4).

      > **Important!**
      >
      > This step is mandatory. If **Backup archive** is not selected, camera is not saved in the list. Configure Backup archive before configuring archive synchronization.

   d. Repeat steps a-c for all required cameras.
   e. Click the **Apply** button (5).

The synchronization of main and backup Servers is now completed.

23.3.8 Configuring the SNMP-service

23.3.8.1 SNMP service setting order

It is possible to create SNMP-service for resending messages about the registered events to SNMP-manager. This opportunity is realized with the use of **SNMP trap** system object.

> **Note.**
>
> Data concerning SNMP-manager is given in the official SNMP protocol reference manual – see, for example, https://technet.microsoft.com/en-us/library/cc738071%28v=ws.10%29.aspx.

> **Note.**
>
> SNMP trap objects use the trap port 162 to send messages in Intellect.

SNMP-service carries out the following functions:

1. Receipt of messages concerning the event, registered in the system;
2. Message conversion concerning the event to SNMP format;
3. Message transfer in SNMP format (trap) to SNMP-manager with the use of TCP/IP net protocol.

> **Note.**
>
> Moreover, SNMP Wrapper module is the part of *ACFA Intellect* – it allows *Intellect* to behave as SNMP manager and get data from external systems – see SNMP Wrapper Settings Guide.

Setting the SNMP-service is done in the following order:

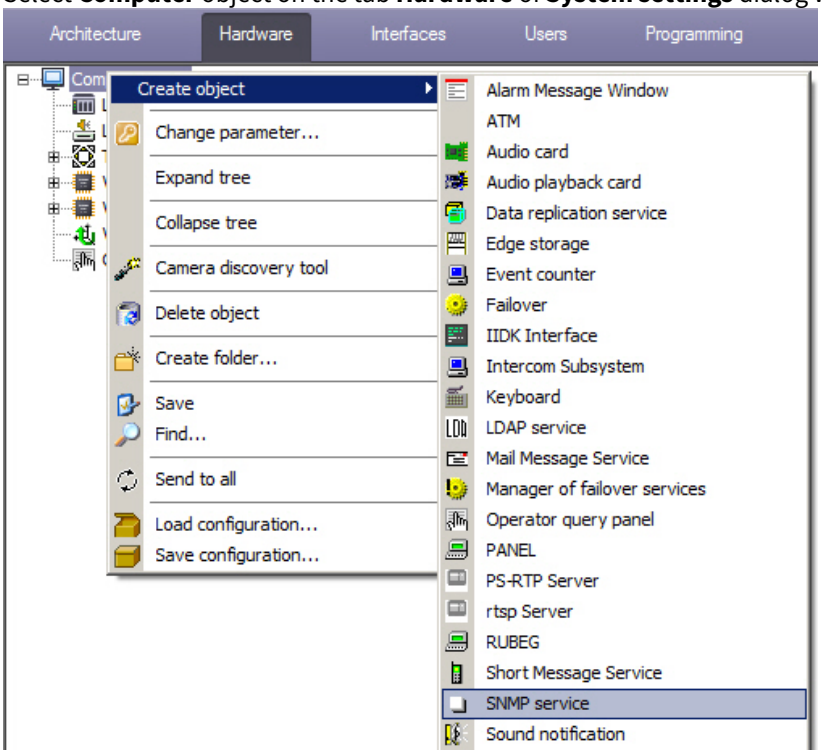
1. Create **SNMP trap** object on the basis of **SNMP service** system objects (see Creating the SNMP trap object).
2. Select the events, which messages should be transferred to SNMP-manager (see Events selection for transmitting to SNMP manager).
3. Set the message conversion to SNMP format (see Configuring the message conversion into SNMP format).
4. Set the trap with SNMP-message (see Setting up the trap with SNMP-message).
5. Check the validity of SNMP configuration, if necessary (see SNMP configuration for traps receiving on remote computer).

> **Note.**
>
> It is not recommended to create lots of SNMP trap objects (more than 10) as it can cause system slowdown.

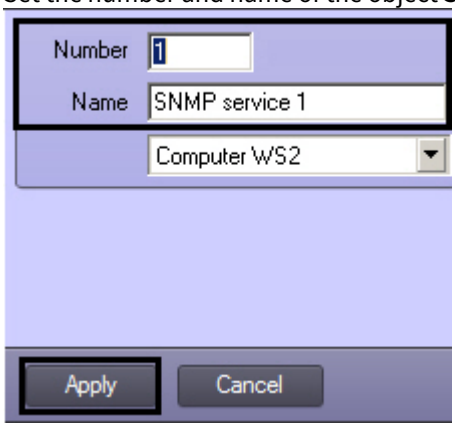
23.3.8.2 Creating the SNMP trap object

Creating the **SNMP trap** object is done in the following way:

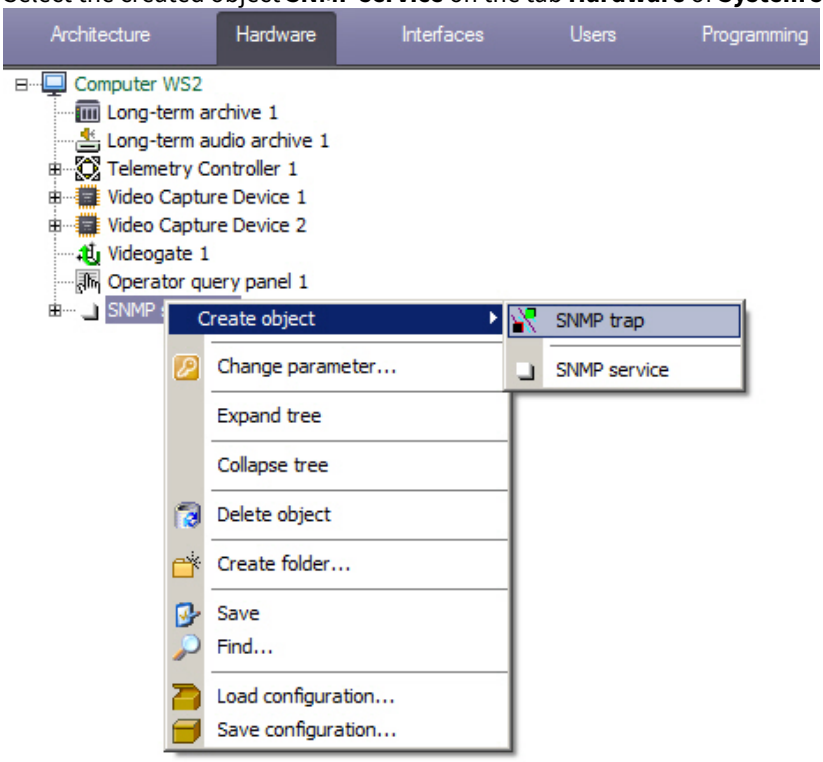
1. Select **Computer** object on the tab **Hardware** of **System settings** dialog window.



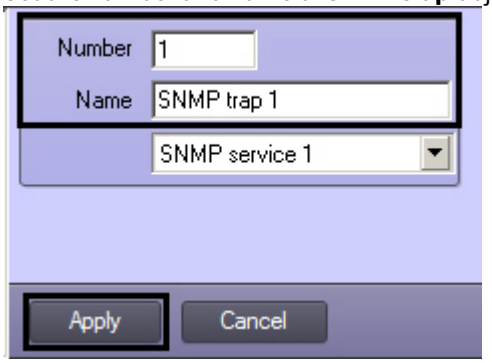
2. Make a right mouse click upon the selected **Computer** object and select **Create object -> SNMP service** in the contextual window.
3. Set the number and name of the object **SNMP service** and then click **Apply**.



4. Select the created object **SNMP service** on the tab **Hardware** of **System settings** dialog window.



5. Make a right mouse click upon the selected object **SNMP service** and select the point **Create object -> SNMP trap** in the contextual window.
6. Set the number and name of **SNMP trap** object in the appeared window and then click **Apply** button.



Note.

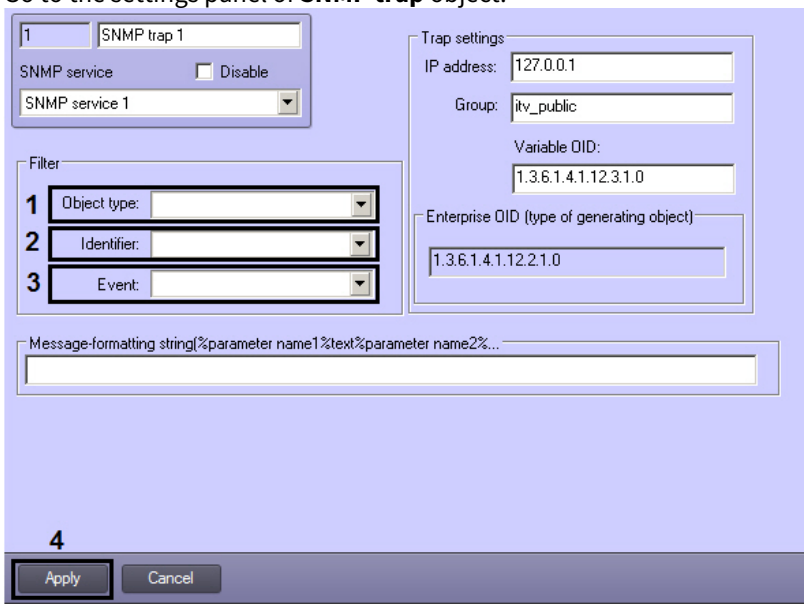
Settings panel of **SNMP trap** object will appear in result.

Creating the **SNMP trap** object is over.

23.3.8.3 Events selection for transmitting to SNMP manager

Selection of events for transmitting to SNMP-manager is done in the following way:

1. Go to the settings panel of **SNMP trap** object.



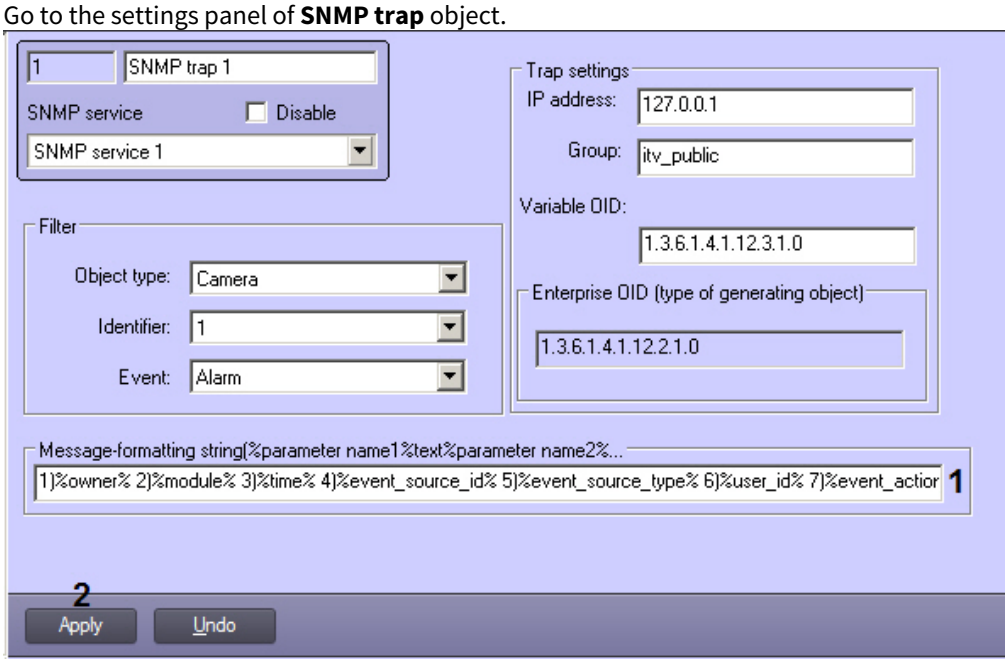
2. From the dropdown list **Object's type** of **filter** group select the object's type for which the required event may be registered (1). If no object's type is selected, all the events concerning all the system objects will be transferred to SNMP-manager.
3. From the dropdown list **Identifier** of **filter** group select the object's identification number, which type has been entered during the second step (2).If the field is not fulfilled, all the events concerning objects of the given type will be transferred to SNMP-manager.
4. From the dropdown list **Event** of **filter** group select the required object for the set during steps 2-3 object (3). If the field is not fulfilled, all the events registered for the given event will be transferred to SNMP-manager.
5. Click **Apply** button to save the changes (4).

Selection of events for transmitting to SNMP-manager is completed.

23.3.8.4 Configuring the message conversion into SNMP format

SNMP-service implements message conversion into SNMP format. SNMP-message is a sequence of parameters, describing the event. Parameter's name is changed by the value of this parameter in the pattern of SNMP-message with the event registration. Changing the SNMP-message is done in the following way:

1. Go to the settings panel of **SNMP trap** object.



2. Enter in the field **Message's format string (%parameter's name1%text% parameter's name2%...** parameters'names in the required sequence. Description of event's main parameters is given in the table.

Parameter's name	Description of parameter	Availability in the message
%event_action%	Event, registered in the system	Is determined by object's type, for which the event may be registered
%event_source_id%	Object's identification number, for which the event has been registered	
%event_source_type%	Object's type, for which the event has been registered	
%owner%	Computer name, from which the message has been received	Obligatory message's parameters
%time%	Time of event's creation	
%user_id%	Computer's user identification number, from which the message has been received	Optional message's parameters
%module%	Module's name, for which the event has been registered	

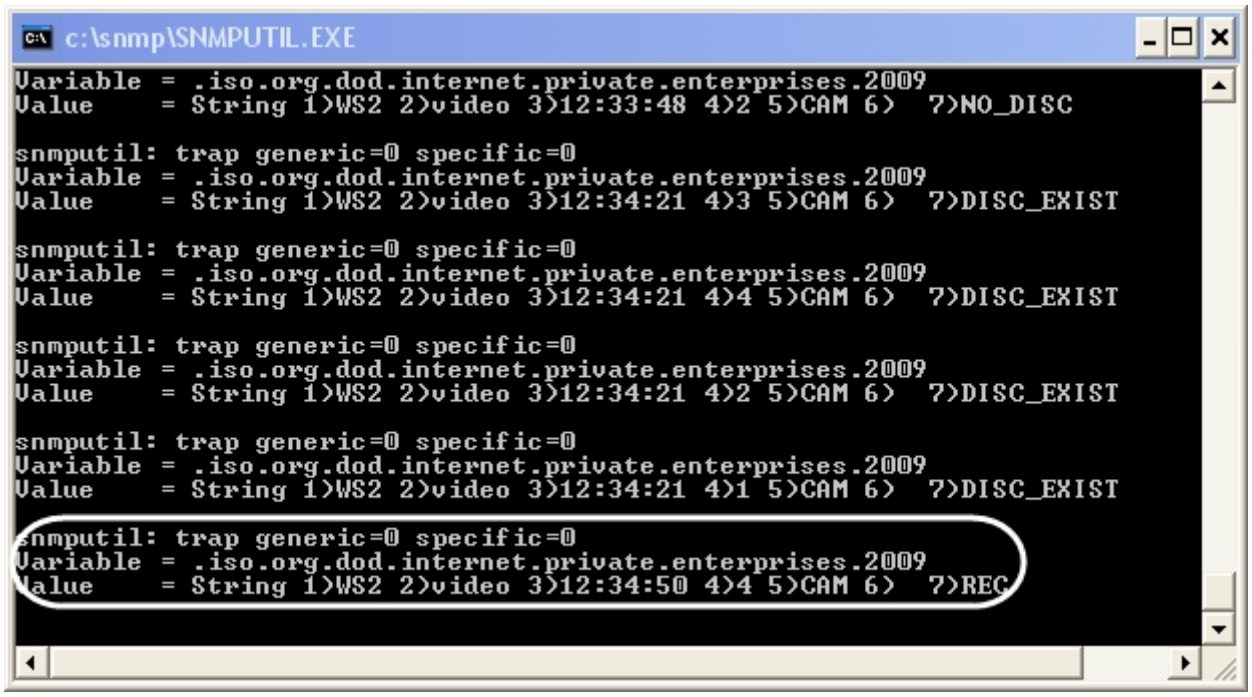
Note.

In case when message's format string is not set, SNMP message is formed in accordance with the pattern %event_action%,%event_source_id%,%event_source_type%, %owner%,%user_id%,%module%.

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

Changing the pattern of SNMP-message is completed.

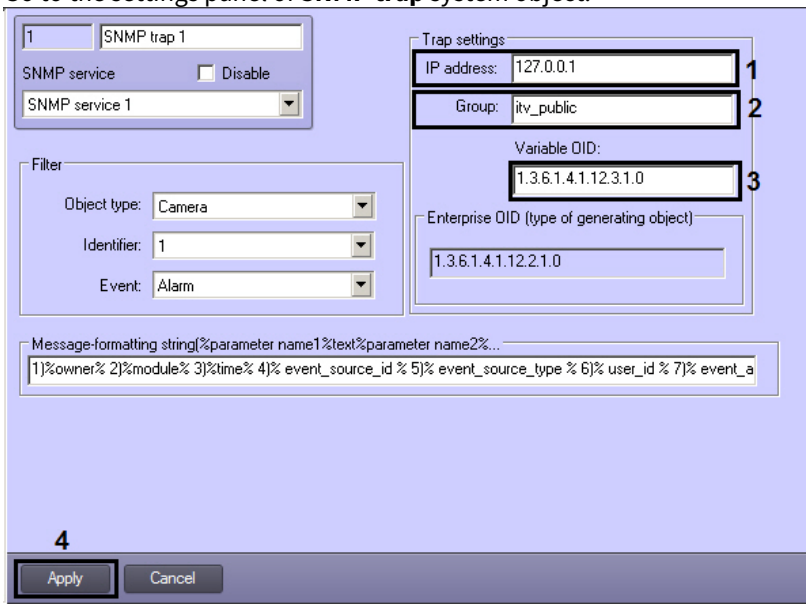
Example of SNMP-message, formed in accordance with the pattern "1)%owner% 2)%module% 3)%time% 4)%event_source_id% 5)%event_source_type% 6)%user_id% 7)%event_action%" is exemplified in the figure below.



23.3.8.5 Setting up the trap with SNMP-message

Setting the trap with SNMP-message is done in the following way:

1. Go to the settings panel of **SNMP trap** system object.



2. In the **ip** field enter IP-address from SNMP-manager, that will receive SNMP-traps with messages concerning the events(1).
3. In the field **Group** enter the community name for SNMP-trap authentication on the computer with installed SNMP-manager(2).

> **Note.**
>
> Safety model on the basis of communities is realized in *Intellect* program complex.

4. In the field **OID** enter the unique trap's number in the tree of SNMP-objects (3).
5. To save the changes click **Apply** button (4).

Setting up the trap with SNMP - message is completed.

23.3.8.6 SNMP configuration for traps receiving on remote computer

It is possible to use SNMPUTIL.EXE utility to check the validity of SNMP configuration. In this case SNMP configuration for traps receiving sent by Intellect software on remote computer is performed as follows:

1. Start the **SNMP Trap** on the computer where SNMPUTIL.EXE utility is run.
2. Specify address of this computer in settings of the **SNMP Trap** object (as described in the Setting up the trap with SNMP-message section).
3. Run the SNMPUTIL.EXE utility with "trap" flag.

> **Note.**
>
> It is not required to run SNMP services on the computer where the **SNMP Trap** object is created.

23.3.9 Setting up and connecting the special keyboard

The *Special keyboard* module is used for efficient control of the main functions of interface objects in the INTELLECT™ software. The *Special keyboard* allows to control the following system's main functions:

1. Video surveillance
2. Audio control
3. Telemetry

4. Events protocol
5. Macros
6. Sensor/Relay

INTELLECT™ software supports any USB or PS/2 keyboard, for example, programmable Posiflex KB-4000 (POS keyboard).

The following models of the *Special keyboard* device were supported in earlier versions:

1. PROMAG KB-840. Out of production.
2. PROMAG KB-950A. Out of production.

Note.

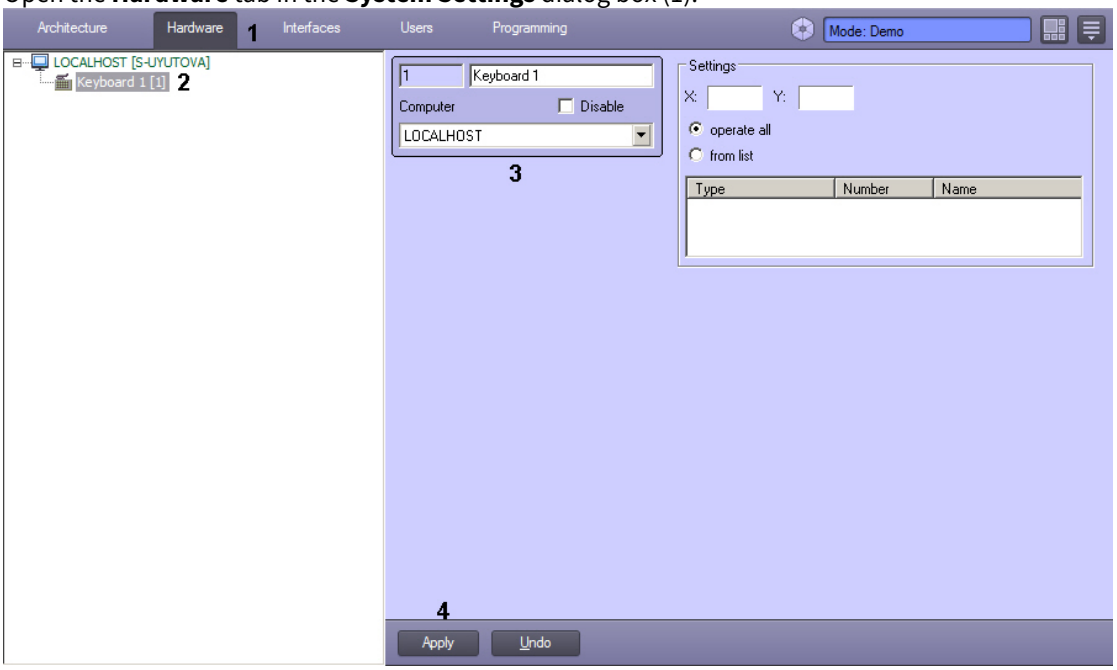
The process of connecting and setting up the PROMAG KB-950A model is the same as for PROMAG KB-840. PROMAG KB-950A setup is described in the documentation for INTELLECT™ version 4.7.4, PROMAG KB-840 – version 4.9.8 (see AxxonSoft documentation repository).

Use of the specialized keyboard

23.3.9.1 Setting up the Keyboard object in INTELLECT™ software

To create and set up the *Keyboard* system object in INTELLECT™ software, follow the sequence:

1. Open the **Hardware** tab in the **System Settings** dialog box (1).



2. Create the **Keyboard** system object on the base of the **Computer** object or select the relevant object in the objects tree on the **Hardware** tab of *Intellect* settings panel (2).
3. Enter the ID of the created object, its name and select the **Computer** system object to be the parent one for the **Keyboard** object (3).
   The **Computer** system object should match the computer, to which the *Special keyboard* device is connected.
4. Click **Apply** (4).

See Settings the interpretation rules of the Special keyboard layout by Intellect program complex section for further configuration.

Note.

Please refer to the INTELLECT™ version 4.9.8 documentation for instructions on the discontinued PROMAG keyboard configuration: Setting up and connecting the special keyboard.

23.3.9.2 Settings the interpretation rules of the Special keyboard layout by Intellect program complex

Pressing of any button on the *Special keyboard* device shall correspond to certain option activation in INTELLECT™ software.

To achieve this, perform the following settings:

1. Create and configure the **Special keyboard** object under the computer to which the special keyboard is connected, e.g. create the **Special keyboard** object under the Client computer if the keyboard is connected to the Client.
2. Set the "1" value for the ProcessAll parameter that is described in details in Registry keys reference guide. The parameter should be created on the computer to which the special keyboard is connected, e.g. create the ProcessAll key on the Client, not Server, if the keyboard is connected to the Client.
3. Run the Client with Windows administrator rights to use the keyboard on the Client.

   Note.

   The run with administrator rights can be avoided if the ProcessAll key is created on the Client in the following registry section: Computer**HKEY_CURRENT_USER**\Software\ITV\Intellect\Keyb\ProcessAll=1
4. In this case keypress on the keyboard will be processed in Intellect as an event like this:
   Event : KEYB|1|NEW_KEY_PRESSED|slave_id<A-BELYAEV>,fraction<43>,owner<A-BELYAEV>,module<keyb.run>,date<01-02-19>,guid_pk<{CEF89AAD-FB25-E911-ACF1-A0F3C1007840}>,core_global<1>,wparam<55>,time<11:30:56>
   where wparam<55> is the key ID.
5. Use these IDs in Scripts and Macros (see Creating and using macros and The Script object. Programming using the JScript language).

23.3.10 Configuring the System restart service

23.3.10.1 General information on the System restart service module

The System restart service is designed to control the workability of *Intellect* software modules and their restart if there is no response during the specified time interval. Software as well as hardware control of workability can be used.

Important!

Only those *Intellect* modules the processes of which are created under Slave.exe process (run under Intellect.exe process) are displayed in the system restart service.

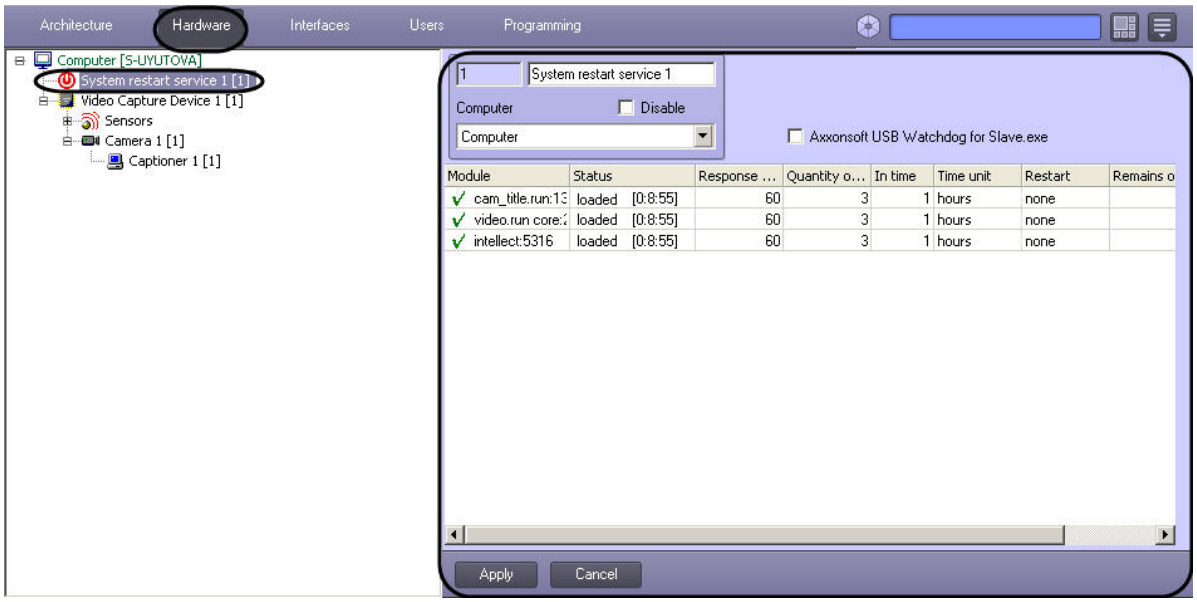
Note.

Use the special utility and the script to control the RTSP Server module workability – see The openRTSP.exe utility for checking RTSP workability.

The System restart service allows performing the following actions if there is no response from the module:

1. Computer restart (hardware operability testing, additional devices are to be enabled). The computer will restart if the slave.exe process is not active.
2. Module restart. Only module which is not replying to requests will restart if there is no response from this module.
3. Core restart. The Intellect core will restart if there is no reply from the module.

The System restart service is configured on the settings panel of the **System restart service** object. This object is based on the **Computer** object in the **Hardware** tab of the **System settings** dialog box.

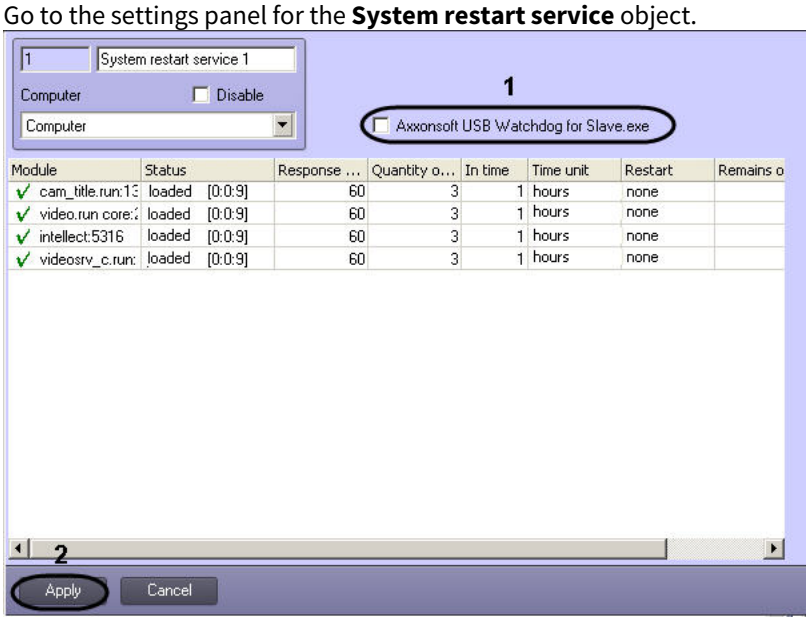


23.3.10.2 Activating the hardware control of workability

Connect the AxxonsoftUSBWatchDog cable to activate the system of hardware control of workability (see Installing and configuring security system components guide).

To activate the hardware control of workability do the following:

1. Go to the settings panel for the **System restart service** object.



2. Set the **Axxonsoft USB WatchDog for Slave.exe** checkbox (1).
3. Click the **Apply** button (2).

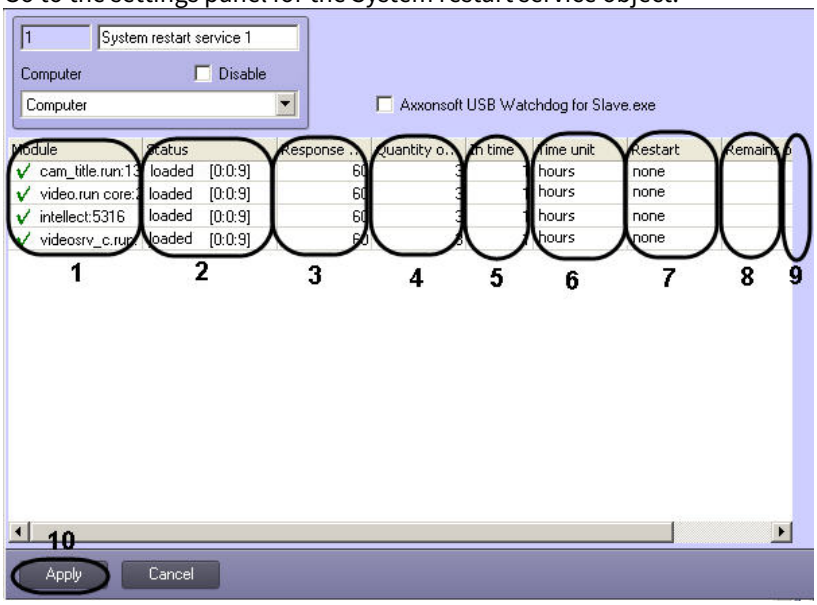
Hardware control of workability is now activated.

23.3.10.3 Configuring the software control of workability

Software control of workability allows restarting the module or Intellect core if there is no response from the module.

To configure the software control of workability, do the following:

1. Go to the settings panel for the System restart service object.



2. The list of run modules on this computer is displayed automatically in the **Module** column (1).

> **Note.**
>
> Modules with the **In process** state are marked with ✓ sign. Modules with the **No response** state (red field) or **Shutdown** are marked with ! sign

3. The current state of modules is automatically displayed in the **Status** column (2). In the square brackets the time of module working since the last restart is displayed in HH:MM:SS format.
4. In the **Response timeout**, sec, type-in the time period in seconds during which the response from the module will be waited (3).

> **Note.**
>
> The system will restart if there is no response from the module within the waiting interval.

5. In the **Quantity of restart** field, type-in the maximum of restarts (module or Intellect core) that can be performed within the specified time period (4).
6. In the **In time** field, type-in the new value and/or select in the **Time unit** dropdown list the required metric unit of period to change the value of time period during which the maximum restarts can be performed (5-6).
7. In the **Restart** dropdown list, select the required method of restart (7).
   a. Select the **module** method, to restart module without response.
   b. Select the **core** method, to restart the Intellect core without response from the module.

> **Note.**
>
> Select the **None** value if the restart is not needed when there is no response from the module.

8. The remaining number of restarts within the specified time period is automatically displayed in the **Remains of restarts** column (8).

> **Note.**
>
> The module changes over to the **Shutdown** state if the number of performed restarts exceeds the maximum.

> **Note.**
>
> The remaining reboots counter may be reset in the following circumstances:
> a. If the period of time in which the maximum number of reboots can be performed has elapsed but the number of reboots performed does not exceed the maximum, then the counter will be reset upon a new reboot.
> b. If the period of time in which the maximum number of reboots can be performed has elapsed and the maximum number of reboots has been performed, then the module will reboot and the counter will be reset.

9. In the **Memory (Mb)** field enter the value of the memory threshold consumed by module. Exceeding of this value requires the system restart (9)
10. To save changes, click the **Apply** button (10).

The software control of workability is now configured.

23.3.10.4 Getting the information on memory consumption for processes

To the slave.log log file corresponding to the **Computer** object based on which the **System restart service** object is created the information about memory consumption by processes run by the *Intellect* software is recorded once in a minute.

Messages look like this:

!WARNING <<<process information>>> name="video.run", committed memory is 83001344 bytes (79MB, 81056KB). DELTA is 22687744 bytes (21MB, 22156KB).

The DELTA value is the difference between the current and previous values of memory consumption by this process.

23.3.11 Configuring backup archiving

23.3.11.1 Purpose and implementation of backup archiving in the Intellect software

The *Intellect* software allows creating the backup copies of video and audio recordings. The *Backup archive* and *Backup audio archive* modules are used for creation of backup multimedia archives. When making a backup copy, the *Intellect* software copies video and audio recordings from the main archive of the videoserver to different storage devices.

Any drive discovered in the operating system can be used for storing the Backup Archive, including local drives, network drives, LTO drives, etc.

The *Backup archive* module copies the video archives received from the specified cameras to any of the available local or network hard drives. Copying of audio archive from specified microphones which are included in the digital video surveillance system is performed while using the *Backup audio archive* software module. Archive files are copied on loop on any of connected disks as the main archive is recorded (see the General information on video archiving section)

The *Backup archive* module supports the following functions:

1. Copying the video archive to local or network hard drives, or USB storage.
2. Changing the frame rate of the signal (grooming) at the time of saving it to *Backup archive*.
3. Changing the rate of data transfer via a local network.
4. Setting up the periodicity of backup archiving.
5. Cyclic copying of the data to the connected storage devices.
6. Viewing the video archive from *Backup archive* on the video surveillance monitor.

> **Note.**
>
> To record the audio archive together with the video archive, configure the **Backup audio archive** object (see Configuring the Backup audio archive module section).

A folder named VIDEO which holds the backup multimedia archive is created on the specified storage devices when setting up the corresponding objects.

The backup copying module can be controlled:

1. Manually using special interface objects.
2. Automatically using the built-in programming capabilities of Intellect software – macros and scripts.

Configuring the Backup archive panel object
Copying video sequence to the Backup archive

23.3.11.2 Configuring the Backup archive module

The *Backup archive* module is used to make backup copies of the video archive from the videoserver. The *Backup archive* module copies the video archives received from the specified cameras to the specified storage device.

Note.

A Remote Administrator's Workstation (RAW), where the *Backup archive* is installed, is to have data about servers archive so that the video archive being copied uniformly from specified cameras. For this the remote workstation gets data about archive indexes from the server once in 30 seconds. After system restarting, data exchange is stopped until the *Backup archive* is started.

The *Backup archive* module is configured by an **Backup archive** system object. When the **Backup archive** object is created, a **Backup audio archive** object with the same identifier is created automatically.

23.3.11.2.1 Configuration procedure for the Backup archive object

To configure the **Backup archive** object, do the following:

1. Create the **Backup archive** object on the base of the **Computer** system object (see Creating the Backup archive object);
2. Select and configure cameras to copy the video archive to the *Backup archive* (see Selecting and configuring the cameras for the Backup archive or Selecting cameras as a group for the Backup archive);
3. Set the parameters of video archive transmission over LAN (see Setting the parameters of video archive transmission over LAN);
4. Select disks to store the *Backup archive* module (see Selecting disks to store the archive of the Backup archive module).
5. Configure the video archive grooming when it is copied to the *Backup archive* (see Configuring the grooming of the video archive);
6. Configure the schedule of video archive copying to the Backup *archive* (see Configuring the schedule of the video archive copying);

   Note.

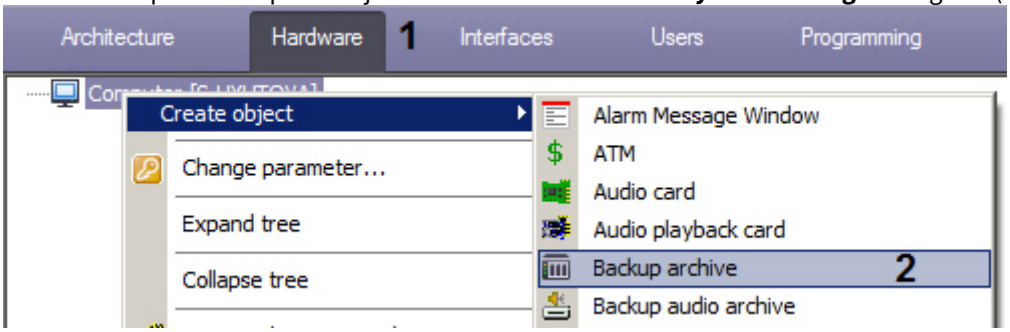
   It is recommended to restart the *Intellect* software after performing actions described above for correct using of **Backup archive** object settings.

7. Configure the **Panel of Backup archive** interface object (see Configuring the Panel of Backup archive object).

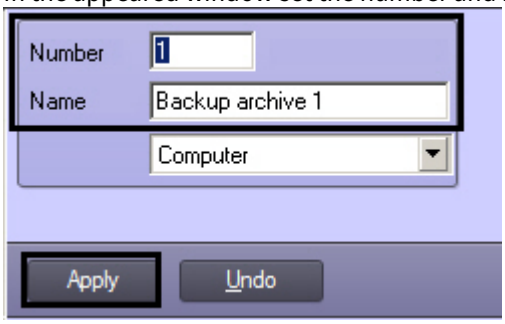
23.3.11.2.2 Creating the Backup archive object

To create the **Backup archive** object, do the following:

1. Select the required computer object on the **Hardware** tab of **System settings** dialog box (1).



2. Click right mouse button upon the selected **Computer** object and select **Create object -> Backup archive** in the context menu (2).
3. In the appeared window set the number and name of the **Backup archive** object and then click the **Apply** button.



> **Note.**
>
> The settings panel for the **Backup archive** object is displayed as a result.

4. Repeat steps 1-3 for all required **Computer** and the **Backup archive** objects.

The **Backup archive** object is now created.

23.3.11.2.3 Selecting and configuring the cameras for the Backup archive

There are two ways to select and configure cameras for copying the video archive to the *Backup archive*:

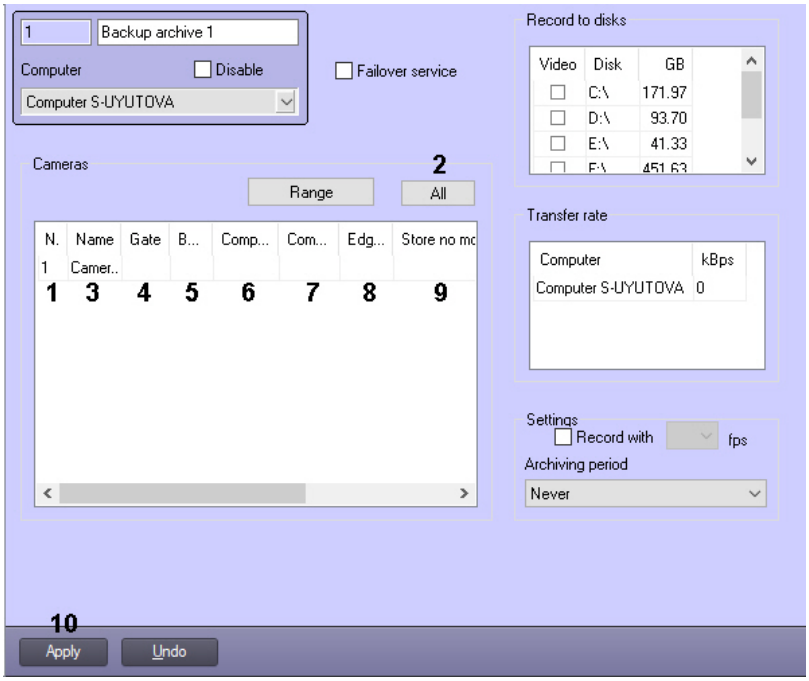
1. Separately. The settings panel for the **Backup archive** object is in use.
2. Integrated selection. The **Add/Edit cameras** dialog box is in use.

> **Note.**
>
> The order of cameras' complex selection for copying the video archive to the *Backup archive* is described in the Integrated selection of cameras for the Backup archive section.

To select cameras on the settings panel of the **Backup archive** object, do the following:

1. Go to the settings panel for the **Backup archive** system object.
2. In the **Number** column of the **Cameras** group, select the name of the required video camera (1).

> **Note.**
>
> To select all the cameras registered in the system, click the **All** button (2).



3. As a result the name of the selected camera is automatically displayed in the **Name** column of the **Cameras** group (3).
4. If a video archive from the selected camera is to be received via the **Videogate** object, then select the name of this object from the **Gate** drop-down list (4).
5. If a video archive from the selected camera is to be transmitted from another **Backup archive** object, select the name of this object in the **Backup archive** drop-down list (5).
6. To change the procedure of video signal compression during the record to the **Backup archive**, select the required procedure of compression from the **Compressor** drop-down list (7).The value in the **Compression** list is to be selected if the compressor is specified (6).
7. To change the level of video signal compression during the record to the *Backup archive*, select the required level of video signal compression from the drop-down list in the **Compression** column (6). The level of bideo signal compression will increase from 0 (no compression) to 5 (maximal compresion).

   Note.

   Re-compression is performed on the side of the *Backup archive*.

8. In the **External storage** dropdown list select the name of the object corresponding to the external storage of IP device from which video recordings are to be imported to the Backup archive (8). For more details see Configuring the access to the archive in edge storage section.
9. In the **Store no more than (hours)** field, enter the time period in hours after which the archive entries of the corresponding camera should be deleted from the Backup archive (9). The rules for setting this parameter are the same as for the main archive – see Configuring video camera archive depth.
10. Repeat steps 2-9 for all the cameras.
11. To save all the changes, click the **Apply** button (10).

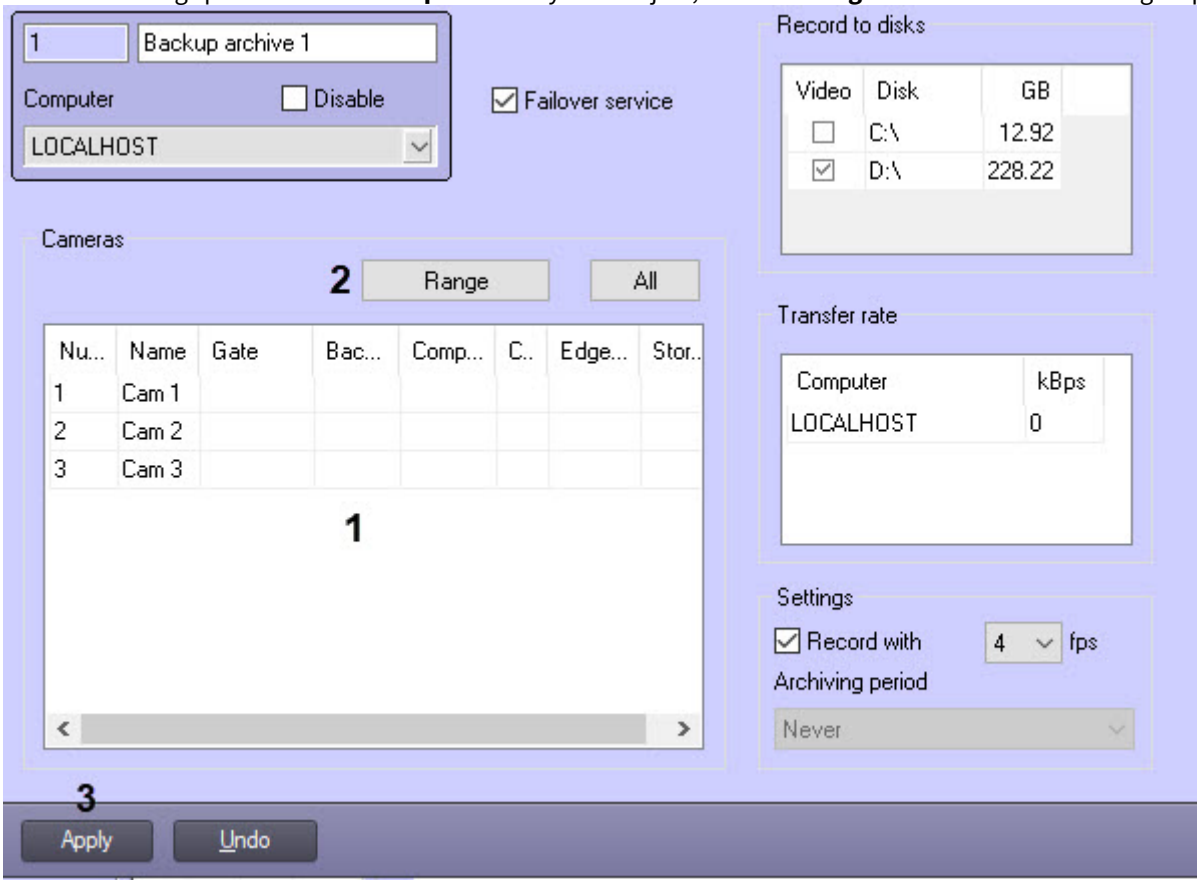
The cameras on the settings panel of the **Backup archive** object are now selected.

23.3.11.2.4 Selecting cameras as a group for the Backup archive

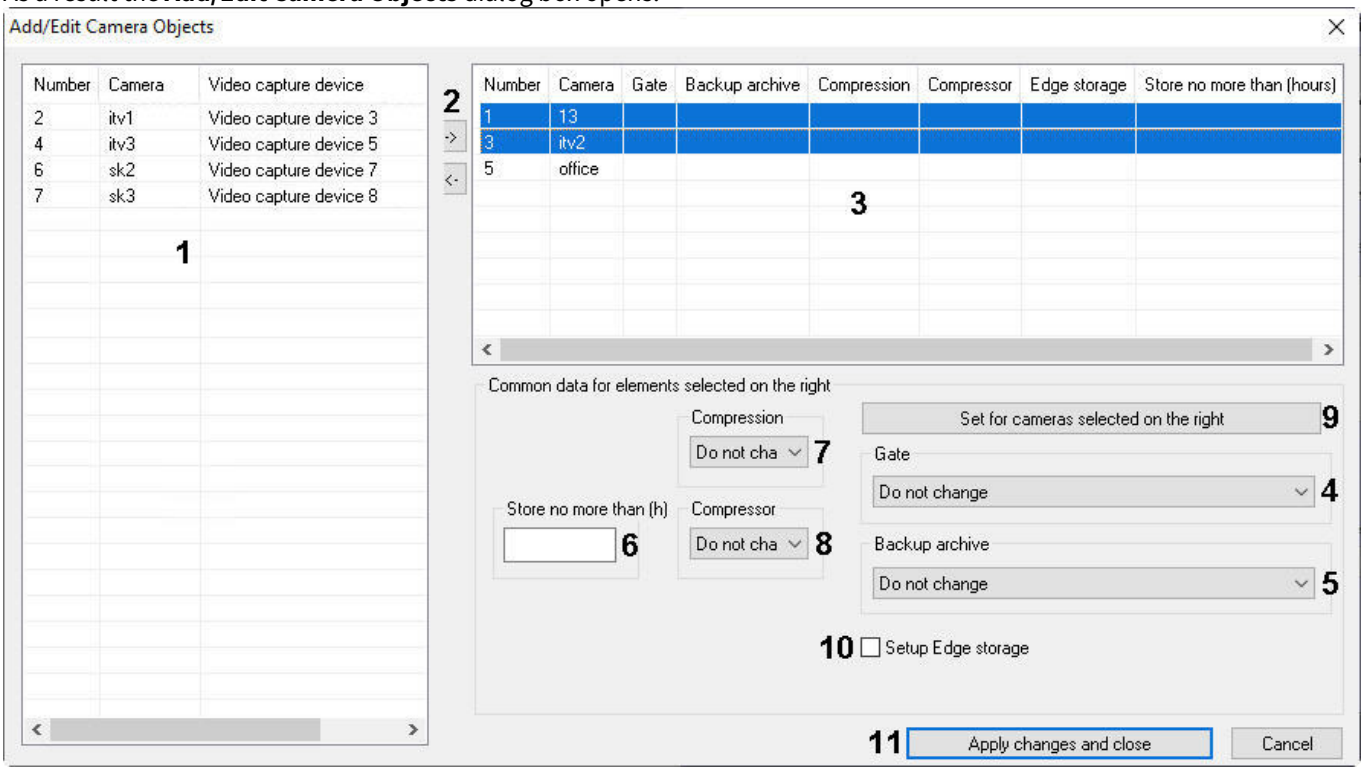
There is an opportunity of integrated selection and editing of cameras' parameters for copying the video archive to the *Backup archive*.

Integrated selection can be performed in the following way:

1. Go to the settings panel for the **Backup archive** system object, click the **Range** button in the **Cameras** group (1).



2. As a result the **Add/Edit Camera Objects** dialog box opens.



3. Select the required cameras in the left list of the **Add/Edit Camera Objects** box (**1**).
4. Move the selected cameras to the right list by clicking the -> button (**2**).

> **Note.**
>
> The list on the right is the list of cameras selected for copying the video archive to the *Backup archive*.
>
> The <- button is used for reverse action that is for moving the selected video cameras from the right list to the left one (**2**).

5. As a result the selected cameras are displayed in the right list of the **Add/Edit Camera Object** box (**3**).
6. If it is necessary in the right list select the names of required cameras for complex editing their parameters (**3**).

> **Attention!**
>
> For all the selected cameras the same parameters will be set.

7. If a video archive from the selected camera is to be received via the **Videogate** object, then select the name of this object from the **Gate** drop-down list (**4**).

> **Note.**
>
> The **Gate**, **Backup archive**, **Setup Edge storage**, **Store no more than (h)**, **Compression**, and **Compressor** settings belong to the **Common data for elements selected on the right** group.

8. If a video archive from the selected camera is to be transmitted from another **Backup archive** object, select the name of this object in the **Backup archive** drop-down list (**5**).
9. In the **Store no more than (h)** field, enter the time period in hours after which it is necessary to delete the records from the corresponding camera from the *Backup archive* (**6**). The parameter should be set according to the same rules as for the main archive — see Configuring video camera archive depth.
10. If it is necessary to change the video signal compression level when recording to the *Backup archive*, select the required video signal compression level from the **Compression** drop-down list (**7**). The video signal compression level increases from 0 (no compression) to 5 (maximum compression).
11. If it is necessary to change the video signal compression algorithm when recording to the *Backup archive*, select the required compression algorithm from the **Compressor** drop-down list (**8**). If a compressor is specified, it is necessary that a value be selected in the **Compression** list (**7**).

> **Note**
>
> Video signal recompression is performed on the *Backup archive* side.

12. Check the **Setup Edge storage** checkbox if it is necessary to apply external storages to the selected cameras, if any (**10**, for more details on external storages, see Importing from edge storages). In this case, the video recordings will be imported into the *Backup archive* from the external storage corresponding to each camera.
13. To save the parameters, click the **Set for cameras selected on the right** button (**9**).
14. As a result, the set parameters are shown in the list on the right of the **Add/Edit Camera Objects** box (**3**).
15. Repeat steps 6-13 for complex editing of all the required cameras.
16. To save the changes and close the **Add/Edit Camera Objects** box, click the **Apply changes and close** button (**11**).
17. Camera settings are shown in the **Cameras** table on the settings panel of the **Backup archive** object (**2**).
18. To save all the changes, click the **Apply** button (**3**).

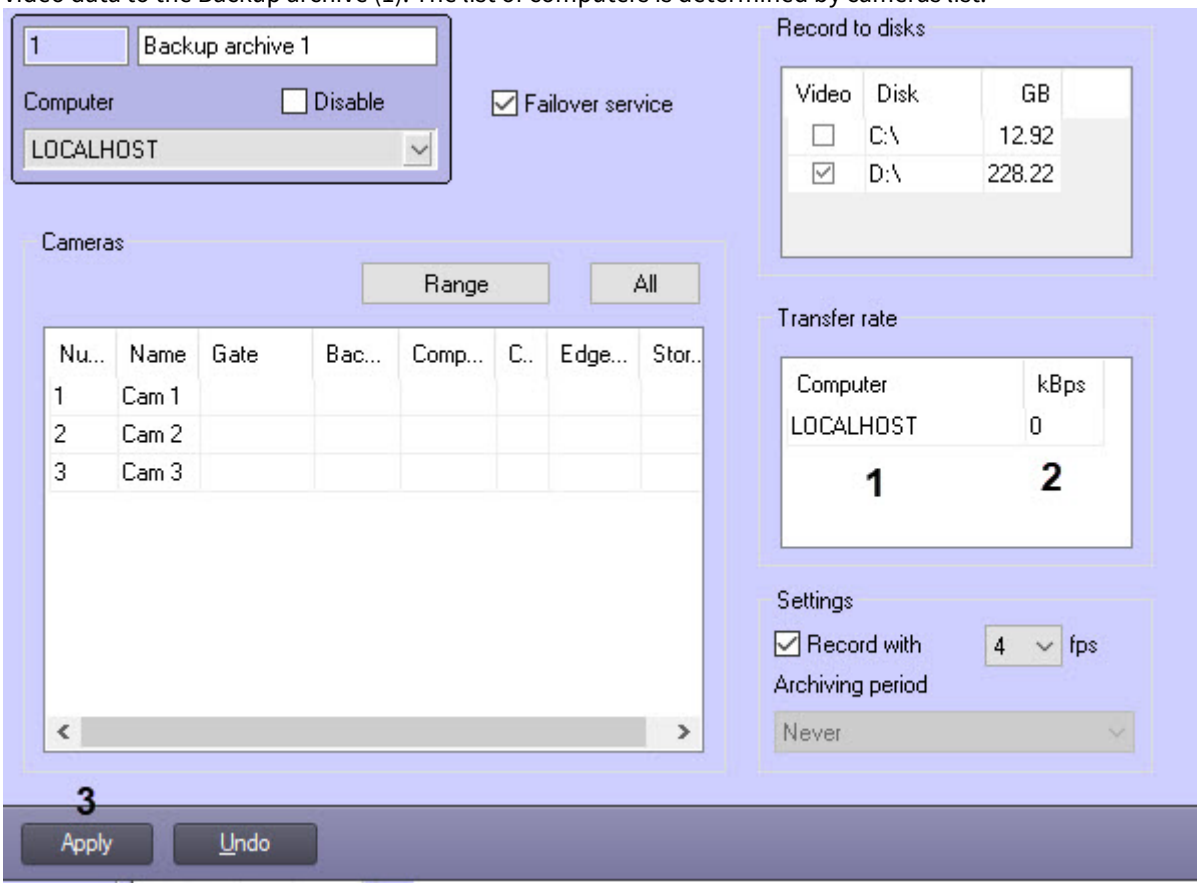
Integrated selection of video cameras is now over.

23.3.11.2.5 Setting the parameters of video archive transmission over LAN

There is a **Transfer rate** table in the setting panel for the **Backup archive** system object. This table limits the bandwidth over LAN for every Server transferring archive to the Backup archive module.

To set the bandwidth parameters, do the following:

1. Go to the settings panel for the **Backup archive** system object. In the **Transfer rate** table there are computers transferring video data to the Backup archive (1). The list of computers is determined by cameras list.



2. In the **kBps** column for each of the computers specify the values of maximum bandwidth for transmitting video over LAN for the computer (2).
3. To save the changes, click the **Apply** button and restart *Intellect* software (3).

The parameters of transmitting video archive over LAN are now set.

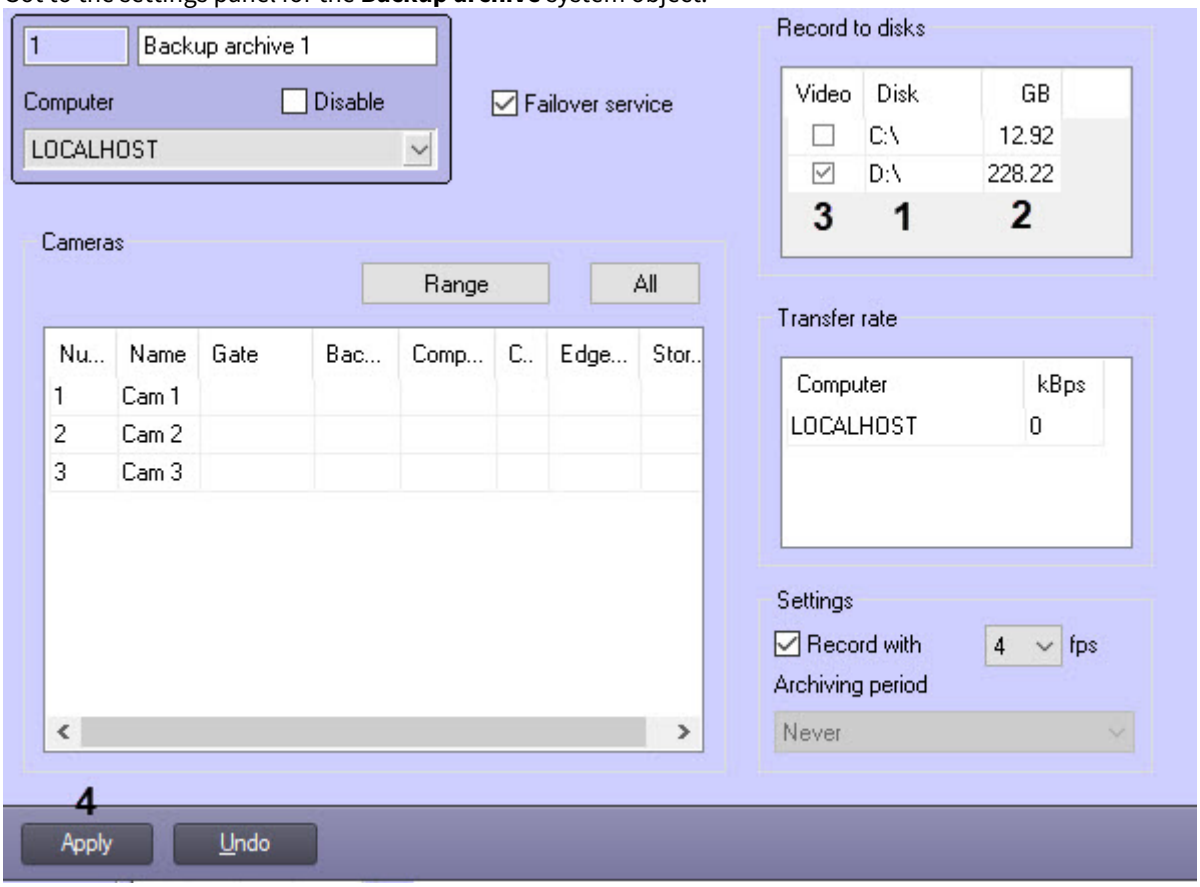
23.3.11.2.6 Selecting disks to store the archive of the Backup archive module

In INTELLECT™ software the backup copy of the video archive for the *Backup archive* module is stored to local and network disks and to connected USB storage. Backup files are stored in the VIDEO folders on these disks.

By default Backup archiving is disabled.

To select disks to store the archive of the *Backup archive* module, do the following:

1. Got to the settings panel for the **Backup archive** system object.

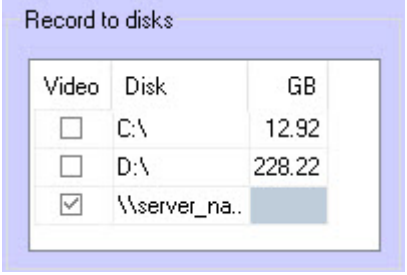


2. Names of local (net, USB) disks available for storing the archive of the *Backup archive* module are given in the **Disk** column of the **Record to disks** table (1).

> **Attention!**
>
> It is necessary to connect net disks via a command prompt with Administrator's rights for Windows Vista and Windows 7 OS with enabled UAC. The way of UAC enabling is described in the Connecting network disks in Windows Vista and Windows 7 OS section.

> **Note.**
>
> To use net disks for a Backup archive, set UNC paths to them in INTELLECT™ software. Details on working with net disks in INTELLECT™ software (installed as a Service) are given in Working with network disks of INTELLECT™ installed as a Service section.

3. Free space on disks (in GB) is given in the **GB** column (2).
4. In the **Video** column, set the checkboxes for disks selected for storing the archive of the *Backup archive* module (3).
5. To add a net disk by giving the UNC path, do the following:
   a. Go to the last line in the **Disk** list and click the down key.

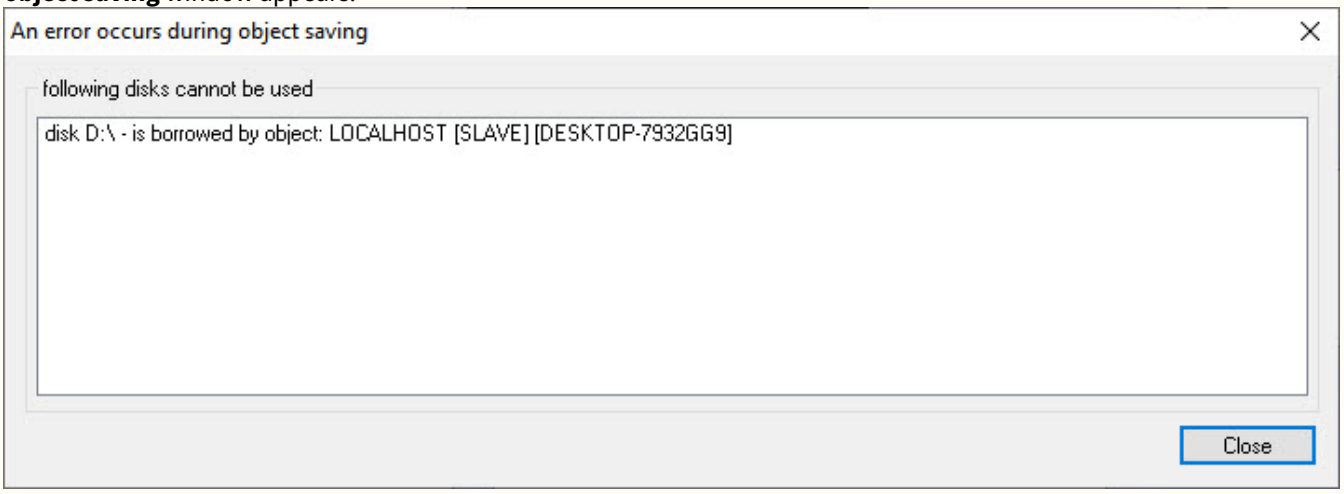


b. Specify the path to a net file in the appeared line in the **Disk** column. The UNC path is set in the "\\server_name\share_name" format, where the "server_name" is the name of file server and the share_name is the net name of general folder.
c. In the **Video** column, set the checkbox for the created disk.

6. To save the changes, click the **Apply** button (4).

Attention!

For storing the Backup archive one should select disks that are not used for storing video archive from cameras (are selected in the settings panel of **Computer** object). Otherwise after saving the given changes the **An error occurs during object saving** window appears.



The disks for storing the archive of the *Backup archive* module are now selected.

Note.

If no disks have been selected, the *Backup archive* backup is disabled.

23.3.11.2.7 Configuring the grooming of the video archive

Video signals can be groomed before they are copied to a backup archive of the *Backup archive* module. Grooming is performed at the Server from which the video signal is transmitted to the Backup archive.

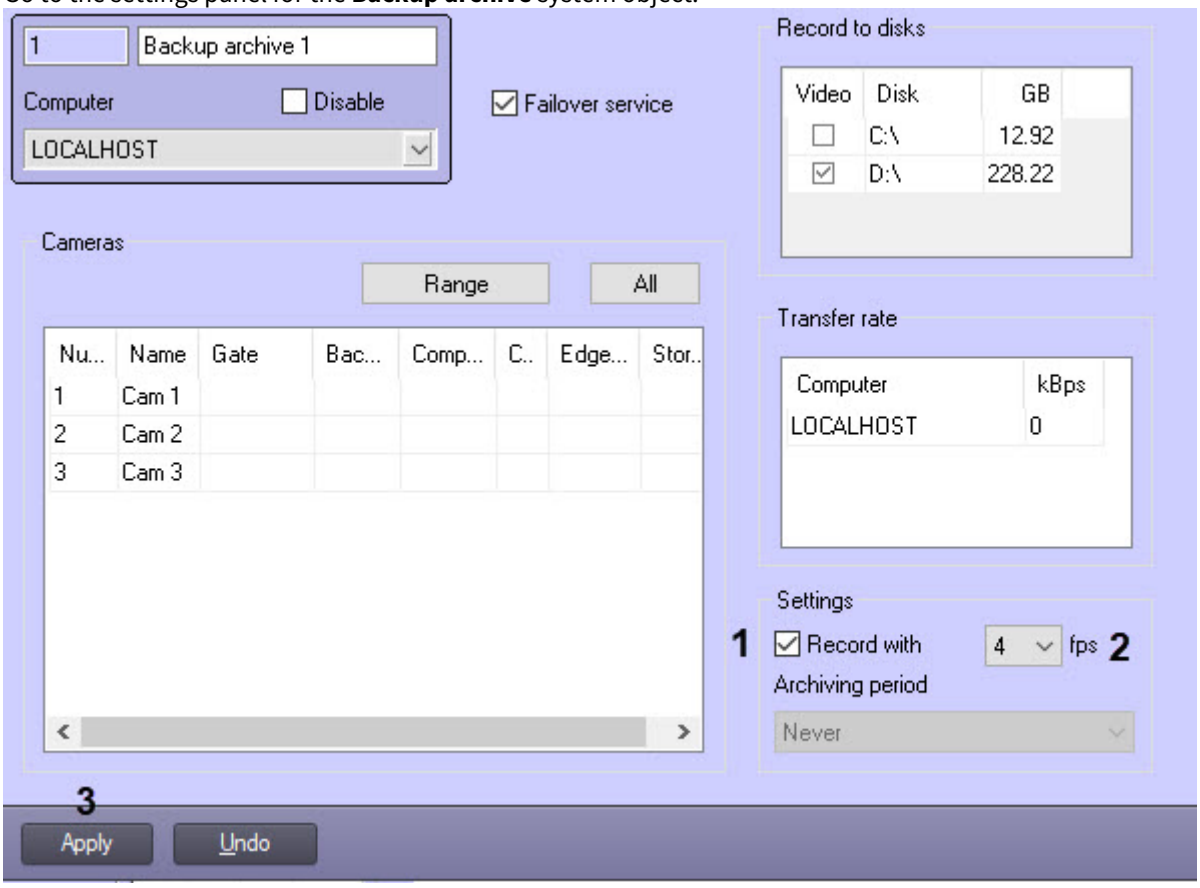
Note.

Grooming in the Backup archive may be performed with such codecs as MJPEG, Motion Wavelet, MPEG, H264 and MxPeg.
If the grooming rate is 25 fps, the video is processed at a lower rate for the first minute (~12 fps).
The maximum allowable grooming rate for MxPeg codec is 12 fps.

By default, a signal is copied from the server to the Backup archive without grooming.

To configure the grooming of video archive frames while copying them to the *Backup archive*, do the following:

1. Go to the settings panel for the **Backup archive** system object.



2. To enable the video archive grooming, set the **Record with ___ fps** checkbox in the **Settings** group (1).
3. In the **Record with ___ fps** drop-down list, select the required frame rate of video archive for transmitting to the *Backup archive* (2).

> **Note.**
>
> The selected **Record with ___ fps** value is to be less than frame rate of video signal digitized by a video capture card. Otherwise the frame rate of a video signal will be the same as the frame rate of digitizing.

> **Note.**
>
> The selected frame rate value of the video archive that is to be transferred to the *Backup archive* is an average value. A real value of frame rate may be different from that one, indicated in the **Record with ___ fps** drop-down list.

4. To save the changes, click the **Apply** button (3).

Video grooming is now configured.

23.3.11.2.8 Configuring the schedule of the video archive copying

The *Backup archive* module can be started in two ways:

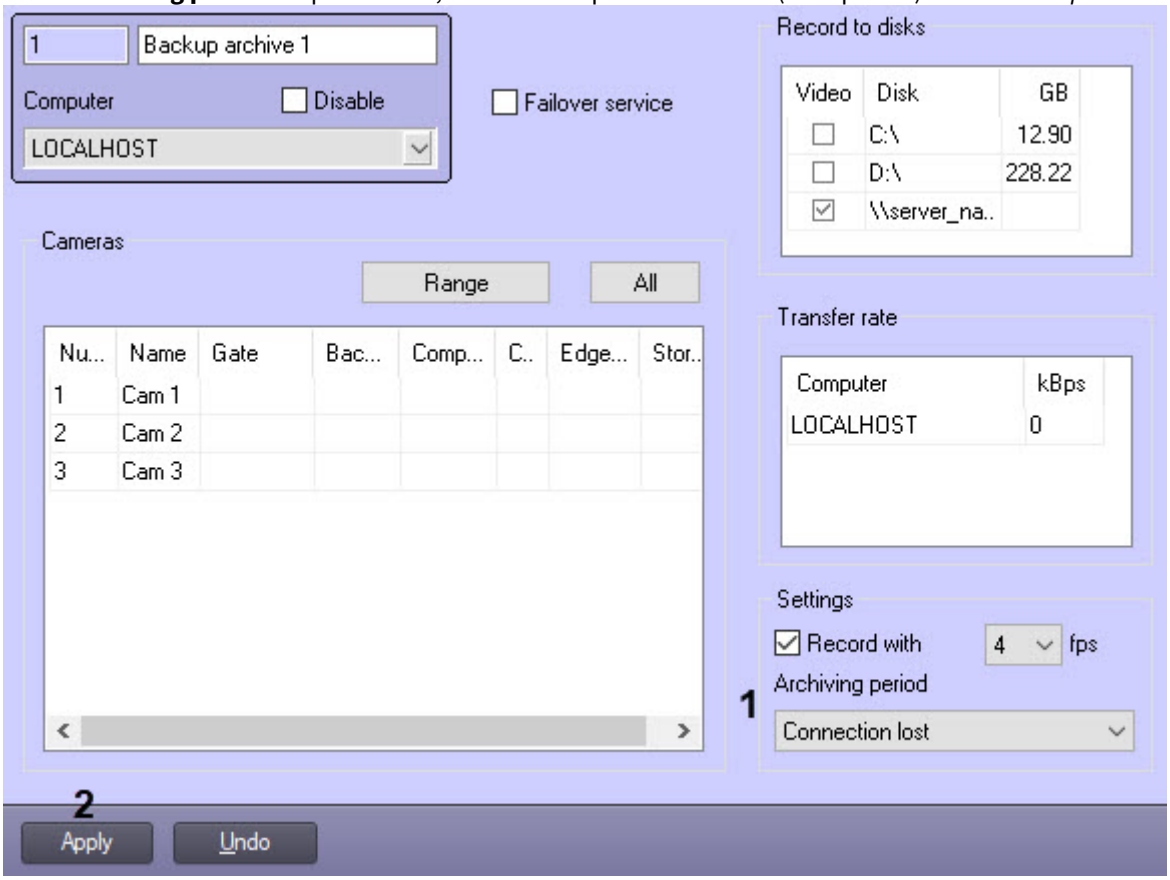
1. Automatically. Due to the schedule of copying on the settings panel of the **Backup archive** system object.
2. Manually. With the help of the **Backup archive panel** interface object (see Backup archive panel).

The process of automatic video archive copying is implemented starting with the latest recordings of video fragments. By default the automatic copying of video archive is not configured.

To configure the schedule of video archive's copying to the *Backup archive*, do the following:

1. Go to the settings panel for the **Backup archive** system object.

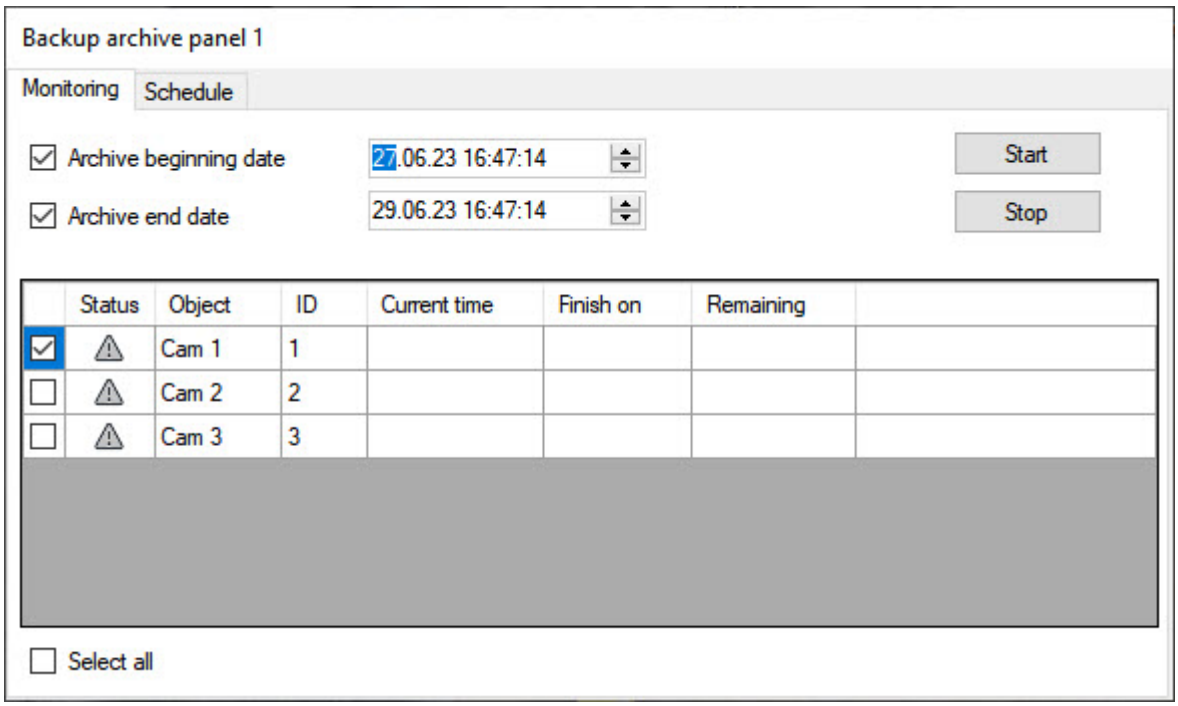
2. In the **Archiving period** drop-down list, select the required time zone (time period) of the *Backup archive* module start (1).



3. To save the changes, click the **Apply** button (2).

The schedule of video archive copying to the *Backup archive* is now configured.

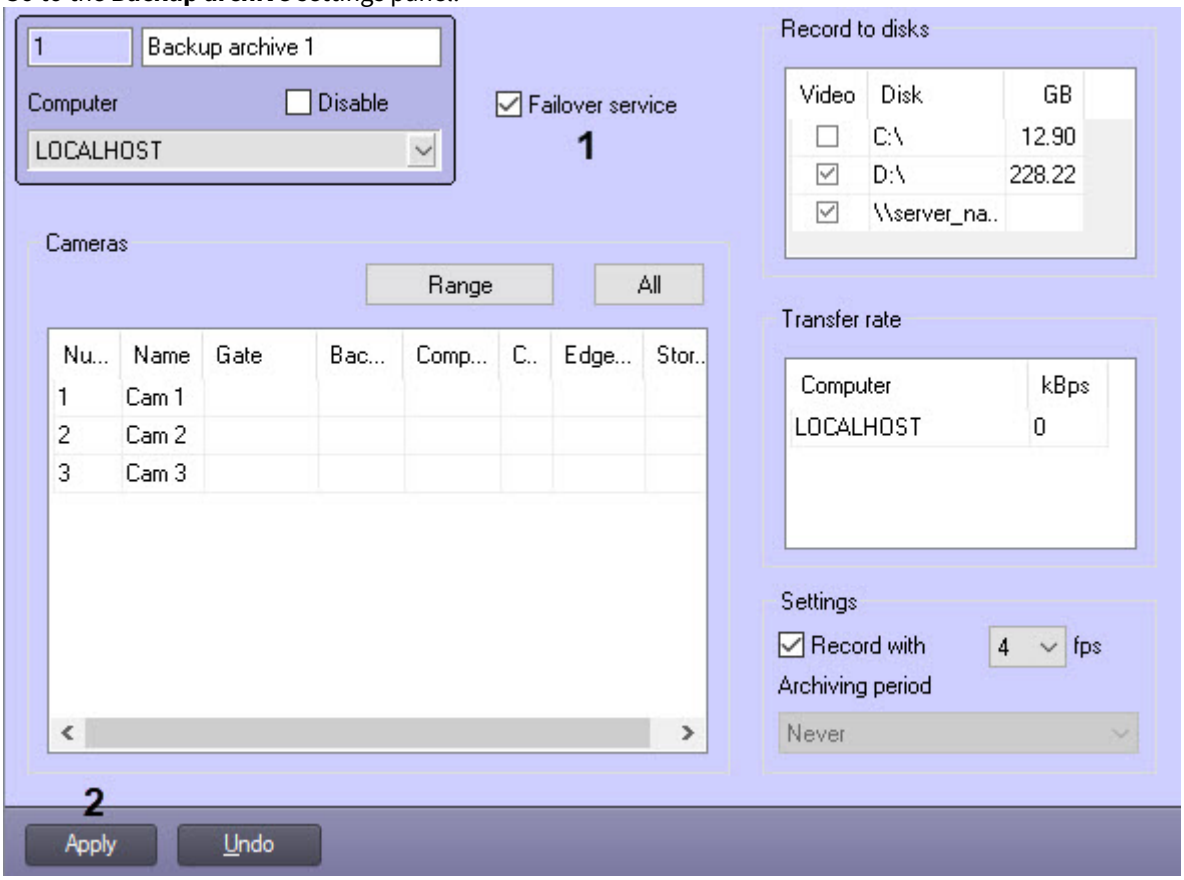
To start the archive backup manually, set the beginning and the ending dates of the archive to be copied and click the **Start** button (see Copying video sequence to the Backup archive).



23.3.11.2.9 Enabling cooperation of Backup archive with Failover service

If the Backup archive operates together with the Failover service, their cooperation is to be configured (see Configuring archive synchronization of main and backup Servers).
Cooperation of these modules is enabled as follows:

1. Go to the **Backup archive** settings panel.



2. Set the **Failover service** checkbox checked (1). The **Record to disks** table becomes unavailable for editing, and when the archive is requested from the main server, the Backup archive will be transferred from the disks specified on the settings panel of the **Computer** object under which the **Backup archive** object is created.
3. Click the **Apply** button (2).

Cooperation of the Backup archive and the Failover service is now enabled.

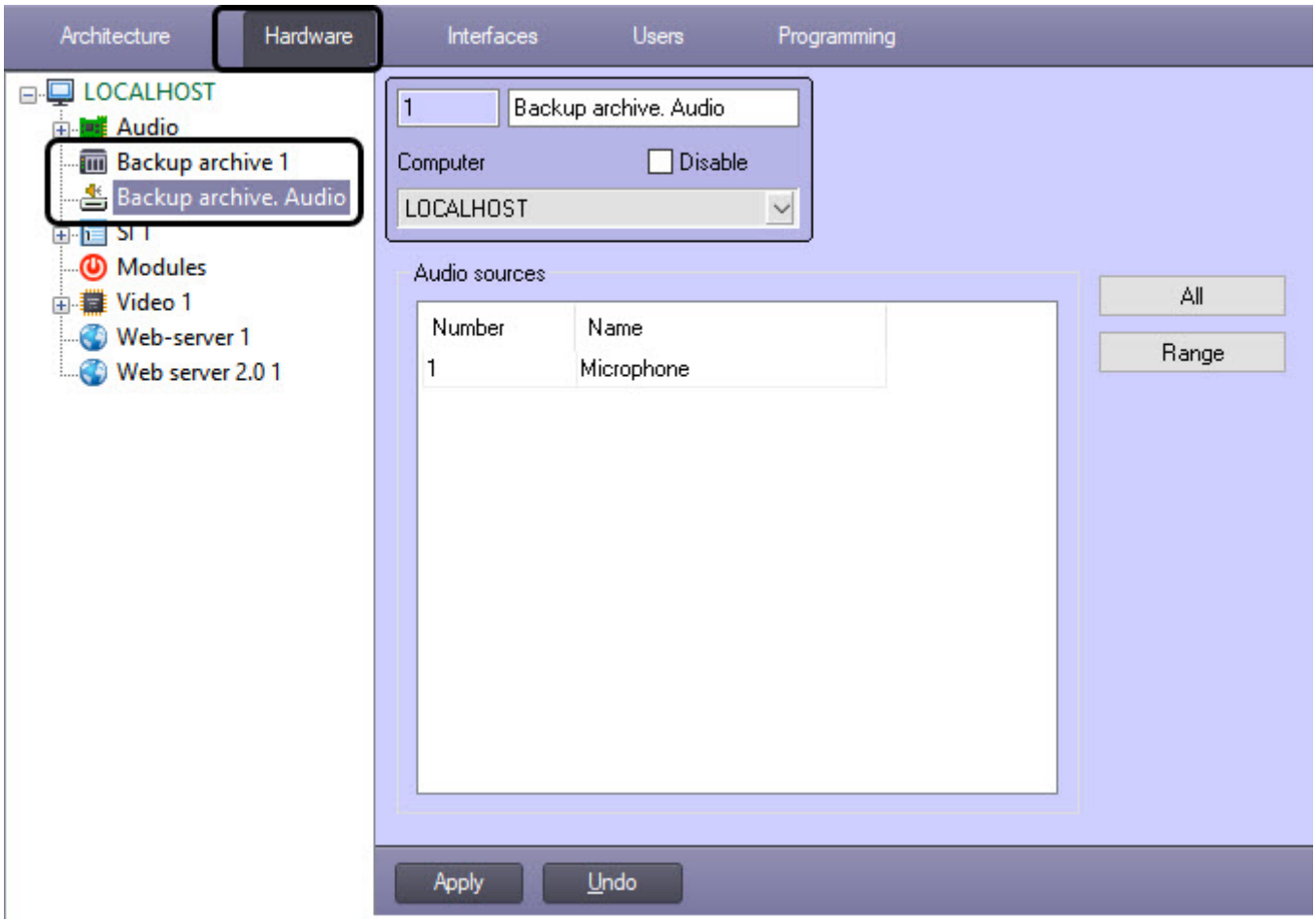
23.3.11.3 Configuring the Backup audio archive module

The *Backup audio archive* program module is designed to create a backup copy of audio archive recorded synchronously with a video archive. When the *Backup audio archive* program module is in use the audio archive recorded synchronously with the video archive from selected cameras included into digital video monitoring system is copied to a storage selected while configuring the *Backup archive* module (see Selecting disks to store the archive of the Backup archive module section). Copying is performed synchronously with a video archive copying.

Configuration of the *Backup audio archive* is performed using the **Backup audio archive** system object. The **Backup audio archive** object is created automatically while creating the **Backup archive** object.

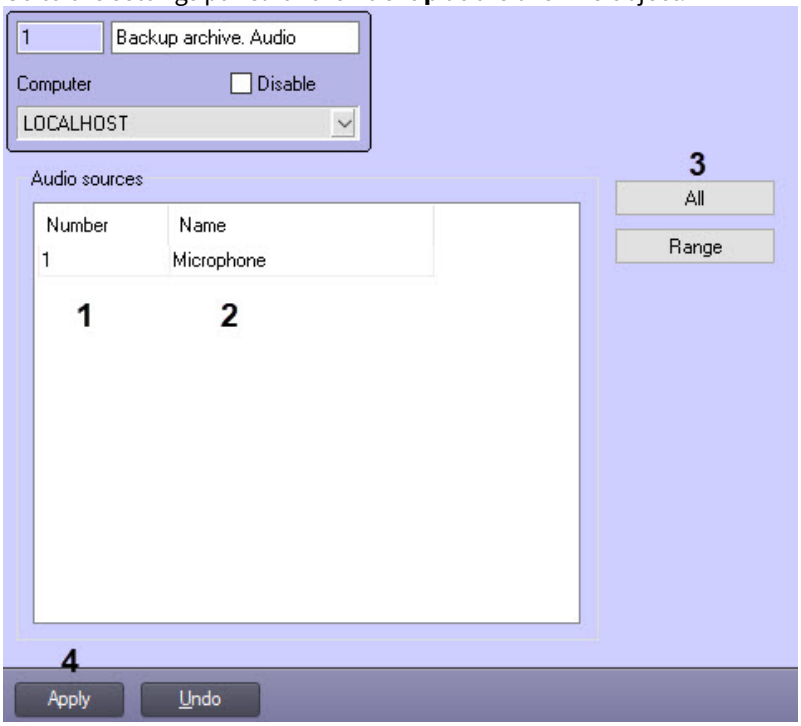
Note.

Deleting the **Backup archive** object the **Backup audio archive** object is deleted automatically.



To configure the Backup audio archive do the following:

1. Go to the settings panel for the **Backup audio archive** object.



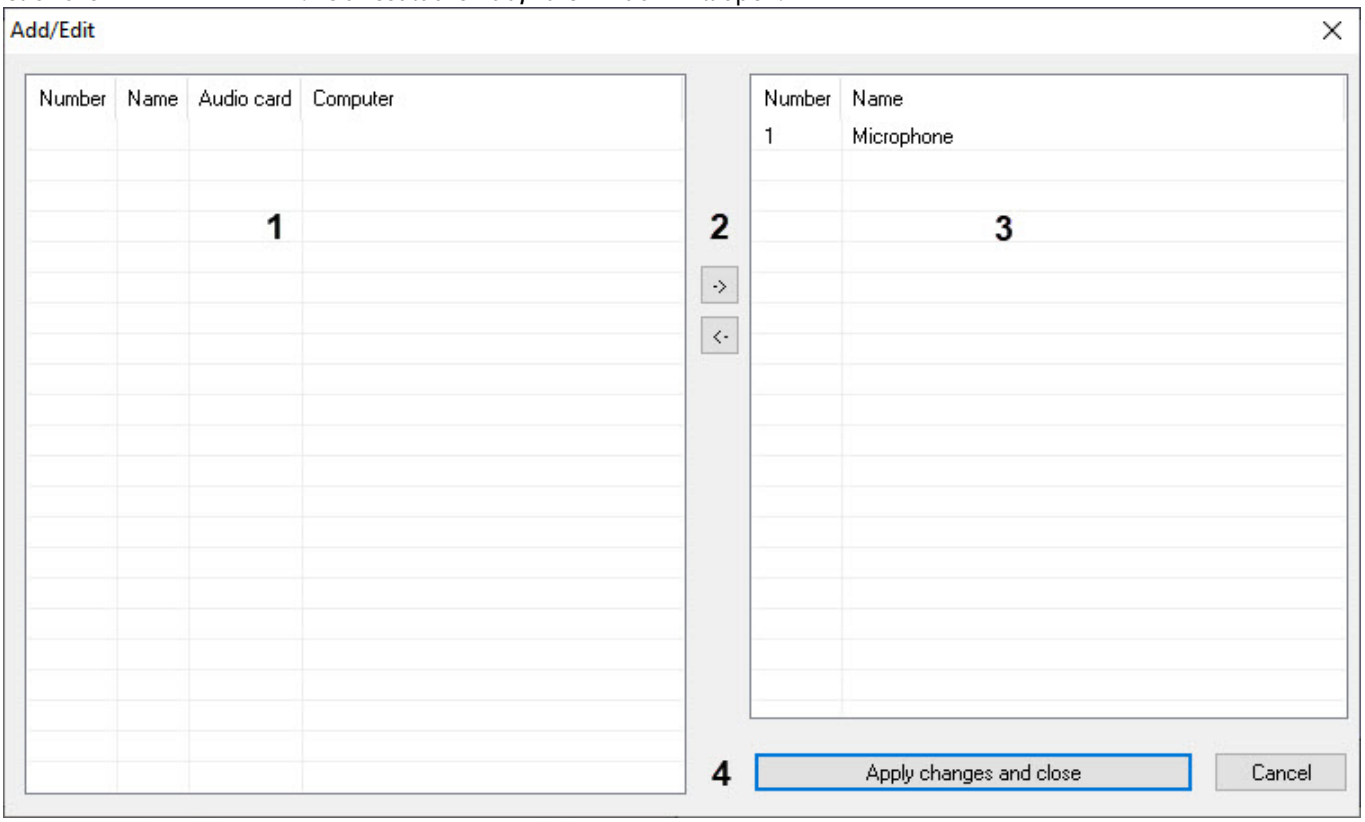
2. In the **Number** drop-down list, select the id of a microphone related to the camera the archive from which is to be moved to the backup archive (1).
3. Left-click in the **Name** field. It will be automatically filled with the name of selected microphone (2).

> **Note.**
>
> To add all **Microphone** objects created in the system to the list click the **All** button (3).

4. Repeat steps 2-3 for all required microphones.
5. Click the **Apply** button.

It is possible to add microphones to the list in a single package. To perform it, do the following:

1. Click the Range. As a result the **Add/Edit** window will open.



2. In the left part of list select required **Microphone** objects using the left mouse button (1). Use Shift and Ctrl keys to select several objects simultaneously.
3. Click the **->** button (2) to replace selected objects to the right part of list (3).

> **Note.**
>
> To replace objects from the right part of the list to the left part select microphones in this list and click the **<-** button (2).

4. Click the **Apply changes and close** button (4). Microphones from the right part of list will be added in the settings panel of the **Backup audio archive** object.

The *Backup audio archive* module is now configured.

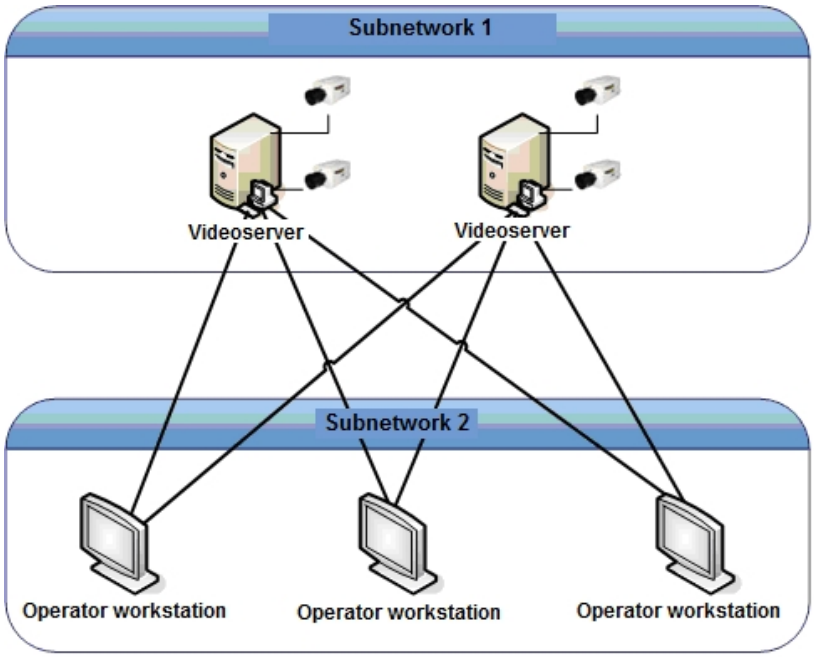
23.3.12 Configuring the Videogate module

23.3.12.1 General information on the videogate

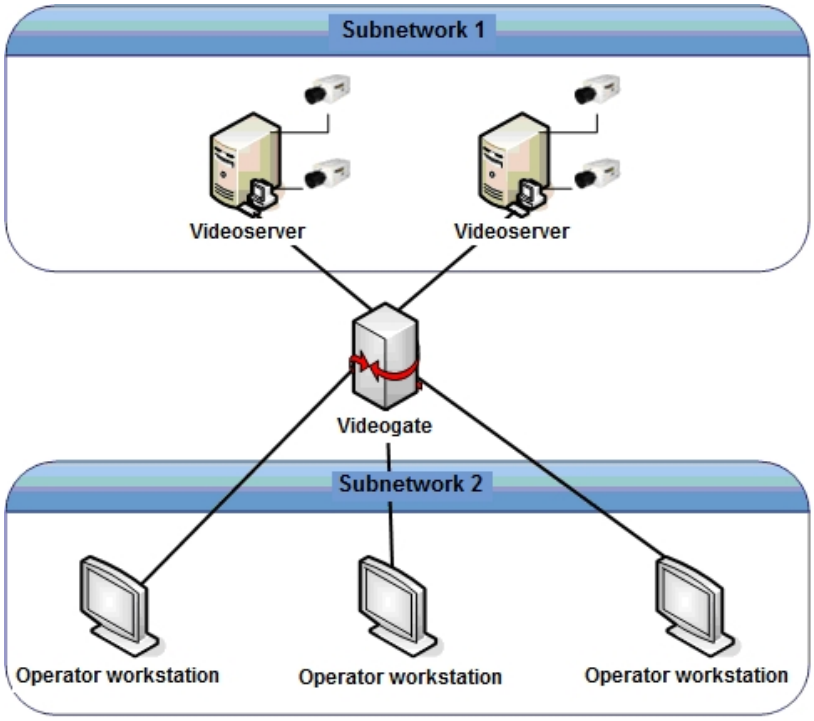
Videogate is used in large distributed video surveillance systems for routing the video signals among servers and clients (or administrator workstations used as operator workstations) located in different subnetworks. Servers and remote workstations are grouped into different subnetworks due to the following reasons:

1. Technical limitations leading to the servers being connected by low band channels and the clients using a high band connection. For example, the servers may be distributed over a large area, while the clients are located in one room of the monitoring center.
2. Security requirements. For example, to eliminate unauthorized access to administrative functions, the servers and clients are isolated into a different subnetwork from the operator workstations. When the subsystem interface uses the videogate, the clients(or rather administration workstations used as operator workstations) do not have access to the administrative functions of the servers and administration workstations of another subnetwork, but receive video signals from the servers.

Figures A and B show the schemes of construction of the video surveillance systems directly to the Videoservers with and via the videogate.



A. without the videogate



B. with the videogate

Note.

Video signal transfer to vertical modules on the basis of the Intellect software is not performing using the Video gate module. These modules always receive video signal directly as others modules.

Important!

There is no sound transmission to the RMW via the Videogate if different subnets are in use.

23.3.12.2 Order of setting up the Videogate object

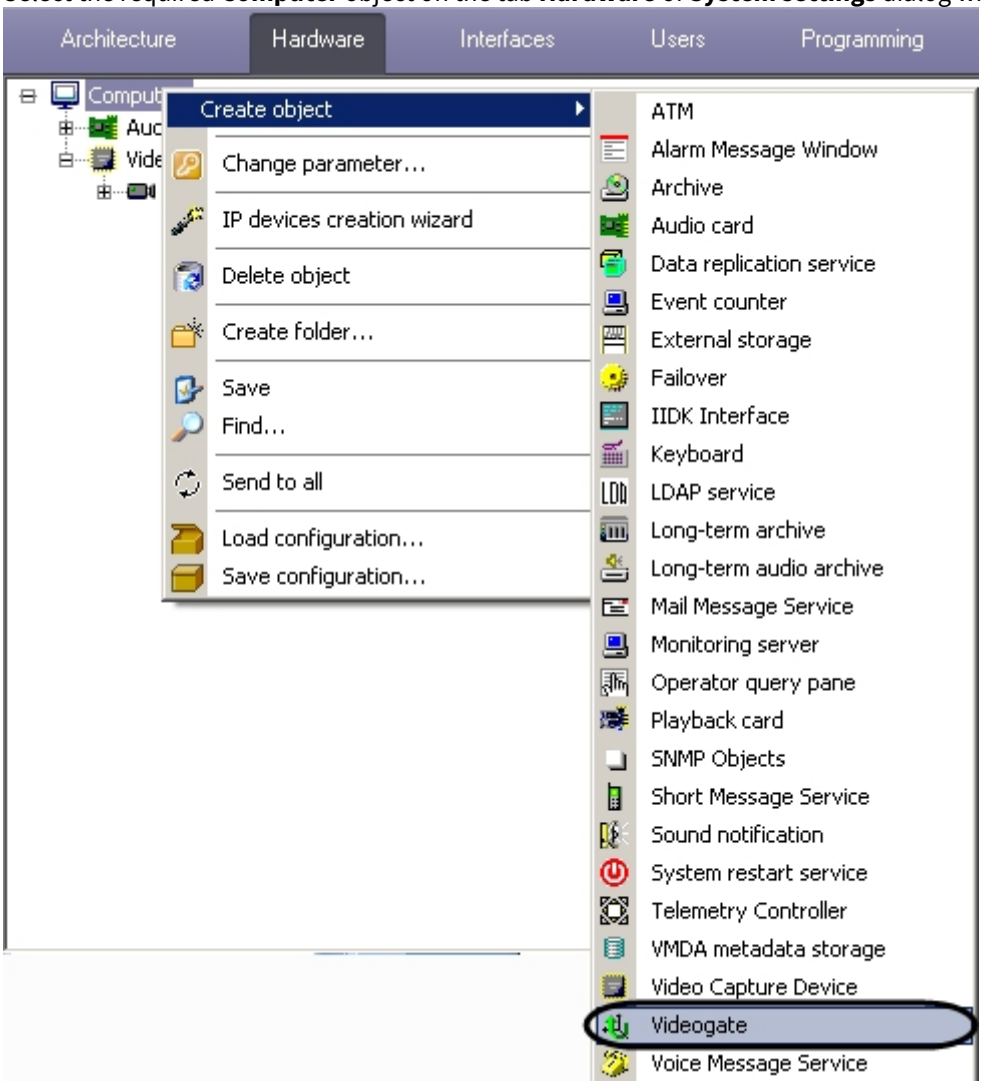
To set the **Videogate** object do the following:

1. Create the **Videogate** object on the basis of the **Computer** system object (see Creating the Videogate object).
2. Select and set cameras for transmitting the video signals through the *Videogate* (see Selecting and configuring the cameras for the Videogate module or Selecting video cameras in bulk for the Videogate module).
3. When necessary select the disks for storing archive of *Videogate* module (see Selecting disks for storing the archive of the Videogate module).

23.3.12.3 Creating the Videogate object

To create the **Videogate** object do the following:

1. Select the required **Computer** object on the tab **Hardware** of **System settings** dialog window.



2. Right mouse click upon the selected **Computer** object and select **Create object> Video gate** in the context menu that will open.
3. In the window, that will open, set the name and the number of **Videogate** object and the click **Apply** button.

> **Note.**
>
> In result settings panel of **Videogate** object will open.

4. Repeat steps 1-3 for all the required **Computer** and **Videogate** objects.

Creation of the **Videogate** object is completed.

23.3.12.4 Selecting and configuring the cameras for the Videogate module

You can select and configure cameras for transmitting the video signals through Videogate in two ways:

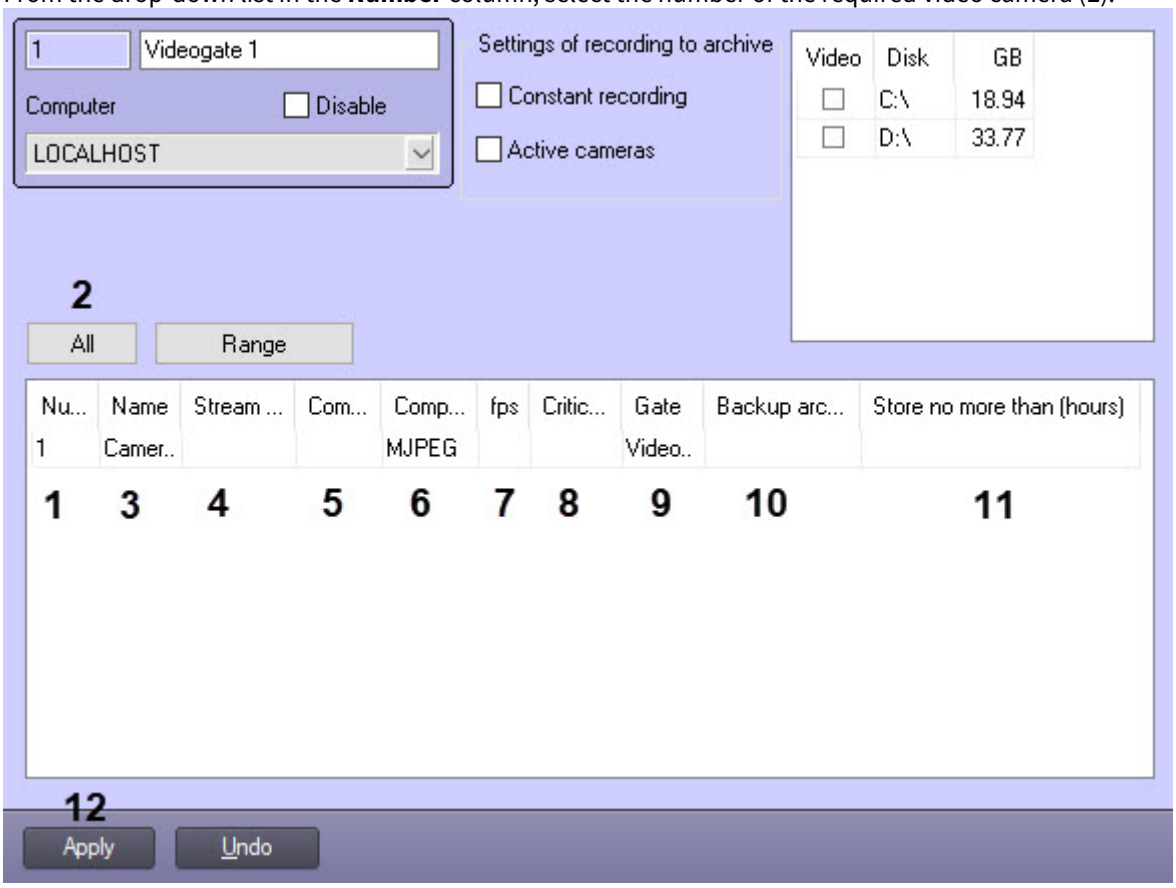
1. Separately. Use the settings panel of the **Videogate** object.
2. In bulk. Use the **Add/Edit Camera Objects** dialog box.

> **Note**
>
> Order of bulk selection of video cameras for transmitting video signals through the Videogate is described in Selecting video cameras in bulk for the Videogate module.

To select cameras on the settings panel of the **Videogate** object, do the following:

1. Go to the settings panel of the **Videogate** system object.

2. From the drop-down list in the **Number** column, select the number of the required video camera (**1**).



> **Note**
>
> To select all cameras, registered in the system, click the **All** button (**2**).

3. As a result, the **Name** column will display the name of the selected camera (**3**).
4. From the **Stream for archive** drop-down list, select the video stream from the Server that you want to use to record the videogate archive (**4**). By default, the **Archive** stream that the Server uses for constant recording is recorded (see also Configuration of multistream video).
5. In case, you want to change the compression level of the video signal for transmitting through the Videogate, from the drop-down list in the **Compression** column, select the required compression level of video signal (**5**). Compression level of the video signal increases from 0 (no compression) to 5 (maximum compression).

> **Note**
>
> If you set the compression level, the video signal on the Server has to be preliminary decompressed, which significantly increases the load on the Server CPU.

6. To change the algorithm of video signal compression for transmitting through the Videogate, from the **Compressor** drop-down list, select the required compression algorithm (**6**). If you specify the compressor, the value in the **Compression** list must be selected (**5**). If you specify the compression level, but don't select the **Compressor**, the Motion Wavelet compressor is used.

> **Note**
>
> Recompression is performed on the Server side.

7. In case, you want to thin out the video signal for transmitting through the Videogate, in the field in the **fps** column, enter the required frame rate of the video signal (**7**).

> **Note**
>
> The specified fps value must be less than the frame rate of the video signal digitizing by the video input device. Otherwise the frame rate of video signal will be equal to the frame rate of digitizing.
> The specified fps value must not be less than 0.01 which corresponds to transmission of one frame in 100 seconds.

> **Note**
>
> For the correct thinning of a video stream compressed using the H.264 or MPEG4 codecs, the fps value must be equal to key frame rate specified in the device (IP camera) or *Intellect* settings (see Configuring video compression).

8. In case, you want to control the transmission of video signals through the local network from the Server to the Videogate, in the field in the **Critical rate** column, enter minimum available value of frame rate of video signals, transmitted to the Videogate (**8**).

> **Note**
>
> The value specified in the **Critical rate** column should not be greater than the frame rate of video signal, transmitted to the Videogate.
> The setting of critical rate on the Videogate must be combined with the settings of the **Alarm Messages Window** system object (see Setting up the Alarm Message window). In this case, with the reduction of rate of input signals below the given value, the Alarm messages window will be displayed with the message **Reduced input rate**.

9. In case, when video signal from the selected video camera should be received from another **Videogate** object, from the drop-down list in the **Gate** column, select the name of this object (**9**).
10. In case, when the video archive for the selected camera has to be received from the **Backup archive** object, from the drop-down list in the **Backup archive** column, select the name of this object (**10**).

> **Attention!**
>
> The selected value must coincide with the value that is specified when configuring video cameras that should be displayed on the Video surveillance monitor for this Camera—see Selecting and configuring video cameras.

11. In the **Store no more than (hours)** field, enter the time period in hours after which you want to delete the recordings of the corresponding camera from the Videogate (**11**). The parameter must be set according to the same rules as for the main archive—see Configuring video camera archive depth.
12. Repeat steps 2-11 for all required cameras.
13. To save all the changes, click the **Apply** button (**12**).

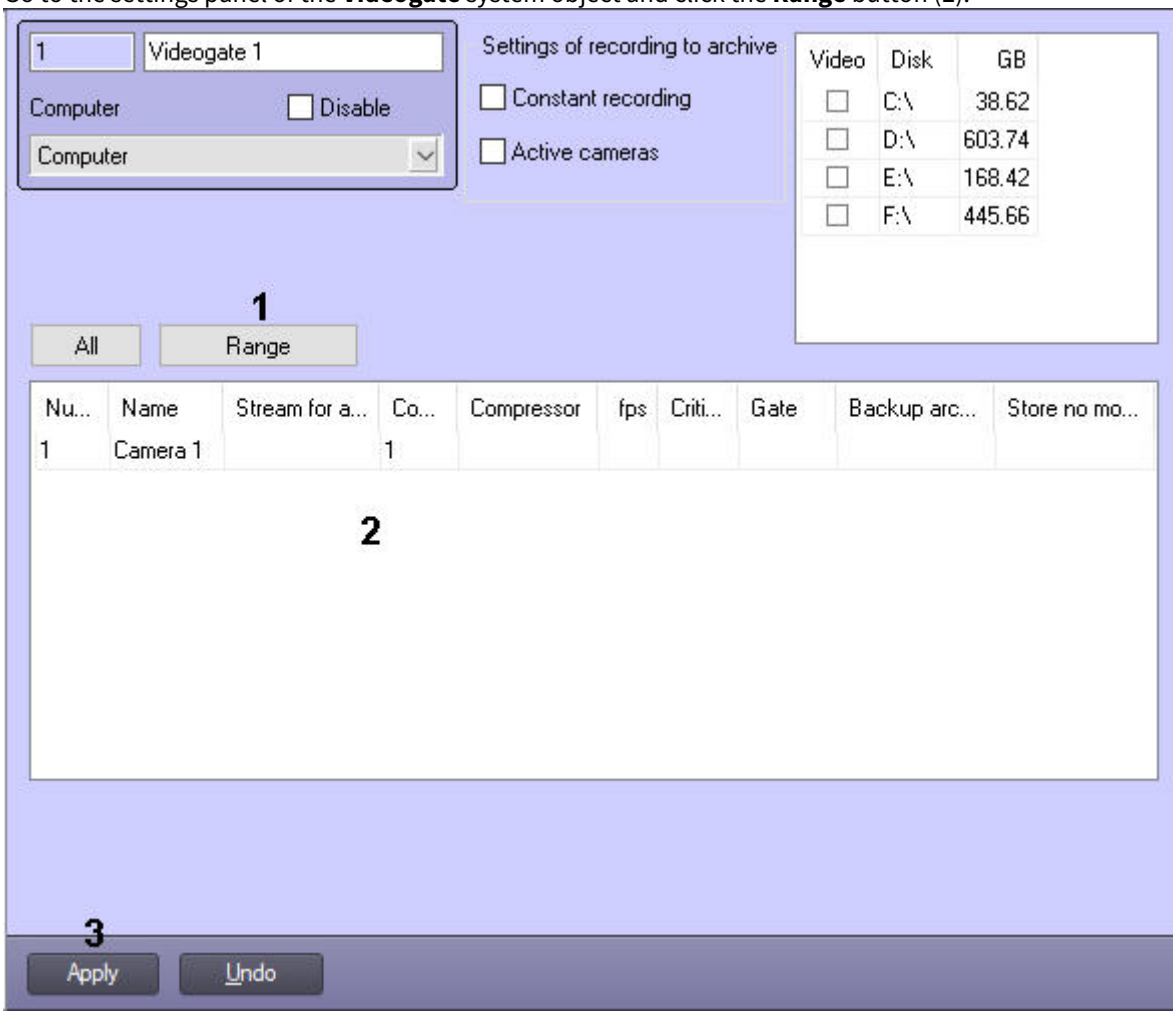
Selecting cameras on the settings panel of the **Videogate** object is completed.

23.3.12.5 Selecting video cameras in bulk for the Videogate module

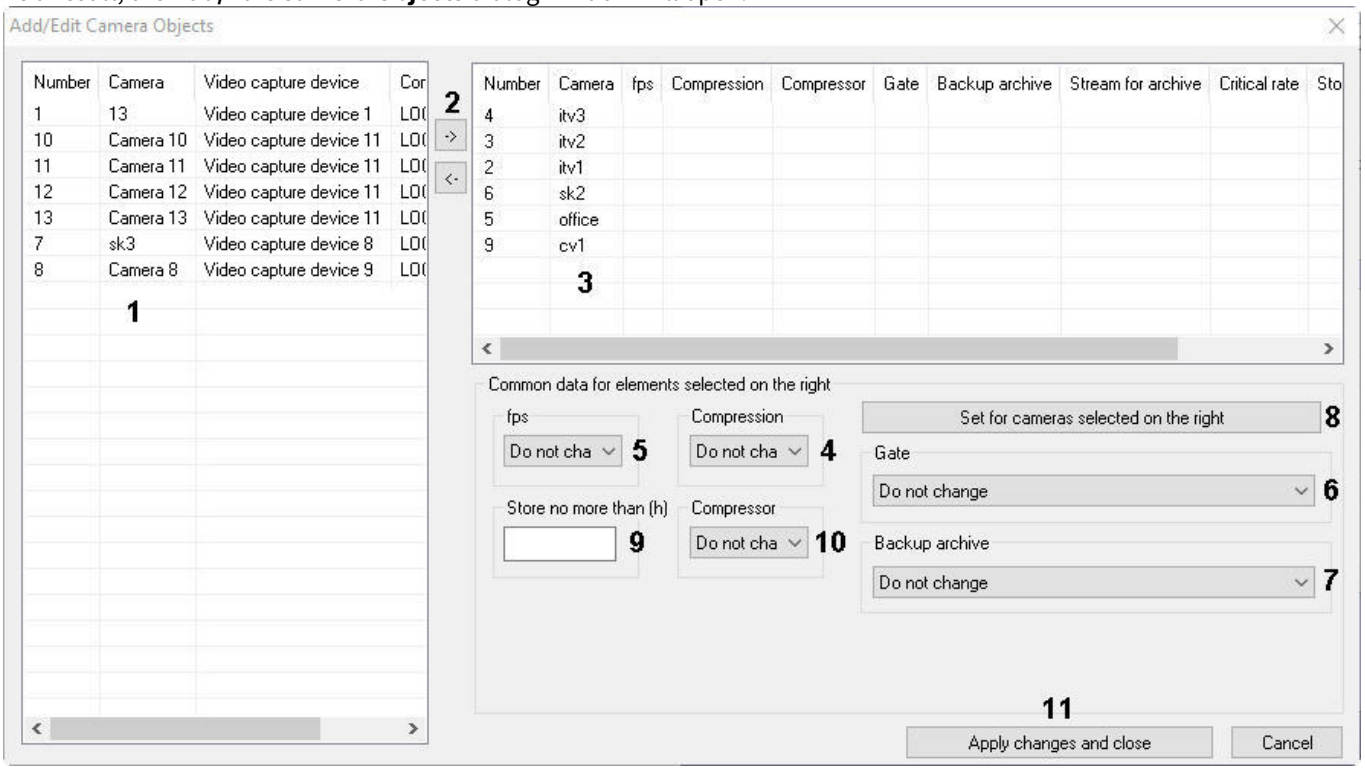
You can select and edit the parameters of video cameras in bulk for transmitting video signal through **Videogate**.

Bulk selection of cameras is performed in the following way:

1. Go to the settings panel of the **Videogate** system object and click the **Range** button (**1**).



2. As a result, the **Add/Edit Camera Objects** dialog window will open.



3. Select the required cameras in the left list of the **Add/Edit Camera Objects** window by clicking with the mouse and holding down the Ctrl key (**1**).
4. Remove the selected cameras to the right list by clicking the button (**2**).

> **Note**
>
> The right list contains a list of cameras, selected for transmitting the video signals through the **Videogate**.
>
> The button is used for back action i.e., for removing the selected cameras from the right list to the left list (**2**).

5. As a result, the selected video cameras will be displayed in the right list of the **Add/Edit Camera Objects** window (**3**).
6. If necessary, in the right list, select the names of the required cameras for bulk editing of the parameters by clicking them with the mouse with the Ctrl key pressed.

> **Attention!**
>
> For all selected cameras the same values of the parameters will be set.

> **Note**
>
> You cannot edit the **Critical rate** parameter using the **Add/Edit Camera Objects** window.

7. If it is necessary to change the video signal compression level for transmission through the **Videogate**, from the **Compression** drop-down list, select the required video signal compression level (**4**). The video signal compression level increases from 0 (no compression) to 5 (maximum compression). Selecting an empty value means that the initial compression level will be applied, the **Do not change** value means that the compression level of the device will be applied.

> **Note**
>
> If you set the compression level, the video signal on the Server has to be preliminary decompressed, which significantly increases the load on the Server CPU.
> The **Compression**, **fps**, **Gate**, **Backup archive** settings belong to the **Set for cameras selected on the right** group.

8. If it is necessary to thin out the video signal for transmission through the **Videogate**, select the required video frame rate from the **fps** drop-down list (**5**). Selecting an empty value means that the initial frame rate will be applied, the **Do not change** value means that the frame rate with which the device transmits the video signal will be applied.

> **Note**
>
> The specified fps value must be less than the frame rate of video signal digitizing by video capture card. Otherwise frame rate of video signal will be equal to the frame rate of digitizing.

9. In case, when video signal from the selected video camera should be received from another **Videogate** object, from the **Gate** drop-down list, select the name of this object (**6**).
10. In case, when the video signal from the selected camera has to be received from the **Backup archive** object, from the **Backup archive** drop-down list, select the name of this object (**7**).
11. If it is necessary to limit the storage time of the **Videogate** archive, enter the maximum number of hours of storage in the **Store no more than (h)** field (**9**). The parameter must be set according to the same rules as for the main archive—see Configuring video camera archive depth.
12. If it is necessary to change the video signal compression algorithm for transmission through the **Videogate**, select the required compression algorithm from the **Compressor** drop-down list (**10**). If a compressor is specified, it is necessary that a value be selected in the **Compression** list (**4**). If a compression level is specified but **Compressor** is not selected, then the *Motion Wavelet* compressor is used. Selecting an empty value means that the initial algorithm will be used, the **Do not change** value means that the algorithm that is used for recording on the device will be used.
13. To save the set parameters, click the **Set for cameras selected on the right** button (**8**).
14. As a result, the set parameters will be displayed in the right list of the **Add/Edit Camera Objects** window (**3**).

15. Repeat steps 6-11 for bulk editing of all required cameras.
16. To save all the changes and close the **Add/Edit Camera Objects** window, click the **Apply changes and close** button (**11**).
17. The specified settings will be displayed on the settings panel of the **Videogate** object (**2**).
18. To save the changes, click the **Apply** button (**3**).

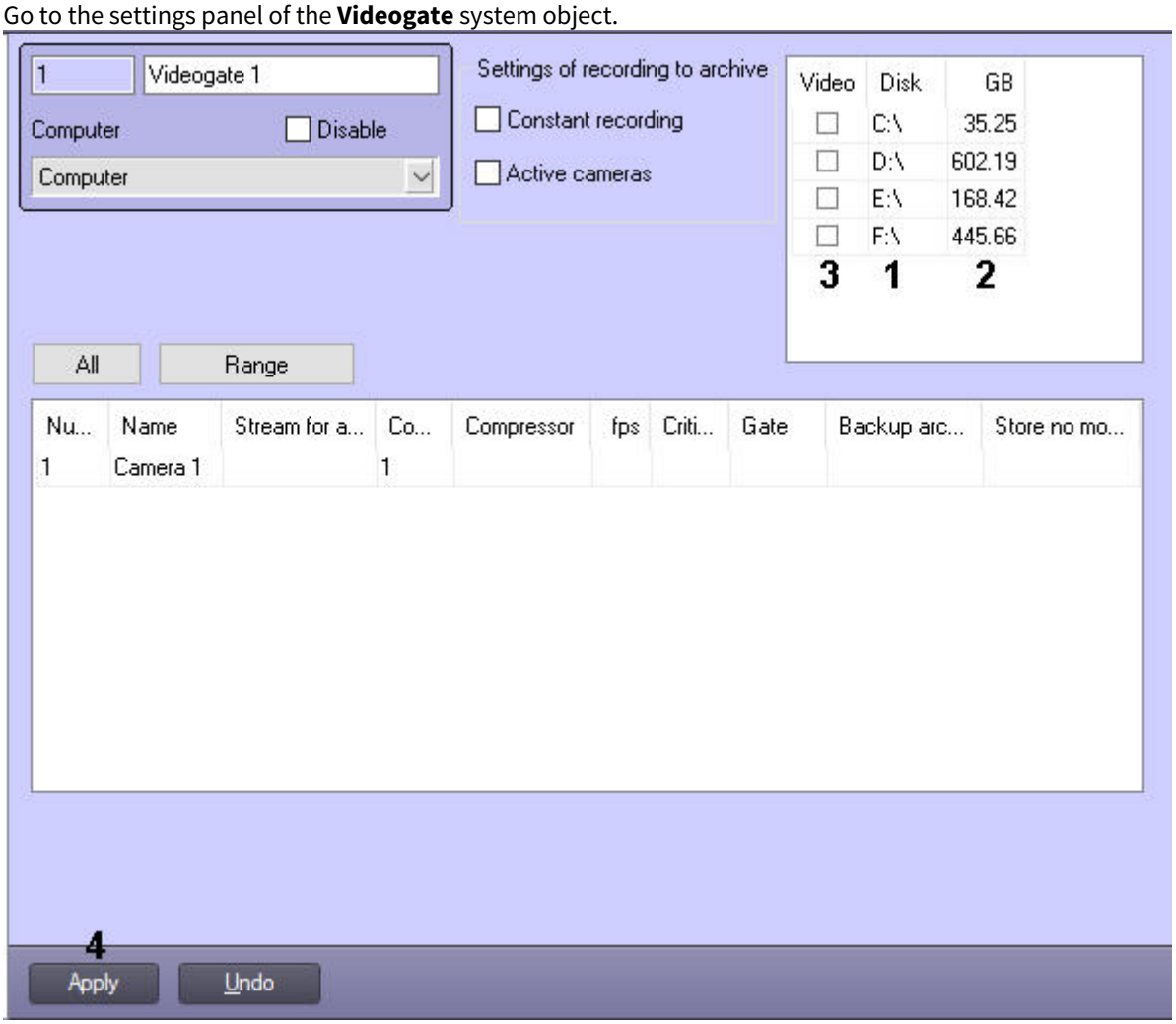
Bulk selection of cameras is completed.

23.3.12.6 Selecting disks for storing the archive of the Videogate module

To enable the archiving of the video signals, passing through the **Videogate,** it is necessary to select the disks for archive storing.

To select the disks for storing the archive of the **Videogate** module, do the following:

1. Go to the settings panel of the **Videogate** system object.



2. The names of the local (network, USB) disks, available for stroing the archive of the **Videogate** module are given in the **Disk** column (**1**).

> **Attention!**
>
> For Windows Vista and Windows 7 OS with UAC enabled, it's necessary to connect the network disks via the command line with Administrator's rights. The connection method is described in Connecting network disks in Windows Vista and Windows 7 OS.

> **Note**

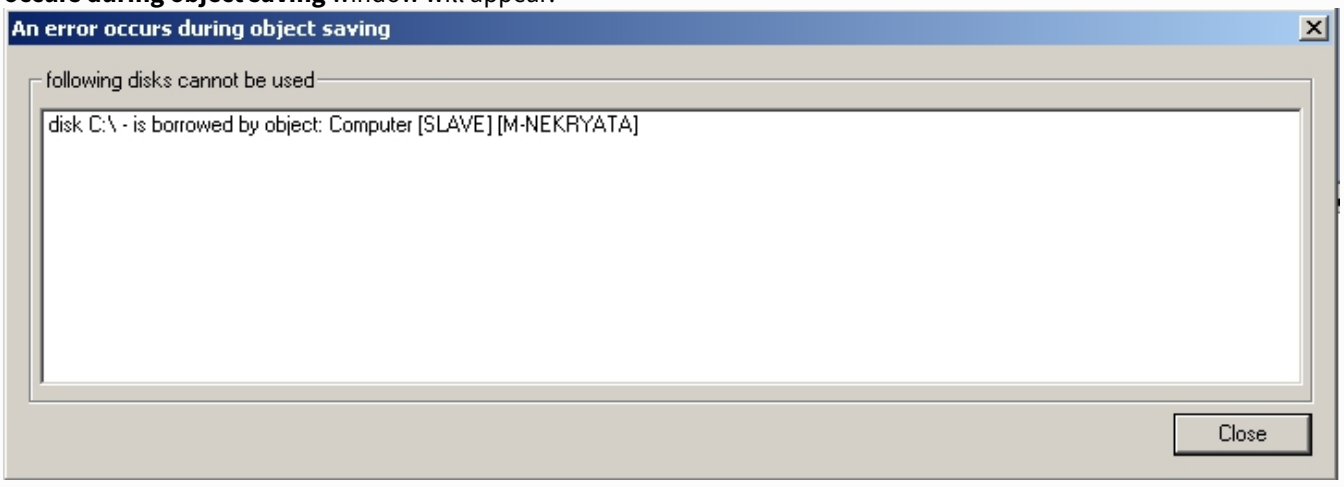
To use network disks as an archive, set the UNC paths to them in *Intellect*. For details on working with the network disks in *Intellect* that is installed as a Service, see Working with Windows OS services for operating Intellect™ installed as a Service.

3. In the **GB** column, you can see the free space on disk in GB (**2**).
4. In the **Video** column, set the checkboxes next to the disks, selected for storing the archive of the **Videogate** module (**3**).
5. To add a network disk via specifying the UNC path, do the following:
   a. Go to the last line in the disks list and click the Down key.

   b. In the appeared line in the **Disk** column, enter the path to a network disk. The UNC path is set in the \ \server_name\share_name format, where server_name is the name of the file server and share_name is the network name of shared folder.
   c. In the **Video** column, set the checkbox next to the created disk.
6. To save the changes, click the **Apply** button (**4**).

Note

For storing the archive of the **Videogate** module, select the disks that are not used for storing video archive from cameras (selected in the settings panel of the **Computer** object). Otherwise, after saving the changes, the **An error occurs during object saving** window will appear.



Note

In case, when no disk is selected for storing video recordings, there is no recording of the video signals to the archive of the **Videogate** module.

Selecting disks for storing the archive of the **Videogate** module is completed.

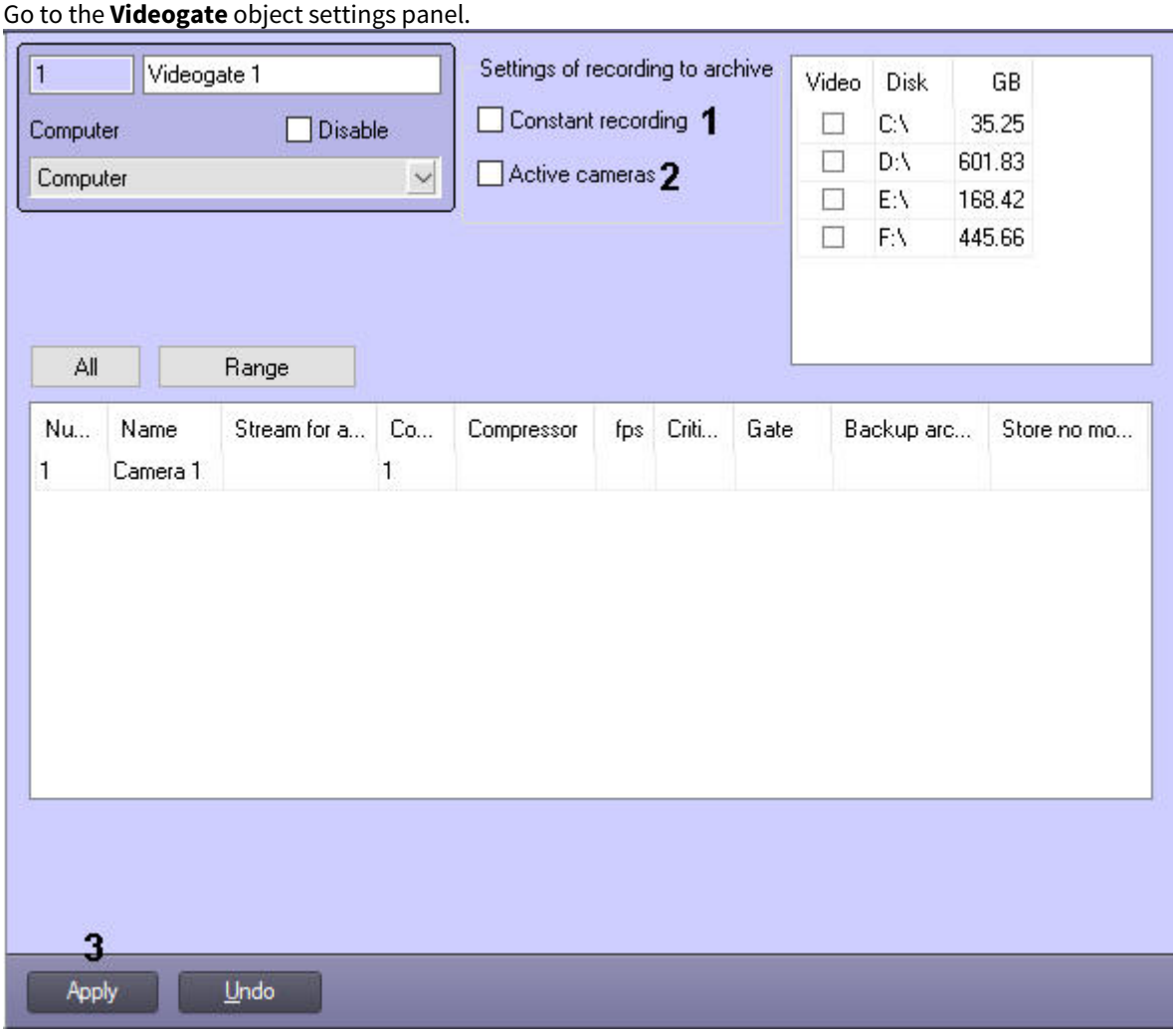
Free disk space (video archive size) required
Video gateway archive playback
Configuring the recording to the Videogate archive

23.3.12.7 Configuring the recording to the Videogate archive

By default, if disks are selected for recording (see Selecting disks for storing the archive of the Videogate module), the **Videogate** requests video streams for all selected cameras (see Selecting and configuring the cameras for the Videogate module) from Server and records archive if recording is configured for these cameras on the Server. You can configure **Videogate** archive recording by all added cameras regardless of Server configuration, as well as recording only on cameras requested on clients.

To configure the recording to the **Videogate** archive, do the following:

1. Go to the **Videogate** object settings panel.



2. If it is necessary to provide recording by all cameras added to the **Videogate** regardless of whether the data is recorded to the main archive of the Server, set the **Constant recording** checkbox (**1**).
3. If it is necessary to provide recording by the cameras the video stream from which is requested and displayed on the **Video surveillance monitor**, set the **Active cameras** checkbox (**2**).
4. Click the **Apply** button (**3**).

Configuring the recording to the **Videogate** archive is complete.

In case no disk is selected for recording, then:

- if the **Constant recording** checkbox is set, then there will be continuous video stream from the Server, and there will be no recording;

- if the **Active cameras** checkbox is set, then the video will stream from the Server only if it is displayed on the **Video surveillance monitor**, and there will be no recording.

Specifics of the **Videogate** operation with different combinations of set checkboxes for archive recording are described in the table:

Constant recording	Active cameras	Disk for storing the archive is selected	Result: video streams and recording
✗	✗	✗	Continuous video stream from the Server, no recording to the Videogate archive
✗	✓	✗	The video streams from the Server only if it is displayed on the Video surveillance monitor, no recording to the Videogate archive
✓	✗	✗	Continuous video stream from the Server, no recording to the Videogate archive
✓	✓	✗	The video streams from the Server only if it is displayed on the Video surveillance monitor, no recording to the Videogate archive
✗	✗	✓	Continuous video stream from the Server, recording to the Videogate archive is similar to the Server
✗	✓	✓	The video streams from the Server only if it is displayed on the Video surveillance monitor. Recording to the Videogate archive is similar to the Server, but only when the video is displayed on the Video surveillance monitor
✓	✗	✓	Continuous video stream from the Server, continuous recording to the Videogate archive
✓	✓	✓	The video streams from the Server only if it is displayed on the Video surveillance monitor. The video is recorded to the Videogate archive only when it is displayed on the Video surveillance monitor

Note

You can also manage the recording to the **Videogate** archive using the START_VIDEO and STOP_VIDEO commands (see GATE Videogate).

23.3.13 Notification services

23.3.13.1 Setting up the Alarm Message window

On the page:

- General description and usage details of the Alarm Message window
- Creating and setting up the

Alarm Message Window object

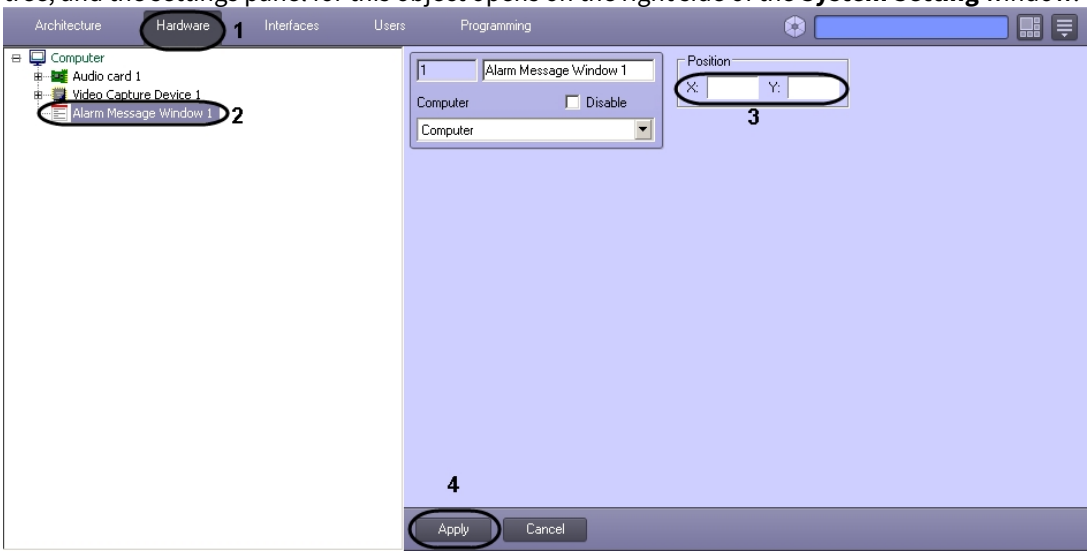
23.3.13.1.1 General description and usage details of the Alarm Message window

The **Alarm Message window** notifies the operator about alarms and opens above all other windows in case of an alarm event on a set device.

23.3.13.1.2 Creating and setting up the Alarm Message Window object

To set up the **Alarm Message window**, do the following:

1. Go to the **Hardware** tab of the **System Settings** window.
2. Create the **Alarm Message Window** object in the **Computer** node in the objects tree. The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.

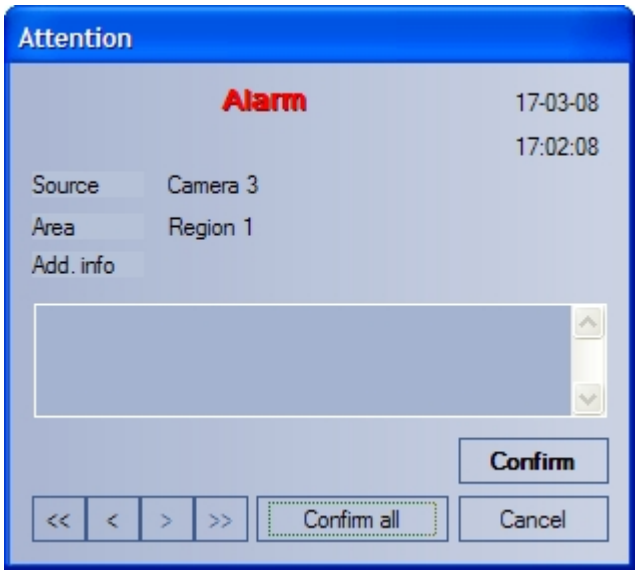


3. Set the coordinates (**X, Y**), in percent, for the position of the **Alarm Message window**.

> **Note.**
>
> By default, X and Y coordinates are 0, thus, if they are not changed, the window opens in the upper left corner of the screen.

4. Press the **Apply** button to save the settings for the **Alarm Message** object.

Figure below shows a general view of the **Alarm Message**: this window will open above all other windows at a set position (60, 60) upon receiving an alarm event from Camera 3.



Note.

To disable opening the **Alarm Message window**, check the **Disable** checkbox in the settings panel of the **Alarm Message Window** object.

23.3.13.2 Setting up the Short Message Service (SMS)

23.3.13.2.1 General description and usage details of the Short Message Service

The Short Message Service (SMS) is used for sending SMS messages to mobile phones about alarm events registered in *Intellect*. An SMS message is sent automatically upon registration of any events specified in the corresponding macro.

Actions on *Intellect* objects can be performed when an SMS message is received. Macros, programs in the language embedded in *Intellect* or Jscript scripts are used for this. When an SMS message is received, the SMS object sends the RECEIVE event to *Intellect* (see SMS Short Message Service).

SMS messages are sent using the services of the mobile providers via GSM. To send SMS messages, the dedicated devices are used: GSM modems, GSM adapters and mobile phones or devices with Android operating system. SMS messages are sent to mobile phones by mobile service providers.

Note

When using SMS in *Intellect*, note the following: mobile service providers usually charge for sending SMS messages.

To be able to send SMS messages, a GSM modem, a GSM adapter, a mobile phone or a device with Android operating system supporting ETSI GSM 07.07 or ETSI GSM 07.05 should be installed on the computer (see Android-based Intellect SMS Sender Mobile Application. User Guide).

The following modem models are currently integrated into *Intellect*:

1. 3G-modem Huawei E160. In Windows OS it is identified as HUAWEI Mobile Connect-3G Modem. Modem control program is required to be run to work with this device.
2. 3G-modem ZTE MF626. In Windows OS it is identified as ZTE Proprietary HS-USB Modem.To use this device it is necessary to install the software. The software installation will run automatically after the modem is connected.
3. 3G-modem Huawei E173. The RECEIVE event is supported if using the ProcessFromSim registry key (see Registry keys reference guide).

Note

Many mobile service providers protect their USB-modems from use in other providers' networks. When you use the modem protected by the provider, run the utility included in the modem bundle simultaneously with *Intellect* to activate the SMS. You do not need to perform any other actions with the utility (connect to 3G, etc.).

Note

When using a modem control application, it takes 10 seconds to deliver a message.

The procedure for creating and sending an SMS message:

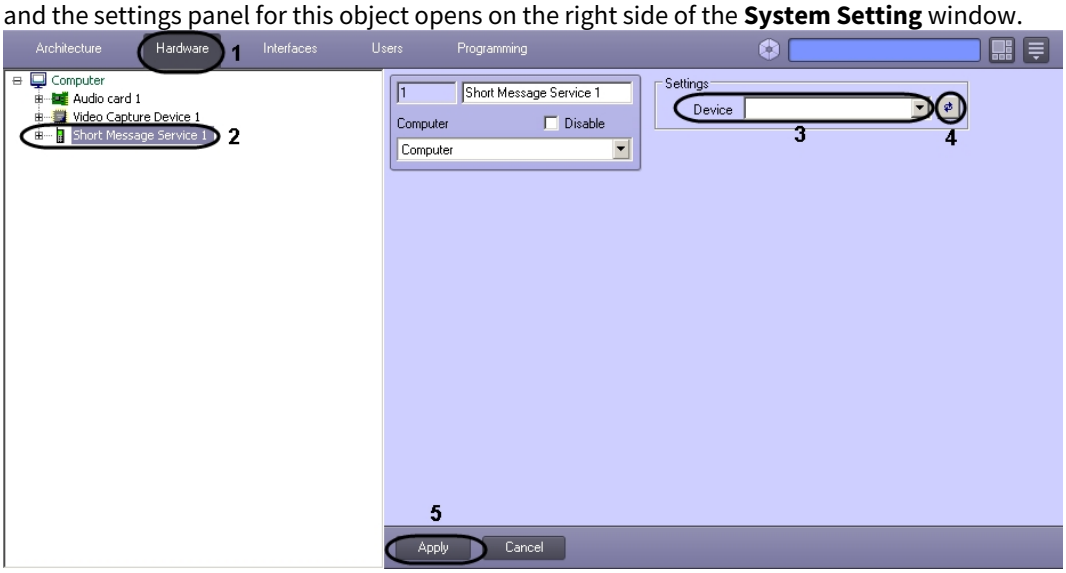
1. Create and set up the **Short Message Service** object.
2. Create and set up the **Short Message** object.
3. Create a macro for sending the short message.

Requirements for GSM Equipment

23.3.13.2.2 Creating and setting up the Short Message Service object

To set up the **Short Message Service** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window.
2. Create the **Short Message Service** object in the **Computer** node in the objects tree. The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.



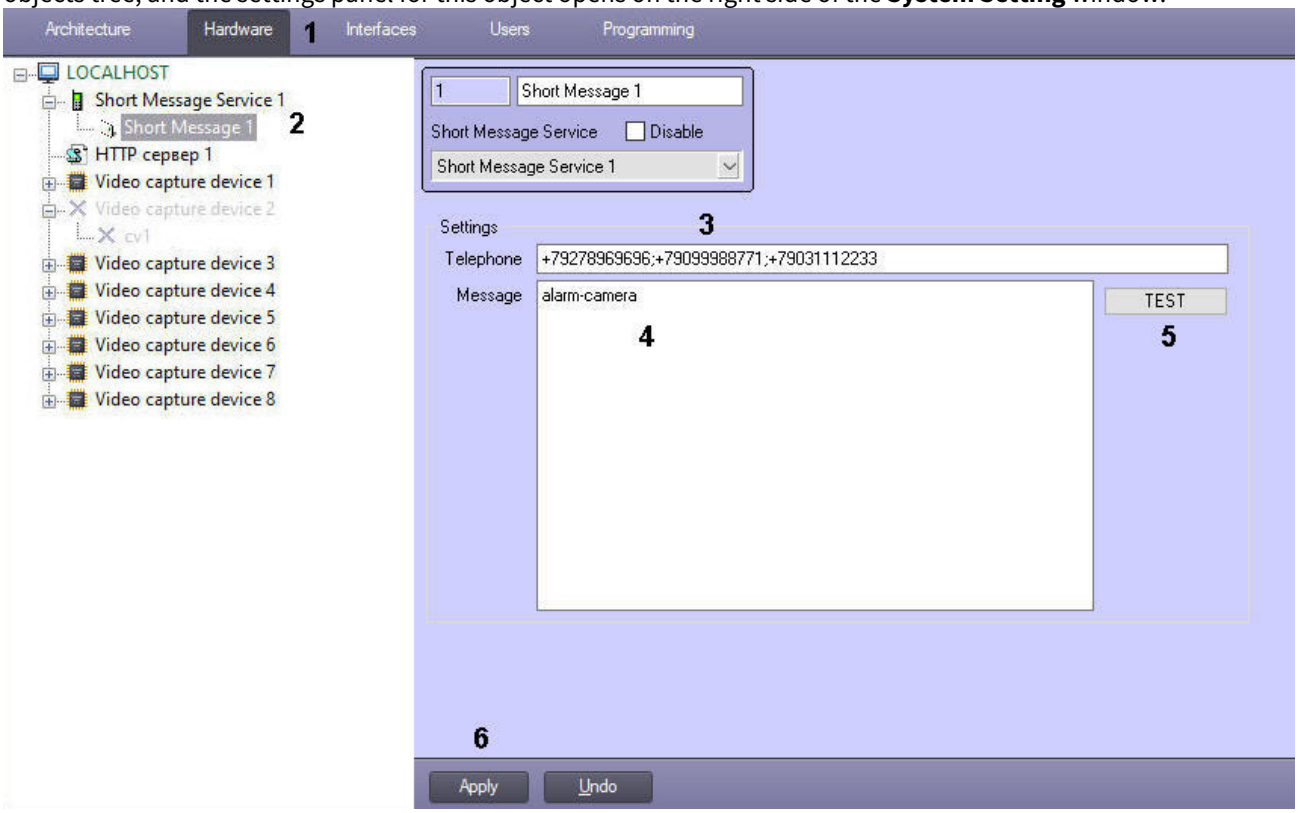
3. Select the GSM-device to be used for sending SMS, in the **Device** drop-down list.
4. Press the refresh button for the system to update the list if the device was not listed.
5. Press the **Apply** button to save the settings for the **Short Messages Service** object.

23.3.13.2.3 Creating and setting up the short messages

To set up the **Short Message** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window (1).

2. Create the **Short Message** object in the **Short Message Service** node in the objects tree (2). The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.



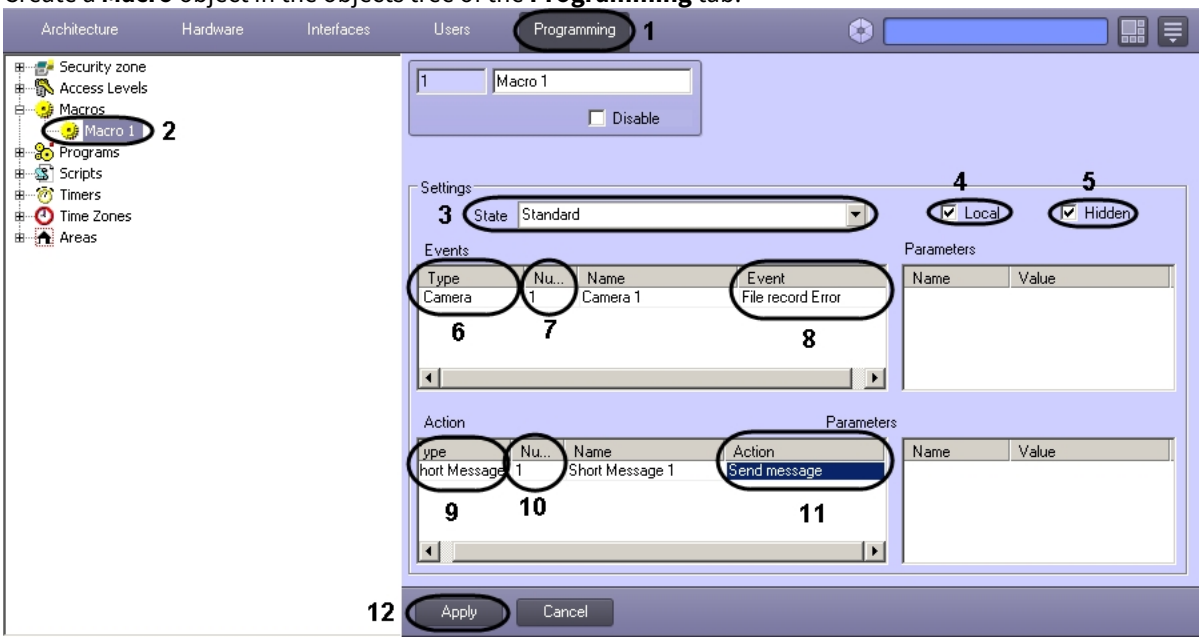
3. Enter the telephone number into the **Telephone** field in the following format: [prefix “+”] [country code] [city/provider code] [phone number] with no spaces or other delimiters (3). If it is necessary to send a message to several numbers, then enter the numbers separated by ";" (semicolon) with no spaces.
4. Enter the message text into the **Message** field (4).
5. If a short message is to be force sent, click the **TEST** button (5). Make sure the message has been received by the recipient. Otherwise check if **Short message service** and **Short message** objects have been configured correctly.
6. Press the **Apply** button to save the settings for the **Short Message** object. (6).

23.3.13.2.4 Creating and setting up the macro for sending the short message

The message is sent upon execution of a macro. The macro is executed immediately after a set event occurs. To create the macro for sending the short message:

1. Go to the **Programming** tab of the **System Settings** window.

2. Create a **Macro** object in the objects tree of the **Programming** tab.



3. Set the **State** parameter.
4. Check the **Local** checkbox to send the message from a local computer only.
5. Choose the event object type for the SMS macro to be related to.
6. Choose the event object number for the SMS macro to be related to.
7. Choose the event name which will trigger the sending of the short message.
8. Choose the **Short Message** object in the **Type** column.
9. Choose the number of the **Short Message** object to be sent by the macro.
10. Choose **Send Message** in the **Action** column.
11. Press the **Apply** button to save the settings for the **Macro** object.

23.3.13.3 Setting up the Mail Message Service (E-mail)

23.3.13.3.1 General description and usage details of the Mail Message Service

The Mail Message Service (E-Mail) is used for sending e-mail messages about the alarm events registered by Intellect software, to remote system users. Sending e-mail messages is triggered automatically upon registration of any of the events set in the macro.

To be able to send e-mail messages, the computer should be connected to the internet via a local area network or remote TCP/IP connection.

The e-mail messages are sent by the Mail Message Service. To send e-mail messages in Intellect, you should first register a mailbox in the Mail Message Service.

Note.

When registering your mailbox in the Mail Message Service, note the following:

1. Intellect's Mail Message Service does not support SMTP servers with Secure Password Authorization (SPA).
2. Intellect's Mail Message Service supports only the following authorization algorithms on SMTP servers: LOGIN, CRAM-MD5, PLAIN.
3. By default the Mail Message Service uses TLS encoding. If SMTP Server does not use TLS, then set the 0 value for the UseTls registry key (see Registry keys reference guide).
4. For proper operation of Mail Message Service two-factor authentication is to be in configured for the e-mail account in use.

To create and send an e-mail message:

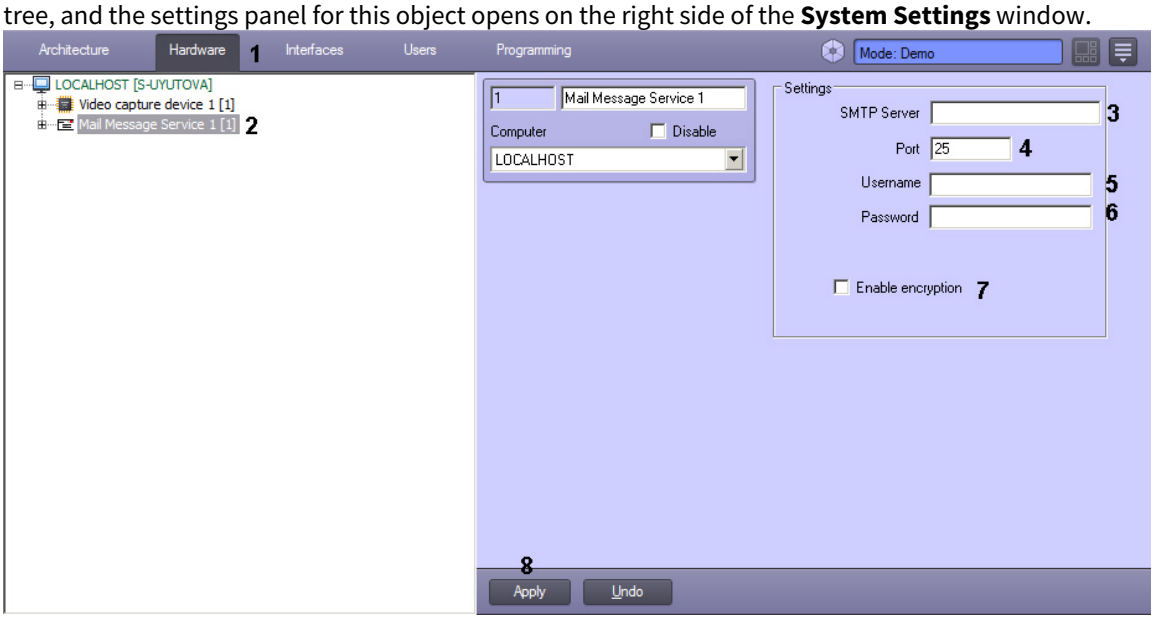
1. Create and set up the **Mail Message Service** object.
2. Create and set up the **Mail Message** object.

3. Create a macro for sending the e-mail message.

23.3.13.3.2 Creating and setting up the Mail Message Service

To set up the **Mail Message Service** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window (**1**).
2. Create the **Mail Message Service** object in the **Computer** node in the objects tree (**2**). The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Settings** window.



3. Enter the URL address of the SMTP server (**3**).
4. Enter the port number for outgoing messages (**4**).
5. Enter the username for authorization on the SMTP server (**5**).
6. Enter the password for authorization on the SMTP server (**6**).
7. Enable encryption if necessary (**7**).
8. Click the **Apply** button to save the settings for the **Mail Messages Service** object (**8**).

Find information on how to set up mail servers in the table.

	Yandex	Yahoo!	Outlook	Google
SMTP Server	smtp.yandex.ru	smtp.mail.yahoo.com	smtp-mail.outlook.com	smtp.gmail.com
Port	587	587	587	587
Username	username@yandex.ru	username@yahoo.com	username@outlook.com	username@gmail.com
Password	User account password or a separate app password created for *Intellect* (see Yandex Support article: https://yandex.com/support/id/authorization/app-passwords.html)	1. If 2-step verification is enabled: password generated for 2-step verification. 2. If 2-step verification is disabled: user password for the Yahoo account. In this case, it is important to let less secure apps access	User account password	1. If 2-step verification is enabled: 16-symbols password generated for 2-step verification. 2. If 2-step verification is disabled: user password for the Gmail account. In this case, it is important to let less

	Yandex	Yahoo!	Outlook	Google
		your account in Yahoo settings.		secure apps access your account in Gmail settings.
Encryption	Yes	Yes	Yes	Yes

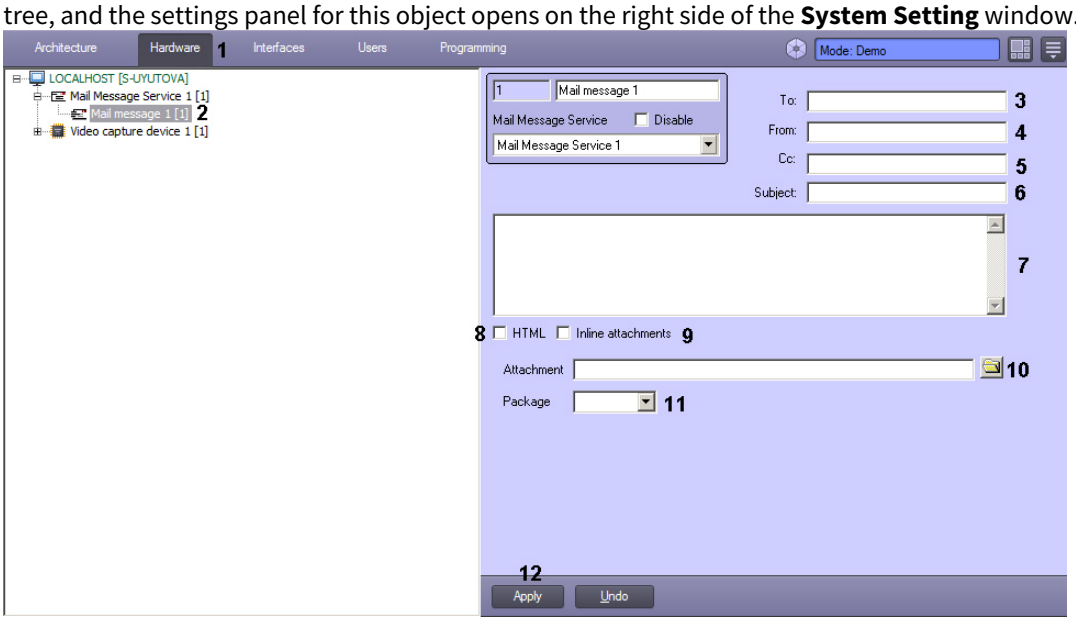
Note

Each company sets a limit on the number of messages sent via the smtp protocol. For example, Google has a limit of about 100 messages per day. You can try to increase the number of messages sent by using the **SendSync** registry key (for details, see Registry keys reference guide).

23.3.13.3.3 Creating e-mail messages

To set up the **Mail Message** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window (1).
2. Create the **Mail Message** object in the **Mail Message Service** node in the objects tree (2). The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.



3. Enter the e-mail address of the recipient (3).
4. Enter the e-mail address of the sender (4).
5. Enter additional addresses (**Cc:**) to send this message to, if necessary (5).
6. Enter the subject of the message (6).
7. Enter the text of the message to be sent to the specified addresses (7).
8. If the message has HTML tags to be applied, set the **HTML** checkbox (8). If not set with HTML tags present, the tags are displayed in the message as plain text.
9. If images selected as **Attachment** (10) are mentioned in the message in HTML format, set the **Inline attachments** checkbox to exclude the images from attachment (9). See the table below for available options:

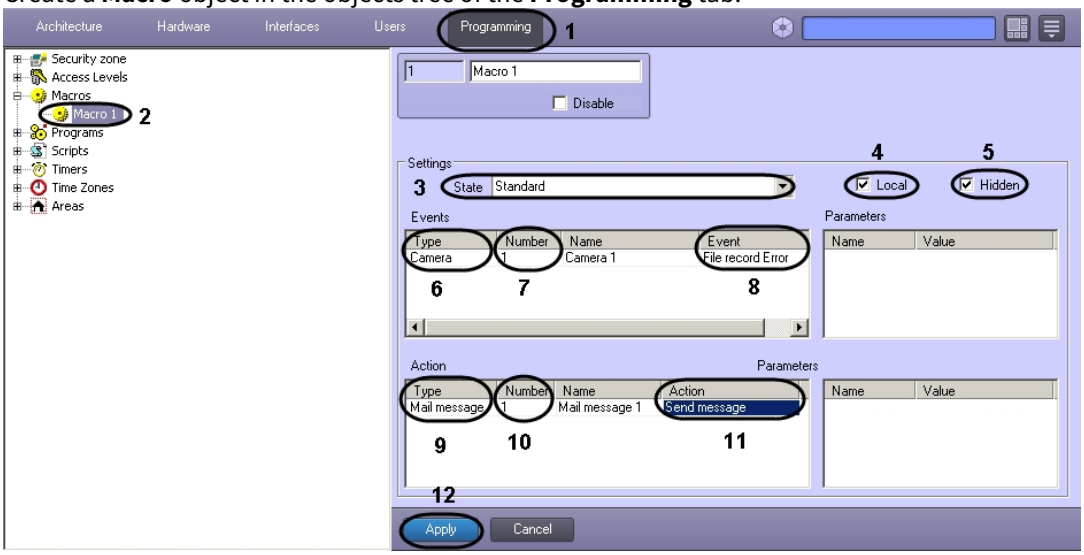
	HTML set	**HTML** not set
Inline attachments set	Images are shown in message text (if mentioned), NOT attached to the e-mail	Images not shown in the e-mail at all
Inline attachments not set	Images are shown in message text (if mentioned) AND in attachments	Images are shown in attachments

10. Attach a file to the alarm message (report, audio, image), if necessary (10). If several files are attached, their addresses are semicolon separated.
11. Specify if the attachment should be packaged (archived) (11).
12. Press the **Apply** button to save the settings for the **Mail Message** object (12).

23.3.13.3.4 Creating and setting up a macro for sending the e-mail message

The message is sent upon execution of a macro. The macro executes immediately after the registration of the event it is set for. To create the macro for sending the e-mail message:

1. Go to the **Programming** tab of the **System Settings** window.
2. Create a **Macro** object in the objects tree of the **Programming** tab.



3. Set the **State** parameter.
4. Check the **Local** checkbox to send the messages from a local computer only.
5. If the manual start of macros from the main control panel of Intellect software should be forbidden, set the **Hidden** checkbox.
6. Choose the event object type for the e-mail macro to be related to.
7. Choose the event object number for the e-mail macro to be related to.
8. Choose the name of the event to trigger the sending of an e-mail message.
9. Choose the **Mail Message** object in the **Type** column.
10. Choose the number of the **Mail Message** object to be sent by the macro.
11. Choose **Send Message** in the **Action** column.
12. Press the **Apply** button to save the settings for the **Macro** object.

23.3.13.4 Setting up the Voice Message Service (V-dial)

23.3.13.4.1 General information and usage details of the Voice Message Service

The Voice Message Service is used to transmit voice messages over telephone lines. The Service automatically dials up the specified phone numbers and plays the audio files. The following dialing options are available: until connection, until answer, until digital acknowledgement of message reception. To be able to send a voice message, a voice modem (V-Dial) should be installed on the computer.

> **Note.**
>
> For proper detection of a voice modem in INTELLECT™, the inf folder is to be created in the Intellect/Modules directory. The drivers of installed modem are to be copied to the Intellect/Modules directory. This action is to be performed for Windows 7 / Server 2012.

To create and send a voice message:

1. Create and configure the **Voice Message Service** object.

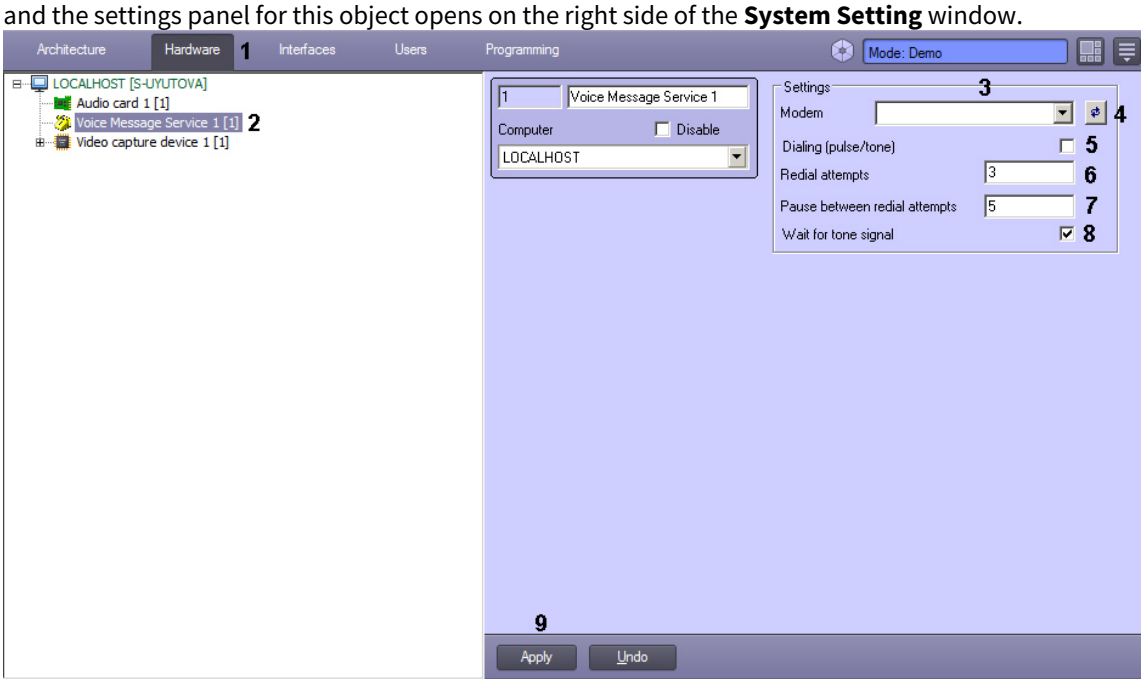
2. Create and configure the **Voice Message** object.
3. Create a macro for sending the voice message.

Requirements for voice modems

23.3.13.4.2 Creating and setting up the Voice Message Service object

To set up the **Voice Message Service** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window.
2. Create the **Voice Message Service** object in the **Computer** node in the objects tree. The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.



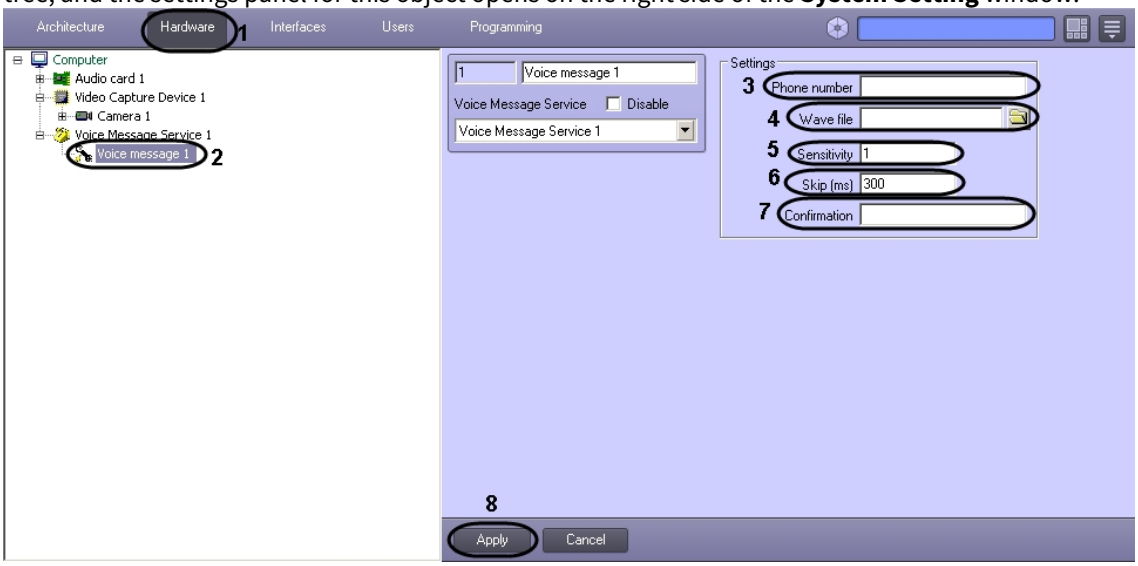
3. Choose a modem in the list of all modems available in the system.
4. If the modem is not in the list or there are no modems in the list, press the modem search button.
5. Check/uncheck the checkbox to choose the dialing mode.
6. Enter the number of dialing attempts.
7. Enter the delay between dialing attempts, in seconds.
8. Check the checkbox to wait for dialtone.
9. Press the **Apply** button to save the settings for the **Voice Messages Service** object.

23.3.13.4.3 Creating voice messages

To set up the **Voice Message** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window.

2. Create the **Voice Message** object in the **Voice Message Service** node in the objects tree. The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.

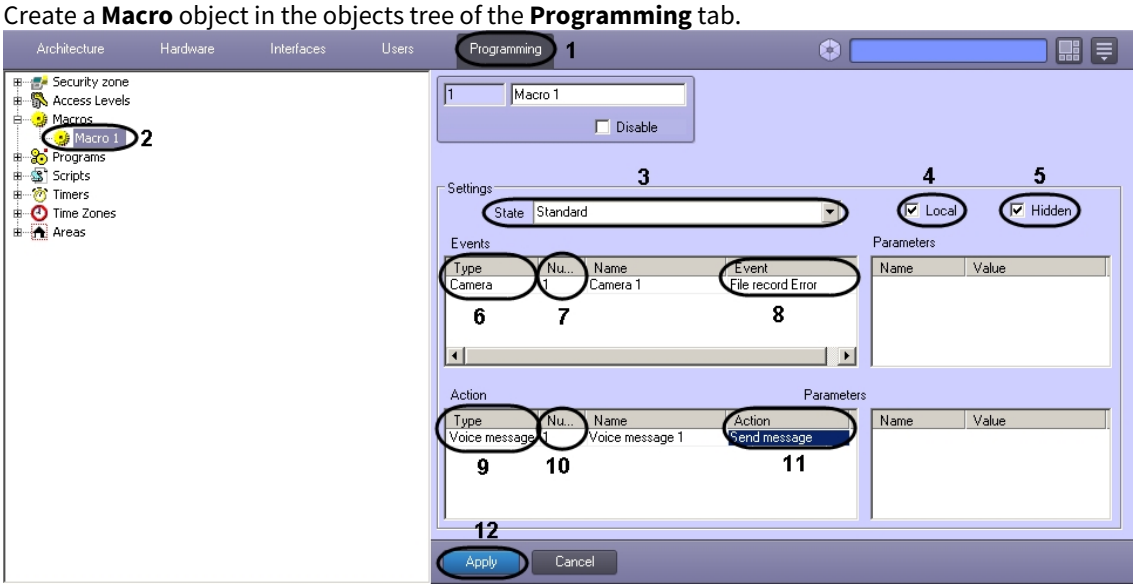


3. Enter the telephone number into the **Phone** field in the following format: [prefix “+”] [country code] [city/provider code] [phone number] with no spaces or other delimiters.
4. Load the wave file to be sent as a voice message.
5. Specify the sensitivity level, which will eliminate noise on the telephone line, ensuring correct message transmission. Values from 1 to 10 are acceptable.
6. Specify the delay between the recipient answering and the beginning of the message. Set in milliseconds (1000 ms = 1 sec).
7. Enter the code for the recipient to confirm receipt of the message. This is a digital code set in the system which the recipient dials in tone mode to confirm receipt of the message.
8. Press the **Apply** button to save the settings for the **Voice Message** object.

23.3.13.4.4 Creating and setting up the macro for sending the voice message

The message is sent upon execution of the macro. The macro executes immediately after the registration of the event it is set for. To create the macro for sending the voice message:

1. Go to the **Programming** tab of the **System Settings** window.
2. Create a **Macro** object in the objects tree of the **Programming** tab.



3. Specify the **State** parameter.
4. Check the **Local** checkbox to send the voice messages from a local computer only.
5. If the manual start of macros from the main control panel of Intellect sofware should be forbidden, set the **Hidden** checkbox.

6. Choose the event object type for the voice message macro to be related to.
7. Choose the event object number for the voice message macro to be related to.
8. Choose the name of the event to trigger the sending of the voice message.
9. Choose the **Voice Message** object in the **Type** column.
10. Choose the number of the **Voice Message** object to be sent by the macro.
11. Choose **Send Message** in the **Action** column.
12. Press the **Apply** button to save the settings for the **Macro** object.

23.3.13.5 Setting up the Voice Notification Service

23.3.13.5.1 General description and usage details of the Voice Notification Service (VNS)

The voice notification service is used for audio notification of Intellect Operators about the alarm event registered by the system. This service allows voice notification of the remote workstations using the following devices: headphones (speakers) connected to the workstation's sound card, IP camera or LinuxHub. The service provides automatic transmission of the voice notification to the specified device IP address and audio file playback.

There are also other ways of configuring voice notification in *Intellect* software – see Setting up the voice notification.

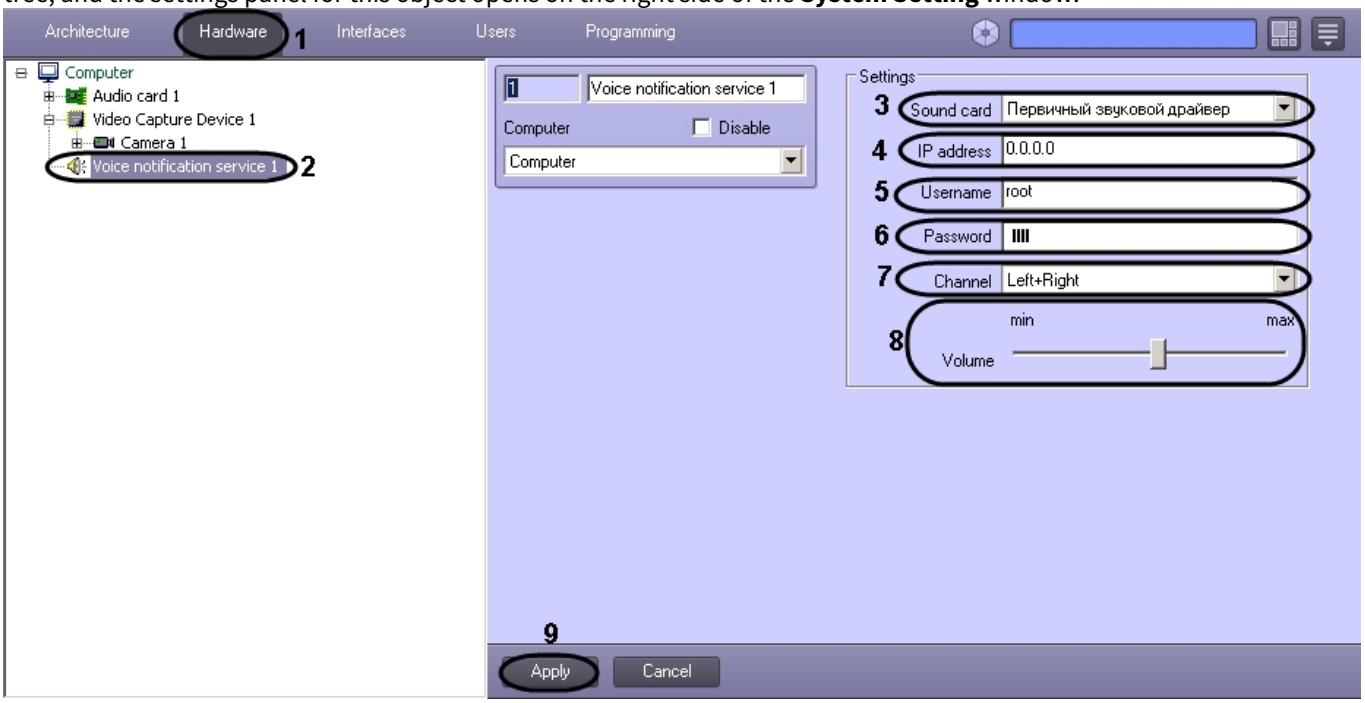
To create and send the voice notification:

1. Create and set up the **Voice Notification Service** object.
2. Create a macro for sending and stop playing the voice notification.

23.3.13.5.2 Creating and setting up the Voice Notification Service object

To set up the **Voice Notification Service** object, do the following:

1. Go to the **Hardware** tab of the **System Settings** window.
2. Create the **Voice Notification Service** object in the **Computer** node in the objects tree. The object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** window.



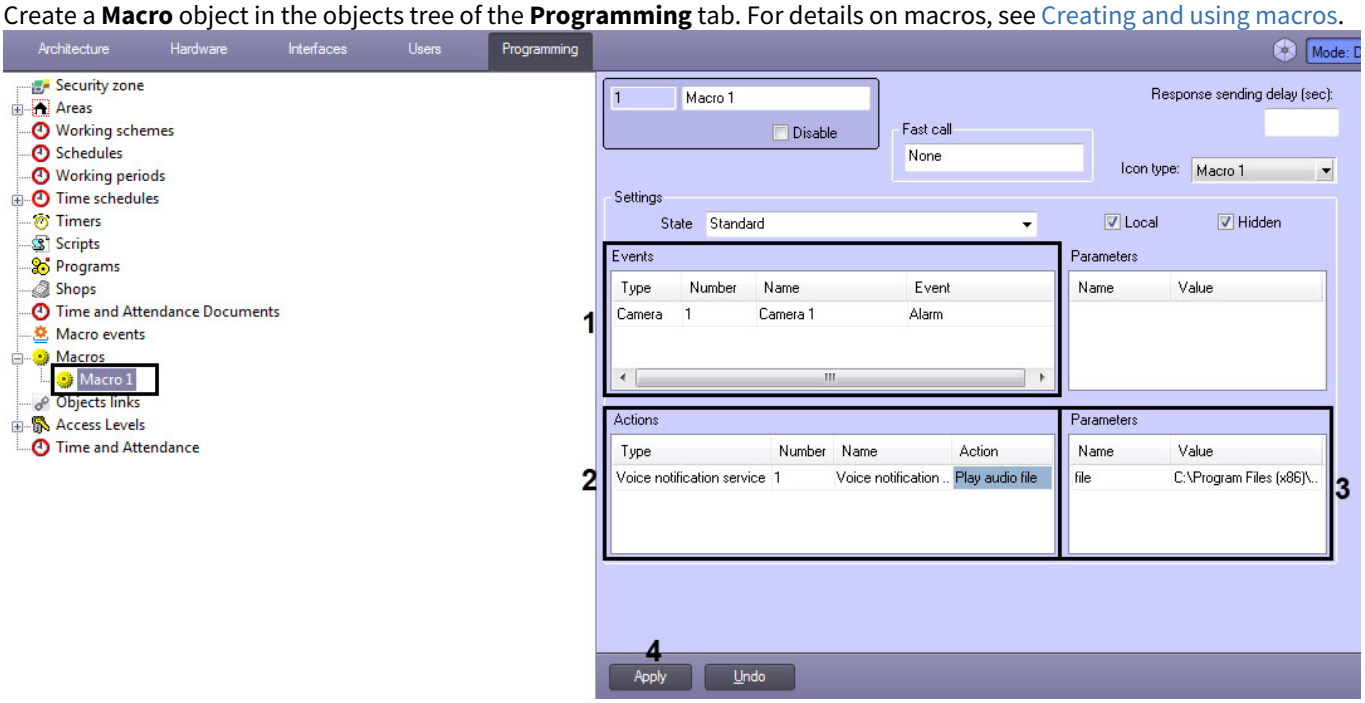
3. Choose the device in the **Sound card** list to send the notification to.
4. Specify the IP address of the network device (sound card, IP camera or Linux Hub), used to access this device over the network. If the sound card of the local computer is selected, this field is disabled.
5. Specify the username of the network device (sound card, IP camera or Linux Hub), used to access this device over the network. If the sound card of the local computer is selected, this field is disabled.
6. Specify the password of the network device (sound card, IP camera or Linux Hub), used to access this device over the network. If the sound card of the local computer is selected, this field is disabled.

7. Choose the headphones (speakers) playback option in the **Channel** drop-down list.
8. If the soundcard has two outputs (left/right), the list contains the following options: a) **Left**, b) **Left + Right**, c) **Right**.
9. If the sound card has N outputs, the list contains the numbered outputs from 0 to N-1.
10. Specify the volume level using the slider.
11. Press the **Apply** button to save the settings for the **Voice Notification Service** object.

23.3.13.5.3 Creating a macro for sending and stop playing the voice notification

The voice notification is sent upon execution of the macro. The macro executes immediately after the registration of the event it is set for. To create the macro for sending the voice notification:

1. Go to the **Programming** tab of the **System Settings** window.
2. Create a **Macro** object in the objects tree of the **Programming** tab. For details on macros, see Creating and using macros.

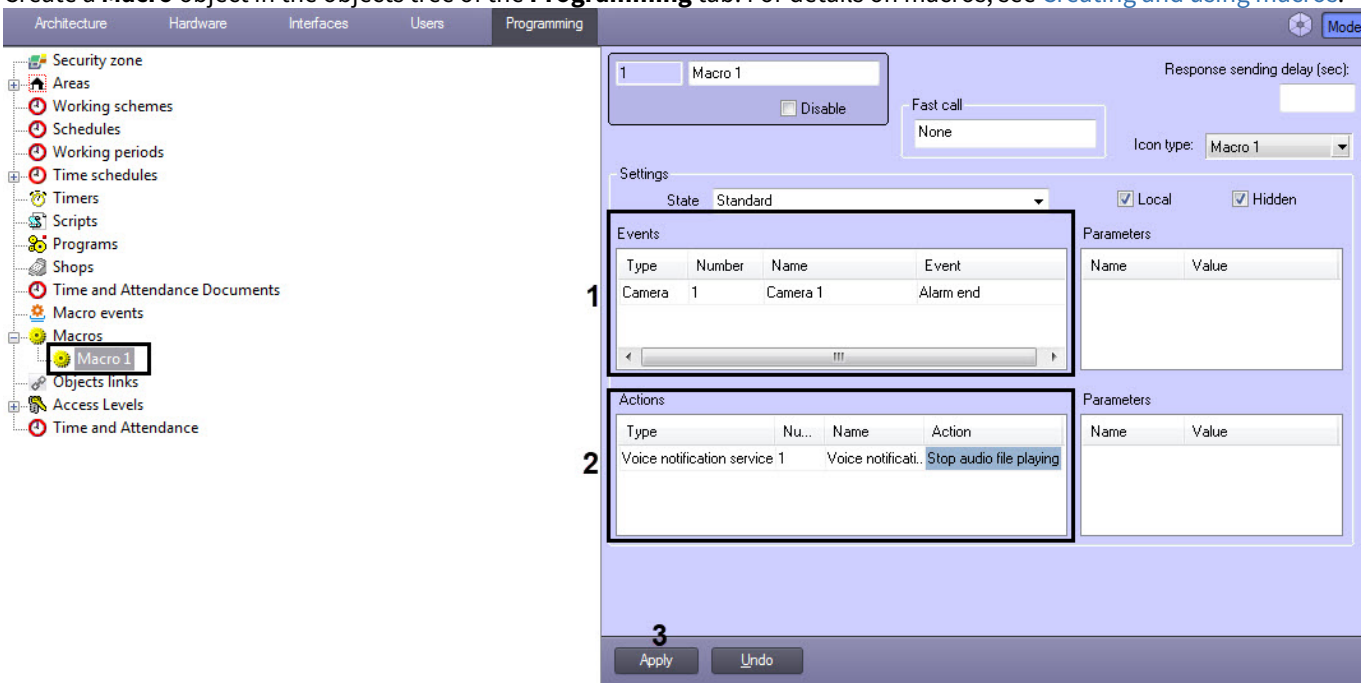


3. Select the object and its number, for which the voice notification macro is related to, and also select the event name for which a voice notification will be sent (**1**).
4. Select the **Voice notification service** object and its number, and also select the **Play audio file** action (**2**).
5. In the **Parameters** table, left-click to activate the **Name** field. Then in the **Value** field specify the full path to the audio file in .wav format (indicating the name of the file being played, for example: C:\Program Files (x86)\Intellect\Wav\cam_alarm_1.wav), that should be used as a voice notification (**3**).
6. Click the **Apply** button to save the settings of the **Macro** object (**4**).

The voice notification will stop after the macro command execution is completed. The macro is executed immediately after the registration of the corresponding event. To create a macro command to stop the voice notification, do the following:

1. Go to the **Programming** tab of the **System Setup** dialog box.

2. Create a **Macro** object in the objects tree of the **Programming** tab. For details on macros, see Creating and using macros.



3. Select the object and its number, for which the stop voice notification macro is related to, and also select the event name for which a voice notification will be stopped (**1**).
4. Select the **Voice notification service** object and its number, and also select the **Stop audio file playing** action (**2**).
5. Click the **Apply** button to save the settings of the **Macro** object (**3**).

23.3.13.6 Sending messages via Telegram bot

On the page:

- Configuring message sending from Intellect to Telegram
- Examples of macros for sending a message to Telegram

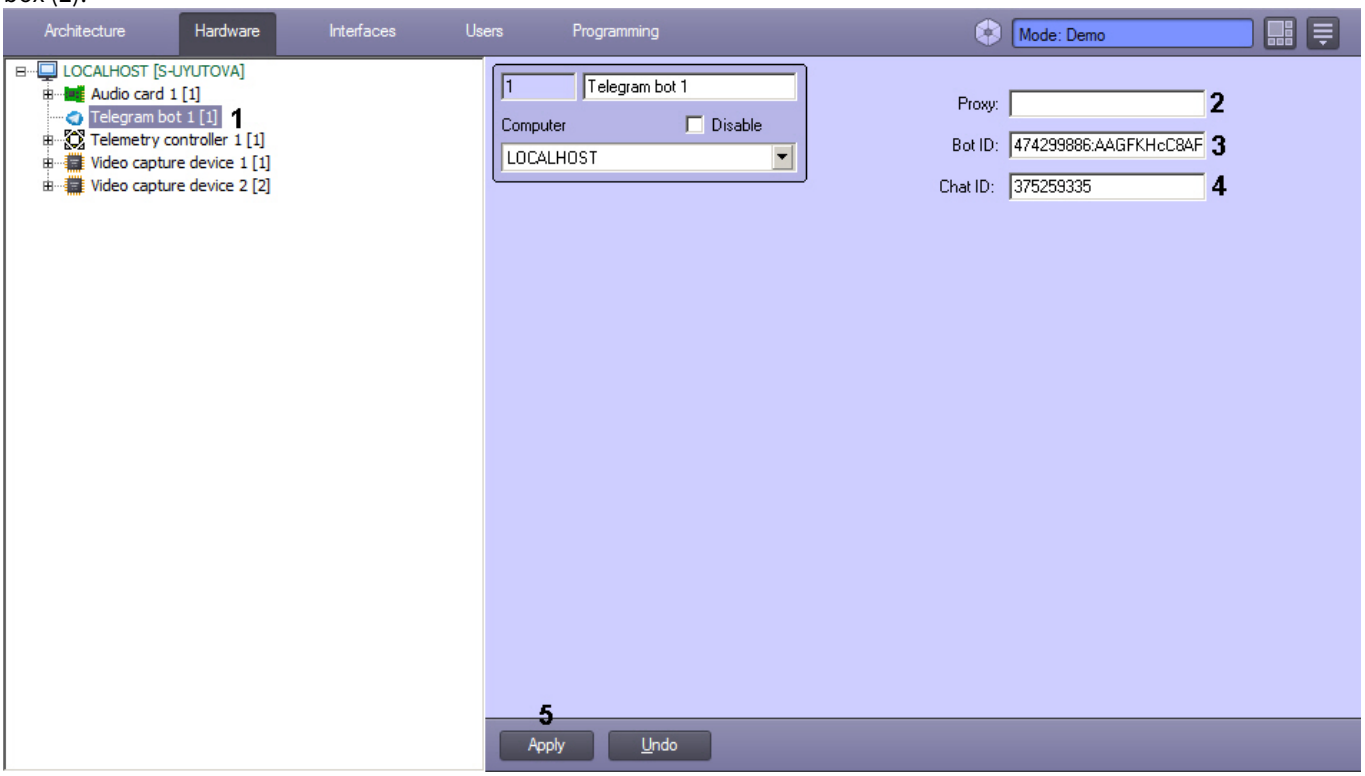
Intellect allows sending text messages, images, or geolocation to Telegram chat on any event from any object created in the *Intellect* objects tree. After configuration, the message sending is initiated by a macro or a script from *Intellect*.

Create the bot and the group chat with it in Telegram before configuring the message sending from *Intellect* to Telegram. You can use the pre-created and configured bot @IntellectNotificationsBot. For the distribution package and the user guide for Telegram messenger, see the developer official website telegram.org.

23.3.13.6.1 Configuring message sending from Intellect to Telegram

To configure message sending from *Intellect* to Telegram, do the following:

1. Create the **Telegram bot** object on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog box (**1**).



2. If the Proxy server should be used to send messages, enter the Proxy server address in the **Proxy** field (**2**).
3. In the **Bot ID** field (**3**), enter the Telegram bot identification number.

> **Note**
>
> The identification number is provided when creating the bot.
> @IntellectNotificationsBot bot identifier is 474299886:AAGFKHcC8ARX9ziXgTlvKnwNhxnwlDhmD3M

4. In the **Chat ID** field (**4**), enter the chat identification number.

> **Note**
>
> To find out the chat identifier, you can add @RawDataBot bot to the chat. After adding, the bot will send a message to the chat containing the result of the getUpdates function. Find ChatId in that message. Then the @RawDataBot bot can be removed from the chat.

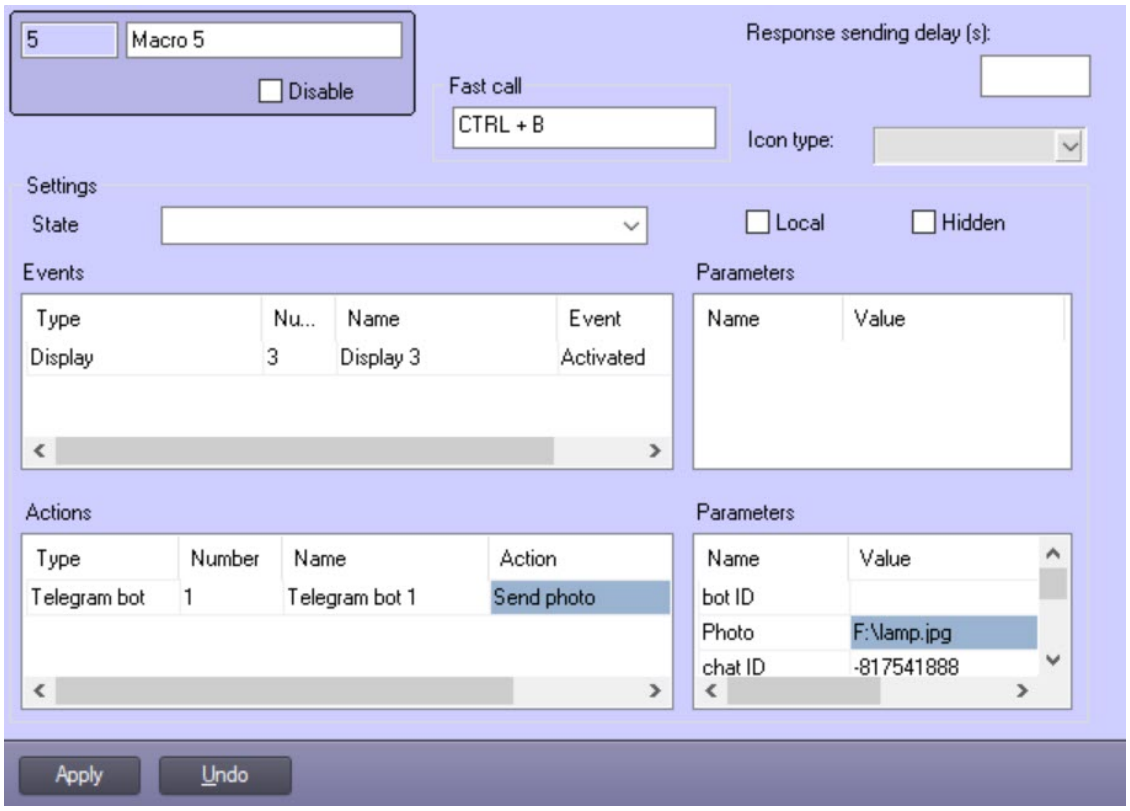
5. Click the **Apply** button (**5**).

Configuring message sending from *Intellect* to Telegram is complete.

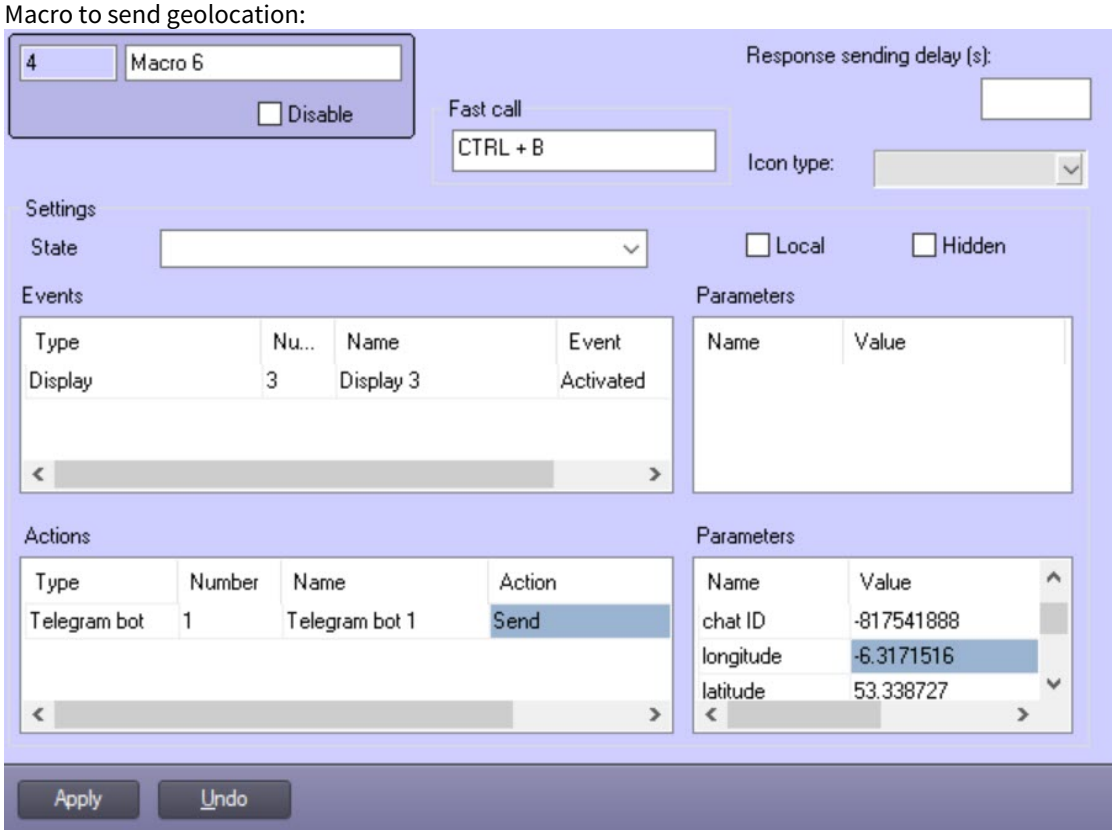
23.3.13.6.2 Examples of macros for sending a message to Telegram

Macro to send a text message:

Macro to send an image:



Macro to send geolocation:



See also examples of commands in TELEGRAM Telegram bot.

23.3.14 Replicating archive from unconnected servers using the removable storage

23.3.14.1 Order of archive replication from unconnected servers

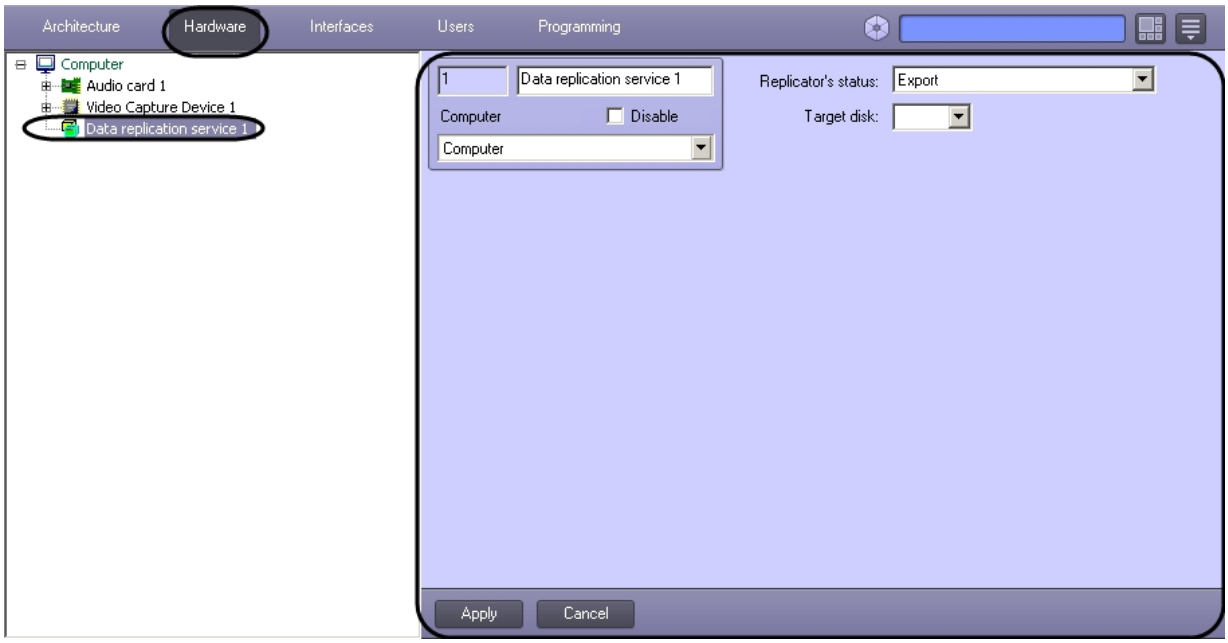
It is possible to receive video and audio archive from unconnected Servers in the *Intellect* software using the removable storage. Records over a specified period are copied from the Source-Server to the Target-Server while replicating archive.

Archive replication is performed in the following order:

1. Configure the **Data replication service** object on the Target and Source;
2. Configure the Target objects tree for data replication;
3. Create a query file on the Target using the schedule.exe utility;
4. Copy the archive from the Source to a removable storage;
5. Restore the archive from a removable storage on the Target.

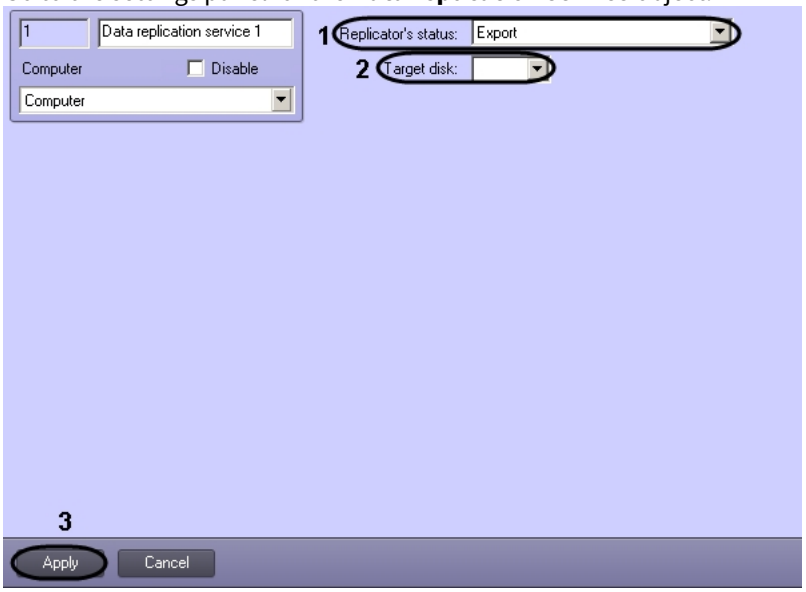
23.3.14.2 Configuring the Data replication service object

Data replication service is configured on the settings panel of the **Data replication service** object. This object is created under the **Computer** object in the **Hardware** tab of the **System settings** dialog box.



To configure the data replication service, do the following:

1. Go to the settings panel for the **Data replication service** object.



2. In the **Replicator's status** dropdown list select the **Export** value if the Server is an archive Source or the **Target** value if the Server is a target (1).
3. If the Server is a Source, then in the **Target disk** dropdown list select the name of a removable storage used for archive transfer. If the Server is a Target, then in the **Target disk** dropdown list select a disk where the archive form a removable storage is to be copied (2).
4. Click the **Apply** button (3).

Configuration of the data replication service is completed.

23.3.14.3 Configuring the Target objects tree for data replication

For proper replication operation the following objects are to be created in the objects tree of the Target objects:

1. In the **Hardware** tab of the **System settings** dialog box create the **Computer** objects with the names corresponding to the names of Sources from which the archive records are to be copied.

2. Under the **Computer** object create the **Video Capture Device** objects with the names that correspond to the same names on Sources (2).
3. Under the **Video Capture Device** objects create the **Camera** objects with numbers corresponding to the camera numbers the archive records from which are to be copied from Sources (3).

> **Note.**
>
> The **Camera** and **Video Capture Device** objects will be disabled because there is no connection between Source and Target.

When replication is completed the archive is available in the interface of Video surveillance monitor on cameras that are in the query.

Configuration of the Target objects tree is completed.

23.3.14.4 Creating the query file

The query file specifies Sources, cameras and time periods for archive replication. This file is created on the Target. To create the query file the following conditions are to be met:

1. Users are created in the INTELLECT™ (see User registration and removal section).

   > **Note.**
   >
   > Users with the same name and password are to be ctreated on Source and Targen for stable operation of the **Data replication service**.

2. Corresponding rights are assigned to users (see Registration of users' rights section).
3. At least one **Camera** object is created in the Target hardware tree.

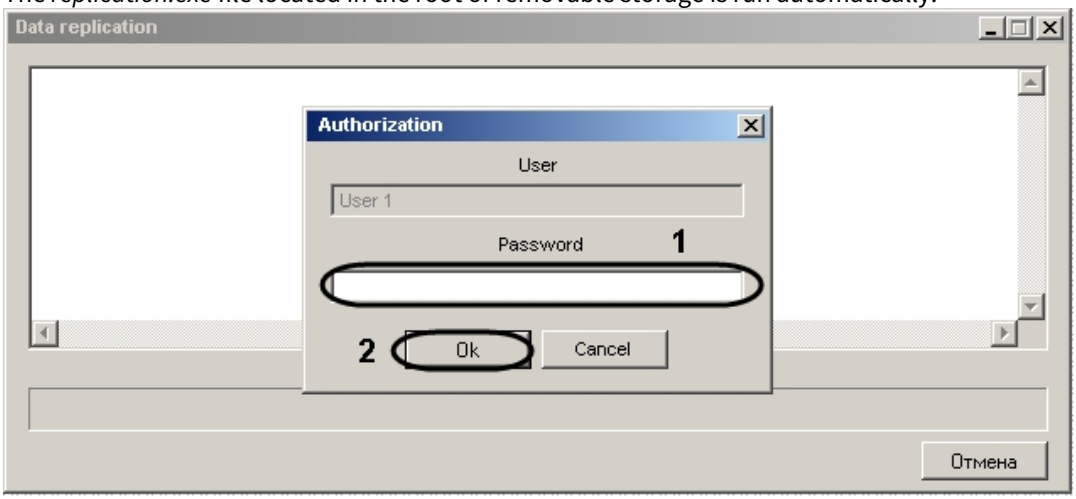
The query file is created using the *schedule.exe* utility (see The shedule.exe utility for creating a replication query file section).

23.3.14.5 Copying the archive from the Source

To copy the archive from the Source, do the following:

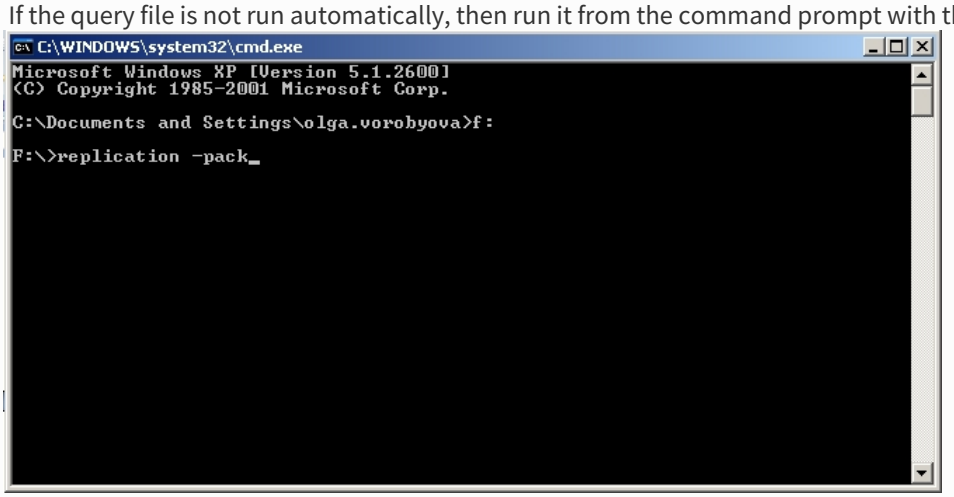
1. Connect the removable storage with a query file to the Source.

2. The *replication.exe* file located in the root of removable storage is run automatically.

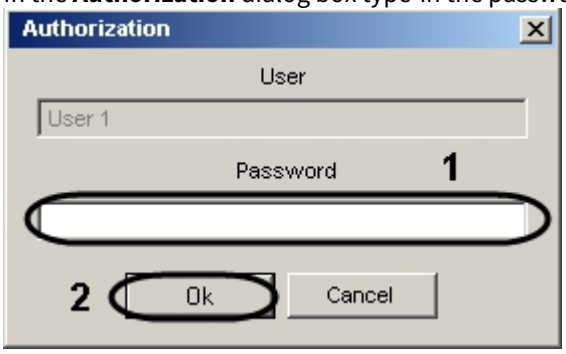


Note.

If the query file is not run automatically, then run it from the command prompt with the **-pack** parameter.



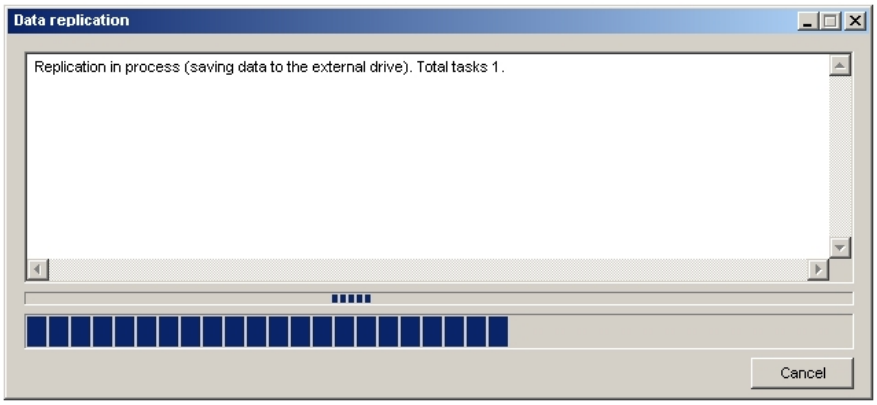
3. In the **Authorization** dialog box type-in the password of user who makes the replication (1).



4. Click the **OK** button (2).
5. Wait when the data copying is complete.

Note.

If there is no enough space for copying all required data, then there will be no copying.



6. Click the **Exit** button.

Requested part of the archive is copied to a removable storage and located in the IntellectBackup/Computer_name directory. Files of log replication with the .LOG extension are located in the IntellectBackup directory.

Removable storage is automatically removed when the copying is complete.

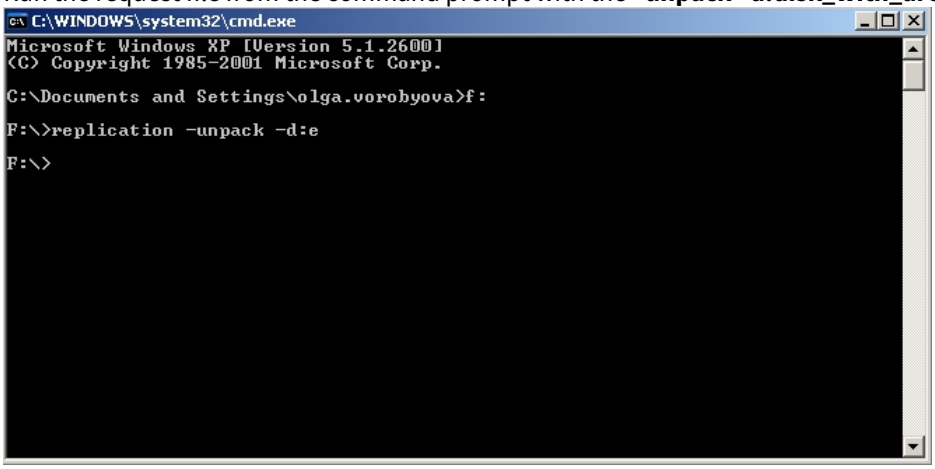
Archive copying from the Source is completed.

23.3.14.6 Restoring the archive on the Target

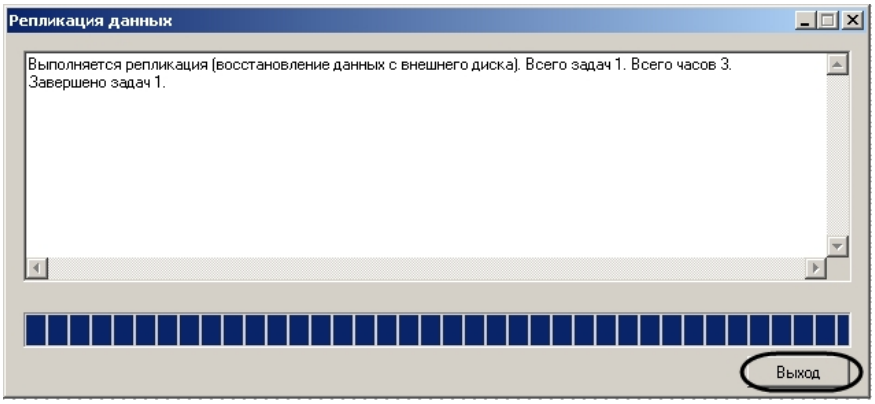
When the archive is restored data is copied from the removable storage to the Target.

To restore the archive do the following:

1. Connect the removable storage to the Target.
2. Run the request file from the command prompt with the **–unpack –d:disk_with_archive** parameters.



3. Wait when the data copying is complete.
4. Click **Exit**.



The archive restoring on the Target is completed.

23.3.15 Configuring the Web-server module

23.3.15.1 General description of the Web-server module

The Web-server module is used for viewing the video surveillance information in a web browser using the TCP/IP communication protocol.

Web-server provides some of the functions of an HTTP server, video transfer gate and HTTP control commands.

Web-server provides the following HTTP server functionality:

1. Access control through authorization.
2. Working as a gate for transferring video data using HTTP/HTTPS protocol.
3. Video monitoring and camera control through the web browser using the TCP/IP environment.
4. Control of camera movement through the web browser using the TCP/IP environment.
5. Setting the layout of the video frames on the screen: 1, 4, 6, 9 windows per screen.
6. Viewing the archives stored on the videoserver for each camera through the video surveillance window.
7. Limiting access rights for viewing the video feed from the cameras, controlling the camera movement, and viewing recordings from the videoserver.
8. Displaying the video signal parameters (frame rate (fps) and frame size (kB) in the surveillance window.

Attention!

Web-server displays only video in MJPEG format. When video is transferred onto Web-server, the Web-server performs video stream recompression and that causes the traffic increment while transmitting video onto Web-server surveillance monitor.

The Web-server interface looks like a video surveillance monitor and is built as an HTML page. This page is called the Web-server's home page. The surveillance monitor and control elements for the camera movement devices are driven by the Java applet.

Intellect software can be set up to require user authorization on entering the Web-server. Access to viewing and controlling the movement of the cameras through the Web-server is defined by the module settings.

System requirements
Video surveillance using the Web browser

23.3.15.2 System requirements

The Web-server module stable opration requires Java Runtime Environment version 1.6. 7 or higher (mentioned software is included into the Intellect software installation package) and browser Internet Explorer version 8.0 and higher (this software is available free of charge).

Installing Java Runtime Environment

23.3.15.3 Installing Java Runtime Environment

The Web-server module working on videoservers and workstations of the *Intellect*-based surveillance system requires Java Runtime Environment. This software is available free of charge.

The option for Java Runtime Environment installation is included in the *Intellect* software installation procedure.

Java Runtime Environment should be manually installed on the remote workstations. The Java installation package is available for downloading from www.java.com. If the Web-server home page is accessed from a computer with no Java installed, the home page will contain a direct link to the Java Runtime Environment installation package ready for downloading.

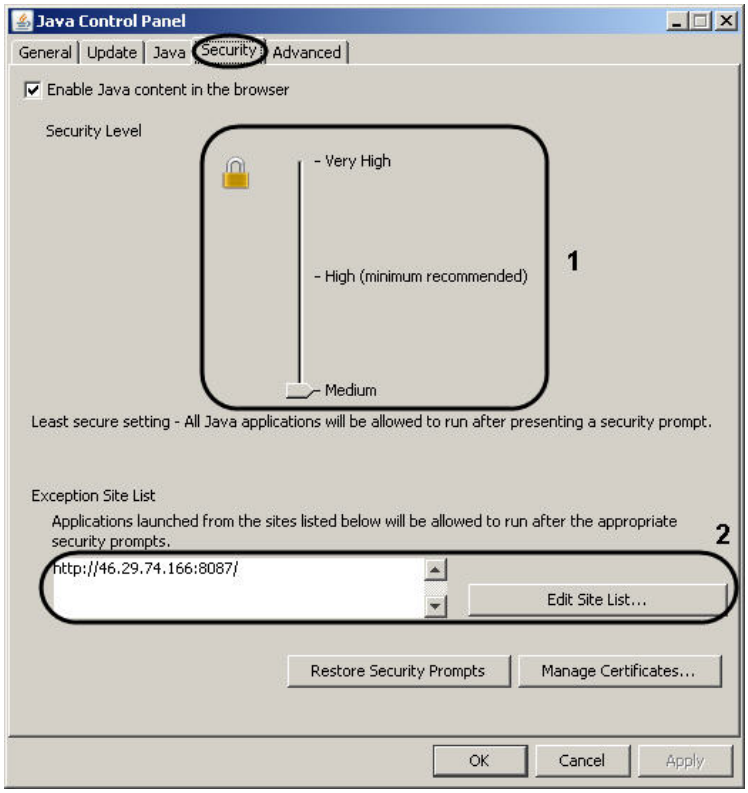
Note.

It is necessary to install Java Runtime Environment not in quiet mode. Otherwise the Intellect may not respond displaying two possible messages:

1. «Error applying transforms. Verify that the specified transform paths are valid». - alternate route s of this error are detailed on the site http://www.java.com/ru/download/help/error_applying_transforms.xml .
2. «Revocation information for the security certificate for this site is not available. Do you want to proceed? » - certificate installation query.

If the message appears when you try to access the Web-server saying that the application is blocked by security settings (see figure below), the Java security policy configuration is required for the computer on which you have received this message.

Configuring security policy is performed with the Java Control Panel utility. To run this utility, go to **Start** -> **Control Panel** -> **Java**. After the utility has been launched, go to the **Security** tab.



For Java Runtime Environment 7 update 45 and lower versions it is required to reduce security level (1).

Starting with Java Runtime Environment 7 update 51 version you need to add Web-server address to the list of Java exceptions (2).

23.3.15.4 Authorization on the Web-server home page

Access to the Web-server home page is restricted by an HTTP user authorization algorithm.

A user can be authorized by any of the passwords registered for the Intellect users. No additional authorization setup for Web-server HTTP server is required.

To authorize users with blank passwords, you need to change the **LimitBlankPasswordUse** registry key to **0** (for detailed description, refer to Working with Windows OS registry) on the PC where the *Web Server* is located. You can find the **LimitBlankPasswordUse** key in the following registry branch:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

Access to viewing the video feed from the cameras and controlling the cameras, sensors and motion devices is restricted according to the Web-server-related settings of the videoserver.

Connection to the Server

23.3.15.5 Starting and setting up the Web-server module

Depending on its operative requirements, the Web-server module can be set up in the following optional stages:

1. Open the **Hardware** tab and select the **Web-server** object in the objects tree.
2. Check if the Web-server is on. This can be checked in the notification area of the Windows taskbar. By default, the Web-server is on. If the Web-server is off, turn it on before starting the setup procedure.

3. Set up the interface for the video surveillance monitor of the Web-server by changing the Java applet parameters shown on the Web-server home page.
4. Set up the display of the data for traffic estimation on the Web-server video surveillance monitor by changing the Java applet parameters shown on the Web-server home page.

Set up the Web-server to act as a gate on another HTTP-server by changing the Java applet parameters shown on the Web-server home page.

23.3.15.6 Configuring the videoserver to connect Clients via the Web-server module

The videoserver configuration to connect Clients via the Web-server is performed on the Server in the **System settings** box. In most cases, the default videoserver settings can be used for proper Web-server operation.

To configure the Web-server module, do the following:

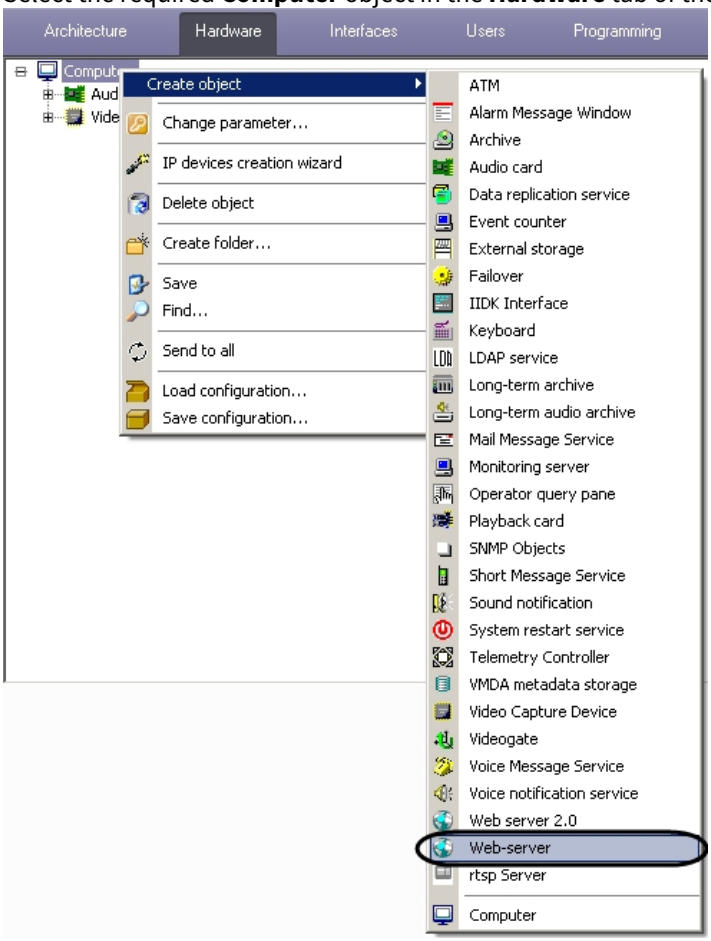
1. Create the **Web-server** object on the basis of the **Computer** system object (see Creating the Web-server object).
2. Select and configure cameras for displaying on the Web-server home page (see Selecting and configuring cameras for the Web-server module or Bulk selecting and configuring cameras for Web-server).
3. Select PTZ control priority for video surveillance in web browser (see Configuring PTZ control priority for Web-server).
4. Set the connection parameters of Clients to the Web-server (see Setting the parameters of connecting Clients to the Web-server).
5. Set the default user for Web-server module (see Configuring the authorization for the Web-server module. Default user).
6. Set up the processing of ECHD requests (Enabling the processing of SDC (ECHD) requests and selecting the RTSP server).

Video surveillance using the Web browser

23.3.15.6.1 Creating the Web-server object

To create the **Web-server** object, do the following:

1. Select the required **Computer** object in the **Hardware** tab of the **System settings** dialog box (1).



2. Right-click upon the selected **Computer** object and select **Create object** -> **Web-server** in the context menu (2).
3. Set the number and name of **Web-server** object and then click **Apply** button.

> **Note.**
>
> As a result the settings panel for the **Web-server** object opens.

4. Repeat steps 1-3 for all required **Computer** and **Web-server** objects.

The **Web-server** object is now created.

23.3.15.6.2 Selecting and configuring cameras for the Web-server module

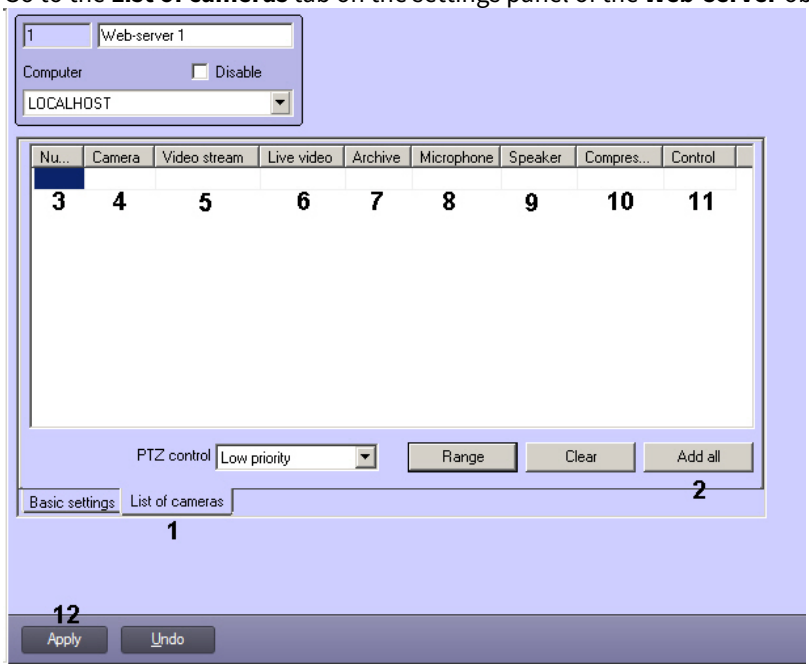
One can select and configure cameras for displaying on the **Web-server** home page in two ways:

1. Individually. The settings panel of the **Web-server** object is used**.**
2. In bulk. The **Add/Edit cameras** dialog box is used.

> **Note.**
>
> Information on how to bulk select cameras in order to stream video via Web-server is given in Bulk selecting and configuring cameras for Web-server section.

To select cameras for displaying on the Web-server home page, do the following:

1. Go to the **List of cameras** tab on the settings panel of the **Web-server** object (1).



> **Note.**
>
> To select all cameras created in the system use the **Add all** button (2).

2. In the **Number** dropdown list select the number of a required camera (3). Being left-clicked the **Camera** field is automatically filled in with the camera name with the selected number (4).

> **Note.**
>
> To select all the cameras registered in the system, click the **Add all** button.

3. In the **Video steam** dropdown list select the number of the stream that is to displayed in the Web-server interface (5). Information on how to configure video streams is given in the *Configuration of multistream video* section.
4. In the **Live video** dropdown list select the source of live video to be displayed in the Web-server interface (6). If the **Server** value is selected, then live video is received from the Server on which the corresponding **Camera** object is created.
   If the **Videogate** value is selected, then video will be received from the corresponding videogate. A camera is to be configured in the corresponding Videogate – see the *Selecting and configuring the cameras for the Videogate module* section.
   If the **Server** value is selected, then archive footage is received from the Server on which the corresponding **Camera** object is created. If the **Videogate** or **Backup archive** value is selected, then archive footage is received from the videogate or backup archive. A camera is to be configured in the corresponding Videogate or Backup archive.
5. In the **Archive** dropdown list select the the source of archive footage to be displayed in the Web-server interface (7).
6. Select the **Microphone** object associated with the camera from the **Microphone** drop-down list if a sound came from the camera is to be passed over the **Web-server 2.0** (8).

7. Select the **Speaker** object associated with the camera from the **Speaker** drop-down list if a sound came from the **Web-server 2.0** is to be played (9).

   Attention!

   Steps 6 and 7 are to be executed only in case if the Web-server runs together with the Web-server 2.0, which, in its turn, is used to work with the iOS-based mobile client. For more information on the Web server 2.0, see section Configuring the Server to connect the Clients via the Web-server 2.0 module

8. By default the compression ratio of video transmitted to the Surveillance monitor through the Web-Server is the same as the compression ratio of video before its recording to the disk or transmitting (the blank value is selected in the **Compression** dropdown list). To change the compression ratio, select the required compression (1-5 where 1 is minimum compression ratio, and 5 is maximum) ratio in the **Compression** dropdown list (10).

   Note.

   The compression level parameter for the signal transmission to remote workstations via the Web-server is inverse to the **Recording quality** parameter of the **Camera** object.
   Increase of video signal's compression level decreases the network traffic while connecting the Client to the Web-server. But video signal on the Server has to be recompressed in case of setting the compression level that results in greater load on Server's central processor. The compression level is selected empirically.

9. By default the camera control (arming/disarming, PTZ control, control over recording to the archive) in accordance with user rights is enabled. To disable the camera control, select the **Disabled** value in the **Control** dropdown list (11). As a result the camera control in the Web-server interface is disabled regardless of the user rights.
10. Repeat steps 2-9 for all required cameras.

    Note.

    To clear the **Cameras** table click the **Clear** button.

11. To save the changes, click the **Apply** button (12).

Cameras for displaying on the Web-server home page are now selected.

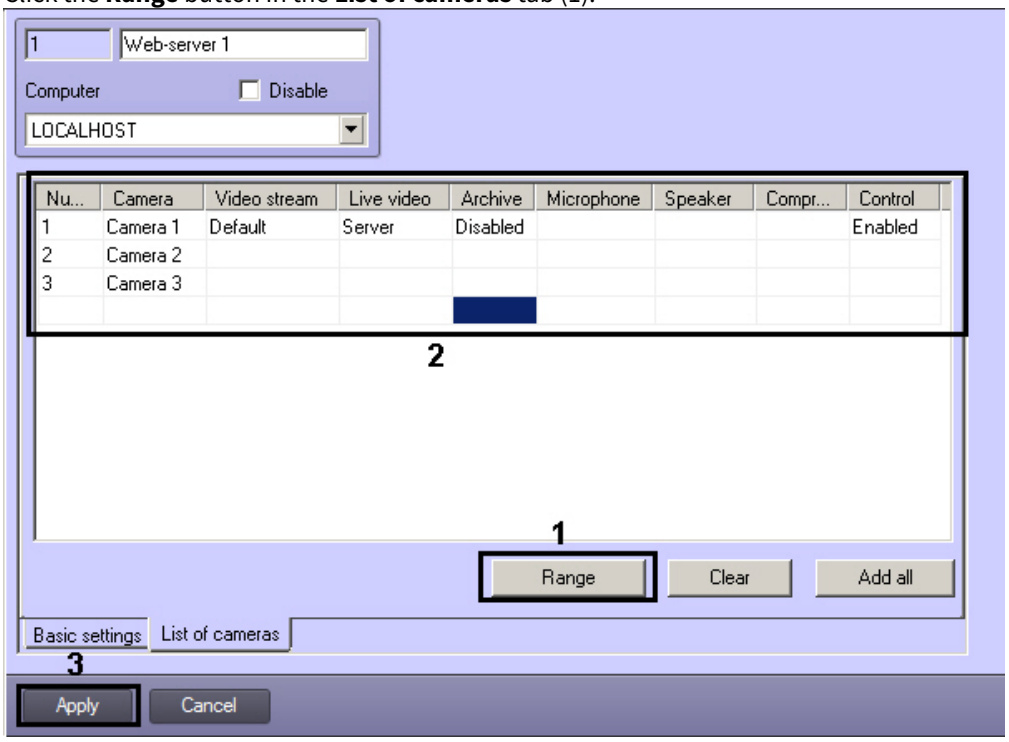
23.3.15.6.3 Bulk selecting and configuring cameras for Web-server

Parameters of cameras can be bulk selected and edited for displaying on the **Web-server** home page.

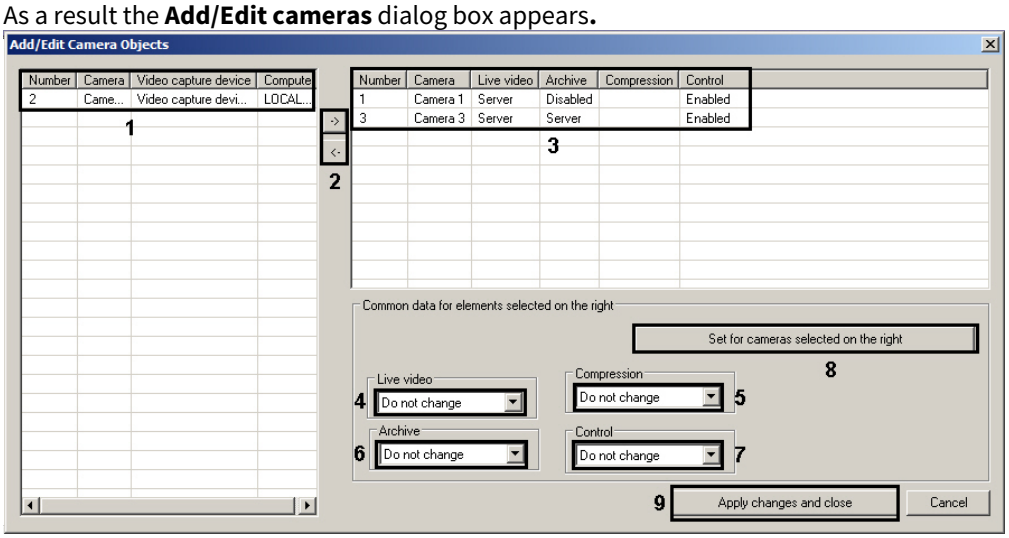
Bulk select cameras as follows:

1. Go to the settings panel of the **Web-server** object**.**

2. Click the **Range** button in the **List of cameras** tab (1).



3. As a result the **Add/Edit cameras** dialog box appears**.**



4. Select required cameras in the list on the left of the **Add/Edit cameras** dialog box (1).
5. Move selected cameras to the list on the right by clicking the button (2).

> **Note.**
>
> The list on the right is the list cameras selected to stream video via Web-server.
> The button performs reverse action, i.e. it is used to move selected cameras from the right list to the left one (2).

6. As a result, selected cameras are displayed in the list on the right of the **Add/Edit cameras** dialog box (3).
7. If necessary, select names of required cameras in the list on the right to bulk edit the parameters (4).

> **Important!**
>
> The same parameter values will be set for all selected cameras.

8. In the **Live video** dropdown list select the source of live video to be displayed in the **Web-server** interface (4). If the **Server** value is selected, then video will be received from the Server on which the corresponding **Camera** object is created. If the

Videogate value is selected, then video will be received from the corresponding videogate and the camera is to be configured in the corresponding Videogate – see Selecting and configuring the cameras for the Videogate module.

9. By default the compression level of video sent to the monitor of the Web-server module is the same as one before storing video on disk or transmitting it over network (an empty value is selected in the **Compression** dropdown list). To change the video compression level select the required compression level (from 1 to 5) in the **Compression** dropdown list. 1 is the minimum compression level and 5 is the maximum compression level (5).

> **Note.**
>
> The video compression level parameter is inversely related to the **Quality** parameter specified in the **Camera** settings.
> Video compression level increase reduces traffic when connecting the Client to Web-server. However, if the video compression level is set video must be recompressed on the Server – it results in significant increase of Server CPU load. The compression level is selected empirically.

10. In the **Archive** dropdown list select the source of archive video to be displayed in the **Web-server** interface (6). If the **Server** value is selected, then archive video will be received from the Server on which the corresponding **Camera** object is created. If the **Videogate** or **Backup archive** value is selected, then video will be received from the corresponding videogate or backup archive and the camera is to be configured in the corresponding Videogate or Backup archive.
11. By default camera control (including PTZ control, arm/disarm and store to archive control) is enabled according to user rights. To disable camera control select the **Disable** value in the **Control** dropdown list (7). As a result camera control in the Web-server interface will be forbidden regardless user rights.
12. To save specified parameters click the **Set for cameras selected on the right** button (8).
13. As a result the specified parameters are displayed in the list on the right of the **Add/Edit cameras** dialog box (3).
14. Repeat steps 4-13 to bulk edit all required cameras.
15. To save the changes and close the **Add/Edit cameras** dialog box click the **Apply changes and close button** (9).
16. The specified camera settings will be displayed in the **List** table on the settings panel of the **Web-server** object (2).
17. To save the changes click the **Apply** button (3).

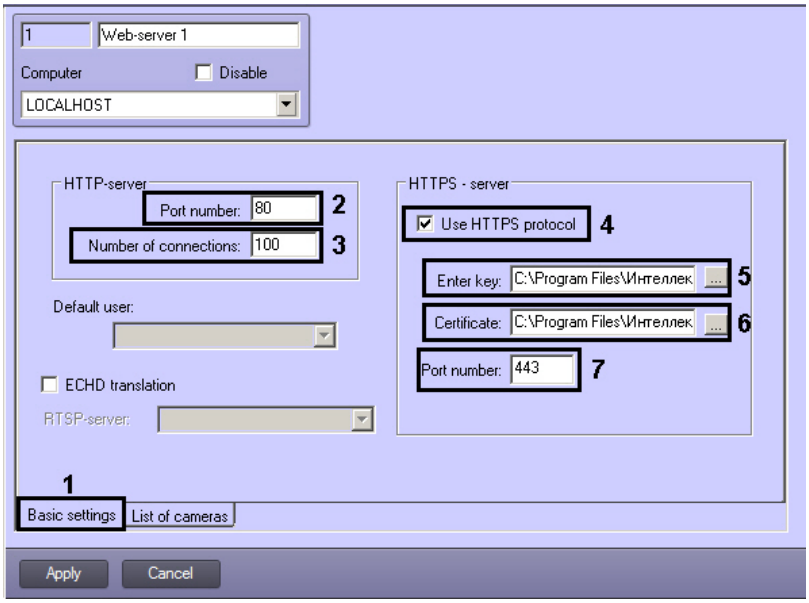
Cameras are now bulk selected.

23.3.15.6.4 Setting the parameters of connecting Clients to the Web-server

To set the parameters of connecting Clients to the Web-server, do the following:

1. Go to the **General settings** tab on the settings panel of the **Web-server** object (1).
2. In the **Port number** field of the **Http-server** group specify the number of the port to connect to Http-server (2).

> **Important!**
>
> This port is used when connecting to the *Web-server* from web-browser. The default port for connection of mobile clients is 8085. To change it, edit the jetty.port parameter value in the start_64.bat file (start_86.bat for 32-bit system) in <Intellect installation>\Modules\Jetty\ folder.



3. In the **Number of connections** field of the **Http-server** group specify the maximum permissible simultaneous connections to Web-server via Http protocol (2). The less there are connections, the less Server load is. This parameter is selected experimentally.

   Note.

   Connections are used to receive video (live or archive), to receive audio (live or archive), to send audio to INTELLECT™, to get data on configuration, to send commands to INTELLECT™, etc. The Client can use the same connection to perform several actions.

4. If data is to be transmitted via Web-server using HTTPS protocol, then perform the following settings in the **HTTPS-server** group:
   a. Set the **Use HTTPS protocol** checkbox checked (4).
   b. Specify path to the key file in the **Key** field using the ... button (5).
   c. Specify path to the certificate file in the **Certificate** field using the ... button (6).
   d. In the **Port number** field of the **HTTPS-sever** group specify the port number in order to connect to HTTPS-server (7).

      Note.

      To connect clients via HTTPS, it is also necessary to set the following settings in the index.htm file located in the installation directory of the *Intellect* software package in the ...\Modules\webroot folder:
      <param name="port.from" value="html">
      <param name="port" value="443">
      <param name="url.protocol" value="https">

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

The parameters of connecting Clients to the Web-server are now set.

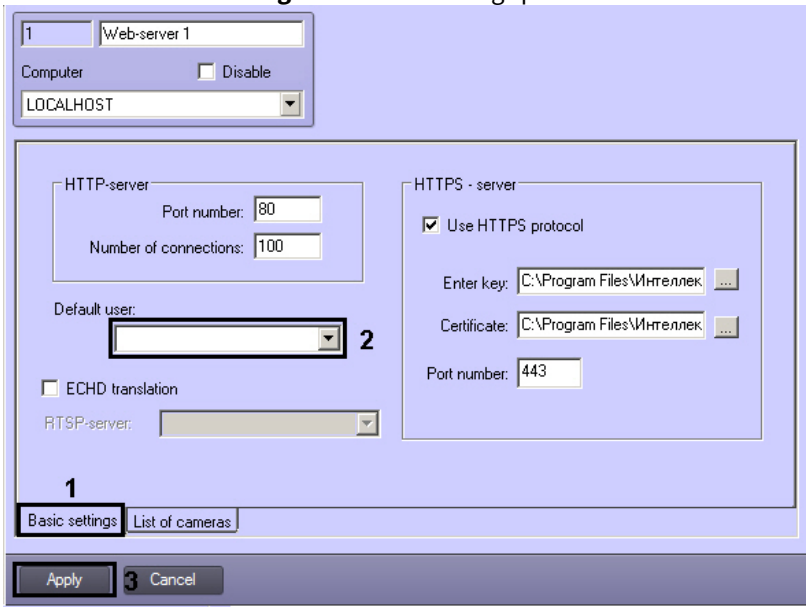
23.3.15.6.5 Configuring the authorization for the Web-server module. Default user

Default user is the user with rights and authorities to conduct video surveillance from a Web browser. If the default user is not specified, then it is necessary to enter a username and password when opening the Web-server page in the browser, and also when connecting via the HTTP API and using the mobile clients.

Before setting the default user, make sure that the users are created and added to the rights in INTELLECT™ (see Rights administration section).

To set default user, do the following:

1. Go to the **General settings** tab on the settings panel of the **Web-server** object (1).



2. Select the default user in the **Default user** dropdown list (2)
3. Click the **Apply** button (3).

The default user for the Web-server module is now set.

23.3.15.6.6 Enabling the processing of SDC (ECHD) requests and selecting the RTSP server

> **Attention!**
>
> Integration with ECHD requires *Intellect* user credentials that do not contain special characters (such as \, /, :, *, ?, |, ", etc.) in the login and password—it is a specific feature of configuring the stream transmission via RTSP.

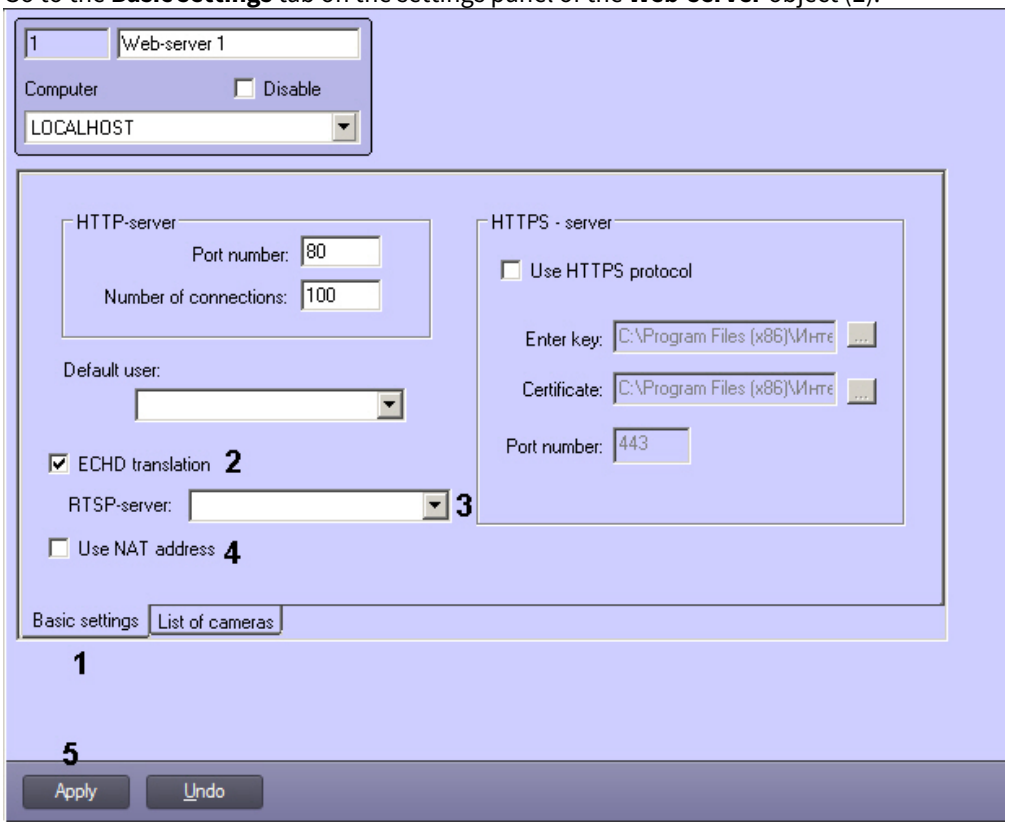
Integration with Single Data Center (ECHD) is supported in *Intellect*. Requests to *Intellect* are made in ECHD using HTTP API—see Intellect HTTP API. Some requests have http/https interface. These requests are used to get info on configuration. The **RTSP Server** bound to the **Web-server** object streams live or archived video.

Besides binding the Web server to the RTSP server, the **ECHD channel** objects are to be created under the **Camera** object for ECHD requests operation.

> **Note.**
>
> Information on how to create and configure the **RTSP Server** object is given in Configuring RTSP Server module section.

Bind **RTSP Server object** to process ECHD requests as follows:

1. Go to the **Basic settings** tab on the settings panel of the **Web-server** object (**1**).



2. Set the **ECHD translation** checkbox (**2**).
3. Select created and pre-configured **RTSP Server** object in the **RTSP Server** drop-down list (**3**).
4. If the CCTV servers are located behind NAT when interacting with the ECHD, then to use the NAT address (**4**), set the **Use NAT address** checkbox to substitute the router address in the ECHD requests.

   > **Note**
   >
   > The address and port of the router are set during the configuration of the RTSP Server object.

5. Click the **Apply** button (**5**).

The **RTSP Server** object is now bound to **Web-server** object.

23.3.15.6.7 Configuring PTZ control priority for Web-server

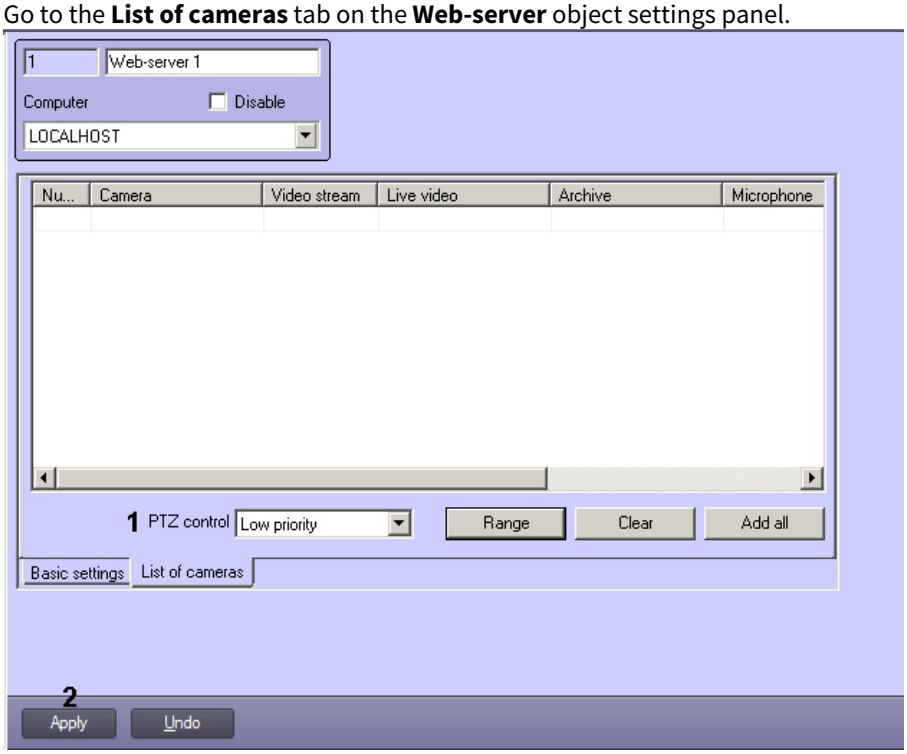
Intellect allows PTZ device control during video surveillance in web browser.

PTZ devices are controlled from web browser with low default priority (see Priorities of PTZ control). Also, PTZ control priority may be altered by the TelemetryPriority registry key (see Registry keys reference guide). When that key is set, the below setting parameter is ignored.

> **Note.**
>
> Enable the general camera control functions when adding the camera in order to enable PTZ control (see Selecting and configuring cameras for the Web-server module).

Configure PTZ control priority for the *Web-server* as follows:

1. Go to the **List of cameras** tab on the **Web-server** object settings panel.



2. Select the required priority from the **PTZ control** drop-down list (1).
3. Click **Apply** (2).

PTZ control priority for the *Web-server* is now configured.

23.3.15.7 Configuring the Server to connect the Clients via the Web-server 2.0 module

The *Web-server 2.0* module is used for video surveillance on the side of a mobile client application. Detailed information on such applications can be found in the corresponding documents (see AxxonSoft mobile Clients. Documentation).

Web-server 2.0 has the following functions:

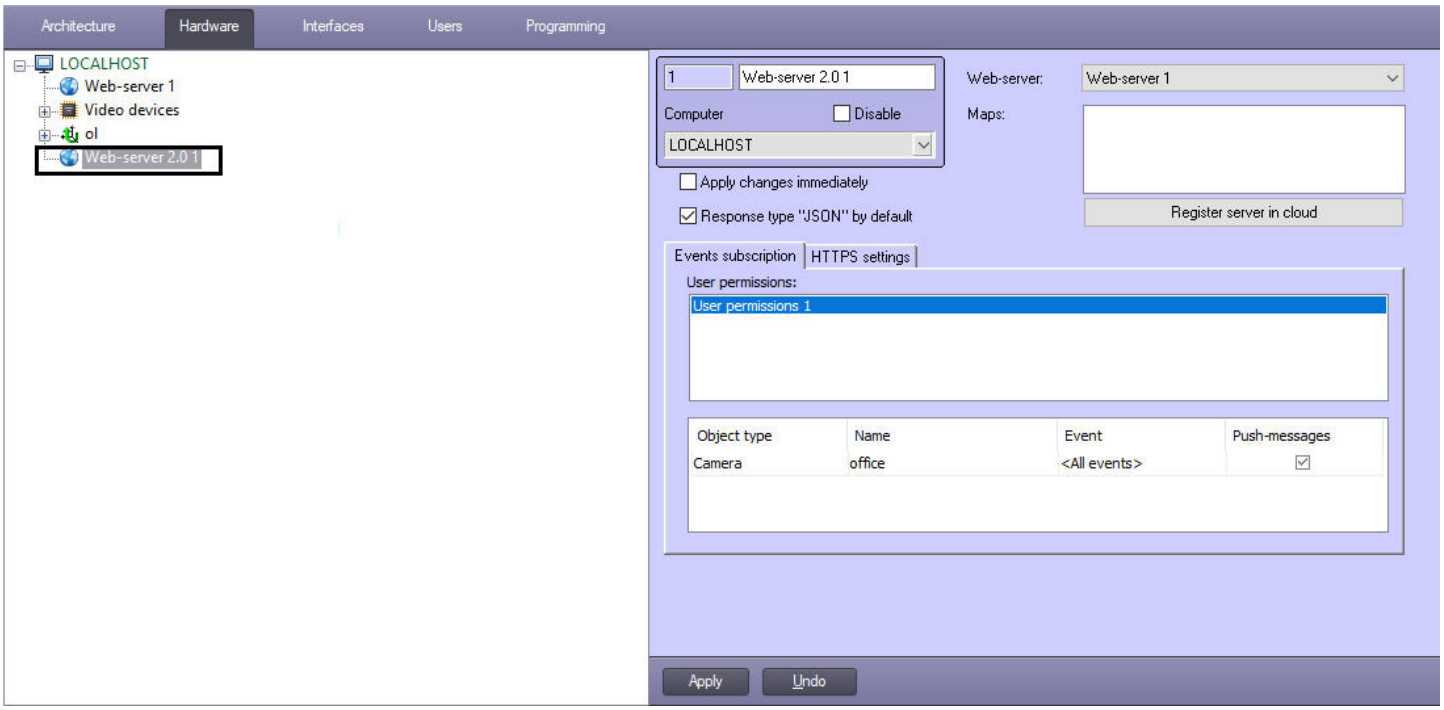
1. sends the video and audio coming from the camera to the mobile client;
2. sends the video and audio coming from the archive to the mobile client;
3. notifies the user about the alarms;
4. runs macros;
5. sends alarms to the mobile client and processes them;
6. controls PTZ cameras;
7. works with maps;
8. sends push notifications to the client.

Also, *Web-server 2.0* is required to use the Intellect HTTP API.

The **Web-server** object should be created and configured for the correct operation of the *Web-server 2.0* module (see Configuring the videoserver to connect Clients via the Web-server module).

23.3.15.7.1 Creating the Web server 2.0 object

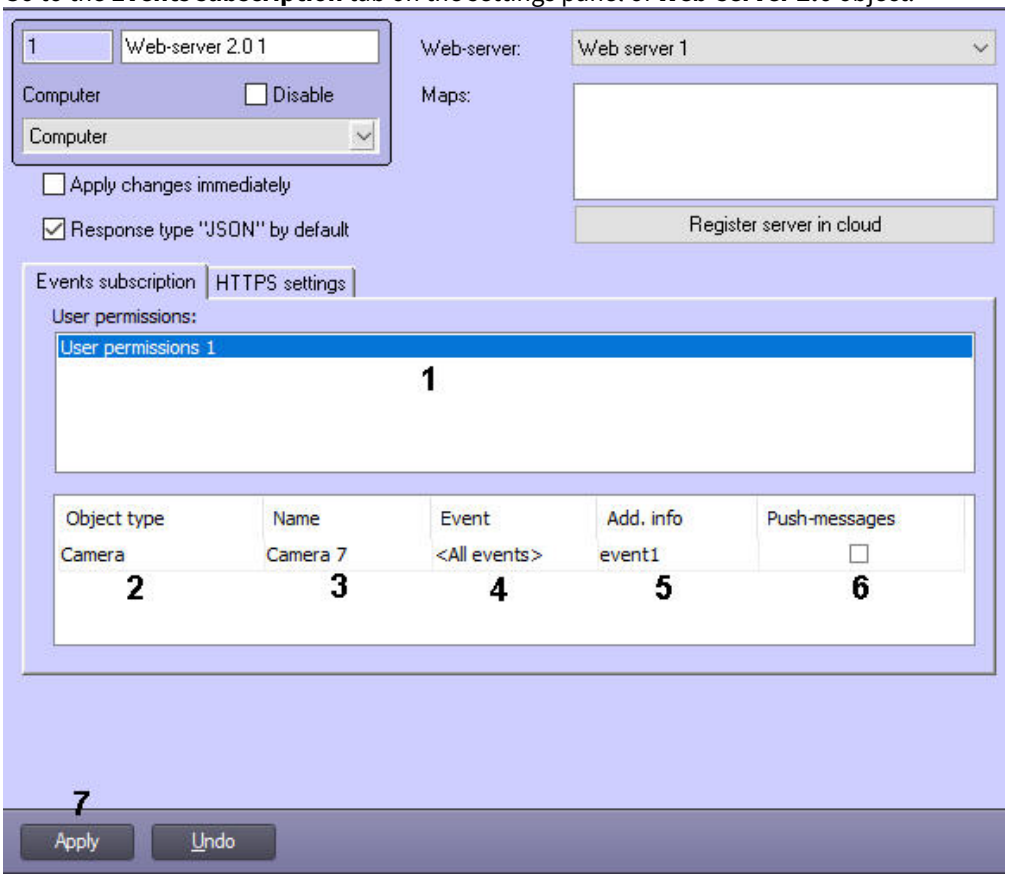
In the Intellect software the **Web server 2.0** object is based on the **Computer** object on the **Hardware** tab of the **System settings** dialog box.



23.3.15.7.2 Configuring the Events filter for the Web-server 2.0 module

To configure the filter of events which are to be received by *Web-server 2.0* module, do the following:

1. Go to the **Events subscription** tab on the settings panel of **Web-server 2.0** object.



2. In the **User permissions** list, select the **User permissions** object for which you want to configure the events filter (**1**). Events that match the filter will be sent only to clients on which users with the selected permissions are connected. Different filters can be configured for different user permissions.

> **Note**
>
> **User permissions** objects are created and configured on the **Users** tab of the **System settings** dialog box (see Rights administration).

> **Attention!**
>
> Only users added to the selected permissions will have access to the *Web-server 2.0*.

3. In the **Object type** drop-down list, select the type of object from which you want to send events (**2**).

> **Note**
>
> The **Object type** list contains only the object types that are included in the user's current permissions. If user permissions have not been selected, the list of object types is empty.

4. From the **Name** drop-down list, select the name of the object of the specified type from which the events are to be sent, if it is needed (**3**).
5. From the **Event** drop-down list, select the type of the event coming from objects of the specified type which is to be sent (**4**).
6. If necessary, in the **Add. info** field, enter additional information about the event to be sent, which will be reflected on the client (**5**).
7. If you want to authorize sending push notifications about events of the selected type to the mobile client, set the **Push-messages** checkbox (**6**). For push notifications to function, it is necessary for the mobile client to have connected to the Server at least once. This enables the Server to get user account information and the ID of the device to which push notifications are to be sent. The device must also have an active Internet connection.

> **Note**
>
> - If sending of push notifications is disabled and the client is not connected to the Server, then when a message of the selected type appears, it will not be sent.
> - Push notifications are not supported in *Intellect 4.11.1* and earlier versions.
> - For push notifications to work in *Intellect* 4.11.2 and later, the server should be registered in the AxxonNet cloud service (for details, see Registering a server in the cloud for Intellect push notifications).

8. Go to the next row of the table (arrow "down" on the keyboard) and repeat steps 3-6 for all required events.
9. Repeat steps 2-7 for all required user permissions.
10. Click the **Apply** button to save settings in *Intellect* (**7**).

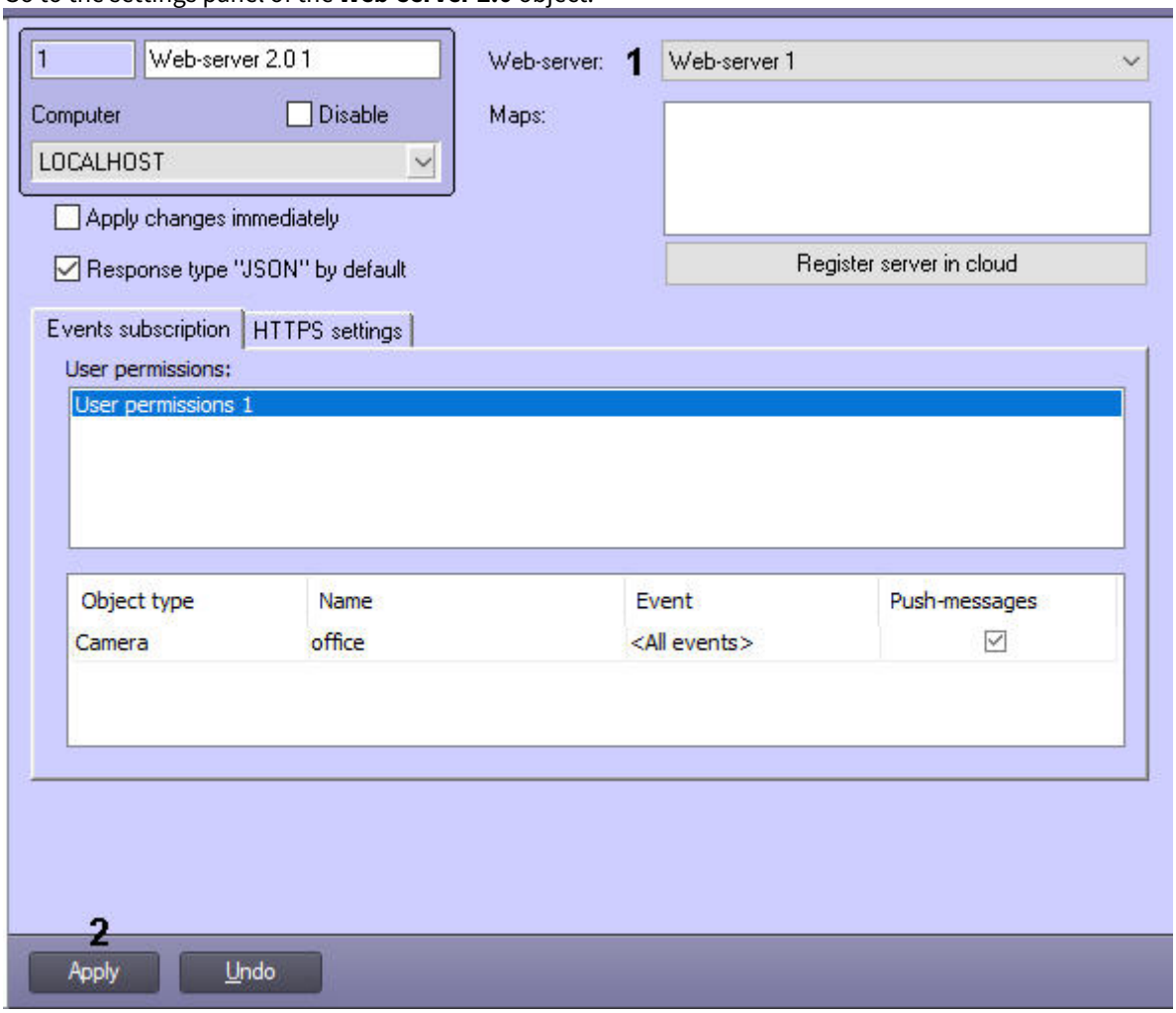
Configuration of the event filter for the *Web-server 2.0* module is completed.

23.3.15.7.3 Using the Web server settings for the Web-server 2.0 module

The **Web-server** object should be created and configured for the correct operation of the *Web-server 2.0* module (see Configuring the Web-server module). The **Web-server 2.0** object uses the settings of the bound with it **Web-server** object.

Binding the *Web-server 2.0* to the *Web-server* is performed in the following way:

1. Go to the settings panel of the **Web-server 2.0** object.



2. From the **Web-server** drop-down list, select the required **Web-server** object (**1**).
3. Click the **Apply** button (**2**).

Binding the *Web-server* to the **Web-server 2.0** object is completed.

23.3.15.7.4 Selecting maps

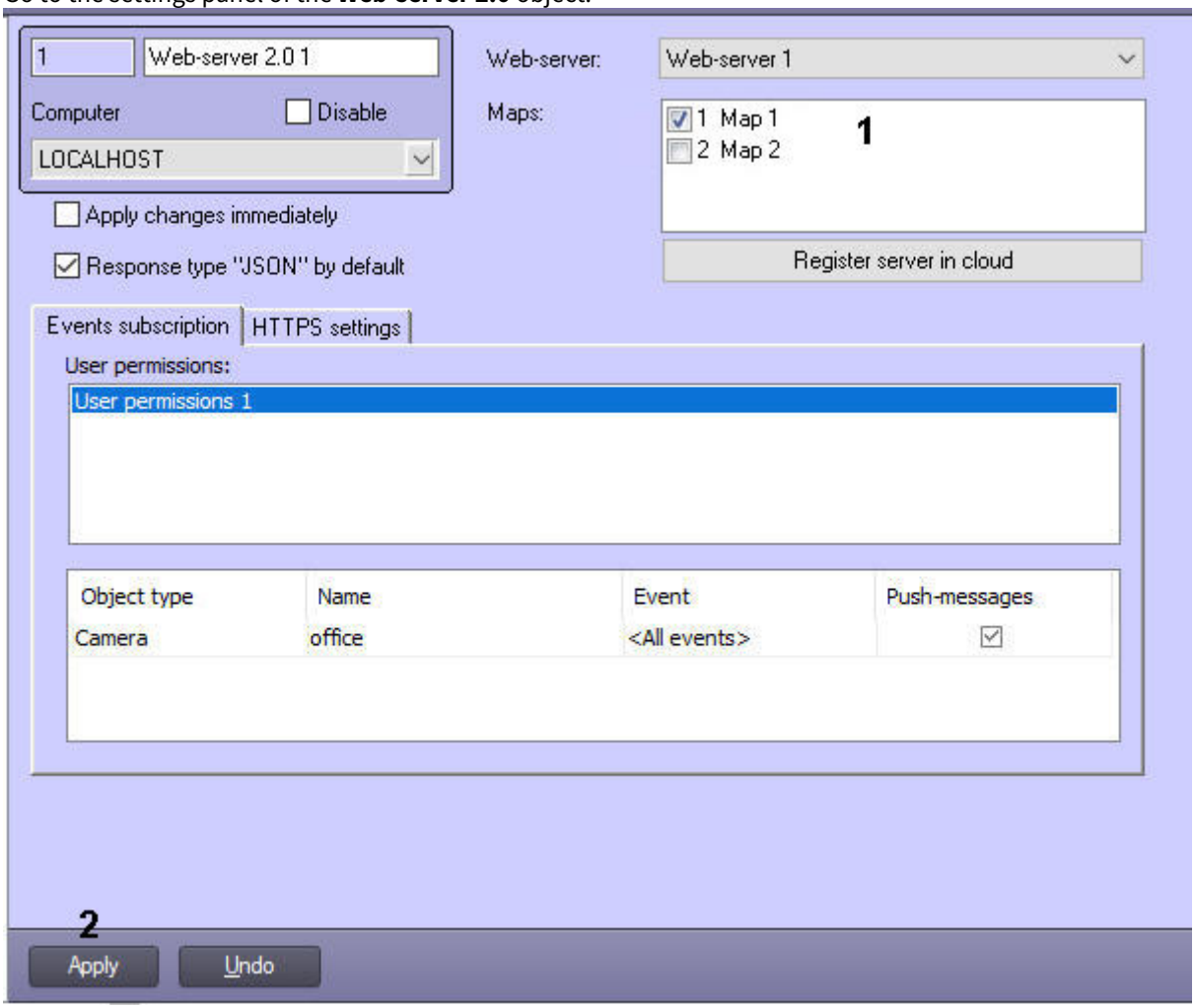
To ensure the correct operation of maps on a mobile client, it is necessary to select the maps used by the *Web-server 2.0* module. All required objects should be previously created in the hardware tree and added to the map. If an object is added to the map after the map is selected in the *Web-server 2.0* module, then it is necessary to restart *Intellect* or *Web-server 2.0* module in order to make such an object available in a mobile client.

Creation and configuration of maps is described in Configuring the interactive map for object state indication and controlling the objects.

> **Note**
>
> Maps attached to the layers of the selected maps are included in the response to configuration request via HTTP API – see Getting list of all server objects.

To select maps for *Web-server 2.0*, do the following:

1. Go to the settings panel of the **Web-server 2.0** object.



2. Set the checkboxes for the required **Map** objects (**1**).
3. Click the **Apply** button (**2**).

Maps are now selected.

23.3.15.7.5 Applying changes of the user rights

By default, when user rights are changed in *Intellect* (objects added or deleted), access rights are not changed in *Web-server 2.0* module until the **Apply** button is clicked on the settings panel of the **Web-server 2.0** object or *Intellect* is restarted, otherwise the mobile client operates as before.

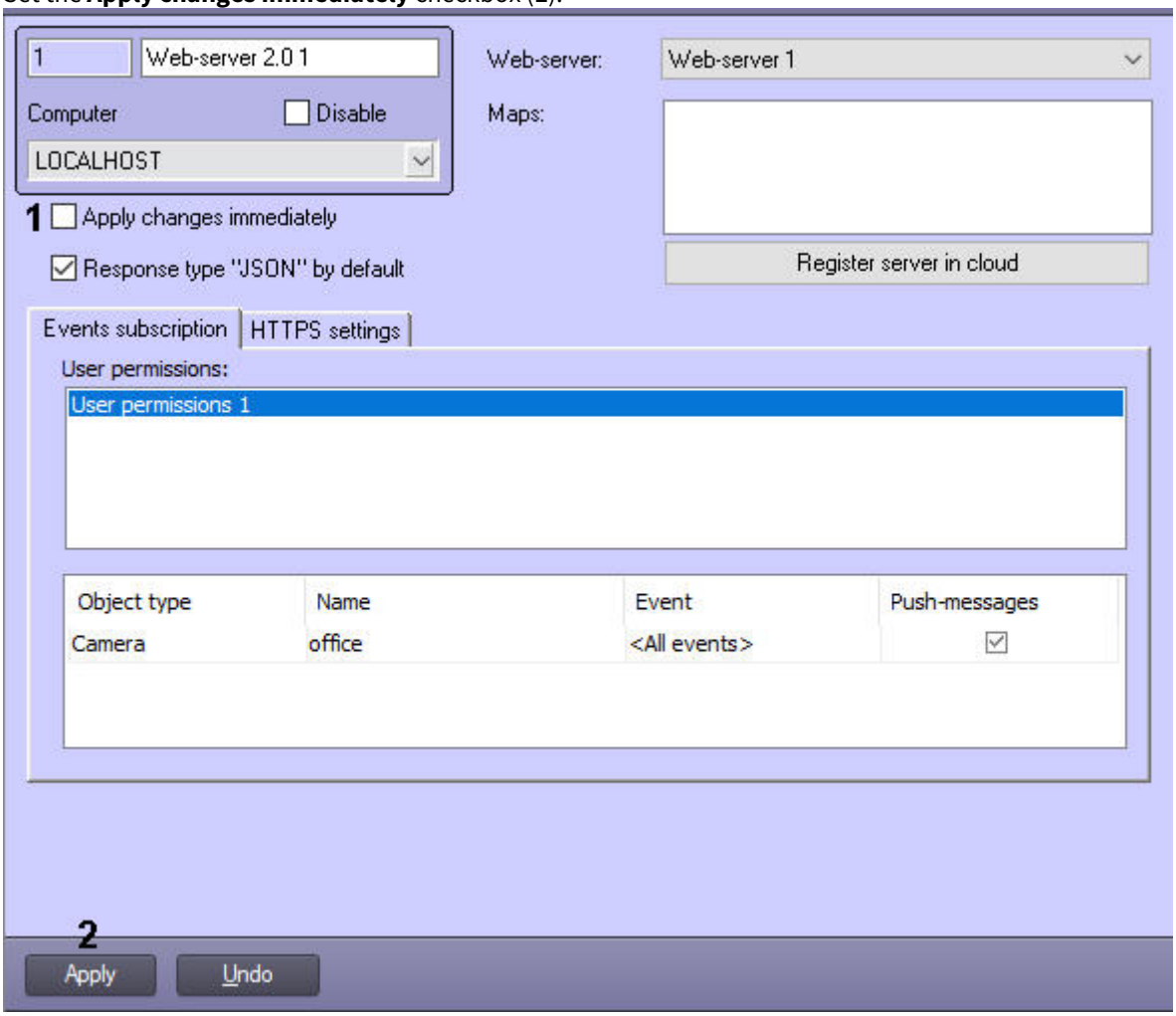
It is possible to enable the **Apply changes immediately** feature. *Web-server 2.0* module will immediately apply these changes of user rights.

> **Note**
>
> It is not recommended to use this feature in large distributed systems that use one Web-server 2.0 for the entire system. If there are several Servers in a distributed system and each Server has its own Web-server 2.0, the feature will work correctly on each Server separately.

Enable the **Apply changes immediately** feature as follows:

1. Go to the **Events subscription** tab on settings panel of the **Web-server 2.0** object.

2. Set the **Apply changes immediately** checkbox (**1**).



3. Click the **Apply** button (**2**).

The **Apply changes immediately** feature is now enabled.

23.3.15.7.6 Network settings of the Web Server 2.0 module

On the page:

- Changing the network interface used by the Web Server 2.0 module
- Changing the port used by the Web Server 2.0 module

Network settings of the Web Server 2.0 module are set via the **start_86.bat** or **start_64.bat** file (depending on whether the 32-bit or 64-bit version of the *Web Server 2.0* module runs). The files are in the <Intellect installation directory>\Modules\Jetty folder. Apart from the network settings the files provide run parameters such as allocated memory etc. Do not change those parameters.

23.3.15.7.6.1 Changing the network interface used by the Web Server 2.0 module

If the computer running *Web Server 2.0* has several network interfaces and the default interface is not the one required for the *Web Server 2.0* module, change the network interface in the following way:

1. Open the **start_86.bat** or **start_64.bat** file.
2. Add the **-Djetty.host=0.0.0.0** parameter, where 0.0.0.0 is the IP address of the desired network.
3. Save changes to the **start_86.bat** or **start_64.bat** file.

Changing the network interface for the Web Server 2.0 module is complete.

23.3.15.7.6.2 Changing the port used by the Web Server 2.0 module

Web Server 2.0 uses 8085 port by default. If this port is already taken, change the port as follows:

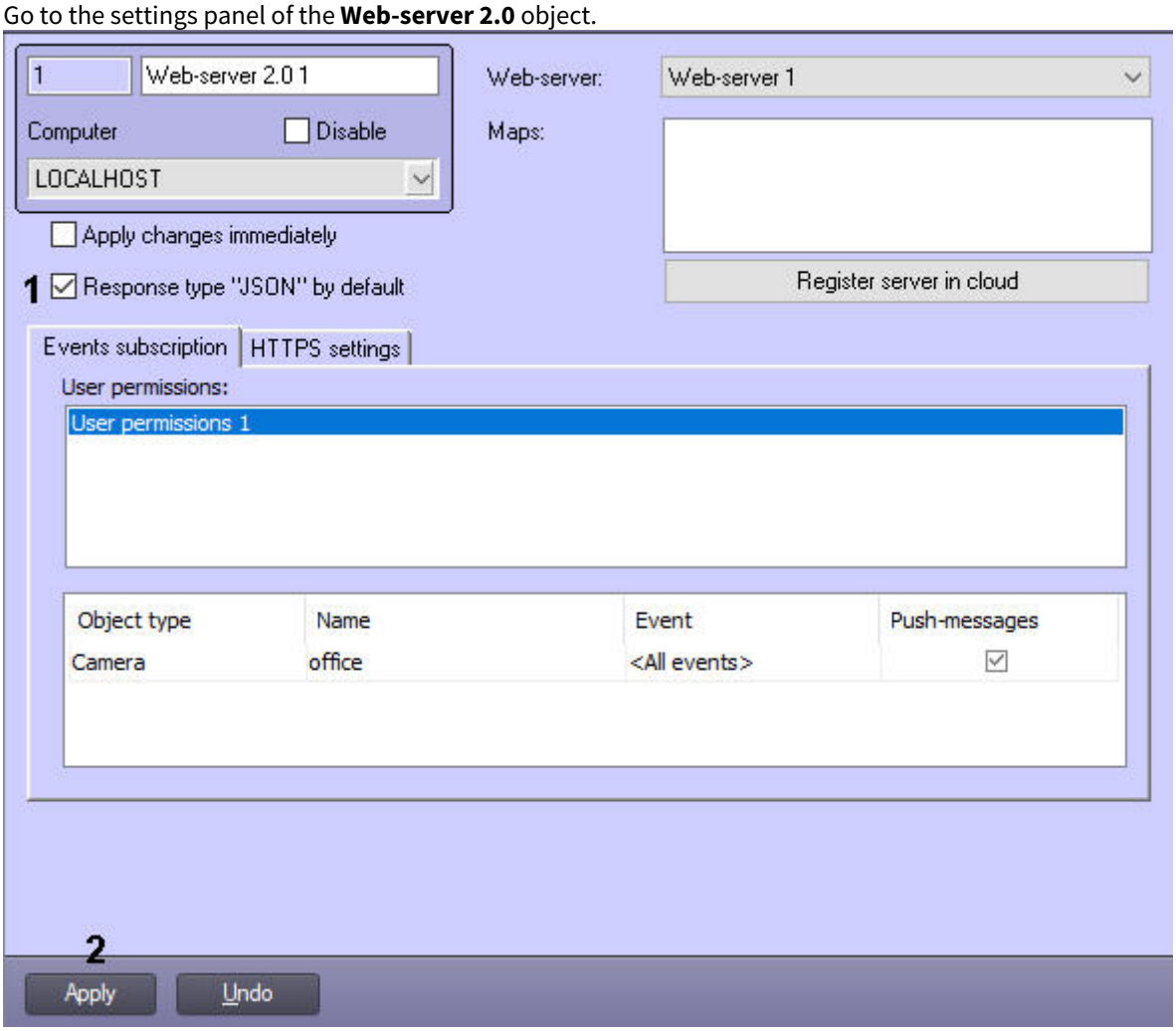
1. Open the **start_86.bat** or **start_64.bat** file.
2. Set the **jetty.port** value to the required port number.
3. Save changes to the **start_86.bat** or **start_64.bat** file.

Changing the port for the Web Server 2.0 module is complete.

23.3.15.7.7 Configuring default response type for HTTP API requests

By default, if the response type is not specified explicitly in the request, HTTP API responses are sent in JSON format (see Intellect HTTP API). To enable XML response by default, do the following:

1. Go to the settings panel of the **Web-server 2.0** object.



2. Clear the **Response type "JSON" by default** checkbox (**1**).
3. Click the **Apply** button (**2**).

> **Note**
>
> If response type is explicitly specified in the request, this setting is ignored.

Configuration of default response type for HTTP API requests is completed.

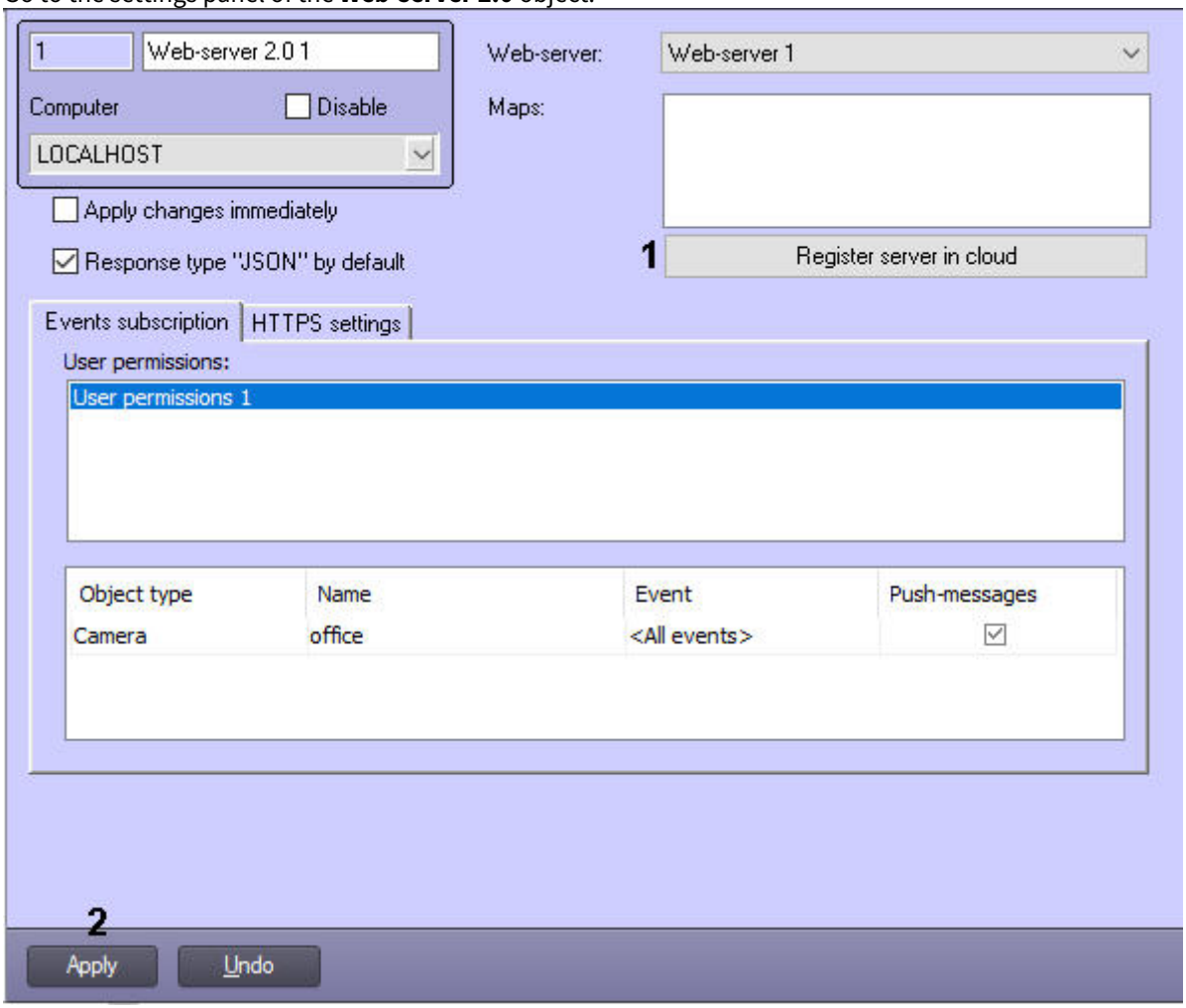
23.3.15.7.8 Registering a server in the cloud for Intellect push notifications

For push notifications to work in *Intellect* version 4.11.2 and later, the server should be registered in the AxxonNet cloud service (for details, see AxxonNet.com).

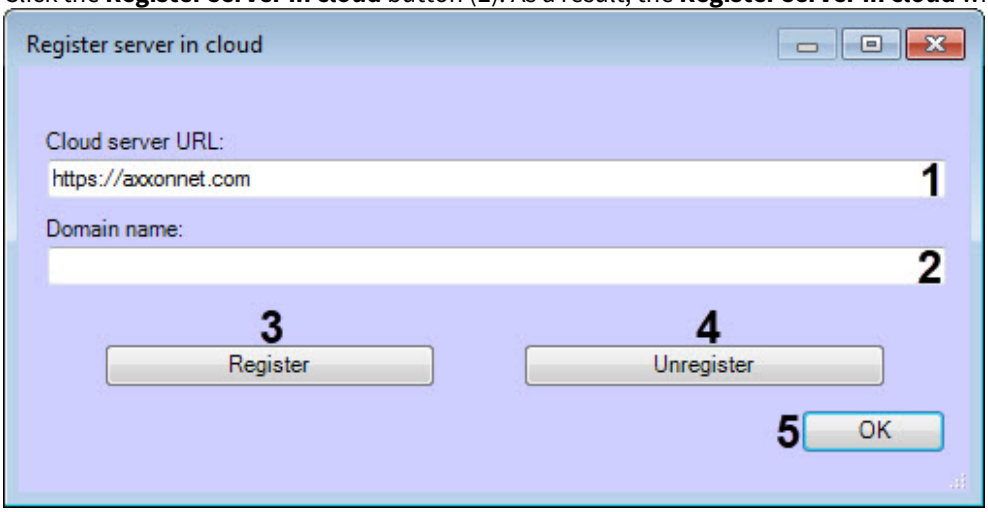
> **Note**
>
> Push notifications are not supported in *Intellect 4.11.1* and earlier versions.

To register or unregister the server, do the following:

1. Go to the settings panel of the **Web-server 2.0** object.



2. Click the **Register server in cloud** button (**1**). As a result, the **Register server in cloud** window will open.



3. In the **Cloud server URL** field (**1**), enter the URL of the AxxonNet cloud service. Default: https://axxonnet.com.
4. In the **Domain name** field (**2**), enter the server name that will be displayed in push notifications.
5. To register the server in the AxxonNet cloud service, click the **Register** button (**3**). To unregister the server in the AxxonNet cloud service, click the **Unregister** button (**4**).

> **Attention!**
>
> To complete the registration, the *Intellect* license key is required (see License key).
> If the **Web-server 2.0** object is deleted, the server will be unregistered automatically. If *Intellect* is uninstalled without unregistering the server (manually or automatically when deleting the **Web-server 2.0** object), it will become impossible to register the server again using the same *Intellect* license key.

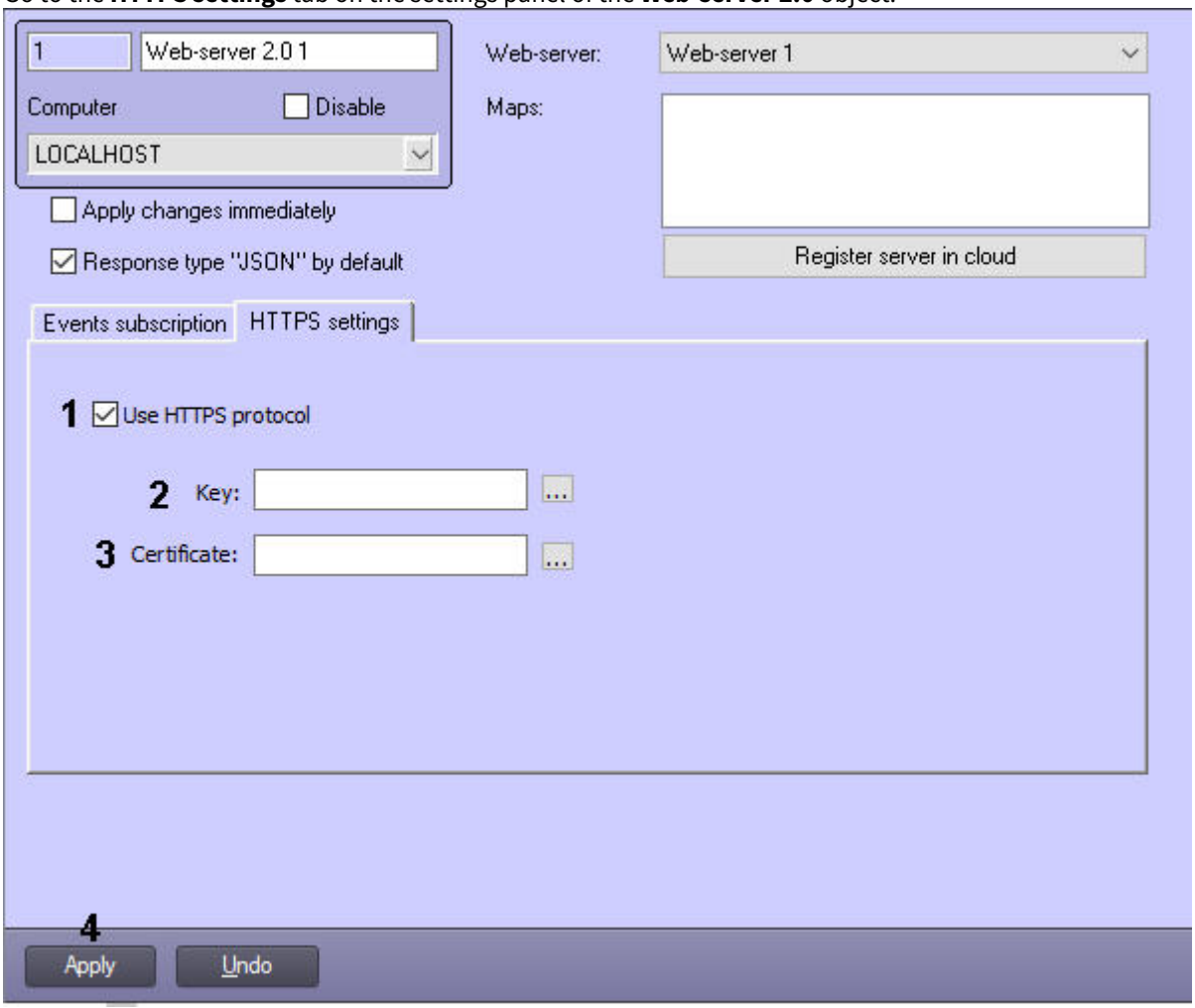
6. Click the **OK** button (**5**).
7. Click the **Apply** button (**2**) to apply the settings.

Server registration in the cloud for push notifications is complete.

23.3.15.7.9 HTTPS settings

By default, Web-server 2.0 uses the HTTP protocol. To transfer data using the HTTPS protocol, do the following:

1. Go to the **HTTPS settings** tab on the settings panel of the **Web-server 2.0** object.



2. Set the **Use HTTPS protocol** checkbox (**1**).
3. Specify the path to the key file in the **Key** field using the ... button (**2**).
4. Specify the path to the certificate file in the **Certificate** field using the ... button (**3**).
5. Click the **Apply** button (**4**).

Configuration of the data transfer using the HTTPS protocol is complete.

23.3.15.8 Web-server home page template and Java applet settings

The template for the Web-server home page is stored in the index.htm file located in the program folder of *Intellect* software, in the …\Modules\webroot subfolder. For example: C:\Program Files\Intellect\Modules\webroot.

The home page template holds the parameters of the page and of the Java applet displaying the surveillance windows.

By changing the Java applet parameters in the home page HTML-code, you can set the parameters of the video and control signal transmission through the gate (in case of using another HTTP-server), add or remove interface elements of the Web-server surveillance monitor, and enable showing the current frame size and frame rate for traffic estimation.

Each applet parameter description takes a separate line and consists of <param name=, followed by the quoted name of the parameter, and value=, followed by the quoted parameter value. The line ends with the > symbol.

The full line has the following format:

<param name=”Parameter name” value=”Parameter value”>.

Note.

If a parameter is not specified in the index.htm template, the default value is used.

Table 8.16—1 shows the available Java applet parameters.

Table 8.16—1

Parameter name	Possible values	Default value	Description
General data			
Version	-	-	HTML file version (must be the same as the client version)
Gate transmission parameters for video signals and controls			
port	number	80	Port number for the applet to receive the video feed and send the controls. The parameter is enabled if the “port.from” parameter has the value "html".
port.from	html|	url by default, this line is not included in index.htm	Specifies the source of the video feed port number for the applet to use: html – “port” parameter of the index.html file; url – URL by which the user accesses the index.html page.
path.from	html|	url by default, this line is not included in index.htm	Specifies the source of the path to the index.html page: html – URL, specified in index.html; url – URL by which the user accesses the index.html page.
path	string	- by default, this line is not included in index.htm	The path to index.html on the HTTP server, in case of a different HTTP server. The parameter is enabled if the “port.from” parameter has the value "html".
User interface display parameters			
layout.available	true|false	true	Enables (true) or disables (false) the windows layout panel on the surveillance monitor.
top.visible	true|false	true	Enables (true) or disables (false) the tools panel on the surveillance monitor.
layout.default	0|1|2|3	0	Specifies the default layout of surveillance windows when the Web-server home page opens. Possible values: 0 – one window 1 – four windows 2 – six windows 3 – nine windows
cam.default.id	number	1	The id of the camera whose window is displayed when the Web-server home page opens. This parameter is enabled, if the “layout.default” parameter has a value of 0.
messages	Text interface elements Visible text	see index.html file	The list of visible text elements of the interface: menu items, information strings in the surveillance window, etc. Only the visible text can be edited. IMPORTANT! The names of text elements are reserved. Editing them will result in their misinterpretation.

Parameter name	Possible values	Default value	Description
Parameters for displaying the data used in traffic estimation			
fs.fps	true|false	false by default, this line is not included in index.htm	Enables (true) or disables (false) the frame rate indication on the surveillance monitor.
fs.size	true|false	false by default, this line is not included in index.htm	Enables (true) or disables (false) the frame size indication on the surveillance monitor.

23.3.15.9 Setting up the surveillance monitor interface of the Web-server module

The interface of the surveillance monitor of the Web-server may be customized: removing the tools panel, choosing the default layout of the surveillance windows, changing the visible text on the menu item and service messages, etc.

Usually, the default interface settings provide quite a comfortable working environment. In case they need to be changed, do the following:

1. Using the text editor, for example Notebook, open the index.html file from the Intellect software program folder ... \Modules\webroot, for example, C:\Program Files\Intellect\Modules\webroot.
2. To remove the tool panel from the surveillance monitor, set the “top.visible” parameter to "false”: <param name="top.visible" value="false">.
3. To remove the layout selection panel from the surveillance monitor, set the “layout.available” parameter to "false”: <param name="layout.available" value="false">.
   To make the tools panel visible at the same time, set the "top.visible" parameter to "true": <param name="top.visible" value="true">.
4. By default, only one surveillance window is displayed when you open the Web-server home page. To open 4, 6, or 9 windows, set the “layout.default” parameter to 1, 2, or 3, respectively. For example, to display 9 windows: <param name="layout.default" value="3">.
5. By default, the surveillance window from camera 1 is displayed when you open the Web-server home page. To display the window from another camera, set the “cam.default.id” parameter to the number of the required camera. For example, to display the window from camera 9:
   <param name="cam.default.id" value="9">.
   To use this setting, the parameter “layout.default” must be set to 0 (default):
   <param name="layout.default" value="0">.
6. To change the visible text of the menu items in the surveillance windows or the texts of service messages, look in the “message” parameter for the text to be replaced and replace it with the required text.
   For example, to replace the message text “Cable detached from the camera…” with the text “No connection to the camera”, make the following changes to the “messages” parameter:
   replace
   <param name="messages" value="name=AxxonSoft WebServer client*detach=Cable detached from the camera… *disable=Camera is off…* ……..>
   with
   <param name="messages" value="name=AxxonSoft WebServer client*detach=No connection with the camera*disable=Camera is off…* ……..>
   When changing the texts in menu items and messages, do not use the following symbols: ‘ * ’, ‘ = ’, ‘ “ ‘.
7. Save changes to the index.htm file.

23.3.15.10 Setting up the display of the data for traffic estimation in the Web-server

Web-server operation uses network traffic. It’s important to estimate the traffic, because it must be paid for.

The volume of network traffic when using the Web-server depends on the following factors:

1. the number of cameras displayed on the surveillance monitor;

2. compression level of the video signal;
3. frame size of the video signal;
4. frame rate of the video signal.

The traffic volume can be monitored on the Web-server surveillance window. When set up, the current frame size and frame rate for each camera are shown in the surveillance windows. The traffic is approximately estimated by the following formula:

Traffic = {Viewing time} * {Number of cameras} * {Average frame size} * {Average frame rate}

By default, the traffic estimation data is not shown. To set up the Web-server module to display the traffic estimation data, do the following:

1. Using the text editor, for example Notebook, open the index.html file from the Intellect software program folder...Modules\webroot. For example, C:\Program Files\Intellect\Modules\webroot.
2. Add the following lines to the Java applet parameter list:
   <param name="fs.size" value="true">
   <param name="fs.fps" value="true">
3. Save changes to the index.htm file.

23.3.15.11 Setting up the Web-server module to act as a gate on a different HTTP-server

By default, the Web-server module is set up to work as an independent HTTP-server. If a different HTTP-server must be used to connect to the remote workstations, the Web-server should act as a gate only for that HTTP-server and additional parameters should be set up.

For example, to use the Web-server for video surveillance, the user must open the page http://www.*****.com:8080/video/index.htm (asterisks "*****" represent the domain name of the site where the cameras can be accessed). To set up the Web-server to act as a gate, do the following:

1. Using the text editor, for example Notebook, open the index.html file from the Intellect software program folder... \Modules\webroot. For example, C:\Program Files\Intellect\Modules\webroot.
2. By default, Java applet receives the video signal from http://www.*****.com address.
3. For Java applet to receive the signal from http://www.*****.com:222/reverse/proxy/, add the following lines to the index.htm file:
   <param name="port.from" value="html"> /add
   <param name="path.from" value="html">
   <param name="path" value="/reverse/proxy/">.
   Set the "port" parameter to 222:
   <param name="port" value="222">.
4. For Java applet to receive the signal from http://www.*****.com:222, add the following line to the index.htm file:
   <param name="port.from" value="html">.
   Set the "port" parameter to 222:
   <param name="port" value="222">.
5. For Java applet to receive the signal from http://www.*****.com/reverse/proxy/, add the following lines to the index.htm file:
   <param name="path.from" value="html">
   <param name="path" value="/reverse/proxy/">.
6. Save changes to the index.htm file.

23.3.15.12 Updating the push notifications certificate for Intellect 4.11.1 and earlier versions

Existence of special certificate from the Apple which is given to the AxxonSoft company and valid for a year is required for working of push-notifications functional in *Intellect* 4.11.1 and earlier versions. Replace certificate if it is expired.

> **Note**
>
> Starting with *Intellect* version 4.11.2, for push notifications to work, the server should be registered in the AxxonNet cloud service (for details, see Registering a server in the cloud for Intellect push notifications).

Updating of push-notifications certificate is performed as follows:

1. Download current web2.war file (the certificate in this archive is valid until July 25th 2020).
2. Copy this file to the \Modules\Jetty\webapps folder in the *Intellect* installation directory.

Updating of push-notifications certificate is completed.

23.3.16 Configuring RTSP Server module

On the page:

- General info
- Creating the RTSP Server object
- Configuring the Unicast mode
- Configuring the Multicast mode
- Additional settings
- Bulk settings for cameras
- Examples of addresses to receive video from RTSP Server

23.3.16.1 General info

The **RTSP Server** object is used for transmitting video from Server to remote workplaces using the RTSP protocol. Use of the RTSP protocol allows viewing video from IP cameras and video archive on remote clients by means of the *Intellect* software or using video players that support this protocol. Transmitting Video gate archive and Backup archive is also supported.

If there is sound with live video or the archive is recorded with sound, then video broadcast with sound through **RTSP Server** is supported—for this specify the ID of microphone from which the archive is recorded when requesting video (see the table with requests examples). For proper operation of this feature set the **VLC media player compatibility mode** checkbox checked in VLC Media Player (see item 14).

Attention!

Transmitted video stream is to be compressed using H.264, H.265, MPEG4 or MJPEG codecs.
When MJPEG codec is in use, video of height and/or width more than 2048 pixels is not supported.
The client is to reconnect to URL when the codec is changed.
To view the archive via **RTSP Server**, the archive should be recorded in the same codec. Otherwise, the archived video will not play.

It is to be taken into account that while configuring each **rtsp Server** loads only one CPU core. To increase the number of rtsp streams several **rtsp Server** objects are to be created and configured on several cameras. Each RTSP Server entity runs in a separate system process (StreamingServer.run).

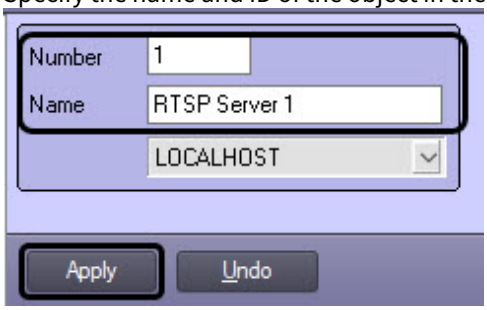
Note

All the ports mentioned below are specified using only natural numbers.

23.3.16.2 Creating the RTSP Server object

Create the **RTSP Server** object as follows:

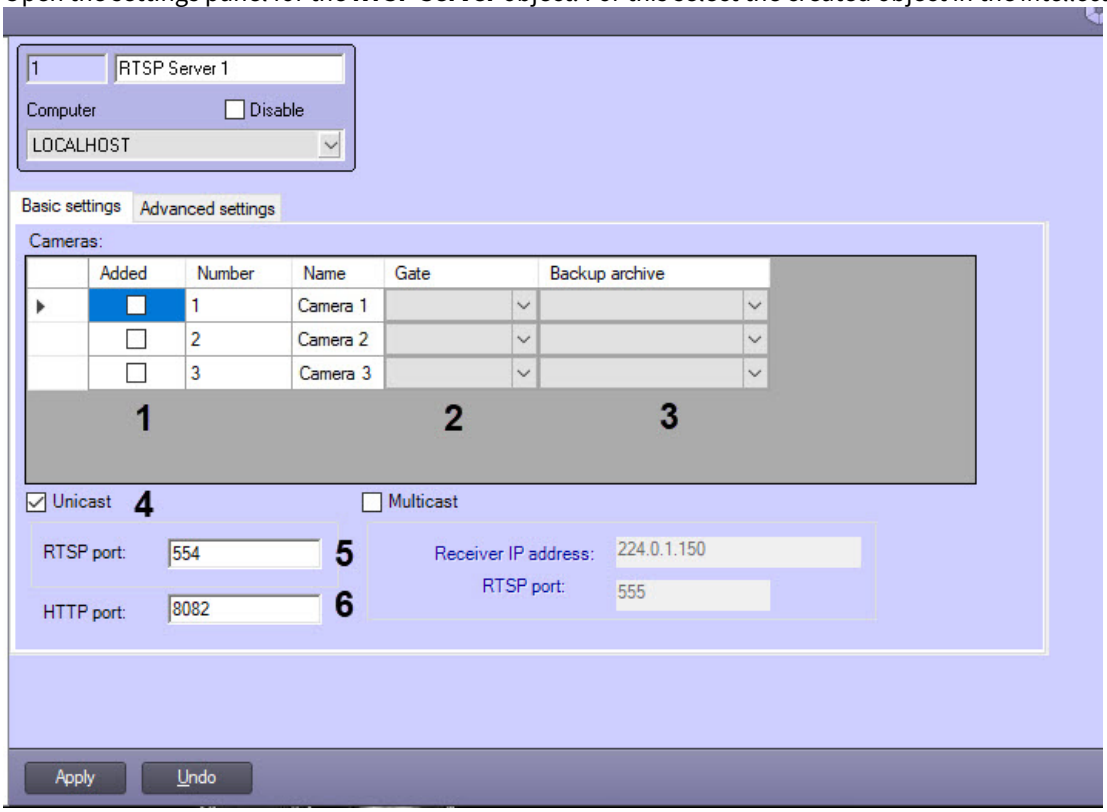
1. In the context menu of the **Computer** object select **Create object** → **RTSP Server**.
2. Specify the name and ID of the object in the opened panel.



3. Click the **Apply** button to create the object.

23.3.16.3 Configuring the Unicast mode

1. Open the settings panel for the **RTSP Server** object. For this select the created object in the *Intellect* objects tree.



2. In the **Cameras** table set the checkboxes next to video cameras video from which is to be displayed (1). If camera has several streams, the default stream is broadcasted.

> **Note.**
>
> If default stream is changed on the corresponding **Camera** object settings panel after applying RTSP Server settings, it is mandatory to click **Apply** on the **RTSP Server** object settings panel to apply changes to it as well. See also Configuration of multistream video.

3. If video from the camera is to be received through the video gate, then select the **Video gate** object in the **Gate** drop-down list (2).
4. If archive from the camera is to be received from the backup archive, then select the **Backup archive** object in the **Backup arch.** drop-down list (3).

5. Set the **Unicast** checkbox checked if signals from all cameras are to be broadcast through one port (4).
6. In the **RTSP port** field specify the port via which the video is transmitted (5).

> **Note.**
>
> The "Windows Media Player Network Sharing" service can use the default port 554. Change the port number or disable this service for broadcast.
> To disable the service go to the **Control panel** → **Administrative Tools** → **Services** and double-click the service name and click the **Stop** button in the opened window.

7. In the **HTTP port** field specify the port that is to be used for transmitting video via http-protocol (6).

23.3.16.4 Configuring the Multicast mode

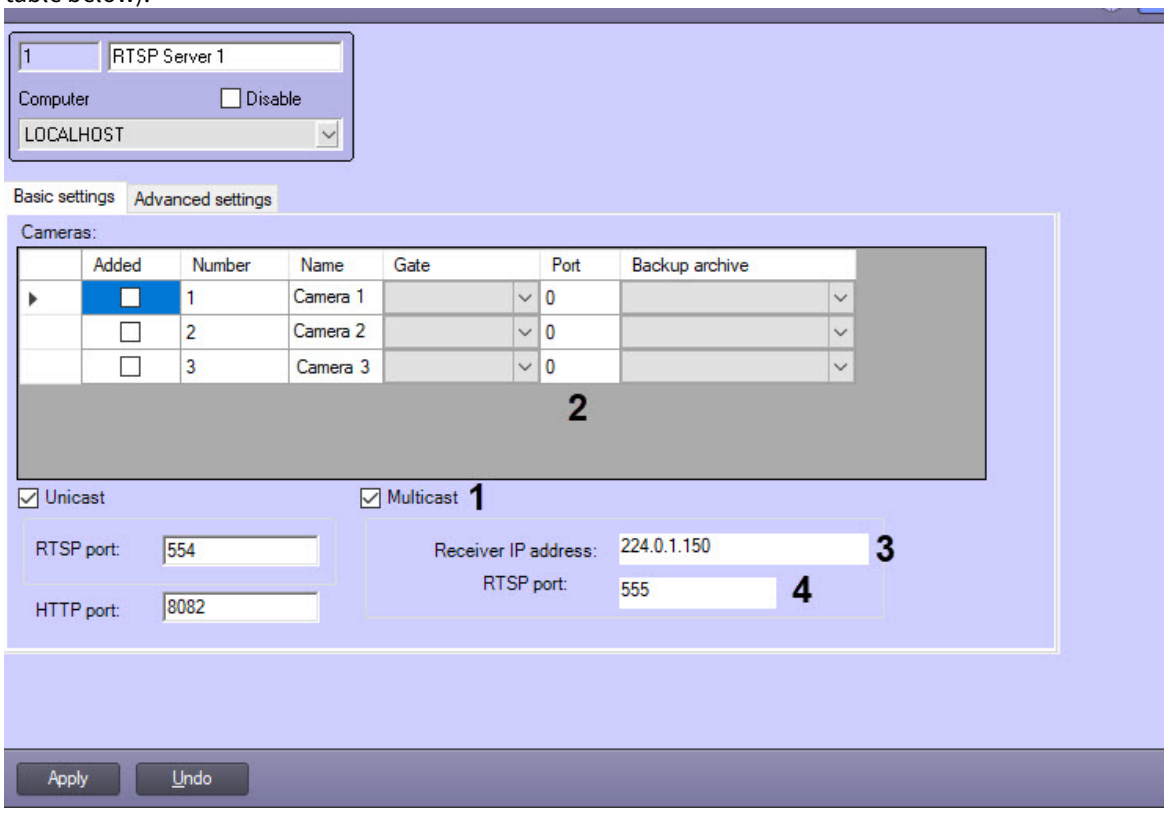
Features of the Multicast mode:

1. To get a multicast video in *Intellect* (see Configuring multimedia receipt using RTSP protocol) set the multicast value to the RTSP parameter in the HKEY_LOCAL_MACHINE \SOFTWARE\ITV\Intellect\Video\TransportProtocols registry section (for 64-bit system the path is HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\Intellect\Video\TransportProtocols) on computer where the **Camera** object is created. For detailed information on this parameter, see Changing the transport protocol used by IP-device.
2. **RTSP Server** can broadcast simultaneously in **Multicast** and **Unicast** modes. Receiving both such streams on the *Intellect* client is impossible due to RTSP key which determines the connection mode (see above). However, the VLC player allows receiving streams in both modes in the same time.
3. The ports that are assigned to each camera in this mode will not be displayed in the Windows OS Resource Monitor and other similar operating system resource monitors.

Using the Multicast mode allows you to reduce the load on the Server by reducing the amount of transmitted data. To distribute the transmitted signal among different RTSP ports, do the following:

1. Go to the **RTSP Server** object settings panel.
2. Set the **Multicast** checkbox (1). The **Port** column is displayed in the **Cameras** table.
3. Specify a data transmission port for each video camera in the **Port** field (2). Bear in mind the following when specifying ports:
    a. The following ports are in use for each camera in the **Multicast** mode: nPort, nPort + 18000 (rtp), nPort + 19000 (rtcp), where nPort—port number specified for camera in the **Port** column.
    For proper operation of RTSP server in the **Multicast** mode these ports are to be vacant.
    b. Specified ports are not addressed directly. Use RTSP port to get video from all cameras in the **Multicast** mode (see item 12).

c. In spite of specifying video data port it is required to specify camera number in the data source address (see the table below).



4. In the **Receiver IP address** field (3) specify the address from which the broadcast in **Multicast** mode will be performed. Address is to be in range from 224.0.1.0 to 239.255.255.255. By default, the receiver IP is 224.0.1.150. Bear in mind the following when specifying **Receiver IP address**:
   a. 224.0.0.0-224.0.0.255 address range is reserved for routing protocols and other service protocols. Destination IP address cannot be set from the specified range.
   b. RTSP-server can broadcast to one network simultaneously. The network with minimal metric is selected by default. To change the broadcast network, go to the **Advanced settings** tab (see below).
   c. Set different **Receiver IP address** and **RTSP port** if several **RTSP Servers** are in **Multicast** mode.
5. In the **RTSP port** field (4) specify the number of port through which video signal will be sent in the **Multicast** mode. When requesting video data from the camera using the RTSP protocol, it is necessary to specify this port. The system itself forwards the request to the port of the requested camera.

23.3.16.5 Additional settings

Perform the additional settings as follows:

1. Go to the **Advanced settings** tab.

2. If the current time is to be sent to VLC Media Player instead of the frame time, then set the **VLC player compatibility mode** checkbox checked (1). This option is to be used in case of problems when playing back the archive received over RTSP in VLC Media Player.
3. If there are captions on the video (see Configuring captions display on a video image), set the **Use captions track** checkbox checked to send them along with video via **RTSP Server** and to display them in the receiving app—VLC player (2).
   Also, when this checkbox is set, time captions are added to the video image in the format YYYYMMDDTHHMMSSZ. If the video is archive (see request examples below), then the captions show the archive time. However, if the **VLC player compatibility mode** is set along with the **Use captions track** check box, the time in the captions is current.

   > **Attention!**
   >
   > Correct video and captions operation are enabled only in VLC Media Player 2.0.0. These features are not guaranteed to work in other versions of VLC Media Player or other programs.

4. From the **Source IP interface** drop-down list, select the name of the network interface that should be used to broadcast the RTSP server (3).
5. If the **RTSP Server** is used for broadcasting the video data to the Single Data Center (ECHD), and the Video Surveillance Servers are behind NAT, then it is necessary to specify the NAT settings:
   a. In the **IP address** field, specify the IP address of the router that performs the NAT broadcasting (4).
   b. In the **Port** field, specify the port of the router, which is accessed by the client when executing the Single Data Center (ECHD) requests (5).

      > **Note**
      >
      > To enable the substitution of the router's specified IP address and port to the Single Data Center (ECHD) requests, it is necessary to set the corresponding checkbox in the settings panel of the Web server object —see Enabling the processing of ECHD requests and selecting rtsp server.

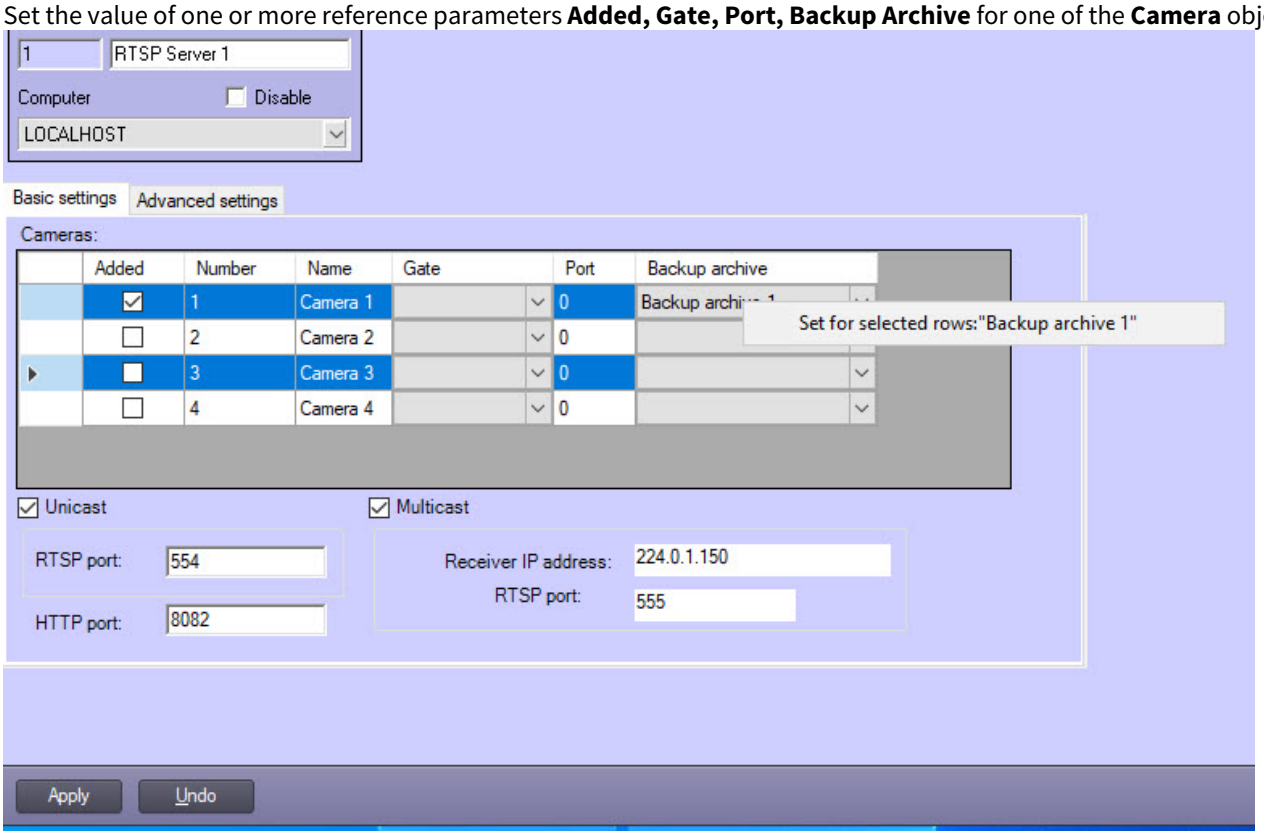
6. Click the **Apply** button to save the changes.

23.3.16.6 Bulk settings for cameras

In case any changeable setting should be the same for several cameras, there is a possibility of bulk setting. This feature is available for editable columns: **Added, Gate, Port, Backup Archive**.

Perform bulk setting of cameras as follows:

1. Go to the settings panel of the **RTSP-Server** object.
2. Set the value of one or more reference parameters **Added, Gate, Port, Backup Archive** for one of the **Camera** objects.



3. While holding down the Ctrl key, select the (full) rows in the table, which should have the same values in the corresponding columns.
4. Right-click in the reference cell.
5. In the opened function menu, select **Set for selected rows: "Value"**. As a result, the corresponding column in all selected rows are filled the value equal to the reference parameter.
6. Repeat steps 4-5 for all parameters that need to be applied to the selected lines.

23.3.16.7 Examples of addresses to receive video from RTSP Server

To connect to Server and display video in the video player that supports RTSP protocol, specify the address of data source in the format given in the table:

> **Note**
>
> The time parameters **time_begin** and **time_end** must be specified in UTC+0.

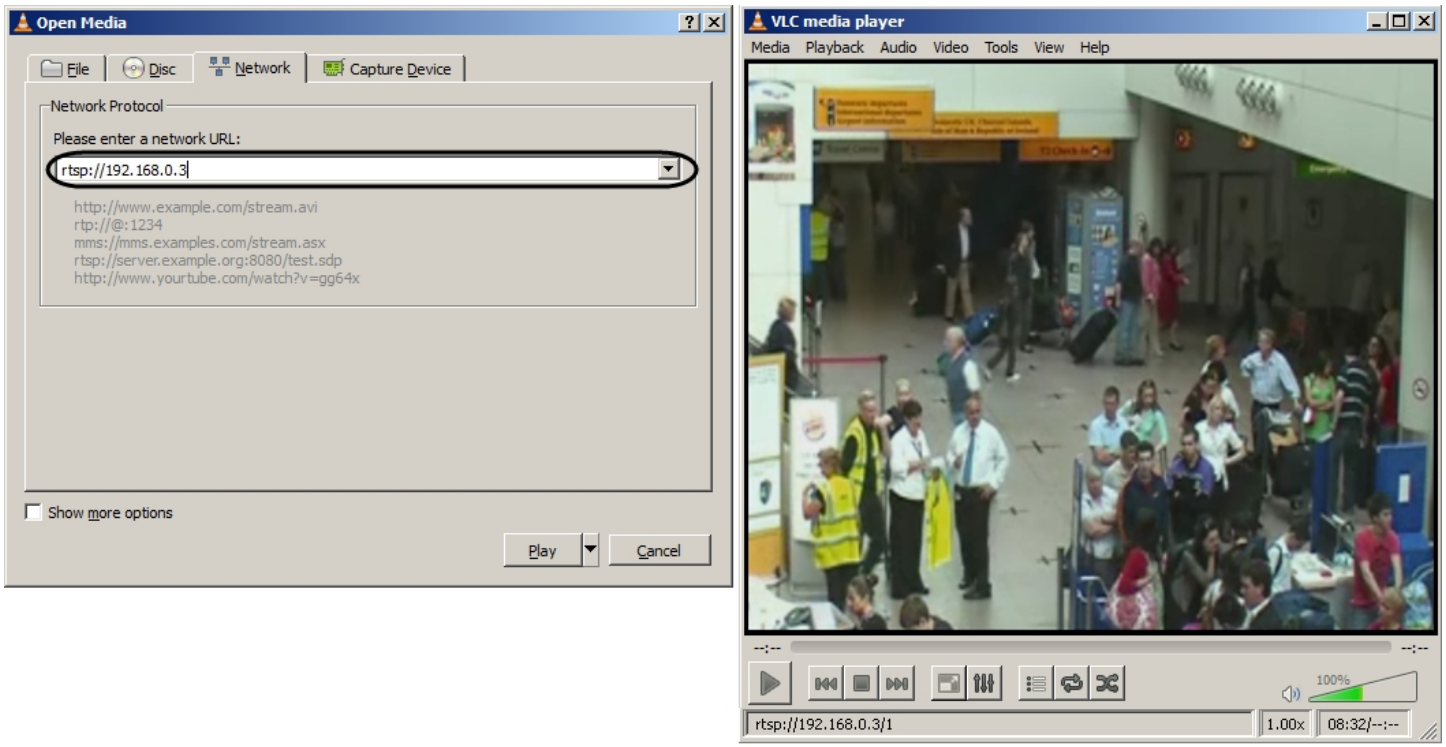
Address	Example
rtsp://Server IP address[:Port]**/**CameraNo[?stream_id=StreamNo]	rtsp://127.0.0.1/1
	rtsp://127.0.0.1:555/1

	rtsp://127.0.0.1:555/7
rtsp://Login:Password@Server IP address[:Port]/CameraNo	rtsp://login:pass@12
	rtsp://login:pass@12
rtsp://Server IP address[:Port]/CameraNo**?mic_id=**Microphone ID	rtsp://127.0.0.1:555/1
rtsp:// Server IP address[:Port]**/?mic_id=** Microphone ID	rtsp://127.0.0.1:555/?
rtsp:// Server IP address[:Port]**/archive?id=** CameraNo.**&time_begin=**yyyy.mm.dd-hh:mm:ss**&time_end=** yyyy.mm.dd-hh:mm:ss	rtsp://127.0.0.1:554/a
rtsp:// Server IP address[:Port]**/archive?id=**CameraNo**&mic_id**= Microphone ID **&time_begin=**yyyy.mm.dd-hh:mm:ss**&time_end=** yyyy.mm.dd-hh:mm:ss	rtsp://127.0.0.1:554/a id=1&mic_id=1&time
rtsp://Server IP address[:Port]**/archive?id=**CameraNo.**&time_begin=**yyyymmddThhmmssZ**&time_end=**yyyymmddThhmmssZ	rtsp://127.0.0.1:555/a
rtsp://Server IP address[:Port]**/archive?id=**CameraNo.**&time_begin=**yyyymmddThhmmssZ	rtsp://127.0.0.1:555/a
rtsp://Server IP address[:Port]**/archive?id=**CameraNo	rtsp://127.0.0.1:555/a
rtsp://Server IP address[:Port]/**archive**?**id**=CameraNo.**&long_term_archive**=BackupArchiveNo	rtsp://127.0.0.1:559/a
rtsp://Server IP address[:Port]**/archive?id=**CameraNo.**&gate**=VideogateNo	rtsp://127.0.0.1:559/a
rtsp://Server IP address[:Port]**/archive? id=**CameraNo.**&time_begin=**yyyymmddThhmmssZ**&time_end=**yyyymmddThhmmssZ**&z**=PlayBackSpeed	rtsp://127.0.0.1:554/a
rtsp://Server IP address[:Port]/archive? id=CameraNo.**&time_begin=**yyyymmddThhmmssZ**&time_end=**yyyymmddThhmmssZ**&long_term_archive=**BackupArchNo	rtsp://127.0.0.1:554/a id=2&time_begin=20

Note

If 554 port is in use (default value), it can be not specified in the address line.
In the examples given above specify the IP address of the computer where the **RTSP Server** object is instead of 127.0.0.1.

The figure shows how to view video from the Server.



23.3.17 Counting the system events

23.3.17.1 General Information on counting the system events

The **Events Counter** system object is designed for counting the specified types of events on the specified objects. Unlike other objects in the **Hardware** tab, this object is not a hardware component, and fulfils auxiliary functions in programming the Intellect system. It is most commonly used together with other system components, since it does not have a separate interface box for data input/output.

The counter notifies the system about the collected statistical data using the “Data Collected (SIGNAL_POINT)" message. Two notification modes are available: for a specified period of time and for a specified number of events. In the first case, the notification is issued upon expiration of a set time period after the start of counting. In the second case, the notification is issued when a certain amount of events has been counted.

An option for conditional count reset is available. Two reset modes are available: for a specified period of time and for a specified number of events. In the first case, the counter is reset upon expiration of a set time period after the start of counting. In the second case, the counter is reset when a certain amount of events has been counted. After resetting the statistic, the counter issues the “Counters have been reset (COUNTERS_FLUSHED)” message.

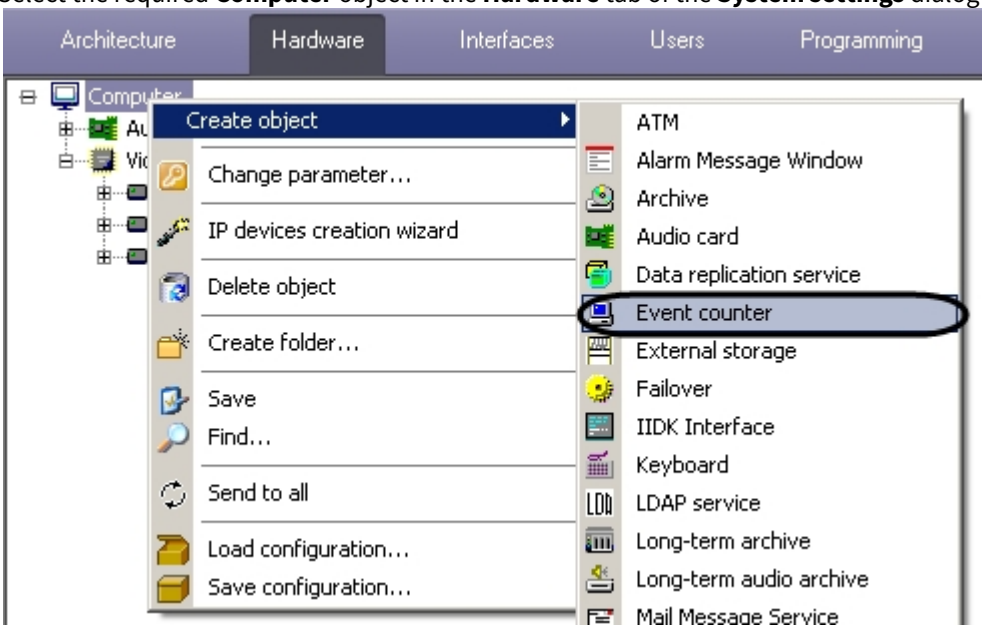
The start time for counting can be set manually, or automatically according to the last change of the **Events Counter** settings.

Besides, one **Events Counter** object allows setting a separate counter for each event.

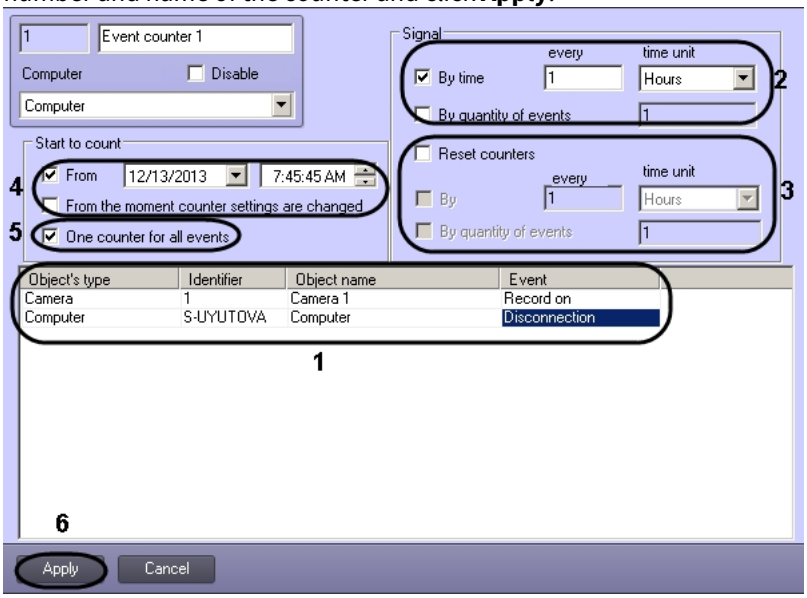
23.3.17.2 Configuring the Event counter

To configure the Event counter, do the following:

1. Select the required **Computer** object in the **Hardware** tab of the **System settings** dialog box.



2. Right-click the selected **Computer** object. In the drop-down menu, select **Create Object**, then **Event counter**. Enter the number and name of the counter and click **Apply**.



3. Select an object type in the **Object Type** column, and an ID in the **Identifier** column (**1**). Then, select an event in the **Event** column for the created object. Repeat these steps for all required objects and events.

> **Note**
>
> If no object is selected, then the Event counter will not count any events. If only the object type is specified, then the counter will count all events for objects of this type; if an identifier with no name is specified, then the counter will count all events of the selected identifier; if the object name with no event is specified, then then the counter will count all events of the selected object.

To add a row to the table, select the last row and press the ↓ button on the keyboard. To delete rows from the table, use the Ctrl + Del key combination.

4. Select the notification mode and set the notification parameters (2).
5. Enable the counter reset option, if necessary. Select the reset mode and set the reset parameters (3).
6. Select the time setting mode and enter the date and time, if necessary (4).
7. Uncheck the option for individual events counting, if necessary (5).

8. Click **Apply** to save the settings (6).

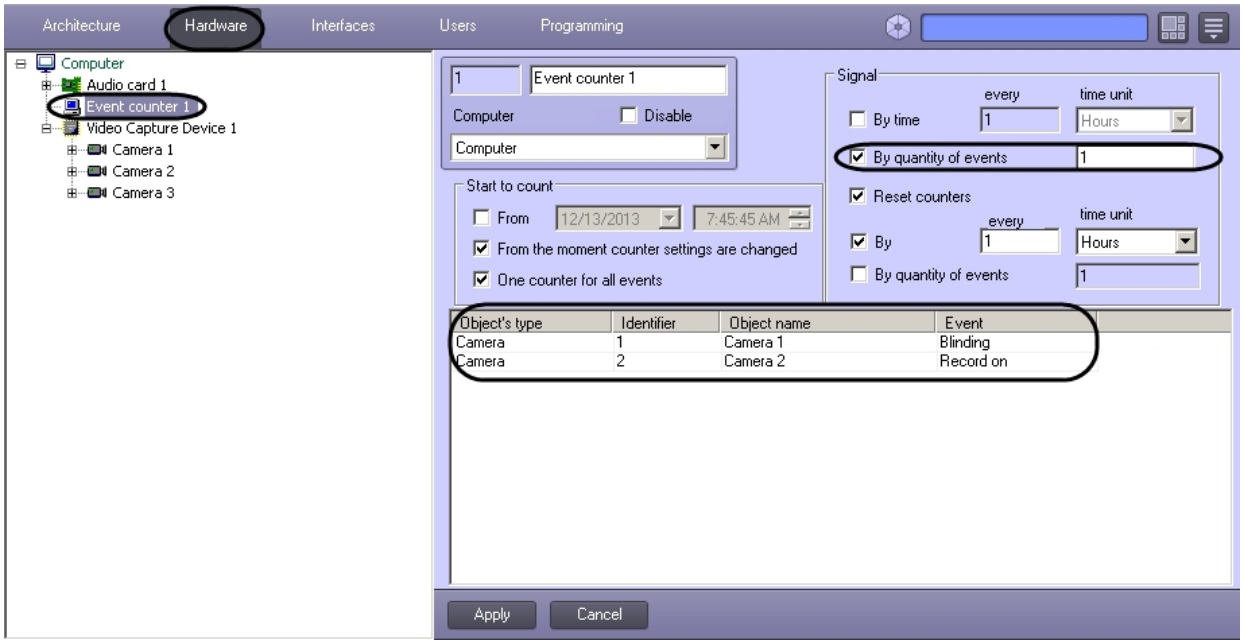
The **Event counter** is now configured.

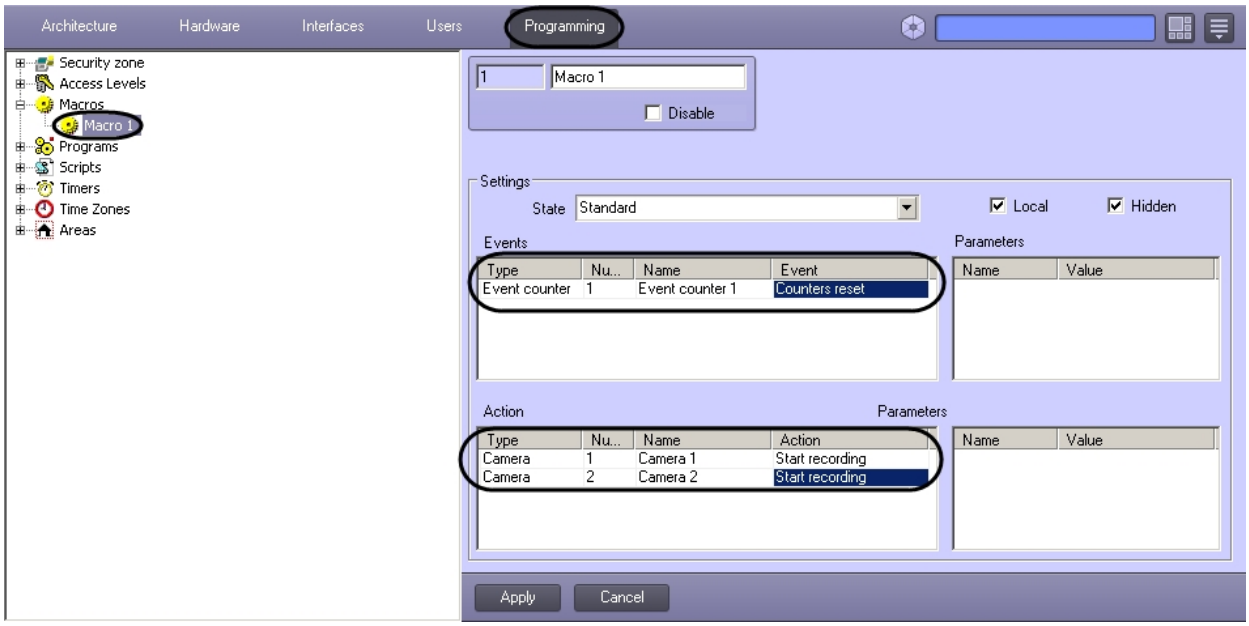
For a detailed description of the Event counter settings, see The Settings panel of the Event counter object.

23.3.17.3 Data output and counter control

The **Event Counter** system object has no separate interface object for data input/output, thus it is used together with other system components. Usually, the data of the **Event counter** object is used in macros to initiate actions with objects.

Figures below show an example of using the **Event counter** object in a macro.





In this example, the counter issues a notification (sends a SIGNAL_POINT (Data collected) message) in any of the following cases: camera №1 is blocked, camera №2 is blocked, camera №1 is broken, camera №2 is broken, unauthorized access attempt, the number of access attempts exceeded the limit. If the Access Abuse Control macro is active at the moment of the counter notification, video recording automatically starts on cameras №1 and №2.

Note.

The macros are described in detail in the Creating and using macros section.

23.3.18 Configuring PS-RTP Server

Attention!

The PS-RTP Server object was excluded from *Intellect* since the version 4.11.3.

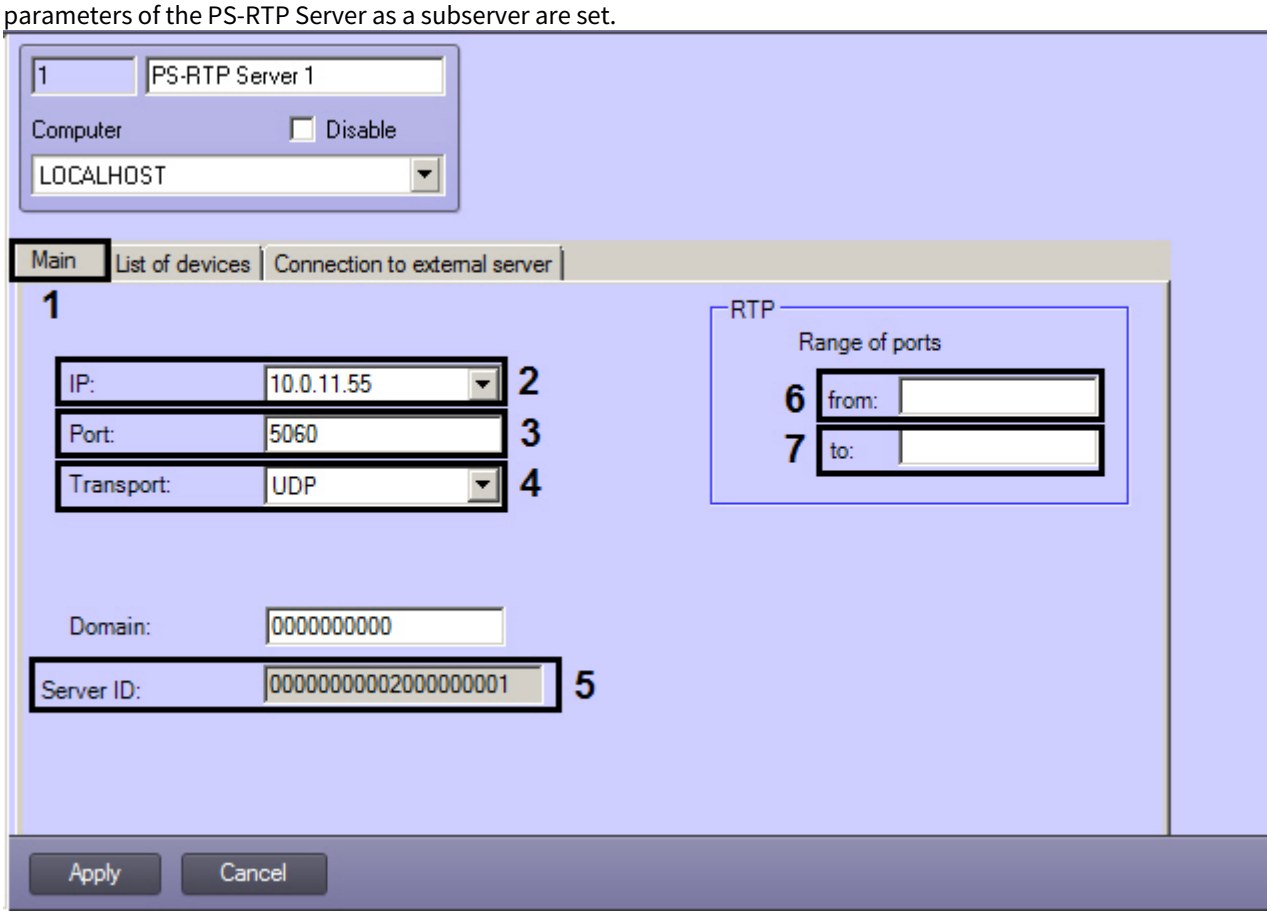
The PS-RTP Server enables the following functions in *Intellect*:

1. From the third-party software, control the cameras, PTZ, relays and sensors configured in *Intellect* using the GB28181 protocol.
2. Watch live and archived video in the third-party software.
3. Depending on the user rights, limit access to the functions listed above.

Intellect acts as a subserver in the server hierarchy. If *Intellect* should act as a supserver, configure Connecting cameras via the GB/T28181 protocol.

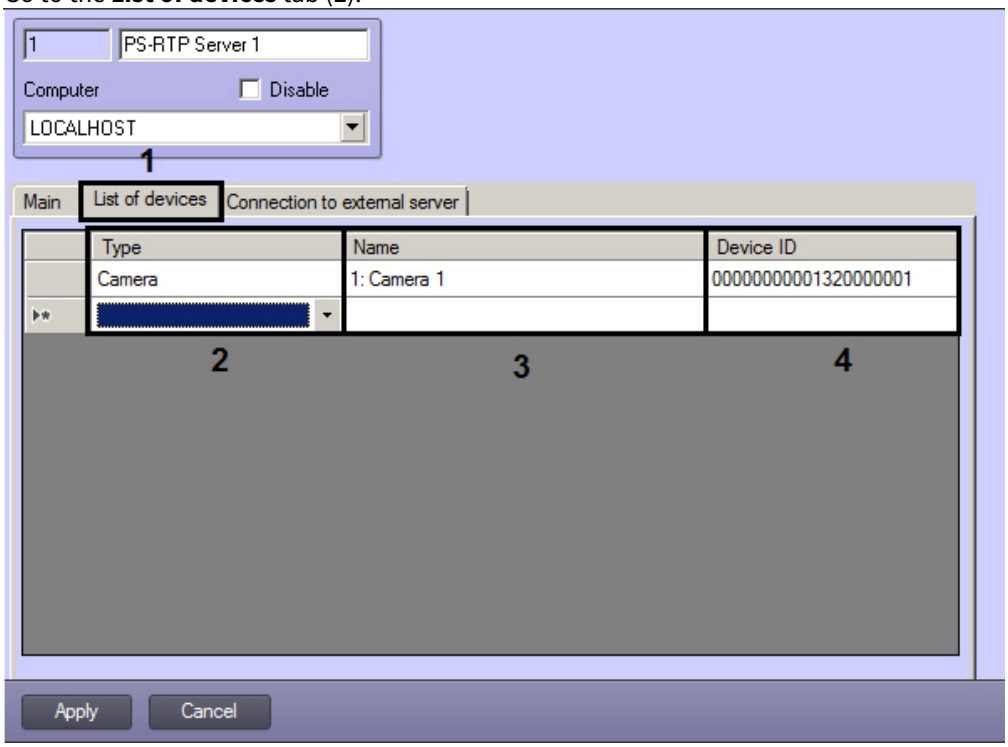
Configure the PS-RTP Server as follows:

1. Create the **PS-RTP Server** object on the basis of the **Computer** object in the **Hardware** tab of the **System settings** dialog box.
2. The settings panel of the object is displayed in the **Main** tab (**1**) on the right of the **System settings** dialog box. Here the parameters of the PS-RTP Server as a subserver are set.



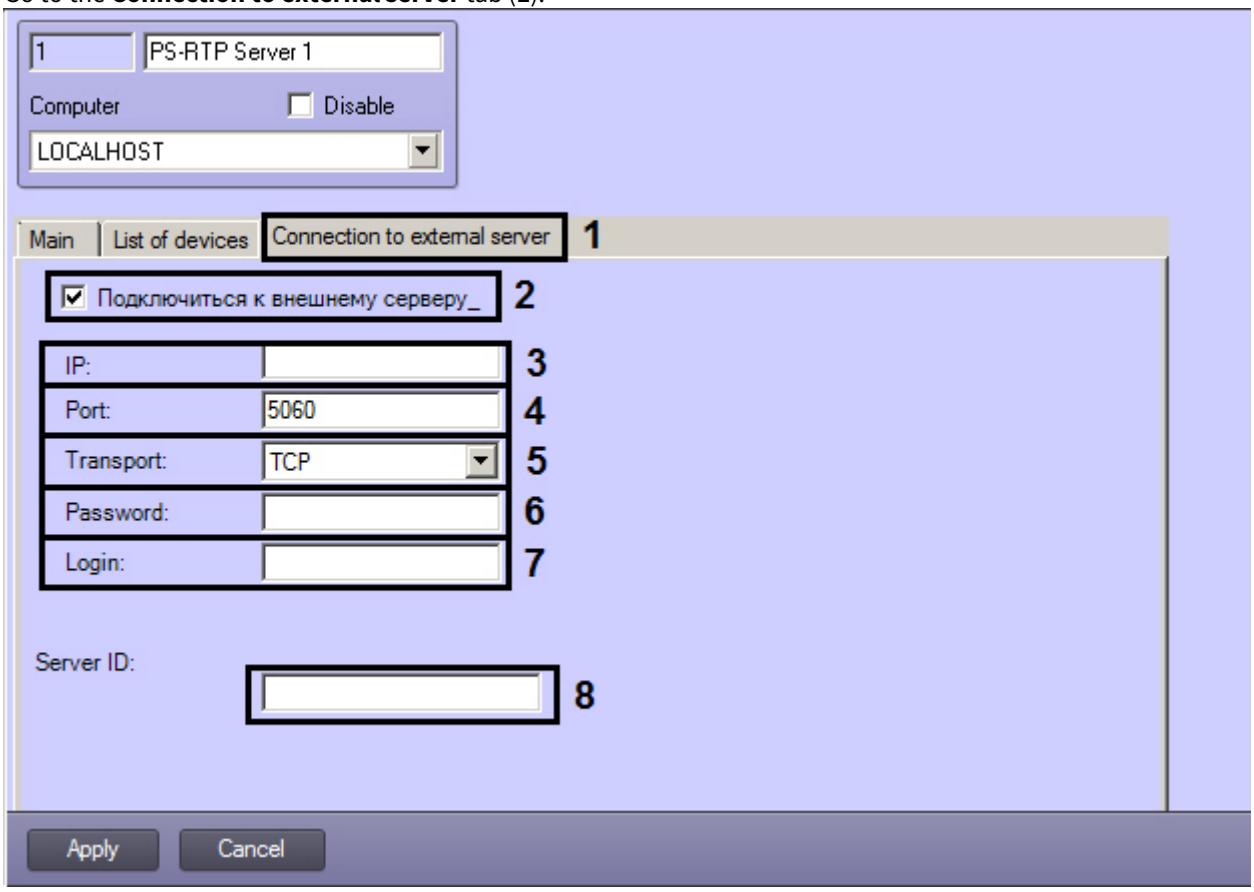
3. From the **IP** drop-down list (**2**) select the address of the network interface via which the third-party software will access the PS-RTP Server using the GB28181 protocol.
4. In the **Port** field (**3**) specify the number of the port to which the third-party software will be connected using the GB28181 protocol.
5. From the **Transport** drop-down list (**4**) select a data transfer protocol: UDP or TCP.

6. In the **Server ID** field (**5**) the ID of *Intellect* server is displayed. It is used by the third-party software to connect to the RS-RTP Server via the GB28181 protocol.
7. In the **from** (**6**) and **to** (**7**) fields set the range of the RTP ports used by the module.
8. Specify the list of objects the access to which should be guaranteed by the RS-RTP Server as follows:
   a. Go to the **List of devices** tab (**1**).



   b. From the **Type** drop-down list (**2**) select the type of object created in *Intellect* objects tree.
   c. From the **Name** drop-down list (**3**) select the name of the required object.
   d. In the **Device ID** field (**4**) the device ID is displayed. It will be used by the third-party software to control objects via the GB28181 protocol.
   e. Repeat steps b-d for all required devices.
9. Set the parameters to connect *Intellect* to the external supserver:

a. Go to the **Connection to external server** tab (**1**).



b. Set the **Connect to external server** checkbox (**2**). As a result, the external server connection parameters are available for editing.
c. In the **IP** field (**3**) specify the external server IP address.
d. In the **Port** field (**4**) specify the external server connection port.
e. In the **Transport** field (**5**) select the transport protocol used for the external server connection.
f. In the **Password** field (**6**) specify the password for external server connection.
g. In the **Login** field (**7**) specify the username for the external server connection.
h. In the **Server ID** field (**8**) specify the ID of the external server via the GB28181 protocol.
i. To save settings click the **Apply** button.

The RS-RTP Server is now configured.

23.3.19 Configuring ONVIF-Server module

23.3.19.1 General information about ONVIF-Server module

The *ONVIF Server* module enables stream transmission in order to get it via ONVIF protocol supporting audio playback, playback of onboard archive with audio, PTZ control, metadata transmission and support of sensors and relays.

The *ONVIF Server* module supports Digest authentication, event filtering according to ONVIF standard as well as Onvif ImagingService specification.

> **Attention!**
>
> The WS-addressing authentication is not supported in the *ONVIF Server* module. To connect the clients which use this authorization method, it is necessary to create a user with the root/root username and password, or log in without authorization.

MPEG, MJPEG and H264 codecs are supported when transmitting video via ONVIF 1.X and H264, H265, MJPEG and MPEG4 codecs when transmitting video via ONVIF 2.X.

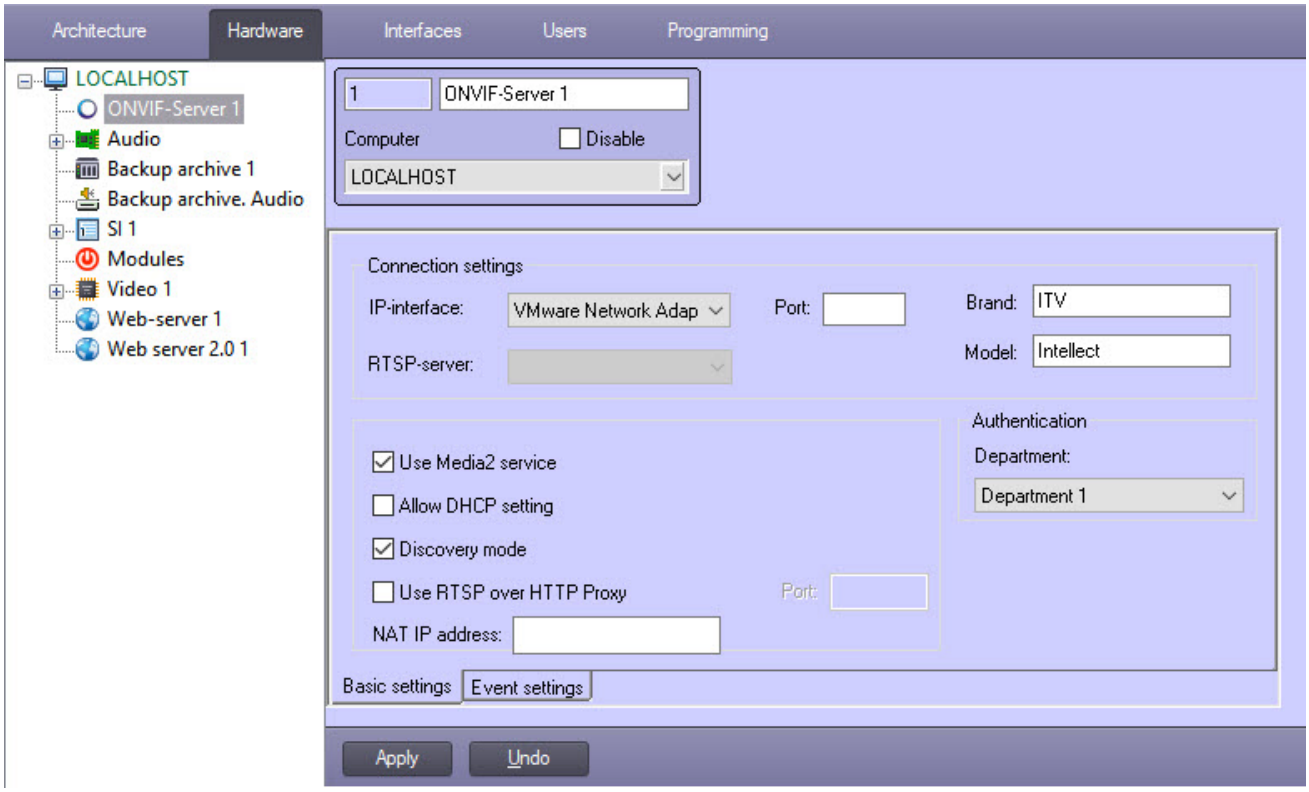
Video is also transmitted via *ONVIF Server* in the multistream mode.

Configure the correspondence between Intellect user rights and ONVIF rights in order to differentiate rights when Clients use *ONVIF Server* - see Configuring rights to use ONVIF Server.

23.3.19.2 Configuring ONVIF-Server object

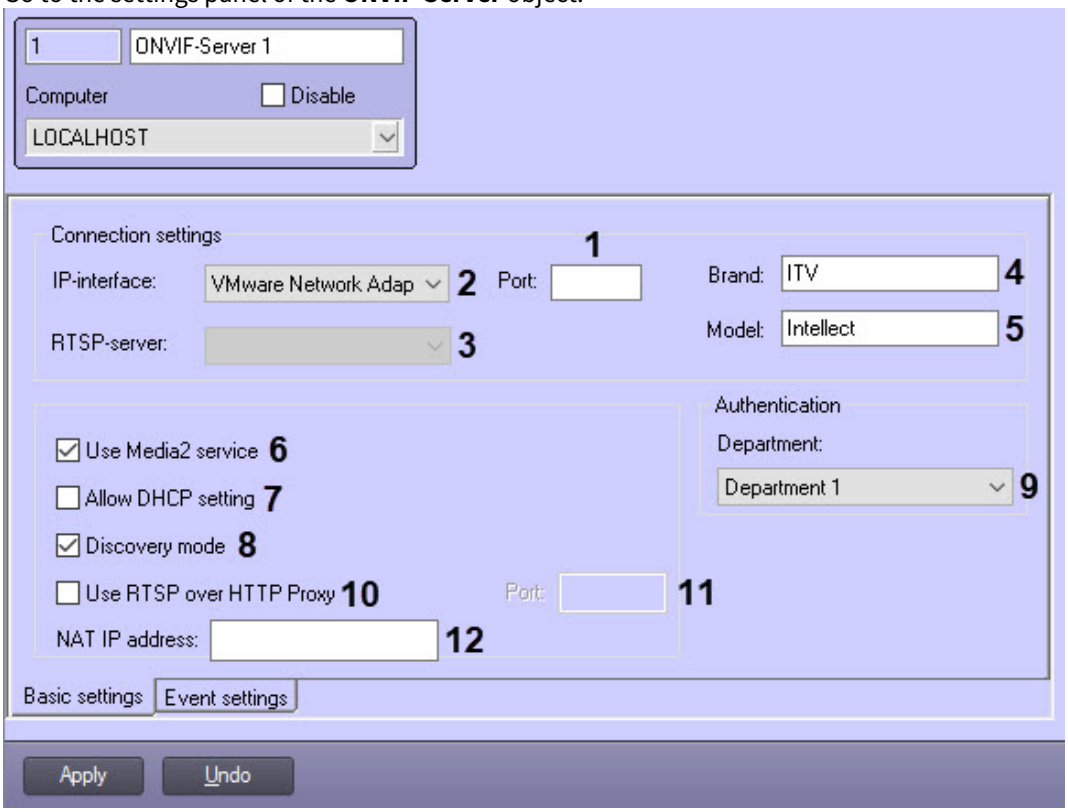
The **RTSP-Server** object is to be created and configured and all the required cameras are to be added to it before configuring the *ONVIF-Server* module—see Configuring RTSP Server module.

The **ONVIF-Server** object is created under the **Computer** object in the **Hardware** tab of the **System settings** dialog box.



Configure the **ONVIF-Server** object as follows:

1. Go to the settings panel of the **ONVIF-Server** object.



2. Specify the port number used to connect to the Server (**1**).
3. Select the network interface used to connect to the Server in the **IP-interface** drop-down list (**2**).
4. In the **RTSP-Server** drop-down list select the **RTSP-server** used along with this **ONVIF-Server** (**3**).
5. In the **Brand** (**4**) and **Model** (**5**) fields specify the names that will be displayed while searching in various clients that support getting the stream over ONVIF, e.g. ONVIF Device Manager.
6. By default, ONVIF 1.X is in use to transmit video in MPEG, MJPEG and H264 formats. If video in H265 or H264 format is to be transmitted, then set the **Use Media2 service** checkbox checked (**6**).
7. Set the **Allow DHCP setting** checkbox checked if DHCP protocol is in use (**7**).
8. By default, the WS-Discovery mode is enabled for ONVIF-Server. Set the **Discovery mode** checkbox unchecked in order to disable it (**8**).

> **Note**
>
> All the applications using port 3702 must be shut down on the computer where the ONVIF-Server is started for proper operation of the Discovery mode.
> Processes and ports occupied by them can be seen using the *Netstat -ano -p udp* command.

9. In the **Department** drop-down list select the department where the users will be created when they are added via the *ONVIF-Server* interface (**9**).

> **Note**
>
> Users are created in the *ONVIF-Server* interface using the third-party software, e.g., ONVIF Device Manager. The Administrator rights are required to create users—see Configuring rights to use ONVIF Server.

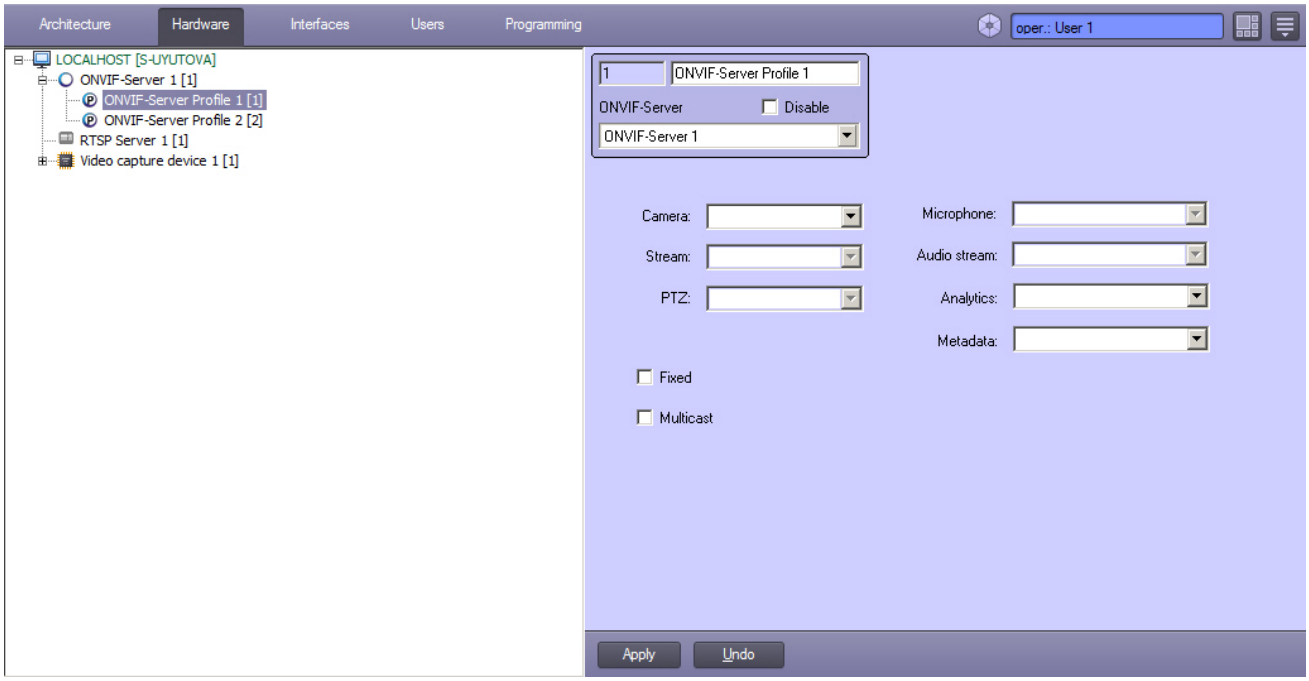
10. If it is required to redirect all RTSP-Server and ONVIF-Server requests to the specified port, set the **Use RTSP over HTTP Proxy** checkbox (**10**) and specify the port number in the **Port** field (**11**). This may be necessary for the ONVIF-Server operation behind NAT.
11. If it is necessary for the ONVIF-Server to use a specific IP address behind NAT in responses to Clients, enter this address in the **NAT IP address** field (**12**). This may be necessary, for example, if Clients connect not from the local network, but from the Internet via an external IP address.
12. Click the **Apply** button.

The **ONVIF-Server** object is now configured. Now it is possible to configure getting video using the *ONVIF-Server* module.

23.3.19.3 Configuring getting video using ONVIF-Server module

This page describes the setup using the example of receiving video from *Axxon One*.
Receiving video using the ONVIF-Server module is configured in *Axxon One*. Information on how to search and add IP devices to *Axxon One* is described in the Axxon One User Guide.

After adding a camera to *Axxon One*, in *Intellect* two **ONVIF-Server Profile** objects will be created under **ONVIF-Server** object for each camera added to the corresponding **RTSP Server.** These objects correspond to video streams of low and high quality in *Axxon One*.



Note

If multistreaming is disabled for the camera, then the parameters of both profiles corresponding to the camera are the same. See Configuration of multistream video.

If user rights are configured in *Intellect* (see Configuration of users and permissions), then the login and password are to be specified in order to connect to the camera. Otherwise there is no need to specify any login or password.

If required it is possible to select the video stream in the **Stream** drop-down list. Available video streams are configured on the settings panel of the **Camera** object—see Configuration of multistream video.

When changing camera parameters in *Axxon One* the corresponding changes will be applied in *Intellect* too. For instance, if the microphone, analytics, metadata transmission and sensor/relays are enabled in *Axxon One*, then the corresponding settings are applied for the **ONVIF-Server Profile** object in *Intellect*:

1. **PTZ**. **PTZ** object is to be created and configured in *Intellect* in order to control PTZ on camera connected via ONVIF-Server on the client. See PTZ configuration section in Installing and configuring security system components guide.
2. **Microphone**, **Audio stream**. **Audio card** and **Microphone** objects are to be created and configured in *Intellect* in order to receive and record audio from ONVIF Server on the client. See Configuring audio acquisition from IP devices section in Installing and configuring security system components guide.
3. **Analytics**, **Metadata**. **Tracker** and **VMDA detection** objects are to be created and configured under the corresponding **Camera** object in *Intellect* in order to receive and record metadata and analytics data from ONVIF Server on the client. See Configuring smart video detection tools. In *Axxon One* the **ONVIF events** detection is to be created for the added camera.

Important!

Changes of the configuration of the **RTSP Server** object corresponding to the **ONVIF Server** object in *Intellect* will be applied in *Axxon One* only after the *Axxon One* Server is restarted or when the camera is deleted and added to *Axxon One* again.

Besides, there are the following checkboxes on the settings panel of the **ONVIF-Server Profile** object:

1. **Fixed**—disables deleting the **profile** using the driver.
2. **Multicast**—enables video transmission in the multicast mode. There are some extra actions besides setting the checkbox checked:

1. Set the registry key:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\Intellect\Video\TransportProtocols
   rtsp = multicast
2. Enable the multicast mode on the settings panel of the **RTSP Server** object corresponding to the **ONVIF-Server** object—see Configuring RTSP Server module.

23.3.19.4 Features of embedded storage operation via ONVIF-Server

It should be noted that when you add an ONVIF-Server as a video camera to other *Intellect* or *Axxon One* Server, or to the third-party software, the embedded storage of the added ONVIF video camera will be associated with the *Intellect* archive and not directly with the video camera's embedded storage. See Configuring getting video using ONVIF-Server module.

If the *Intellect* archive is connected as a video camera's embedded storage on other *Intellect* or *Axxon One* Server, or the third-party software, the following features will be available:

1. Accelerated playback of the embedded storage's video archive.
2. Playback of the audio recorded synchronously with the video.

If the smart video detection tools are configured for the cameras which video is transmitted via the ONVIF-Server (see Configuring smart video detection tools), then if the are connected via the ONVIF-Server on other *Intellect* or *Axxon One* Server, or the third-party software, the smart video detection tools triggers will be transmitted as the events from the embedded video camera detectors. The procedure of setting up the embedded detectors in *Intellect* is described in the Embedded Detectors section. The instructions for setting up the embedded detectors in *Axxon One* and the third-party software can be found in the corresponding documentation.

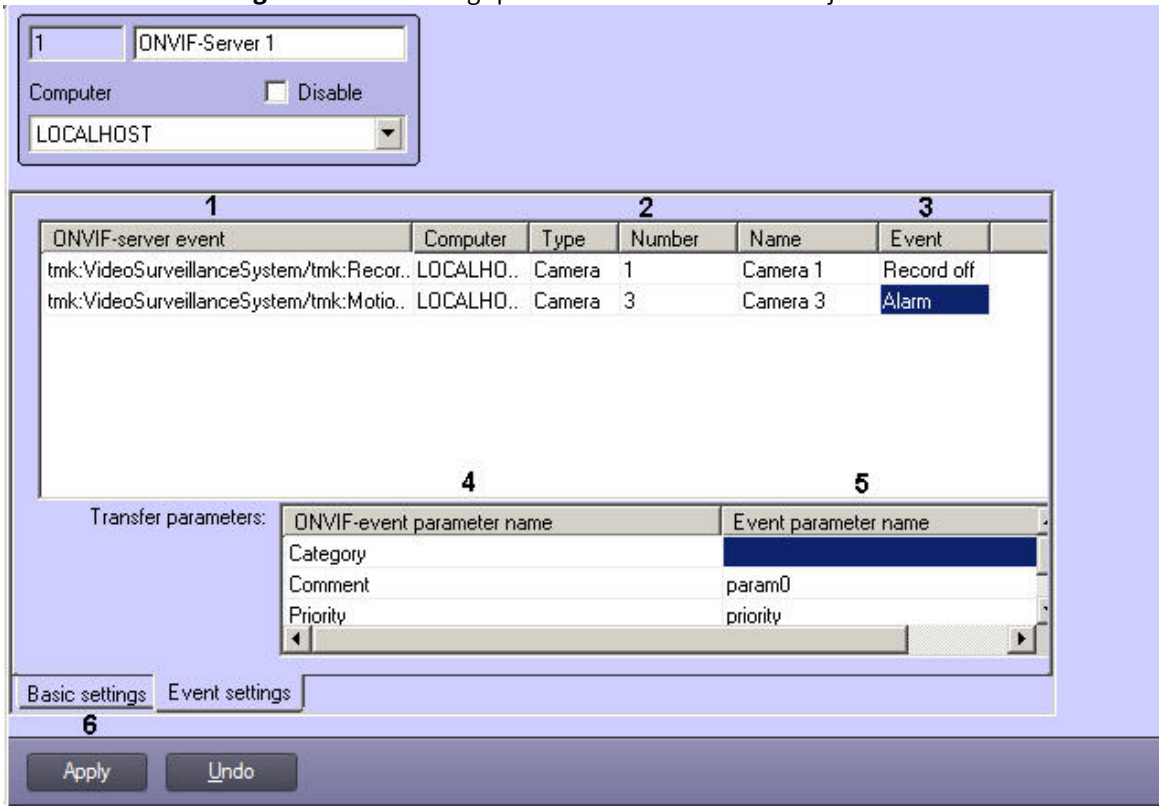
23.3.19.5 Filtering the ONVIF-Server events

The *ONVIF-Server* module supports filtering of messages and events transmitted in the metadata stream according to the ONVIF standard: Topic Filter and Message Content Filter.

You can configure the correspondence of messages for Topic Filter and the *Intellect* events. These are the *ONVIF-Server* events that start with tns and tmk in the examples below on this page. *Intellect* will transmit only those events for which the correspondence is configured. The remaining events and messages are sent automatically according to the specification (for example, when changing the server, profile or MotionAlarm settings, etc.).

The correspondence of messages for Topic Filter and the *Intellect* events is configured in the following order:

1. Go to the **Event settings** tab on the settings panel of the **ONVIF-Server** object.



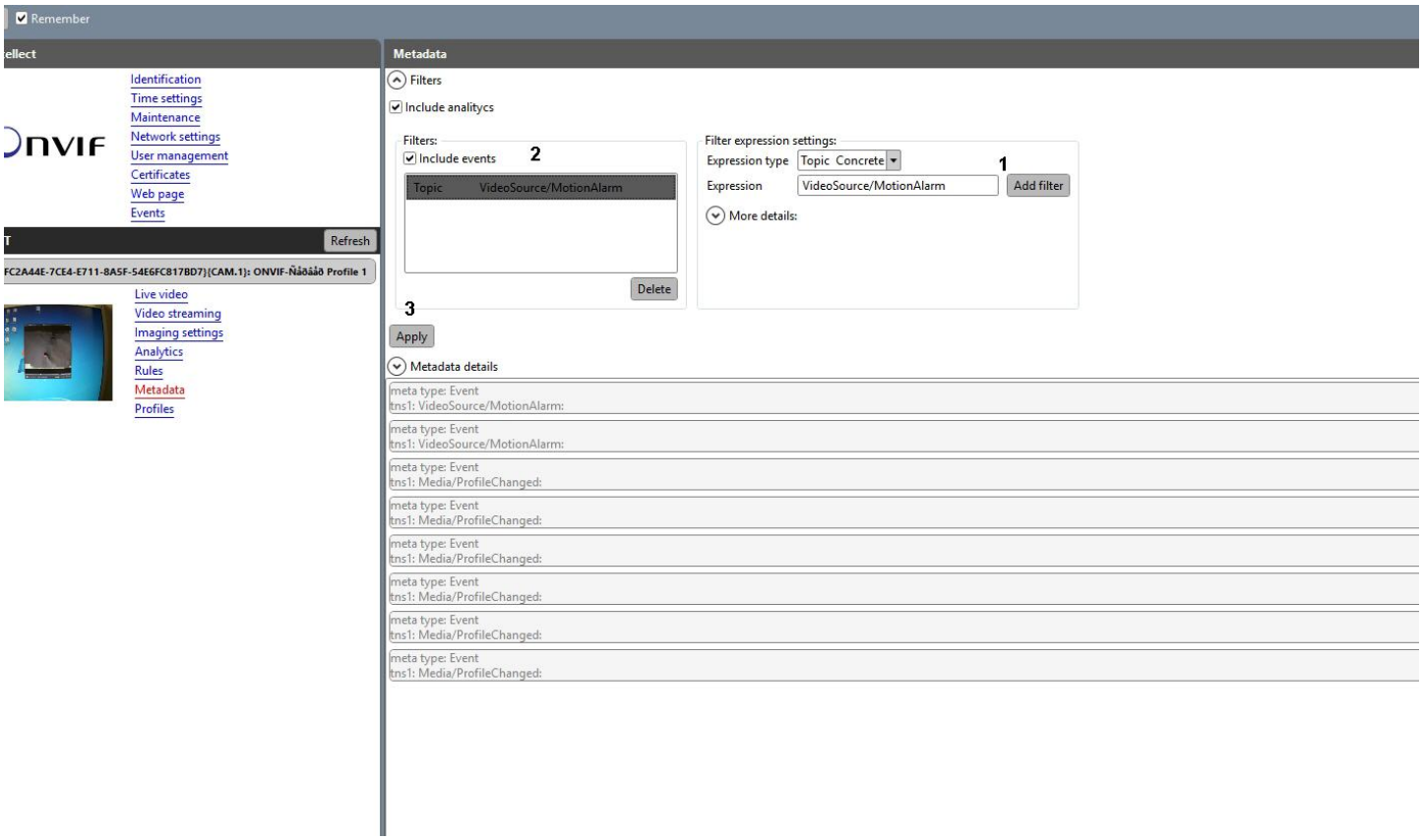
2. From the drop-down list of the **ONVIF-server event** column, select the ONVIF-Server event (**1**). See the events description in the table at the bottom of the page.

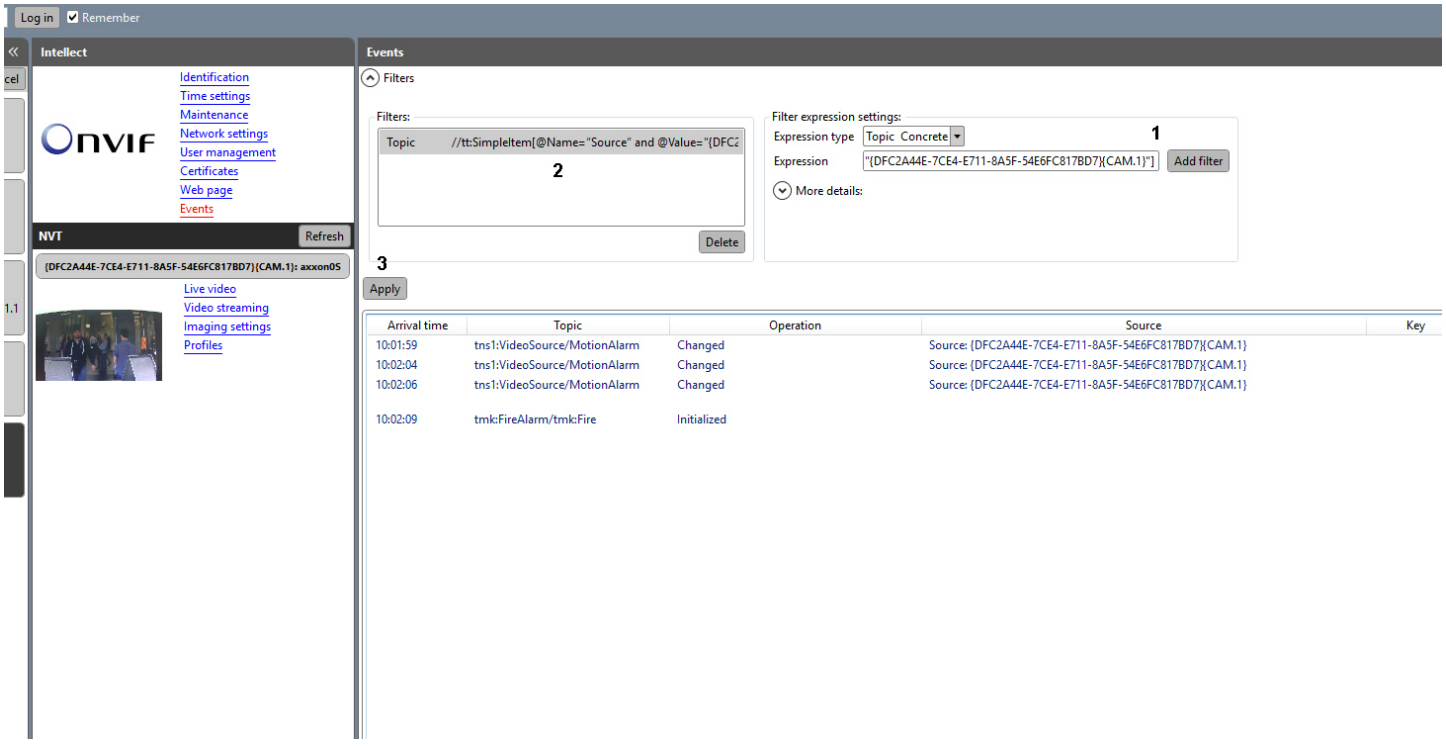
> **Note**
>
> To add a row to the table, press the "down" button on the keyboard; to delete a row, use the Ctrl+Del keyboard shortcut.

3. In the **Computer**, **Type** and **Number** columns specify the parameters of the object, from which the corresponding event comes (**2**). The **Name** field will be filled in automatically when you left-click it. If any column parameter is empty, it means that the message will be sent for any value of the corresponding parameter.
4. From the **Event** drop-down list, select an event which comes from the selected object and corresponds to the specified ONVIF-Server message (**3**).
5. If the specification requires that the event should contain certain parameters (see the table at the bottom of the page), it is necessary to specify their values or the correspondence to the *Intellect* event parameters in the **Transfer parameters** table:
   a. The **ONVIF-event parameter name** column contains the required parameters of the ONVIF-Server event (**4**). They are set according to the specification.
   b. In the **Event parameter name** column, it is necessary to specify the parameter value or the *Intellect* event parameter names (**5**). Event parameters can be found in the Debug window, and some of them are described in the Description of events and reactions of system objects section (see Guide for creating scripts (programming)).
6. Repeat steps 2-5 for all required events.
7. Click the **Apply** button (**6**).

You can check the message and event filtering in the third-party software, for example, in the ONVIF Device Manager utility.

To do this, go to the **Events** or **Metadata** page, depending on what messages you want to see, set the filtering conditions (**1**) that will be displayed in the list (**2**), and then click **Apply** (**3**). As a result, only the events that match the filter should be displayed.





Examples of filters used in the ONVIF Device Manager utility:

1. Topic Filter
   a. **tns1:VideoSurveillanceSystem//.**
      Events where the topic starts with tns1:VideoSurveillanceSystem/
   b. **tns1:VideoSource/MotionDetectorTrigger**
      MotionDetectorTrigger events only

c. **tns1:VideoSurveillanceSystem//.|tns1:FireAlarm/Alarm**
   Events where the topic starts with tns1:VideoSurveillanceSystem/, as well as FireAlarm/Alarm events
d. **tns1:VideoSource/**
   All events of the video system, they contain a comment in *Intellect* format

2. Message Content Filter
   a. **//tt:SimpleItem[@Name="Source" and @Value="{DFC2A44E-7CE4-E711-8A5F-54E6FC817BD7}{CAM.1}"]**
      Events only from the source with the {DFC2A44E-7CE4-E711-8A5F-54E6FC817BD7}{CAM.1} identifier

Note

When the ONVIF-Server restarts, the filters are reset, and they need to be set again.
Before changing the filter in the Events section, it is necessary to click the **Refresh** button for the camera in ODM.

Event	Event description	Parameters	Is configuration required
tns1:Device/AccessControl/Accident	Access Control System incident	Name Comment Place	Yes
tns1:Device/AccessControl/Fault	Access Control System failure		
tns1:Device/FireAlarm/Alarm	Fire Alarm System alarm	Category Zone Comment	Yes
tns1:Device/FireAlarm/Fire	Fire message from Fire Alarm System		
tns1:Device/FireAlarm/Fault	Fire Alarm System failure		
tns1:Device/GasAnalysis/ ConcentrationExceeded	Increased concentration of hazardous gases	Place ConcentrationLimit GasType Concentration Comment	Yes
tns1:Device/Introscopy/LimitExceeded	Detection of metal objects and organic matter	Account Picture Result	Yes
tns1:Device/NeutronProbing/Detect	Detection of explosives	Place ExplosiveType Location Comment	Yes
tns1:Device/RadiationMonitoring/ Detect	Increased radiation	Picture Category Measures Account	Yes
tns1:Device/SteamDetector/Detect	Detection of vapors and trace amounts of explosives which exceed the established threshold values	Measures Picture Account	Yes

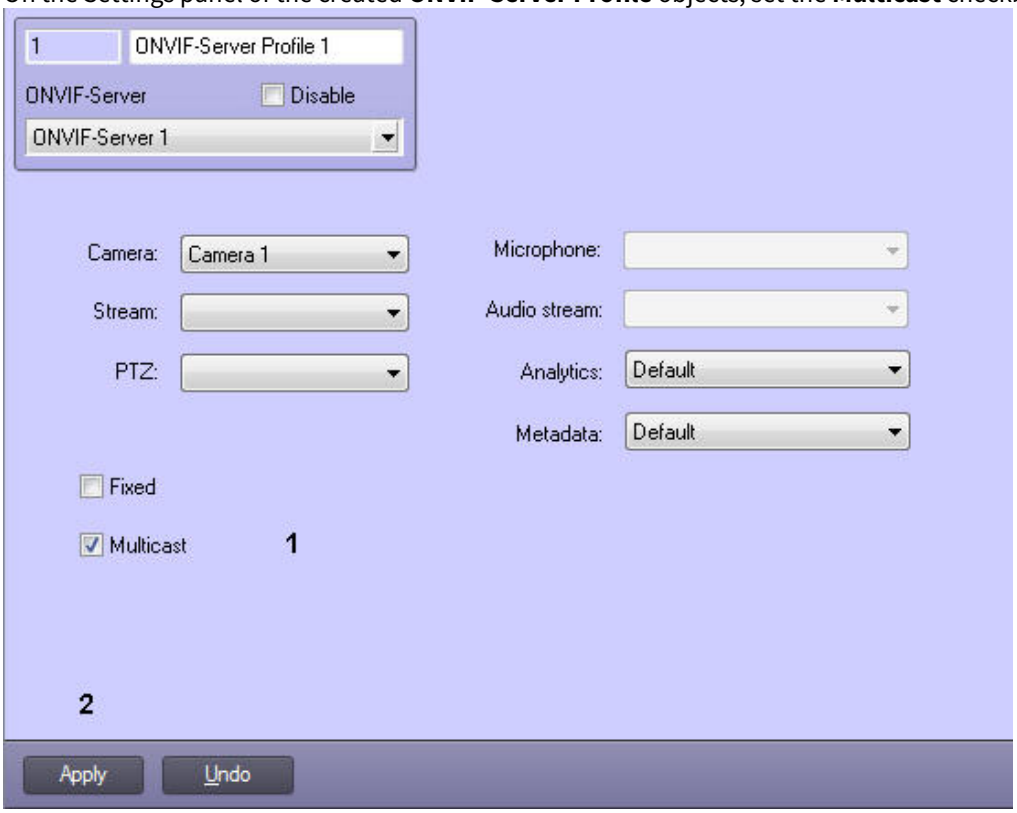
Event	Event description	Parameters	Is configuration required
tns1:Device/MetalDetector/Detect	Detection of metal objects which exceed the specified values.	Picture Account	Yes
tns1:Device/VideoSurveillanceSystem/ ChannelDisconnect	Video channel disconnection	Category Comment Priority	Yes
tns1:Device/VideoSurveillanceSystem/ ChannelConnect	Video channel connection		
tns1:Device/VideoSurveillanceSystem/ RecordTurnOff	Recording turned off		
tns1:Device/VideoSurveillanceSystem/ RecordTurnOn	Recording turned on		
tns1:Device/VideoSurveillanceSystem/ MotionDetectorTrigger	Motion detector triggering		
tns1:Device/VideoSurveillanceSystem/ ReadRecordRequest	Request for the record reading		
tns1:Device/VideoSurveillanceSystem/ DeleteRecordRequest	Request for the record deletion		
tns1:Device/VideoSurveillanceSystem/ EditDbRecordRequest	Request for the event database editing		
tns1:Device/VideoSurveillanceSystem/ CopyDbRecordRequest	Request for the event database copying		
tns1:Device/VideoSurveillanceSystem/ Authorization	System user authorization		
tns1:Device/VideoSurveillanceSystem/ ServerPowerOn	Server switched on		
tns1:Device/VideoSurveillanceSystem/ ServerPowerOff	Server switched off		
axn:HDDrive/axn:Fault	Hard disk error (hard disk missing)	-	No
axn:HDDrive/axn:RecordingFault	Hard disk failure	-	No
axn:HDDrive/axn:DriveFull	Hard disk full (if overwriting on a loop is not enabled)	-	No
axn:VideoSurveillanceSystem/ axn:ChannelDisconnect	Video camera disconnection	-	No
axn:VideoSurveillanceSystem/ axn:ChannelConnect	Video camera connection	-	No

Event	Event description	Parameters	Is configuration required
axn:VideoSurveillanceSystem/ axn:ServerPowerOn	Any *Intellect* Servers switching on in a distributed architecture	-	No
axn:VideoSurveillanceSystem/ ServerPowerOff	Any *Intellect* Servers switching off in a distributed architecture	-	No
tns1:VideoSource	Events with comments in *Intellect* format (for examples, see The Debug window)	-	No

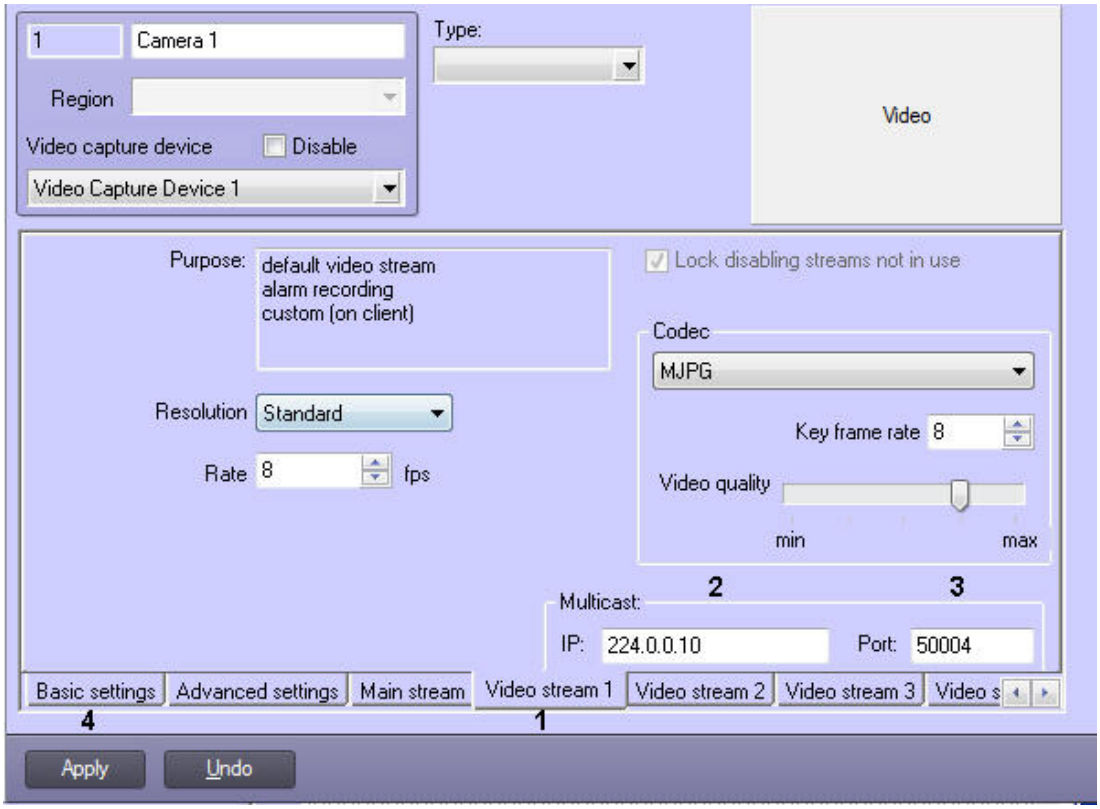
23.3.19.6 Configuring ONVIF-Server module for the Multicast mode

To configure the ONVIF-Server to operate in the Multicast mode, do the following:

1. Configure the **ONVIF-Server** object (see Configuring ONVIF-Server object).
2. Connect to the ONVIF-Server in the software that receives the ONVIF-Server stream (the *Intellect* or *Axxon One* Server, or the third-party software, for example, ONVIF Device Manager). For the information about setting up a connection, see the appropriate software documentation.
3. If the connection is established, the **ONVIF-Server Profile** objects will be created on the basis of the ONVIF-Server object (see Configuring getting video using ONVIF-Server module).
4. On the Settings panel of the created **ONVIF-Server Profile** objects, set the **Multicast** checkbox.



5. Go to the settings panel of the **Camera** object that corresponds to the video camera, which video stream is transmitted via the ONVIF-Server.
6. Go to the video stream tab. If multistreaming is not enabled on the camera, then go to the **Main stream** tab (**1**). If multistreaming is enabled, go to the corresponding video stream tab (see also Configuration of multistream video).



7. In the **IP** field, enter the IP address from which the client will receive the video data in the **Multicast** mode (**2**). The IP address should be in the range of 224.0.0.0 - 239.255.255.255.
8. In the **Port** field, specify the port number for transmitting the video data in the **Multicast** mode (**3**). For each camera, the following ports are used in the **Multicast** mode: nPort, nPort + 18000 (rtp), nPort + 19000 (rtcp), where nPort is the port number specified on the video stream tab.
   For the proper ONVIF-Server operation in the **Multicast** mode, it is necessary that these ports are not busy.
9. Click the **Apply** button (**4**).

10. Repeat steps 5-9 for all cameras, which video stream is transmitted via the ONVIF-Server.

The multicast stream can be received either via the http-request to the corresponding RTSP-Server (for the request examples, see Configuring RTSP Server module), or directly using the multicasting IP address and Port specified in the streams settings. Using the link in the rtsp://ip:multicast_port/cam_num format, the client can receive the information via the RTSP protocol about the internal IP address and port used to transmit the stream.

The configuration of the ONVIF-Server to operate in the **Multicast** mode is completed.

23.3.20 Configuring integration with third-party systems

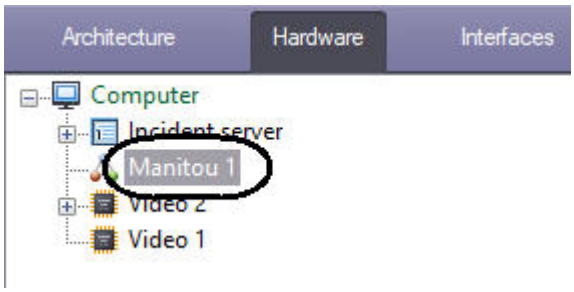
23.3.20.1 Configuring interaction with Manitou software

Interaction with *Manitou* software means sending messages on the event from *Intellect* to the Server with installed *Manitou* software. Messages contain info on the events, and alarm video connected with the event can be attached to such a message.

> **Attention!**
>
> Non-stop recording should be performed on the corresponding camera in order to attach a video fragment to the message correctly—see Recording by Operator command.

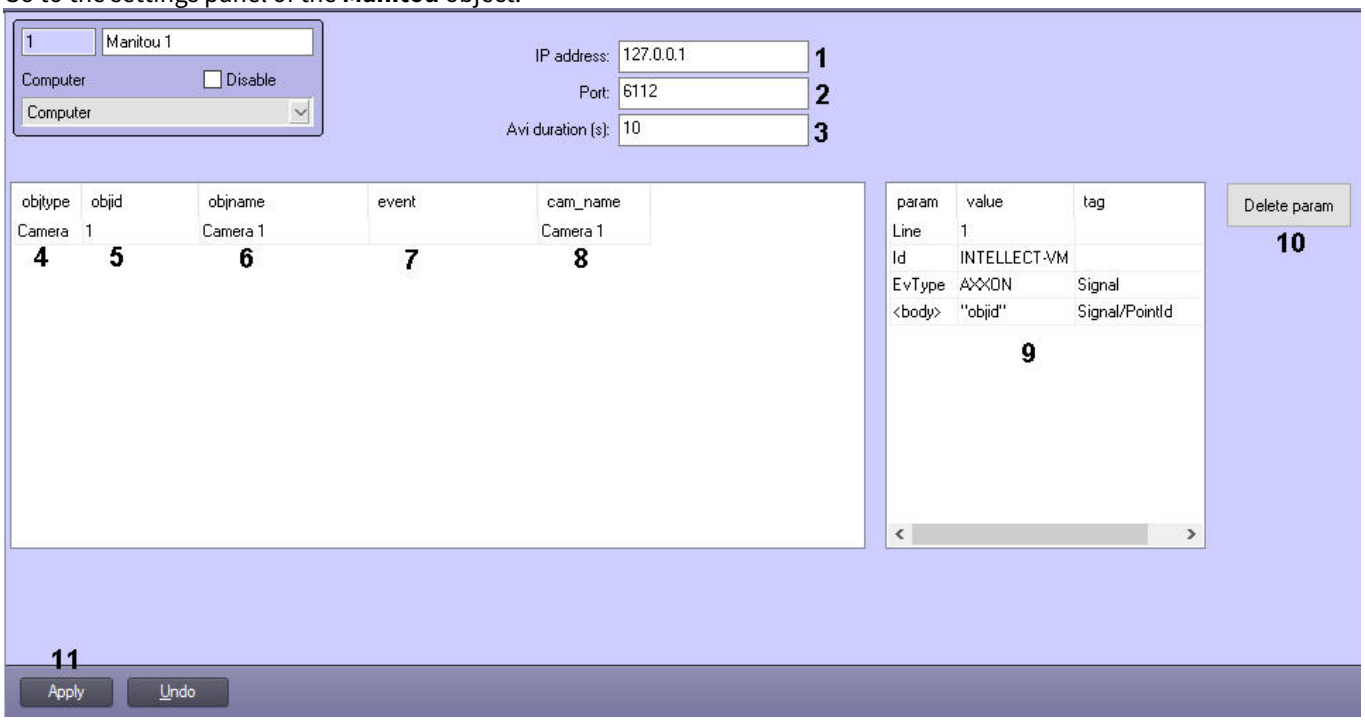
Manitou integration module stands as a client in *Intellect*.

Interaction with *Manitou* software is configured on the settings panel of the **Manitou** object created on the basis of the **Computer** object in the **Hardware** tab of the **System settings** dialog box.



To configure interaction with *Manitou* software, do the following:

1. Go to the settings panel of the **Manitou** object.



2. In the **IP address** field, specify the IP address of the Server where *Manitou* software is started and to which the connection should be performed (**1**).
3. In the **Port** field, specify the port number to connect to the Server with *Manitou* software (**2**).
4. In the **Avi duration (s)** field, specify the period of delay after the event happens and before sending the message with an attached video (**3**).

> **Note**
>
> For the correct video export, in the Tweaki.exe utility set the maximum frames in one video file so the video fragment duration is shorter than the delay (for instance, 100). Otherwise it may happen that recording of the required fragment of video archive has not stopped yet when sending the message. See The Settings panel of the Video subsystem section (the **Frame count** parameter).

5. From the **objtype** drop-down list, select the type of object by the event from which the message should be sent to *Manitou* software (**4**).

> **Attention!**
>
> If you don't select any object, messages about all objects of the system will be sent to *Manitou* software. This can significantly increase the system load, as a large number of video fragments will be generated.

6. From the **objid** drop-down list, select the ID of the object of the selected type (**5**).
7. Left-click in the **objname** field (**6**). It is automatically filled with the name of the corresponding object.
8. From the **event** drop-down list, select the event from the object of the selected type. When this event happens, the message will be sent to *Manitou* software (**7**). If the event is not selected, then messages will be sent on any event from the selected object.
9. From the **cam_name** drop-down list, select the **Camera** object the video fragment from which needs be attached to the message (**8**).
10. Repeat steps 5-9 for all required objects and events.

> **Note**
>
> Press the down arrow ↓ on the keyboard to add a line to the table.

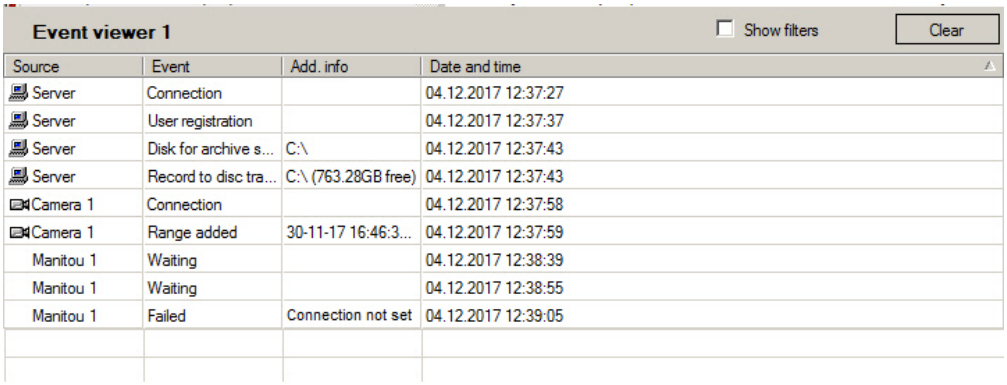
11. If necessary, set the transfer values of the tags in the table (**9**):

a. The **tag** column determines in which tag the attribute will be created or its value set. If the field is left blank, the <Packet> root tag will be selected. This field should be left blank for a string—for it the <Packet> tag is selected by default. The format of setting the field: **Tag/Tag** (tag names with a slash) without specifying the root tag. Example: **Signal/PacketId** will be initialized as <Packet><Signal><PacketId></PacketId></Signal></Packet>.
b. The **param** and **value** columns specify the value of the attribute and the attribute, respectively. Usage options:
- if you specify <body> in the **param** column, and the required value in the **value** column, it will be specified directly in the tag. For example, if <body> is specified in the **param,** 2 is specified in the **value** and **Signal/PacketId** is specified in the tag, the result will be the following entry: <Packet><Signal><PacketId>2</PacketId></Signal></Packet>;
- if <body> isn't specified in the **param** column, the value specified in the **value** column will be written to the attributes of the specified tag;
- to specify a value from the objects table, you have to specify **value** in **"**quotation marks**"**. For example, if **"objid"** is specified, the object ID will be transferred. If **objid** is specified without quotation marks, the **objid** string will be transferred.

> **Note**
>
> There are limitations caused by the XML syntax:
> - you cannot set a value to a tag if it has child tags, and vice versa;
> - you cannot use the following characters in the **value** field: '/', '\', 'space', 'quotes', '<', '>', '&', 'apostrophe';
> - you cannot use the following characters in the **param** field: '<', '>', '&';
> - you cannot use the following characters in the **tag** field: 'space', 'apostrophe', '<', '>', '&', 'quotes'.
>
> If these characters are found, the parameter will not be saved and the reason will be logged.
> To clear the tag table, click **Delete param** (**10**).

12. Click the **Apply** button (**11**).

The *Manitou* connection status is displayed in the **Event viewer**.



Interaction with *Manitou* software is now configured.

23.3.20.2 Configuring the integration with VideoIntellect software

The *VideoIntellect* software provides the video analytics functions. The integration of the *VideoIntellect* and *Intellect* software has the following functional capabilities:

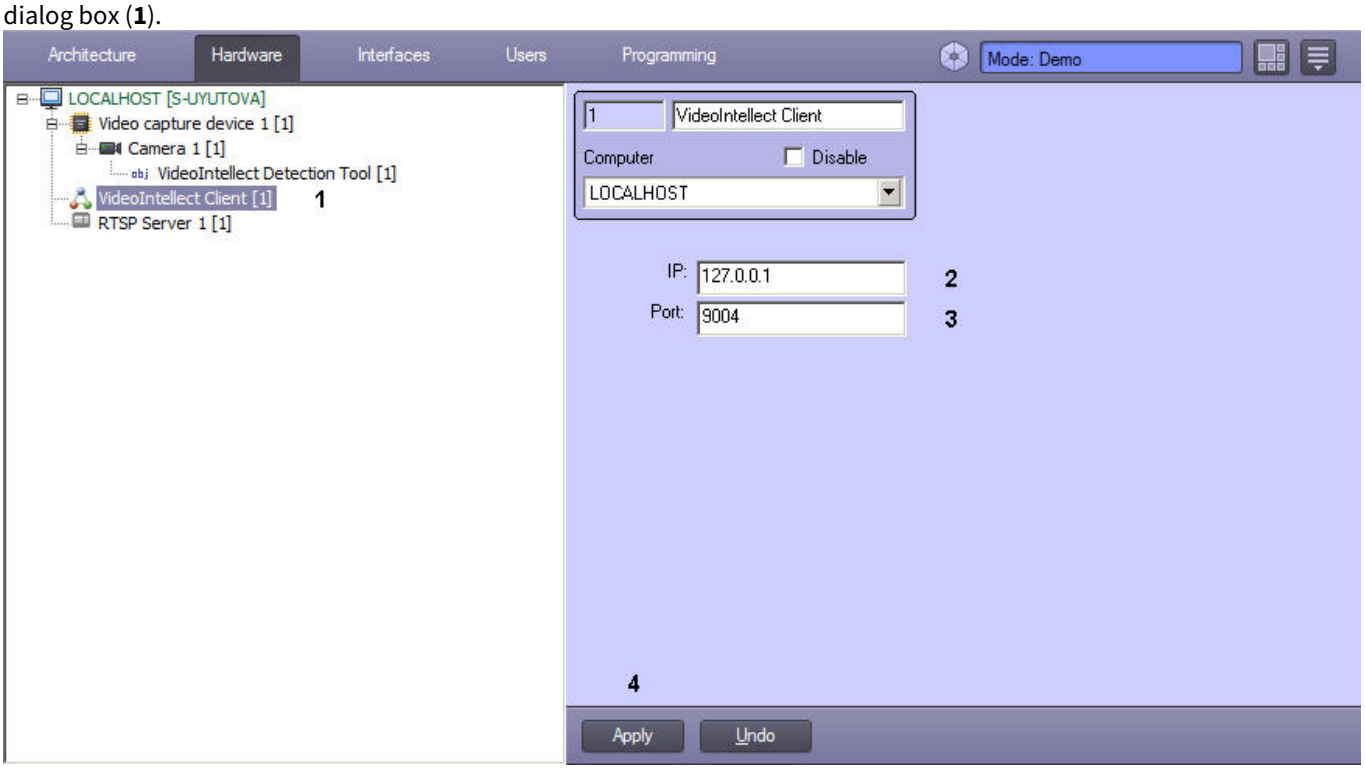
1. Transferring the video from the *Intellect* video cameras to the *VideoIntellect* server via the RTSP protocol.
2. Receiving the results of the video streams analysis (the video analytics detectors triggerings) and metadata from the *VideoIntellect* software.

Prior to configuring the integration with *VideoIntellect* software, it is necessary to create and configure the **RTSP Server** object - see Configuring RTSP Server module. It is also necessary to configure the video reception from the video cameras via the *Intellect* RTSP Server, and configure the required detectors for these video cameras in the *VideoIntellect* software.

23.3.20.2.1 Setting up the connection to VideoIntellect

The connection to the *VideoIntellect* software is set up in the following way:

1. Create the **VideoIntellect Client** object on the basis of the **Computer** object on the **Hardware** tab of the **System Settings** dialog box (**1**).



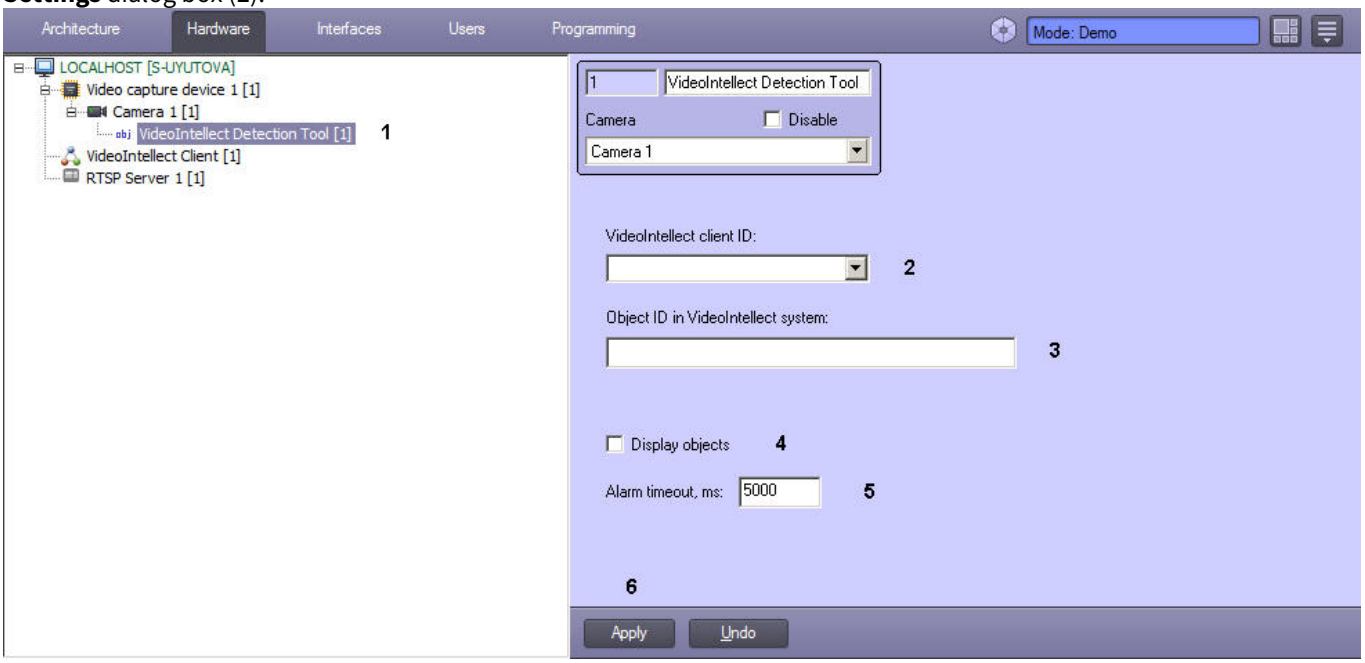
2. In the **IP** field (**2**), enter the IP address of the *VideoIntellect* server.
3. In the **Port** field (**3**), specify the connection port of the *VideoIntellect*.
4. Click **Apply** (**4**).

Setting up the connection to the *VideoIntellect* software is complete.

23.3.20.2.2 Setting up the detector triggering reception from VideoIntellect

The reception of the video analytics detector triggering from the *VideoIntellect* software is set up in the following way:

1. Create the **VideoIntellect Detection Tool** object on the basis of the **Camera** object on the **Hardware** tab of the **System Settings** dialog box (**1**).



2. From the **VideoIntellect Client ID** drop-down list (**2**), select the **VideoIntellect Client** object identifier used to connect to the *VideoIntellect* software .
3. In order to receive the triggerings from the camera that is not configured in the *Intellect*, in the **Object ID in VideoIntellect system** field (**3**), enter the video analytics detector identifier in the *VideoIntellect* software terms. The identifier should be entered in the following format: **{4f4dfe1d-7109-44fd-8a6f-8d40ea198710}**.
4. If it is necessary to generate an alarm on the camera when receiving a detector triggering, set the **Display objects** checkbox (**4**).
5. In the **Alarm timeout, ms** field (**5**), enter the time period in millisecond after which the *Intellect* alarm will be forcibly terminated, even if the corresponding message to terminate the alarm has not been received from the *VideoIntellect* software.
6. Click **Apply** (**6**).

After the detectors are configured, the transfer of the events from the detectors configured in the *VideoIntellect* software to the **Event log** begins. In addition, the metadata from the *VideoIntellect* detector can be used by the smart detection tools, for example, for smart search in the archive and for displaying events on the video image (see Creating and configuring the Tracker object).

Configuring the receipt of video analytics detector triggerings from *VideoIntellect* software is completed.

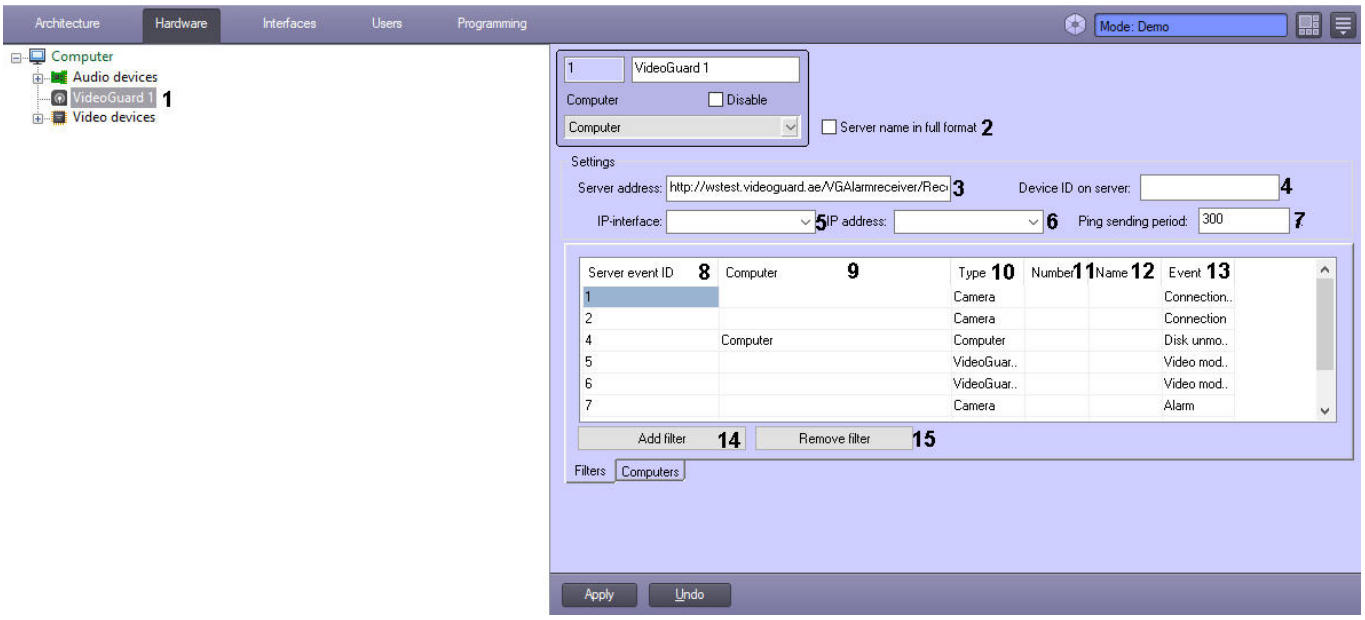
23.3.20.3 Configuring integration with VideoGuard system

Intellect allows sending events from the system objects to the VideoGuard server (see http://videoguard.ae/). In this case, *Intellect* acts as a client of the VideoGuard system.

The integration with the VideoGuard system is configured as follows:

1. Create the **VideoGuard integration client** object on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog box (**1**). If data from several *Intellect* servers in a distributed system should be sent to VideoGuard, then create and configure a separate **VideoGuard integration client** object on the basis of each server.

> **Note**
>
> A single **VideoGuard integration client** object is enough to send messages about the loss of connection with any server. See also step 7.

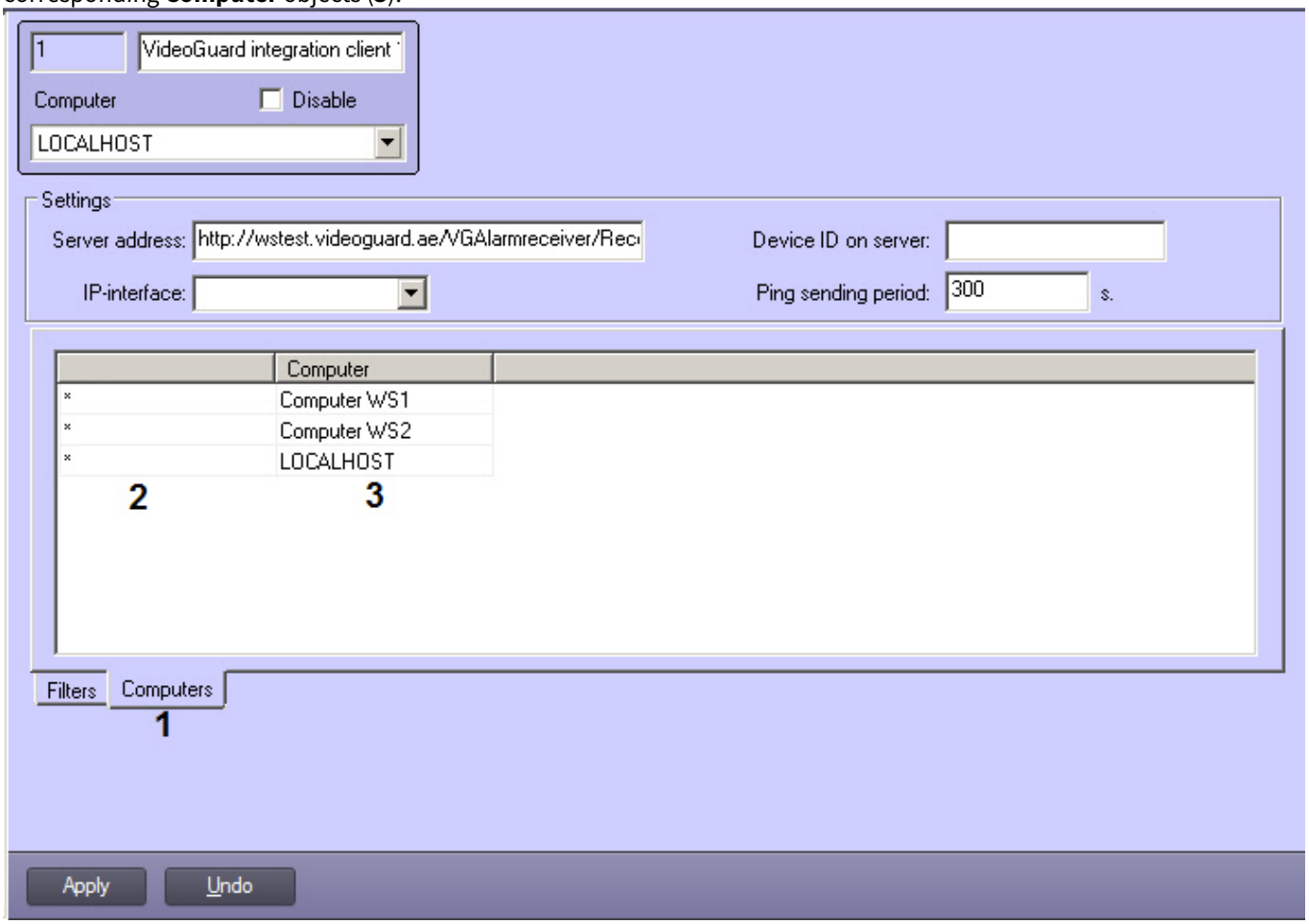


2. Set the **Server name in full format** checkbox (**2**), if it is necessary to display the full server name. By default, short server name is displayed.
3. In the **Server address** field, enter the connection address to the VideoGuard server (**3**).
4. In the **Device ID on the server** field, enter the identifier which is assigned to *Intellect* on the **IP interface** server (**4**). There should be no more than 6 digits in this field.
5. From the **IP-interface** drop-down list, select the network adapter which is used to connect this computer to the VideoGuard server (**5**).
6. From the **IP address** drop-down list (**6**), select the IP address that will be sent to VideoGuard as *Intellect* server address.

> **Note**
>
> The IP address list displays all addresses from all available IP interfaces. If you specify an IP address that doesn't belong to the selected IP interface, the system will send a random IP address from those available in the selected IP interface.

7. In the **Ping sending period** field, specify the Heart Beat messages sending frequency in seconds (**7**). By default, the Heart Beat message is sent right after the *Intellect* starts and then every 5 minutes (300 seconds).
8. Configure the correspondence between the VideoGuard and *Intellect* events. By default, the correspondence table contains the mandatory events, and their correspondence with the *Intellect* objects events is configured. If necessary, you can change this correspondence, add or remove additional events:
    a. From the **Server event ID** drop-down list, select the event identifier on the VideoGuard server (**8**). See the supported values in the table below.
    b. From the **Computer** drop-down list, select the name of the **Computer** object. The selected events of the objects, which are based on this **Computer** object, will be sent to the VideoGuard (**9**). If the value is not specified, the events are sent from the specified objects, regardless of which **Computer** object they are based on; in this case such events may not be processed correctly in VideoGuard.
    c. From the **Type** drop-down list, select the *Intellect* object type, the events from which should be sent to the VideoGuard server (**10**).
    d. From the **Number** drop-down list, select the *Intellect* object identifier, the events from which should be sent to the VideoGuard server (**11**). If the identifier is not specified, then events are sent from all objects of the selected type.
    e. After you select the object type and identifier, the **Name** field will be automatically filled with the name of the selected *Intellect* object (**12**).
    f. From the **Event** drop-down list, select the event which is coming from the *Intellect* object of the selected type and which corresponds to the VideoGuard server event with the specified identifier (**13**).
    g. To add new event, click **Add filter** (**14**), then perform steps a-f to configure it.
    h. To remove an event, select corresponding row in the table and click **Remove filter** (**15**).
9. If there is one **VideoGuard integration client** object and several **Computer** objects, then connection loss events from all computers in the distributed system are transmitted to VideoGuard software by default. If you do not need to transmit connection loss events from some computers, go to the **Computers** tab (**1**) and clear the checkboxes (**2**) next to the

corresponding **Computer** objects (**3**).



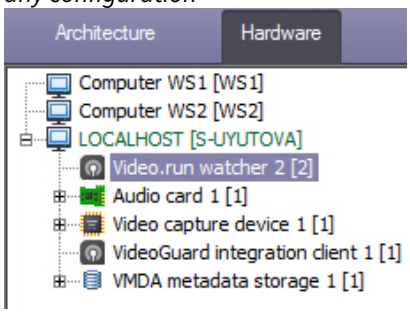
10. Click the **Apply** button.

The integration with the VideoGuard system is configured.

Restart *Intellect* after connecting to the VideoGuard server to synchronize the time with the VideoGuard server. After *Intellect* restart, the time zone in Windows is synchronized with the specified VideoGuard server. Subsequently, the *Intellect* server will synchronize with the NTP server of the VideoGuard system (by calling the GetNTPServerInfo method). During synchronization, the VideoGuard system server will return the time synchronization period (120 seconds by default), and within 24 hours after synchronization with the NTP server, time synchronization will be performed at the specified interval.

The event identifiers supported on the server:

ID	Description	Corresponding Intellect event
1	No video signal	Camera: Connection lost
2	Video source connection	Camera: Connection
3	Disk overflow	-
4	Error writing to disk	Computer: Disc unmounted
5	Client connection	VideoGuard integration client: Video module started *Note. The event is generated in the following cases:*

ID	Description	Corresponding Intellect event
		• *If the video module has loaded. Create the **Video.run Watcher** object on the basis of each **Computer** object from which this event should be received. The object doesn't need any configuration*  • *If Intellect has loaded* • *If the network is on*
6	Client disconnection	VideoGuard integration client: Video module unloaded *Note. The event is generated in the following cases:* • *If the video module is unloaded. Create the **Video.run Watcher** object on the basis of each **Computer** object from which this event should be received. The object doesn't need any configuration* • *If Intellect has unloaded* • *If the network is off, the event is received after the network is turned on*
7	Motion detection trigger	Camera: Alarm
8	Case opening (Shelter Alarm)	-
9	Start of recording to the archive	Camera: Harddisk rec
10	End of recording to the archive	Camera: Record on disk stopped
11	Change of recording to the archive schedule	-
100	Additional event	Used to send additional events to the VideoGuard server. In this case, the event source identifier is added to the event identifier Example: The event with the 101 identifier will be sent to the VideoGuard server

Server event ID	Computer	Type	Number	Name	Event
100		Camera	7	Camera 7	Alarm
4	Computer	Computer			Disk unmo..

Note

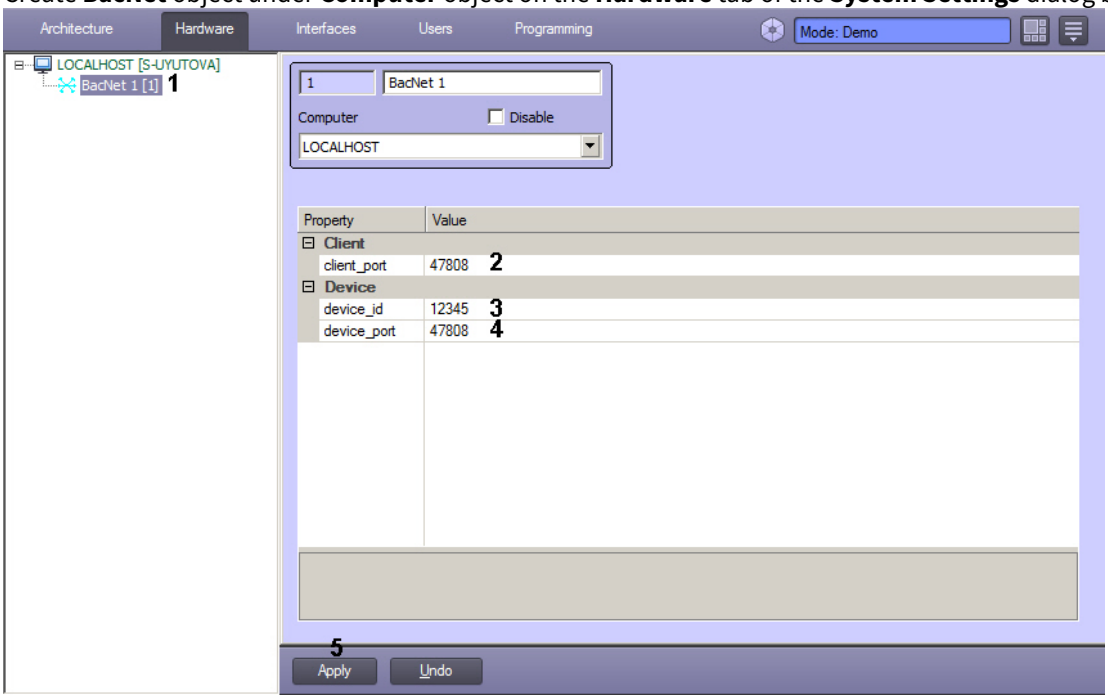
If several Servers are added to the configuration, then after the restart of the main Server, the events with the 5 identifier will be sent to those Servers that are turned on or were turned on at the time of the restart of the main Server. At the same time, the event with the 6 identifier won't be sent to those Servers that were turned off at the time of the restart of the main Server.

23.3.20.4 Configuring BACnet integration

Intellect base supports connection to external devices via BACnet protocol. See also BACnet Wrapper Settings Guide

Configure BACnet device connection as follows:

1. Create **BacNet** object under **Computer** object on the **Hardware** tab of the **System Settings** dialog box (1).



2. In the **client_port** field, enter the client connection port (2).
3. In the **device_id** field, specify the device identifier (3).
4. In the **device_port** field, specify the device port (4).
5. Click the **Apply** button (5).

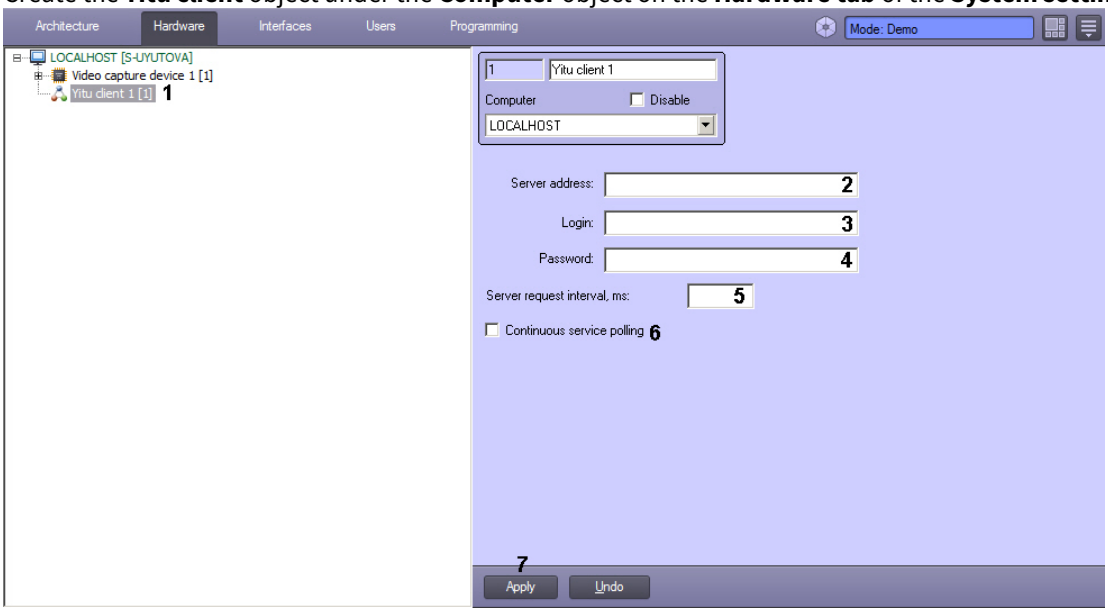
Further work with the BACnet device is carried out using scripts – see BACNET.

23.3.20.5 Configuring integration with YITU face recognition system

Integration with the YITU face recognition system is designed to request events about recognized faces from the YITU server.

Integration with the YITU face recognition system is configured in the following order:

1. Create the **Yitu client** object under the **Computer** object on the **Hardware tab** of the **System settings** window (1).



2. In the **Server address** field (2), enter the YITU server IP and port in the format https://IP:port, for example: https://192.168.7.107:9812
3. In the **Login** field, enter the YITU user name (3).
4. In the **Password** field, enter the YITU user password (4).
5. In the **Server request interval, ms** field enter the time period to send requests to the server (5).
6. If the YITU system is to be polled continuously, set the **Continuous service polling** checkbox (6).
7. Click **Apply** (7).

After completing these actions, *Intellect* will send an authorization request with the corresponding login and password to the specified address and receive an authorization token in response. If authorization is successful, *Intellect* software will be sending requests for new events to the YITU server at the specified frequency and output the information received to the Event Viewer.

Note.

Events are requested from the last request. If necessary, set the time from which to request events using the registry key:
KEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ITV\INTELLECT\Yitu\{**Yitu client** ID}\DefaultStartRequestTimestamp

Integration with the YITU face recognition system is now configured.

23.3.21 Configuring SIP-terminal

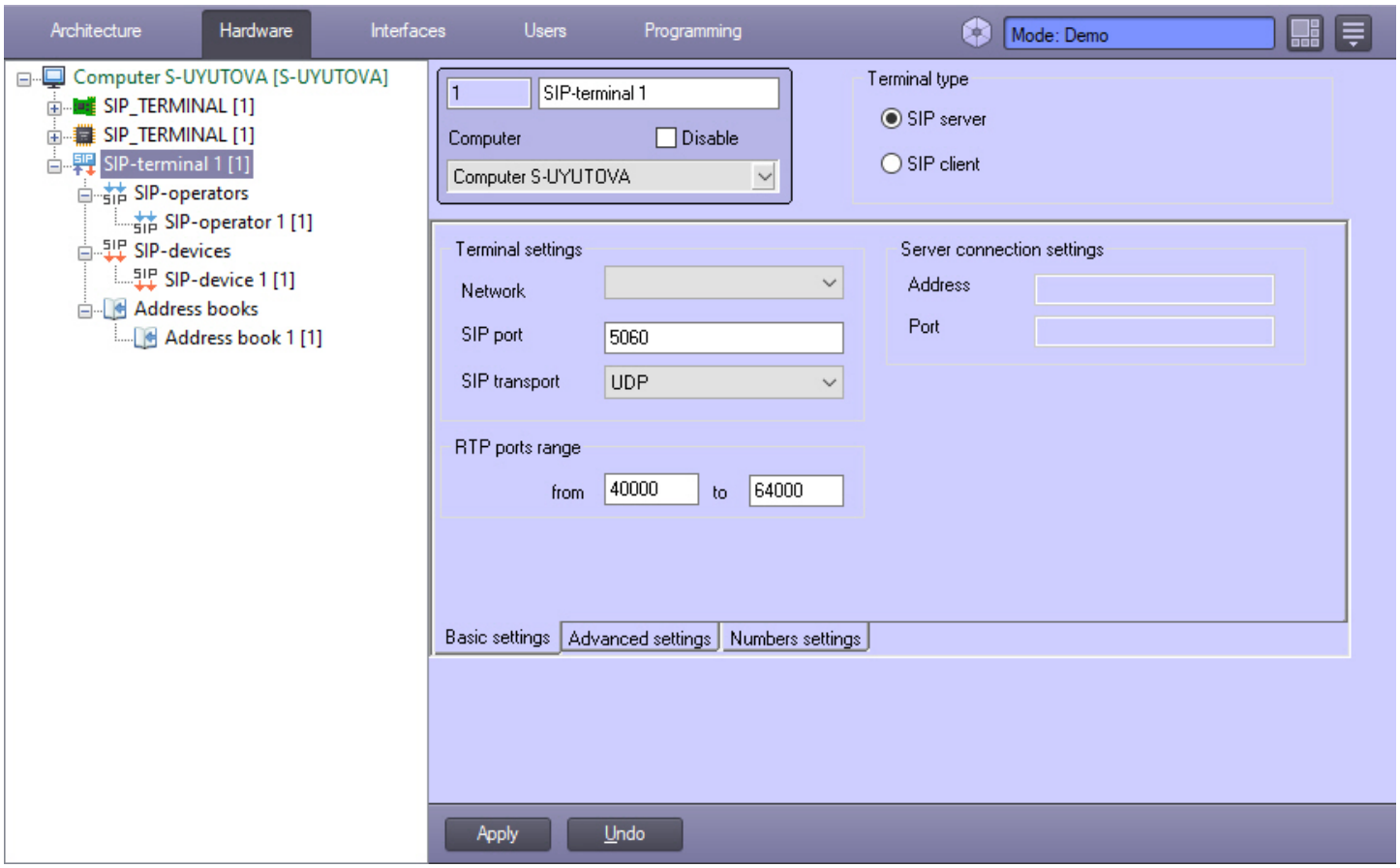
SIP-terminal is designed to implement IP telephony within the distributed system configuration. IP telephony can be implemented with or without physical SIP-devices. Thus, the SIP-terminal allows organizing single and group calls between operators and SIP-devices in the Server/Remote Admin Workstation/Remote Client configurations.

Note

SIP-devices are IP devices, mainly intercoms and call panels, connected to *Intellect* via the Session Initiation Protocol (SIP).

Intellect can act both as a server and as a client. The SIP server for the *Intellect* SIP client can be either third-party Asterisk software or the *Intellect's* SIP server.

SIP-devices are configured on the settings panel of the **SIP-terminal** object created on the basis of the **Computer** object on the **Hardware** tab of the **System Settings** dialog box, and also on the settings panel of its child objects.



The SIP-terminal (both server and client) is configured in the following order:

1. Configure the *Intellect* SIP server (see Configuring the Intellect's SIP server).
2. Configure the *Intellect* SIP client (see Configuring the Intellect's SIP client).
3. Create and configure objects corresponding to address books (see Configuring address book of SIP-terminal).
4. Configure special terminal numbers (see Configuring special numbers of SIP-terminal).
5. If necessary, create and configure macros for working with a SIP-terminal (see Macros for working with SIP-terminal).
6. Configure terminal numbers (see Configuring numbers of SIP-terminal).
7. Select a speaker, microphone, and camera for each SIP-operator (see Selecting speaker, microphone and camera for SIP-operator).
8. If you need to work with SIP-devices and SIP-operators from the map, add the corresponding objects to the map (see Attaching objects to the layers of interactive map).
9. Configure the **SIP Panel** interface object (see Configuring the SIP-panel interface object).

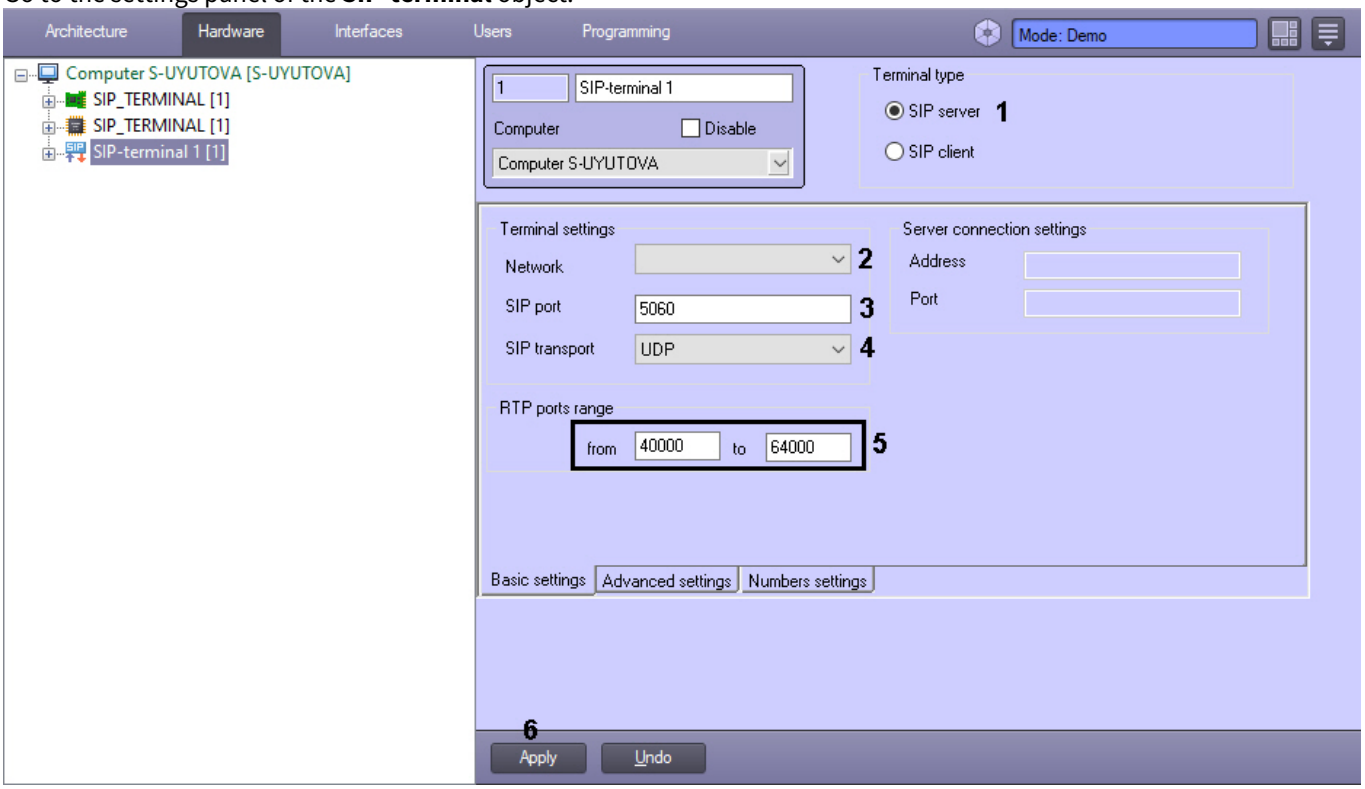
SIP-panel

23.3.21.1 Configuring the Intellect's SIP server

23.3.21.1.1 Network settings of the Intellect's SIP server

The network settings of the *Intellect* SIP server are set in the following order:

1. Go to the settings panel of the **SIP-terminal** object.



2. Set the **Terminal type** switch to the **SIP server** position (**1**) — the SIP-terminal acts as a server, any SIP-clients can be connected to it (both *Intellect*-based and the third-party SIP-devices).
3. From the **Network** drop-down list (**2**), select the IP address of the network adapter that will be used to connect to the network where the SIP-clients are located.
4. In the **SIP port** field (**3**), specify the port number which will receive the data from the SIP-clients.
5. From the **SIP transport** drop-down list (**4**), select the transport level protocol to be used: TCP or UDP.
6. If necessary, specify the RTP ports range in the corresponding text fields (**5**).
7. Click **Apply** (**6**).

The network settings of the *Intellect's* SIP server are set.

23.3.21.1.2 Configuring SIP-devices of the Intellect's SIP server

On this page:

- Configuring the SIP-device
- Configuring the SIP-device connection to Intellect
- Configuring the Video / Audio
- Configuring the tone DTMF commands

23.3.21.1.2.1 Configuring the SIP-device

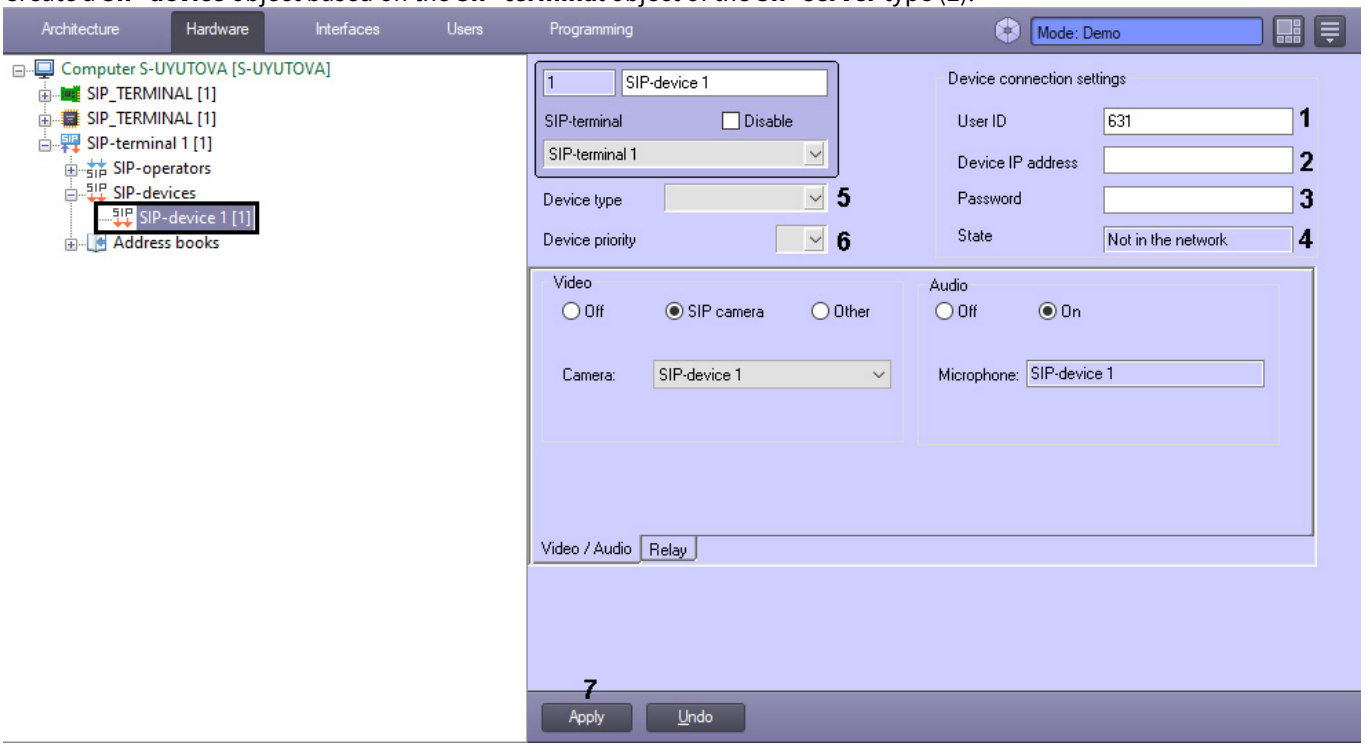
Before you start configuring the SIP-device connection to *Intellect*, it is necessary to configure the device itself. Each SIP-device is configured individually according to the manufacturer's documentation, however, it is always necessary to perform the following basic steps:

1. Specify the IP address of the *Intellect* server that acts as a SIP server.
2. Check or specify the SIP-device identification number (the number used for calls).
3. Set the password for the SIP-server connection.
4. If the SIP-device does not support dialing from the keyboard and has only one button for calling the concierge, it is necessary to configure this button to call the *Intellect* operator (see Configuring SIP-operators of the Intellect's SIP server).

23.3.21.1.2.2 Configuring the SIP-device connection to Intellect

The SIP-devices connection to the Intellect SIP-server is configured as follows:

1. Create a **SIP-device** object based on the **SIP-terminal** object of the **SIP-server** type (**1**).

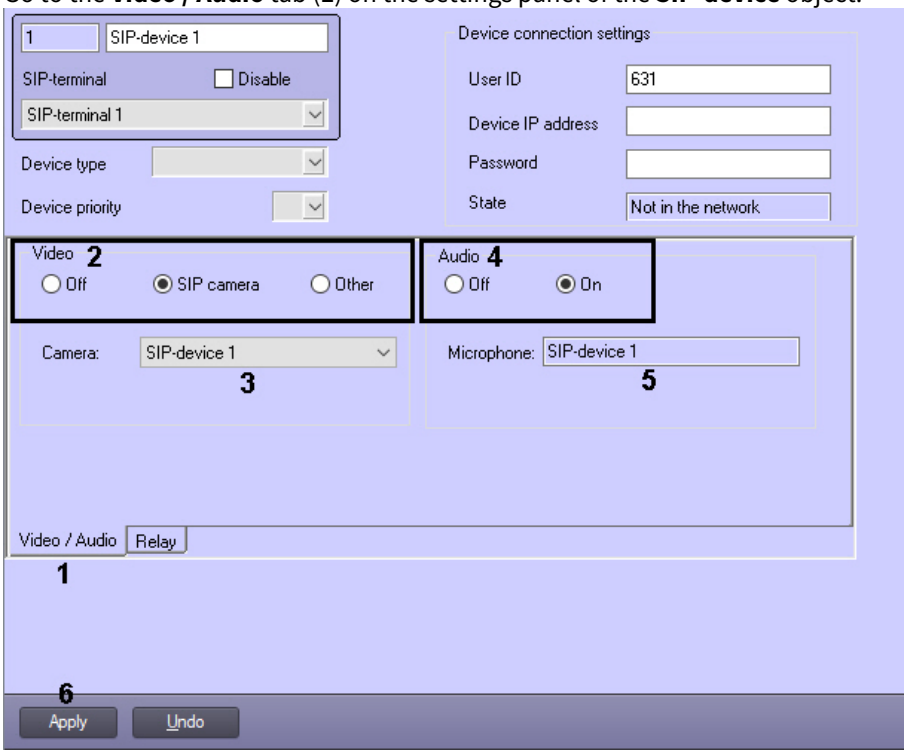


2. In the **User ID** field (**1**), enter the SIP-device identification number, i.e. the number to call it.
3. In the **Device IP address** field (**2**), enter the SIP-device IP address. If you are not going to send data to the SIP-device, this field is optional.
4. In the **Password** field (**3**), enter the password specified on the SIP-device. The SIP-device with the specified identifier will be connected to *Intellect* only if the passwords on the device and in *Intellect* are identical.
5. The **State** field (**4**) indicates the current status of the SIP-device.
6. From the **Device type** drop-down list (**5**), select the icon type used to display the device on the Map.
7. From the **Device priority** drop-down list (**6**), select the priority of calls from this device when displayed on the SIP panel. The lower the number, the higher the priority and, hence, the higher the call is displayed in the list. If the field is left blank, the priority is considered minimal. Calls from devices with the same priority will be sorted by the time of the call.
8. Click **Apply** (**7**).

23.3.21.1.2.3 Configuring the Video / Audio

Configure the SIP-device's video and audio in the following order:

1. Go to the **Video / Audio** tab (**1**) on the settings panel of the **SIP-device** object.



2. Set the **Video** switch (**2**) to the position corresponding to the video camera used for calls:
   a. **Off** — the video is not used during the call.
   b. **SIP camera** — a SIP-device camera connected via the SIP protocol is used. If the wrong device is selected by default in the **Camera** (**3**) drop-down list, change the selection. The corresponding **Camera** object may not be created in the *Intellect* objects tree at this step; in this case, it will be created automatically after clicking the **Apply** button.
   c. **Other** — any other camera from the *Intellect* hardware tree is used. In this case, select the name of the required **Camera** object from the **Camera** drop-down list (**3**).
3. Set the **Audio** switch (**4**) to the position corresponding to the microphone used for calls:
   a. **Off** — the audio is not used during the call.
   b. **On** — when making a call, the microphone of the SIP-device, displayed in the **Microphone** information field (**5**), is used. The corresponding **Microphone** object may not be created in the *Intellect* objects tree at this step; in this case it will be created automatically after clicking the **Apply** button.
4. Click **Apply** (**6**).

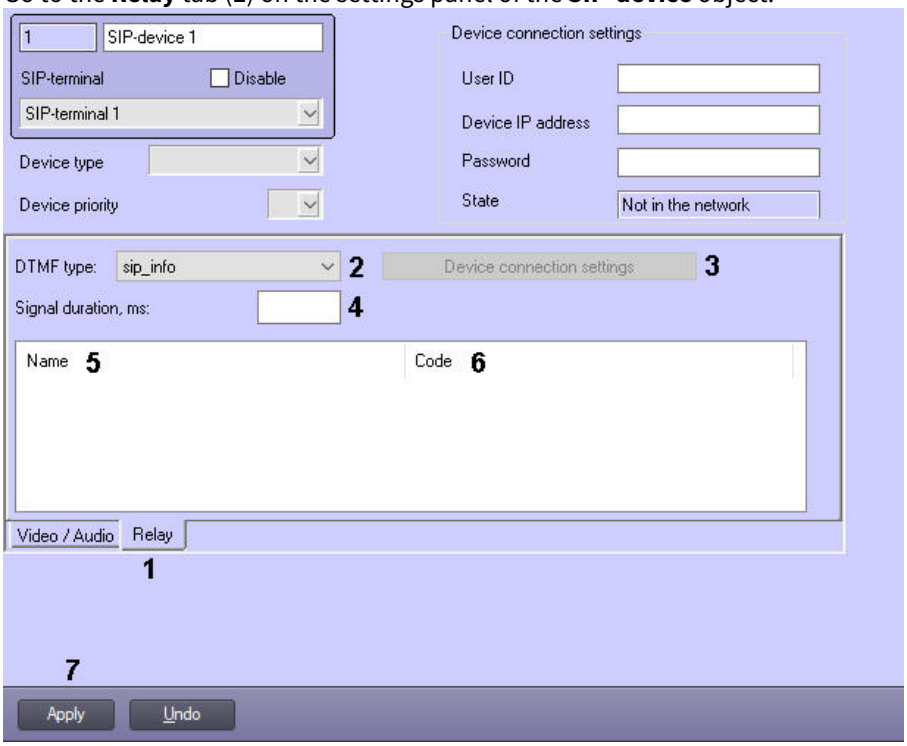
> **Note**
>
> If necessary, the pre-configured missing **Camera** and **Microphone** objects will be automatically created in the *Intellect* objects tree.

23.3.21.1.2.4 Configuring the tone DTMF commands

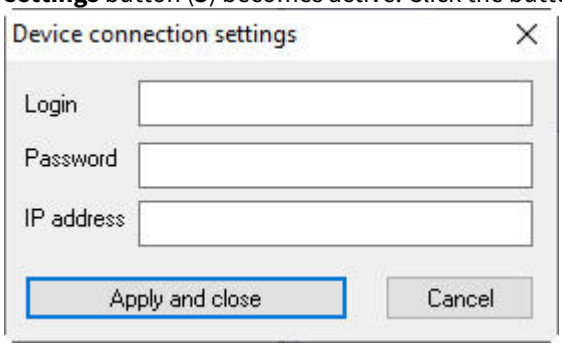
The setting of sending tone messages to a SIP-device (for example, a combination for opening a door) is carried out by setting the relay.

The SIP-device relays are configured in the following order:

1. Go to the **Relay** tab (**1**) on the settings panel of the **SIP-device** object.



2. Select the type from the **DTMF type** drop-down list (**2**):
   a. **sip_info** – signals are transmitted in the SIP INFO message.
   b. **sip_notify** – signals are transmitted in the SIP NOTIFY message.
   c. **in_band** – the signal is transmitted as normal sound in an audio stream.
   d. **http_bas** – signals are transmitted over HTTP. When this type of tone is selected, the **Device connection settings** button (**3**) becomes active. Click the button to open the connection settings window:



   In this window, specify the **Login**, **Password** and **IP address** of the SIP device. If the port is different from the actual one (for example, it's 8180, not 80), then specify the port in the **IP address** field also. If the **IP address** field is left blank, then the IP address will be taken from the session, and the port will be presumed to be **80.**
3. In the **Signal duration, ms** field (**4**) set the time period in milliseconds during which the command is to be sent. This value is applied if duration is not set for a specific command.
4. In the **Name** field (**5**), enter the name of the command displayed on the SIP panel.
5. In the **Code** field (**6**), enter the unique command code.

> **Note**
>
> If the **http_bas** tone type is selected, then enter a request according to the documentation of the SIP device in the **Code** field, for example: GET access/general/lock/open/remote/accepted/1

6. Click **Apply** (**7**).

> **Note**

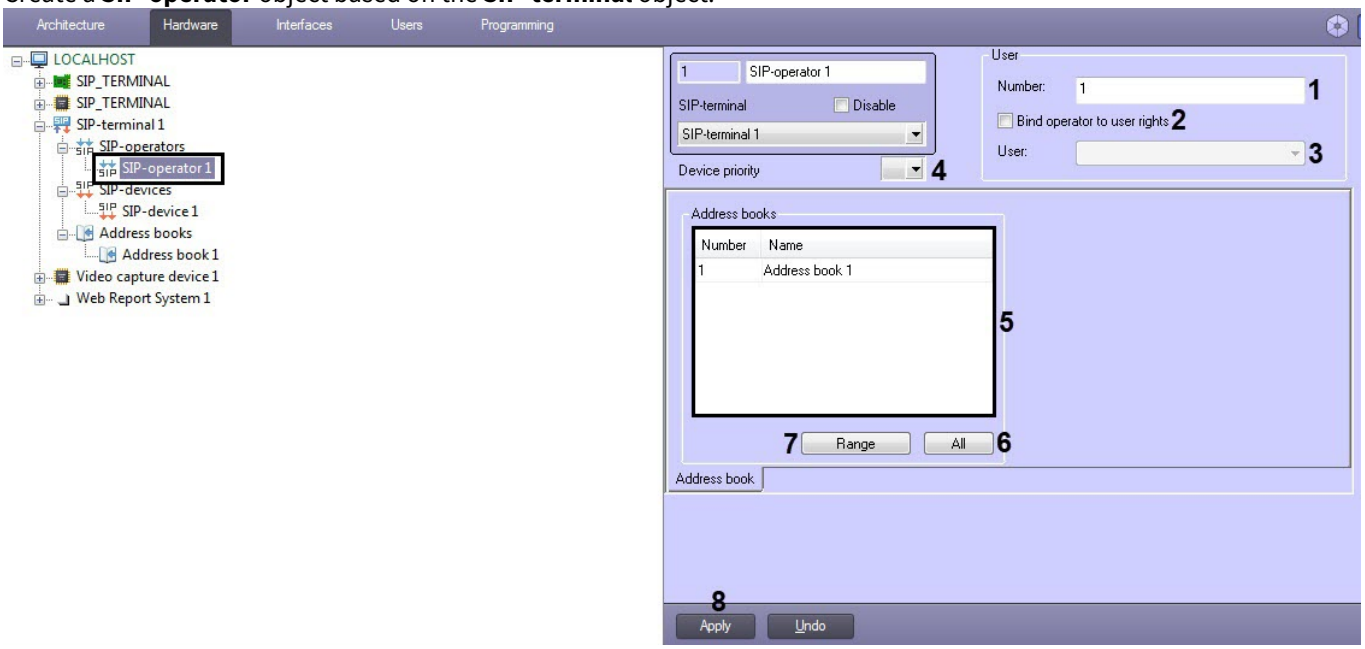
The corresponding **Relay** object will be created in the *Intellect* hardware tree.

The SIP-device of the *Intellect's* SIP server is configured.

23.3.21.1.3 Configuring SIP-operators of the Intellect's SIP server

SIP-operators are configured as follows:

1. Create a **SIP-operator** object based on the **SIP-terminal** object.



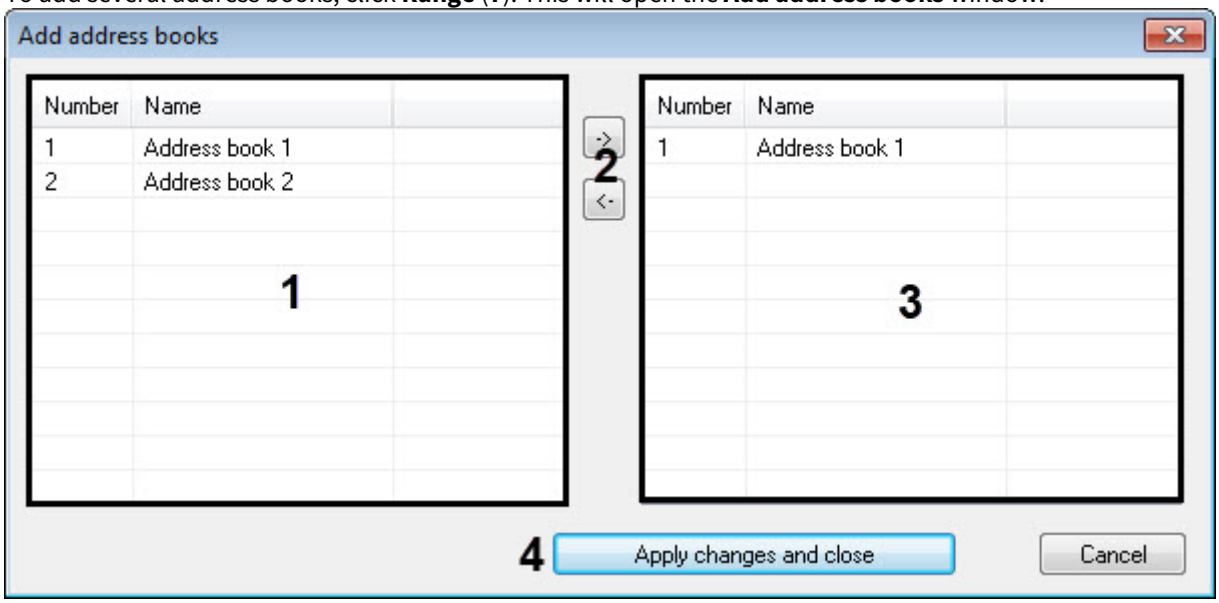
2. In the **Number** field (**1**) enter the identification number for calls.
3. If it is necessary to bind a SIP-operator to the *Intellect* user rights, set the **Bind operator to user rights** checkbox (**2**) and select the corresponding *Intellect* user from the **User** drop-down list (**3**). It is used when the **User rights** are selected by default on the operator's SIP panel.
4. From the **Device priority** drop-down list (**4**), select the priority of a call from this operator in the incoming calls window of the SIP panel. The lower the number, the higher the priority, hence, the higher the call is displayed in the list. If the field is left blank, the priority is considered to be minimal. Calls from operators with the same priority will be sorted by the time of the call.
5. In the **Address books** table (**5**), select the required address books, the numbers of which should be available for this SIP-operator (see Configuring address book of SIP-terminal).

   Note

   To add new lines to the table, use the Down key on your keyboard. To delete a line, use the Ctrl+Del key combination.

   a. To add all address books, click **All** (**6**).

b. To add several address books, click **Range** (**7**). This will open the **Add address books** window.



i. Select the required address books from the left list (**1**) and use the buttons (**2**) to move them to the right list (**3**).

ii. Click the **Apply changes and close** button (**4**).

6. Click **Apply** (**8**).

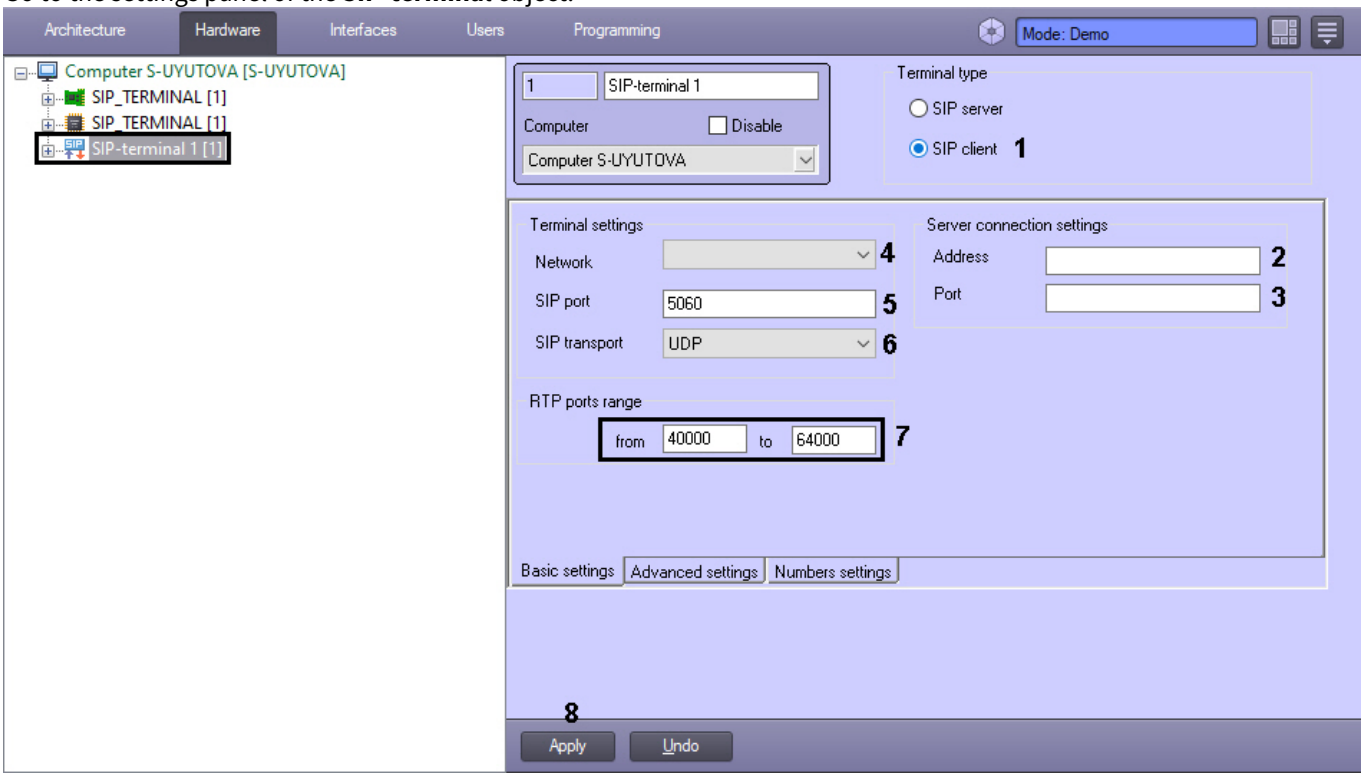
The SIP-operators of the *Intellect's* SIP server are configured.

23.3.21.2 Configuring the Intellect's SIP client

23.3.21.2.1 Network settings of the Intellect's SIP client

The network settings of the *Intellect's* SIP client are set in the following order:

1. Go to the settings panel of the **SIP-terminal** object.



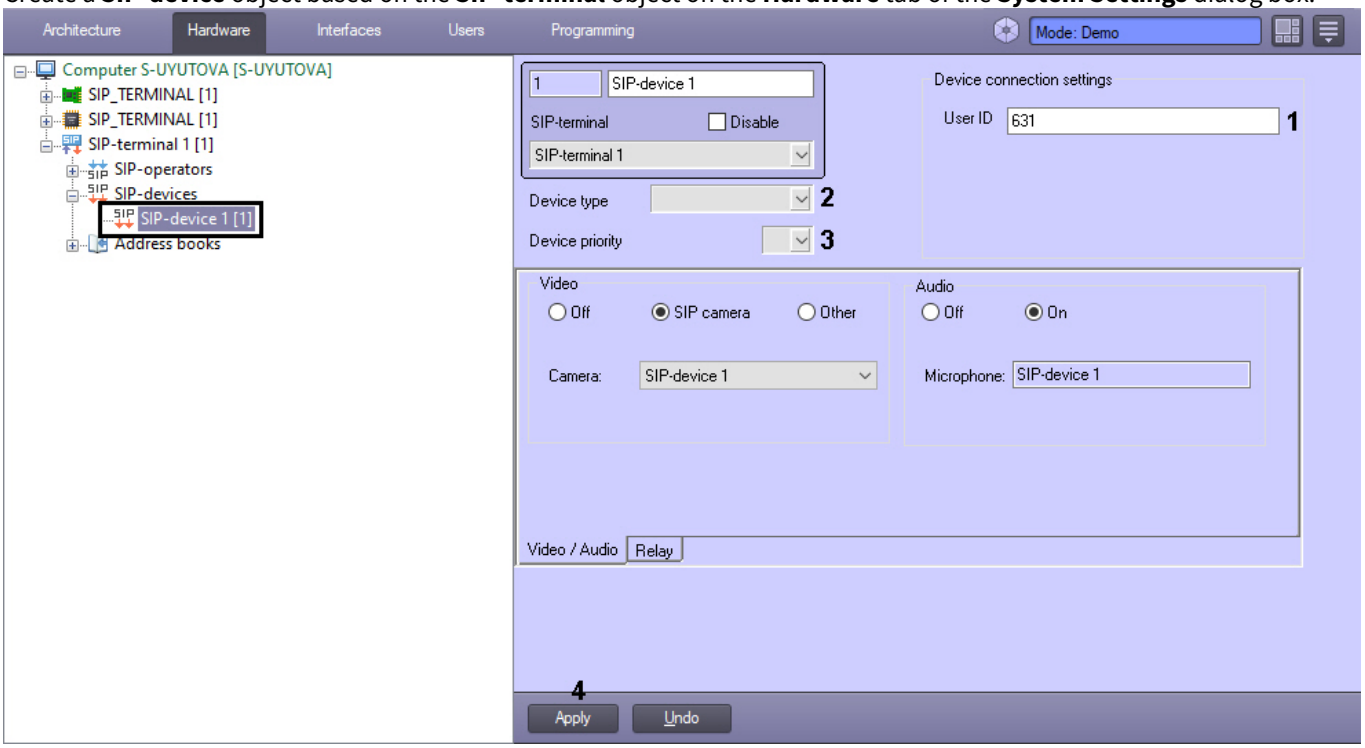
2. Set the **Terminal type** switch to the **SIP client** position (**1**) — the SIP-terminal acts as a client, it can be connected to any SIP-server (based on the *Intellect* or Asterisk software). If this terminal type is selected, the **Server connection settings** become editable.
3. In the **Address** field (**2**), specify the IP address of the SIP server.
4. In the **Port** field (**3**), specify the port for the SIP server connection.
5. In the **Terminal settings** group:
   a. From the **Network** drop-down list (**4**), select the IP address of the network adapter that will be used to connect to the network where the SIP clients are located.
   b. In the **SIP port** field (**5**), specify the port number which will receive the data from the SIP-clients.
   c. From the **SIP transport** drop-down list (**6**), select the transport level protocol to be used: TCP or UDP.
   d. If necessary, specify the RTP ports range in the corresponding text fields (**7**).
6. Click **Apply** (**8**).

The network settings of the *Intellect's* SIP client are set.

23.3.21.2.2 Configuring SIP-devices of the Intellect's SIP client

The SIP-device of the *Intellect's* SIP client is configured as follows:

1. Create a **SIP-device** object based on the **SIP-terminal** object on the **Hardware** tab of the **System Settings** dialog box.



2. In the **User ID** field (**1**), specify the SIP-device identification number, i.e. the number to call it.
3. From the **Device type** drop-down list (**2**), select the icon type used to display the device on the Map.
4. From the **Device priority** drop-down list (**3**), select the priority of calls from this device when displayed on the SIP panel. The lower the number, the higher the priority and, hence, the higher the call is displayed in the list. If the field is left blank, the priority is considered minimal. Calls from devices with the same priority will be sorted by the time of the call.
5. Click **Apply** (**4**).

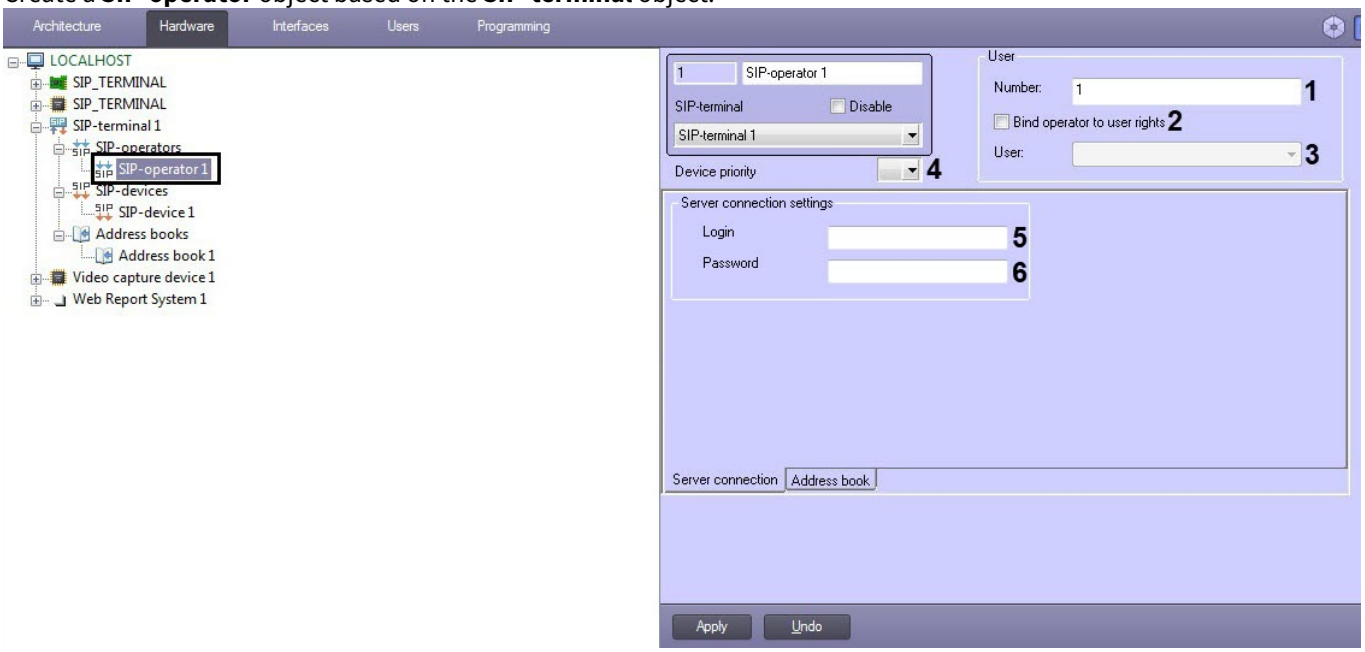
> **Note**
>
> The **Video / Audio** and **Relay** tabs are intended for configuring a SIP-device only for the **SIP server** terminal type (see Configuring SIP-devices of the Intellect's SIP server).

The SIP-device of the *Intellect's* SIP client is now configured.

23.3.21.2.3 Configuring SIP-operators of the Intellect's SIP client

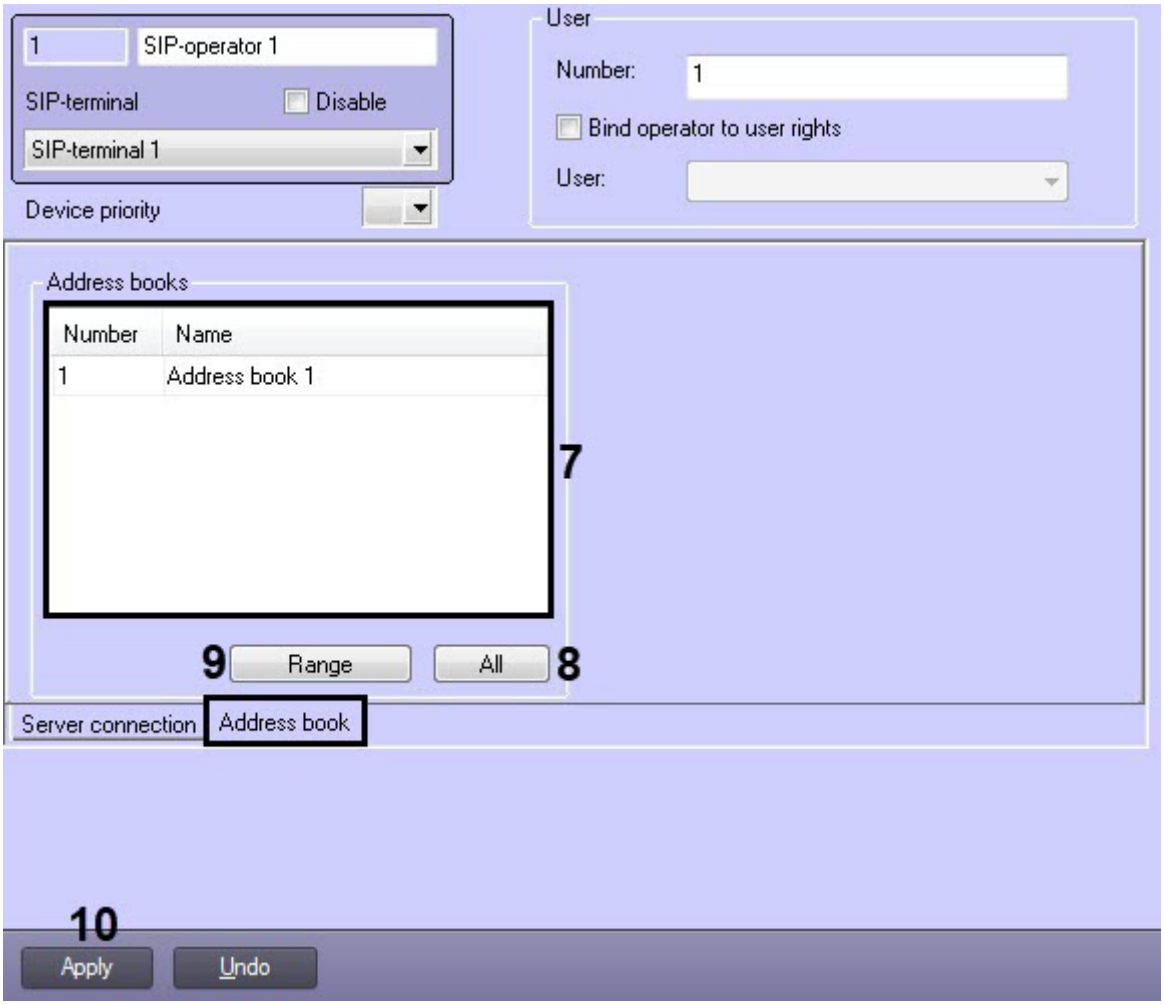
SIP-operators of the *Intellect's* SIP client are configured as follows:

1. Create a **SIP-operator** object based on the **SIP-terminal** object.



2. In the **Number** field (**1**) enter the identification number for calls.
3. If it is necessary to bind a SIP-operator to the *Intellect* user rights, set the **Bind operator to user rights** checkbox (**2**) and select the corresponding *Intellect* user from the **User** drop-down list (**3**). It is used when the **User rights** are selected by default on the operator's SIP panel.
4. From the **Device priority** drop-down list (**4**), select the priority of a call from this operator in the incoming calls window of the SIP panel. The lower the number, the higher the priority, hence, the higher the call is displayed in the list. If the field is left blank, the priority is considered to be minimal. Calls from operators with the same priority will be sorted by the time of the call.
5. In the **Login** field (**5**), enter the username for connecting to the SIP-server.
6. In the **Password** field (**6**), specify the password for connecting to the SIP-server.

7. Go to the **Address book** tab.

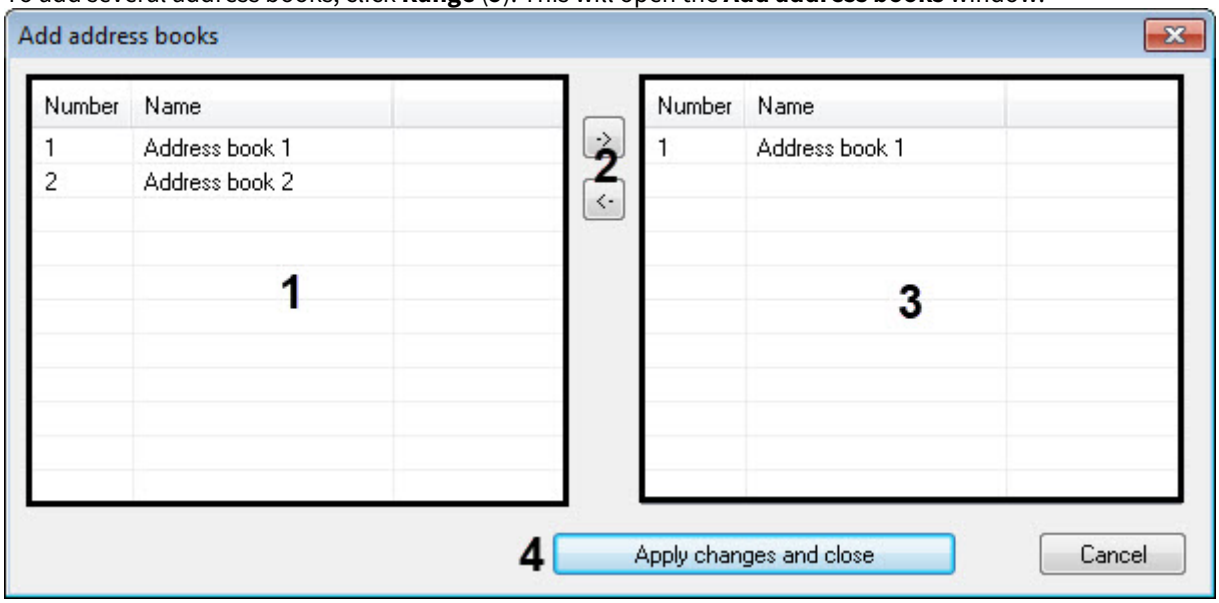


8. In the **Address books** table (**7**), select the required address books, the numbers of which should be available for this SIP-operator (see Configuring address book of SIP-terminal).

> **Note**
>
> To add new lines to the table, use the Down key on your keyboard. To delete a line, use the Ctrl+Del key combination.

   a. To add all address books, click **All** (**8**).

b. To add several address books, click **Range** (**9**). This will open the **Add address books** window.



i. Select the required address books from the left list (**1**) and use the buttons (**2**) to move them to the right list (**3**).
ii. Click the **Apply changes and close** button (**4**).

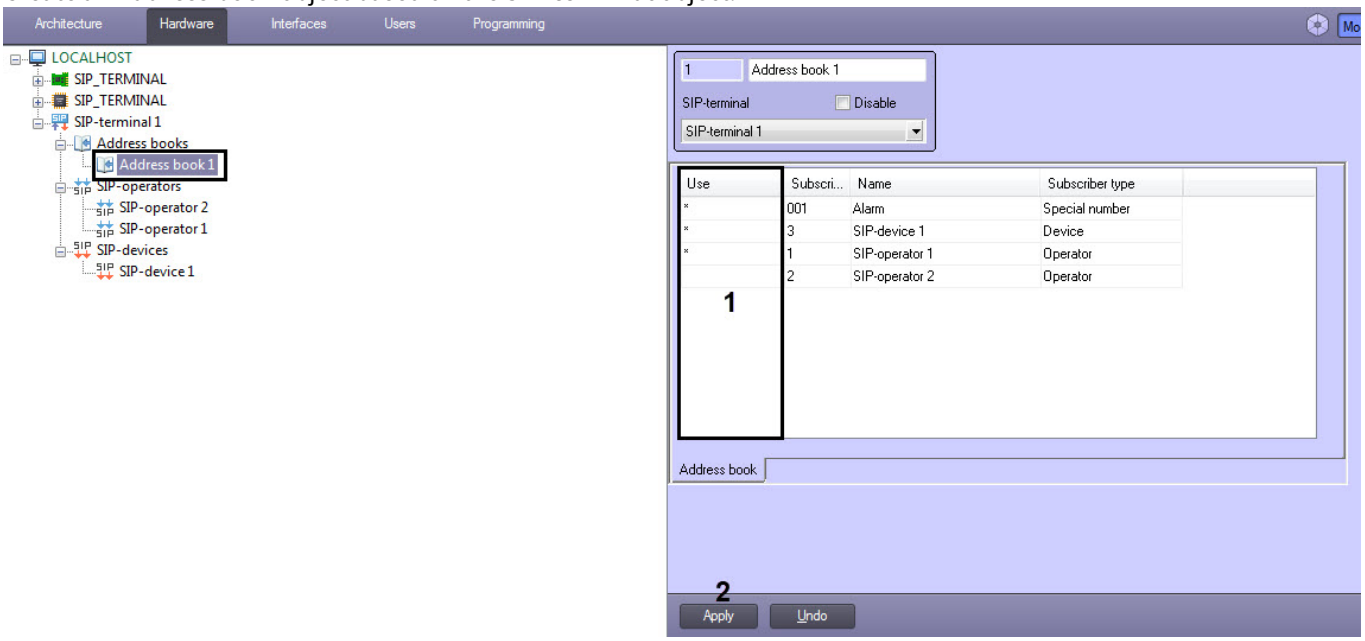
9. Click **Apply** (**10**).

The configuration of SIP-operators on the *Intellect* SIP-client is complete.

23.3.21.3 Configuring address book of SIP-terminal

The address book of SIP-terminal is configured as follows:

1. Create an **Address book** object based on the **SIP-terminal** object.



2. In the **Use** column (**1**), select the required subscribers (SIP-operators, devices or special numbers), whose numbers should be available in this address book.
3. Click **Apply** (**2**).

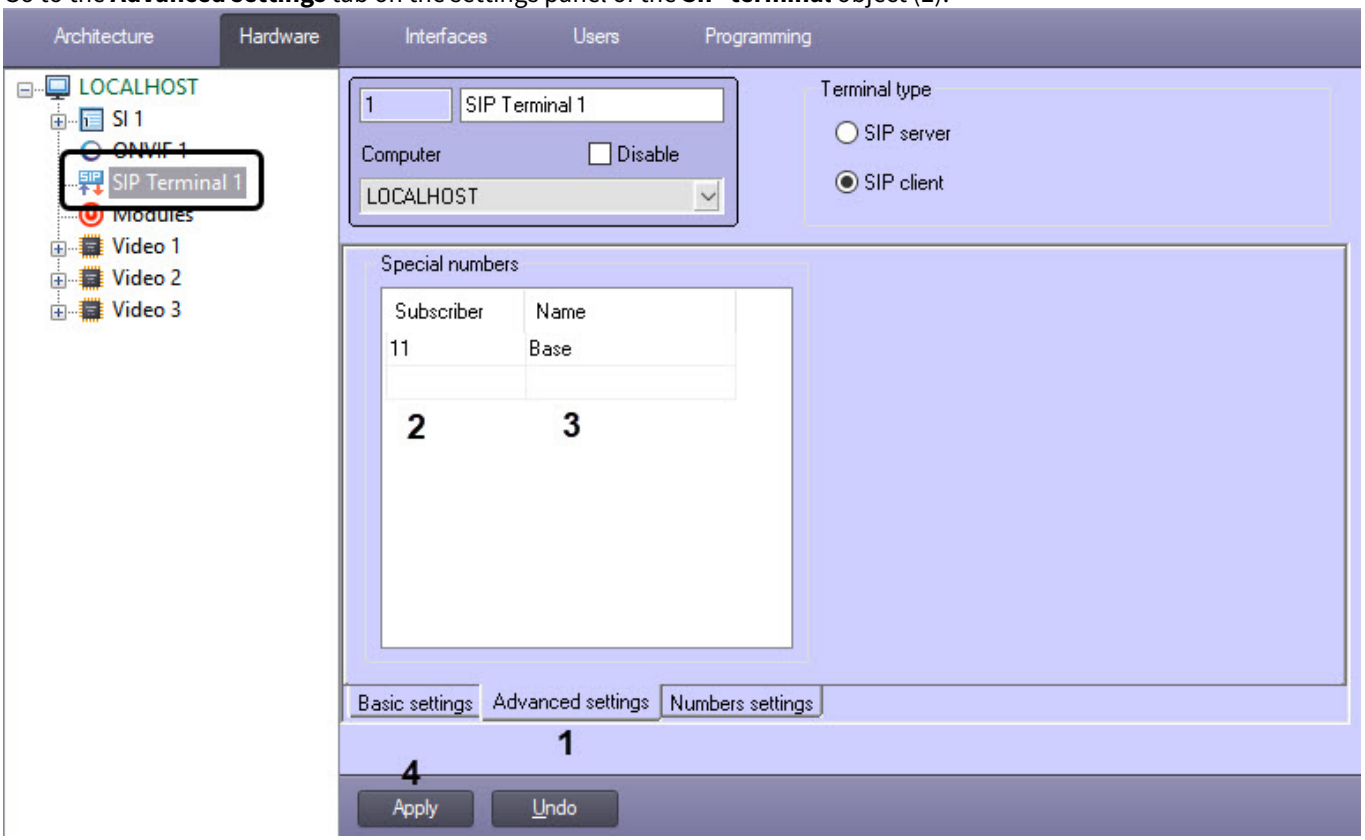
The address book of SIP-terminal is now configured.

23.3.21.4 Configuring special numbers of SIP-terminal

Special numbers do not correspond to certain devices or operators; they are designed to configure special functions, such as group calls or alarm messages.

The special numbers of the *Intellect*'s SIP-terminal are configured as follows:

1. Go to the **Advanced settings** tab on the settings panel of the **SIP-terminal** object (**1**).



2. Add special numbers to the **Special numbers** table:
   a. In the **Subscriber** field, enter a special number (**2**).
   b. In the **Name** field, enter the name of the special number (**3**).

   > **Note**
   >
   > To add new rows to the table, use the "Down" key on the keyboard. To delete a line, use the keyboard shortcut Ctrl + Del.

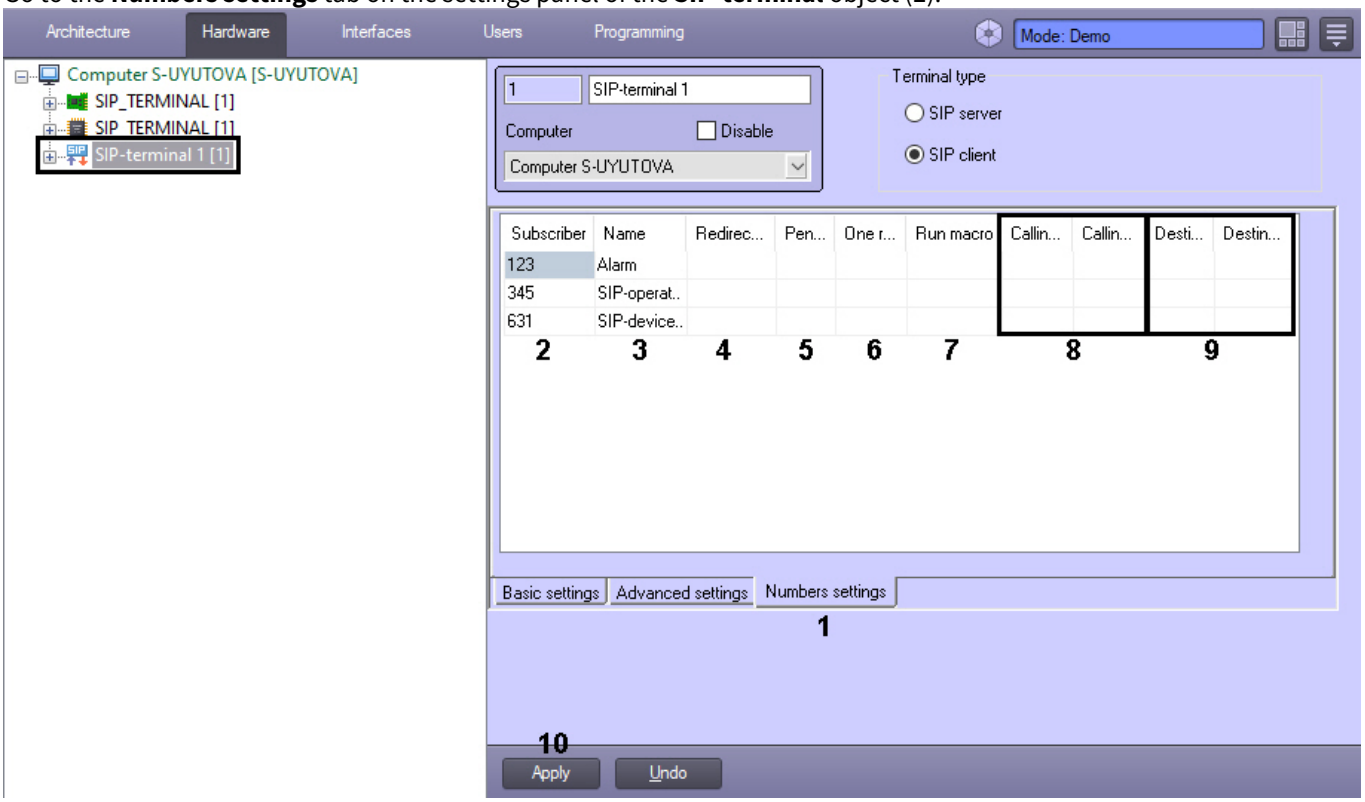
3. Click **Apply** (**4**).

The special numbers of the *Intellect*'s SIP-terminal are configured.

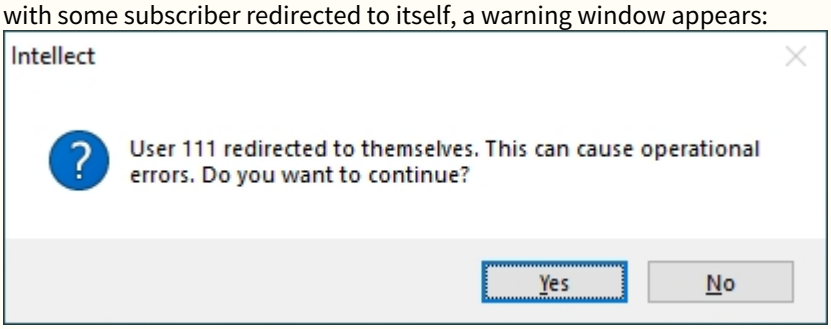
23.3.21.5 Configuring numbers of SIP-terminal

The numbers of the *Intellect*'s SIP-terminal are configured as follows:

1. Go to the **Numbers settings** tab on the settings panel of the **SIP-terminal** object (**1**).



2. The **Subscriber** column (**2**) lists the numbers of all devices and operators registered on the SIP-terminal, as well as special numbers.
3. The **Name** field (**3**) lists the names of the corresponding devices, operators, and special numbers.
4. In the **Redirecting** field (**4**), enter the number to which the corresponding subscriber's calls should be forwarded to. Several numbers can be specified separated with semicolon allowing the call redirection to several devices or operators. This option enables conference calls.

> **Important!**
>
> It is strongly not recommended to redirect subscribers to themselves, i.e. specify the same number in the **Redirecting** and **Subscriber** fields. The system may not work correctly in this case. When trying to save settings with some subscriber redirected to itself, a warning window appears:
>
> 
>
>
> Click **No** to clear the **Redirecting** field for affected subscribers or click **Yes** to continue configuration without changes.

5. In the **Pending, sec** field (**5**), enter the time period in seconds, during which it is necessary to wait for a response from the subscriber. If the value is not set in the field, it is defined by the CallTimeout registry key; 30 sec. by default (see Registry keys reference guide). The value greater than set by CallTimeout will not be applied, i.e. the least of **Pending, sec** and CallTimeout is selected as a timeout.
6. If several numbers were specified in the **Redirecting** field, and only one device or operator should be able to answer the call, set the **One responder** checkbox (**6**). When the checkbox is not set, the call can be answered by any and all devices and/or operators as per the redirecting list; this is the way to implement conference calls. When the checkbox is set, the

call comes to all devices and/or operators until any one of them answers it to end the call for all the other devices and/or operators.

7. From the **Run macro** drop-down list (**7**), select the **Macro** object which should be run when calling the subscriber. See also Creating and configuring Macro events and Macros for working with SIP-terminal.
8. In the **Calling number multicast (video)** / **Calling number multicast (audio)** fields (**8**), specify the IP address for broadcasting the video stream and audio stream from the calling device in the multicast mode.
9. In the **Destination number multicast (video)** / **Destination number multicast (audio)** fields (**9**), specify the IP address for broadcasting the video stream and audio stream from the destination device in the multicast mode.
10. Click **Apply** (**10**).

The numbers of *Intellect*'s SIP-terminal are configured.

23.3.21.6 Macros for working with SIP-terminal

The SIP-terminal functionality in *Intellect* can be expanded using the flexible macro configurations - see Creating and using macros. Below is a description of the main available macros and their parameters.

> **Attention!**
>
> Macros are paired, i.e. if a macro is created for an outgoing call, then it is necessary to create a macro for ending a call.

Macro	Parameter	Description
SIP-terminal object		
Outgoing call	operator's camera id	Identification number of the operator's camera If not specified, the camera of the selected operator will be used
	operator's microphone id	Identification number of the operator's microphone **Attention!** The parameter is required
	called subscriber	The identification number of the subscriber (operator or device) which rec **Attention!** The parameter is required
	calling user (operator)	The identification number of the subscriber (operator or device) which ma **Attention!** The parameter is required
	file playback volume	The playback volume of the selected file (see the **playback file** parameter)
	play file on loop	Specifies whether the file should play once (the **no** value) or on a loop until
	call ID	The unique identifier of the call in the system; it is used to end the call. **Attention!** The parameter is required

	multicast address for outgoing video	IP address and port to send video in "multicast" mode. For example, 224.0.
	multicast address for outgoing audio	IP address and port to send audio in "multicast" mode. For example, 224.0
	playback file	The full path to the .wav file which should play when receiving a call.
Group call	operator's camera id	Identification number of the operator's camera If not specified, the camera of the selected operator will be used
	operator's microphone id	Identification number of the operator's microphone **Attention!** The parameter is required
	called subscribers	The identification numbers of subscribers separated by ";" participating in
	calling user (operator)	The identification number of the subscriber (operator or device) which mal **Attention!** The parameter is required
	volume of file being played	The playback volume of the selected file (see the playback file parameter),
	play file on loop	Specifies whether the file should play once (the **no** value) or on a loop until
	group call ID	The unique identifier of the group call in the system; it is used to end the ca **Attention!** The parameter is required
	one responder	If **No** is selected, then one call can be answered by several operators or dev by any operator and device, after which it will be automatically ended for c
	playback file	The full path to the .wav file which should play when receiving a call.
End a call	call ID	The unique identifier of the call in the system, specified when initiating the
End all calls	-	-
SIP-device and **SIP-operator** objects		
A call (make/receive)	-	-
End a call	-	-
Hold	-	-

Note

Loop playback of long and short beeps, as well as the files "There is an unanswered call" and "Call on hold" can be configured using the registry keys **wavCallLooped**, **wavWaitLooped**, **wavTryingLooped**, **wavBusyLoopedCount** (see Registry keys reference guide).

23.3.21.7 Selecting speaker, microphone and camera for SIP-operator

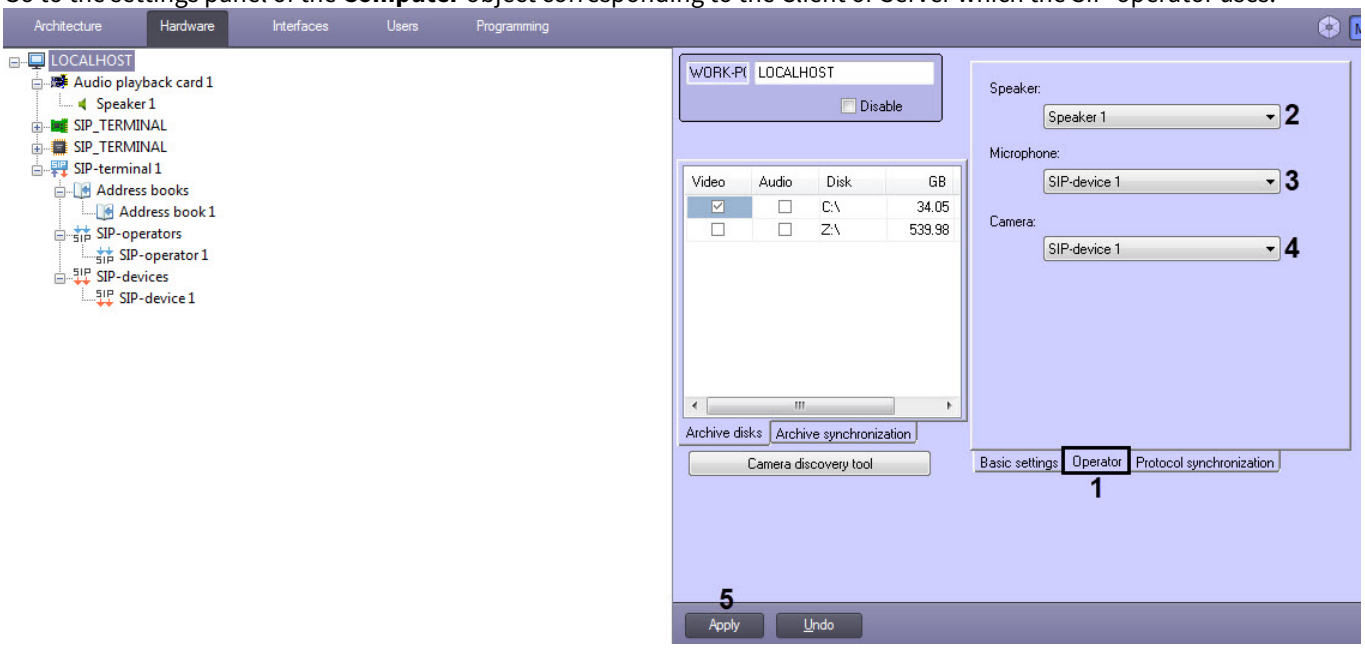
The speaker, microphone and camera are selected for calls via the SIP-panel.

Before selecting those, create and configure the corresponding objects as described in the following sections:

1. Creating and configuring the Speaker object
2. Creating and configuring the Microphone object
3. Configuring video acquisition from IP devices (for IP camera) or Creating and configuring the Camera object (for analog camera).

Having the objects created and configured, proceed as follows:

1. Go to the settings panel of the **Computer** object corresponding to the Client or Server which the SIP-operator uses.



2. Go to the **Operator** tab (**1**).
3. Select the operator's speaker from the **Speaker** drop-down list (**2**).
4. Select the operator's microphone from the **Microphone** drop-down list (**3**).
5. Select the operator's camera from the **Camera** drop-down list (**4**).
6. Click **Apply** (**5**).

Selecting a speaker, microphone and camera for SIP-operator is now complete.

23.3.21.8 Configuring SIP trunk

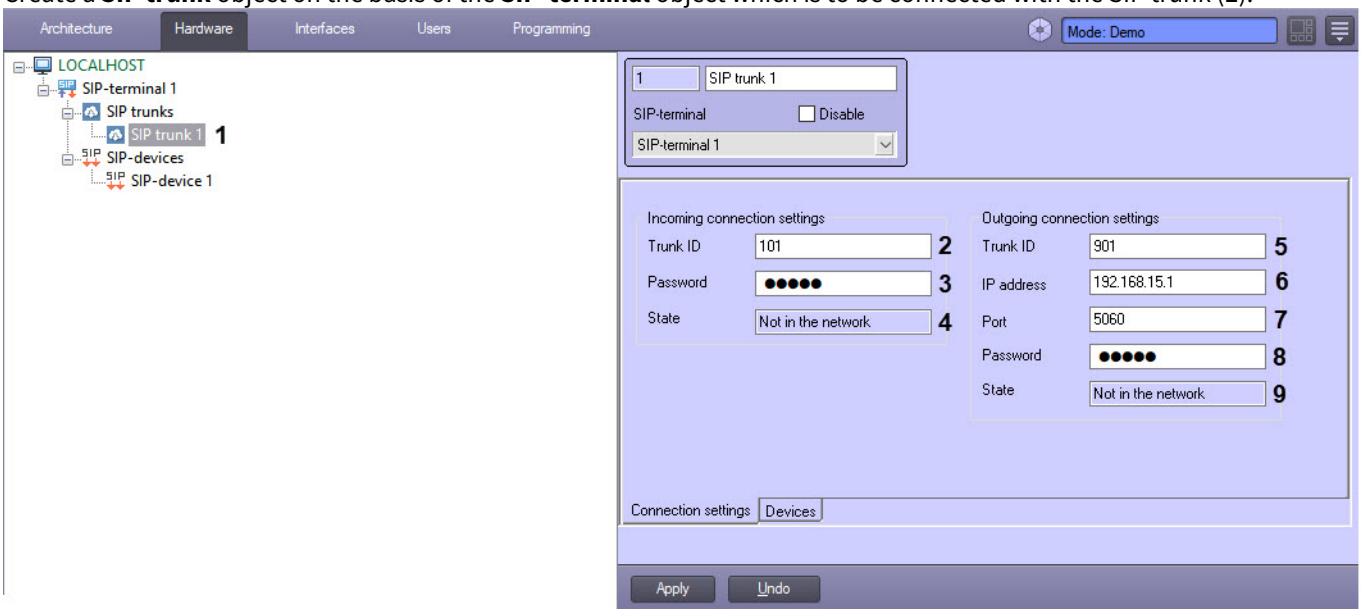
A SIP trunk is used to create a virtual communication channel between two SIP servers. It can be two *Intellect* SIP servers, or the *Intellect* SIP server and a third-party SIP server.

Before you start configuring the SIP trunk, it is necessary to add to *Intellect* the SIP-devices of a third-party server based on the same SIP-terminal on which the SIP trunk will be added (see Configuring SIP-devices of the Intellect's SIP server).

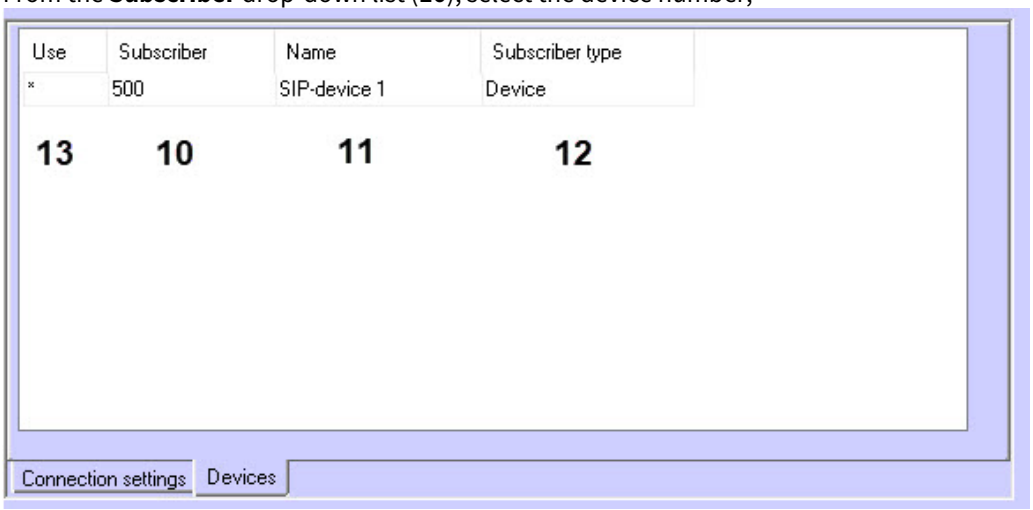
In the following description of the SIP trunk configuration procedure, the connection between the *Intellect* SIP server and a third-party SIP server is used as an example.

The SIP trunk is configured as follows:

1. Create a **SIP trunk** object on the basis of the **SIP-terminal** object which is to be connected with the SIP trunk (**1**).



2. On the **Connection settings** tab, in the **Incoming connection settings** group:
   a. In the **Trunk ID** field (**2**), specify the ID of the third-party SIP server that is registered in *Intellect*;
   b. In the **Password** field (**3**), enter the password for connecting to a third-party SIP server;
   c. The **State** field (**4**) displays the current status of the registered SIP server.
3. On the **Connection settings** tab, in the **Outgoing connection settings** group:
   a. In the **Trunk ID** field (**5**), specify the ID of the *Intellect* SIP server, which is registered on a third-party SIP server;
   b. In the **IP address** field (**6**), enter the IP address of the third-party SIP server;
   c. In the **Port** field (**7**), specify the port of the *Intellect* SIP server;
   d. In the **Password** field (**8**) specify the password for connecting to the *Intellect* SIP server;
   e. The **State** field (**9**) displays the current status of the *Intellect* SIP server.
4. On the **Devices** tab, select the devices of the third-party SIP server that will be used on the *Intellect* SIP server:
   a. From the **Subscriber** drop-down list (**10**), select the device number;



   b. The **Name** (**11**) and **Subscriber type** (**12**) fields will display the device name and type, respectively;
   c. In the **Use** column (**13**), put ***** (asterisk) in front of the devices that will be used.
5. Click the **Apply** button.

> **Note**
>
> After you click the Apply button, the specified settings will be sent to the second server, and the registration will be received from it, that is, the connection will be updated. Then, the connection will be updated every 10 minutes. You can change this time interval using the **ClientExpires** key (see Registry keys reference guide).

The SIP trunk is configured.

> **Attention!**
>
> To ensure the SIP trunk operation, it is necessary that similar settings are made on the server, with which the communication should be set.

23.3.21.9 Configuring a SIP-terminal for Failover service

If **Failover service** is used in *Intellect*, then in order to maintain the operability of IP telephony if the connection with the main server is lost, it is necessary to configure the transfer of the SIP-terminal configuration to the backup server as follows:

1. Add the objects that should be transferred to a backup server in case of connection loss to **Failover service** (see Configuring Failover service).
2. In the sip_terminal.config file located on the backup server, specify the IP address of this backup server: <sip_ip>IP_address_of_backup_server</sip_ip>.
   By default, the file is located in the <Intellect installation directory>\Modules folder. It should be filled out and saved in the same folder. Below is an example of a filled out file for a backup server with an IP address of 192.168.0.187:

   ```
   <?xml version="1.0"?>
   <configuration>
       <sip_ip>192.168.0.187</sip_ip>
   </configuration>
   ```

   > **Note**
   >
   > The operation principle is as follows: if **Failover service** is enabled, the value from this file will be used, and the current network settings of the **SIP-terminal** will be ignored. Therefore, it is not necessary to change the network settings in the **SIP-terminal** after enabling **Failover service**.
3. In the web interface of SIP devices used in the IP telephony configuration, specify the same IP address of the backup server as an additional address of the main SIP server.

As a result, if the connection with the main server is lost, the IP telephony configuration will be transferred to the backup server and it will remain operational.

23.3.22 Configuring Incident server and Incident handler

The **Incident server** is used for storing events that need to be processed using the **Incident handler**. By default, **Incident server** events are stored in the PROTOCOL_INC_SERVER table of the *Intellect* database. The event storage period is set using the **Events archive length** setting of the **Computer** system object (see Configuring events logging).

The **Incident handler** is used for selecting the events to be processed, and for configuring the processing rules for the Operator.

Both of these modules are required for the **Incident manager** interface object operation—using the **Incident manager**, the Operator can process events according to the specified rules.

The **Incident server** and **Incident handler** are configured as follows:

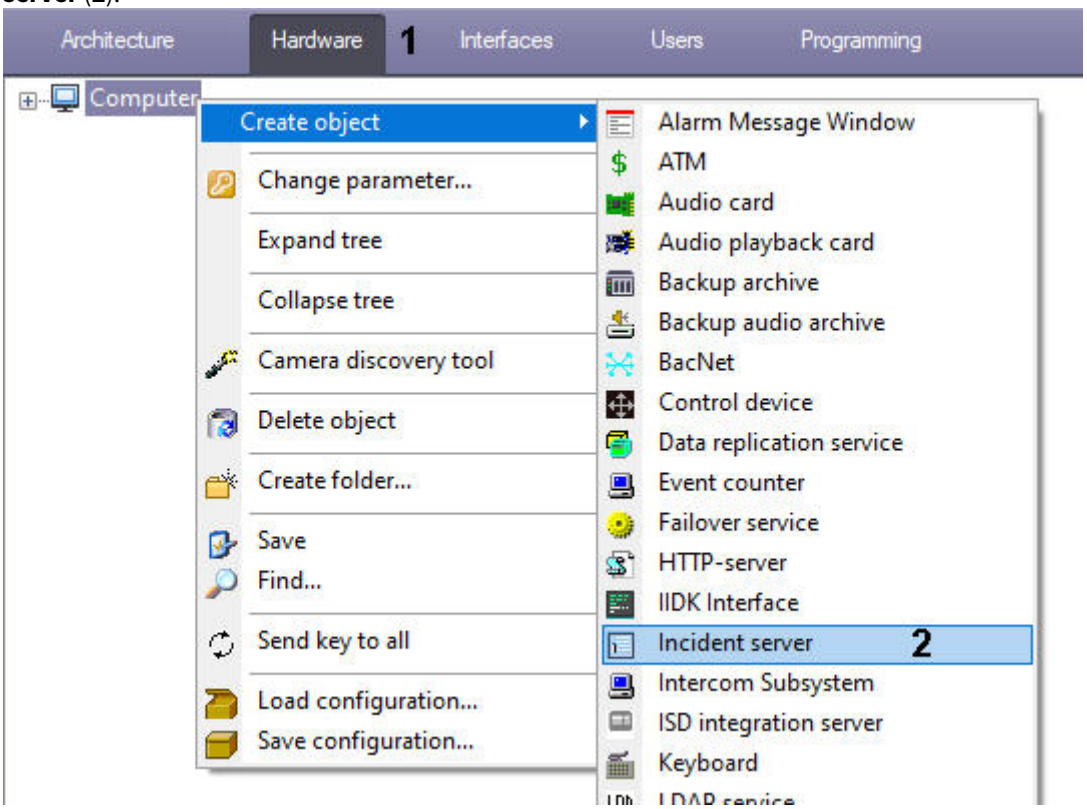
1. Create the **Incident server** and **Incident handler** objects (see Creating the Incident server object, Creating the Incident handler object).
2. Configure the logic of event handling (see Creating and configuring the logic of event handling).
3. Set the event priority (see Setting the events priority).
4. Select the events that need to be handled (see Selecting events to display and handle).
5. Configure the display of logic (see Configuring the display of logic).
6. If it is necessary to use a non-default database to store events, configure the connection to the required database (see Configuring the use of an external database).

Configuring the Incident manager interface object
Events control and processing using the Incident manager

23.3.22.1 Creating the Incident server object

To create the **Incident server** object, do the following:

1. Select the required **Computer** object on the **Hardware** tab of the **System settings** dialog box (**1**).
2. Right-click on the selected **Computer** object and in the context menu that appears, select **Create object** -> **Incident server** (**2**).



3. In the window that appears, enter the number and name of the **Incident server** object.

4. Click the **Apply** button.

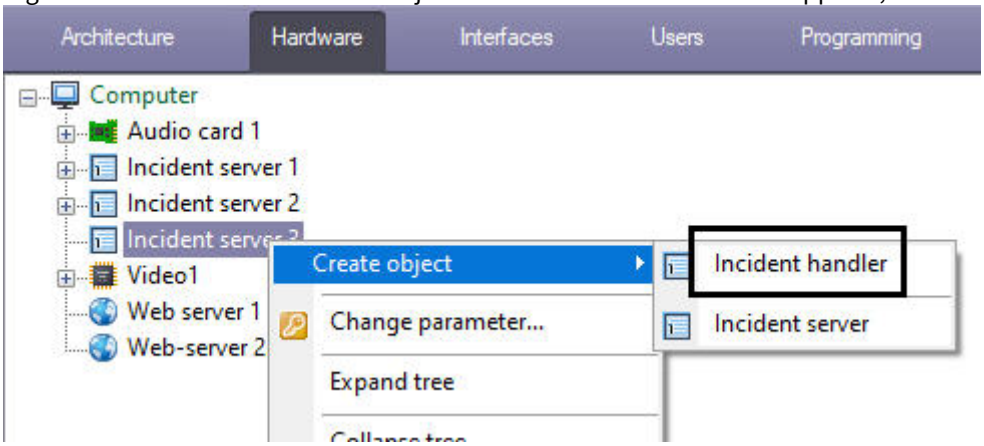
The **Incident server** object is created.

23.3.22.2 Creating the Incident handler object

To create the **Incident handler** object, do the following:

1. Go to the **Hardware** tab of the **System settings** dialog box.

2. Right-click on the **Incident server** object and in the context menu that appears, select **Create object** -> **Incident handler**.



3. In the window that appears, enter the number and name of the **Incident handler** object.

4. Click the **Apply** button.

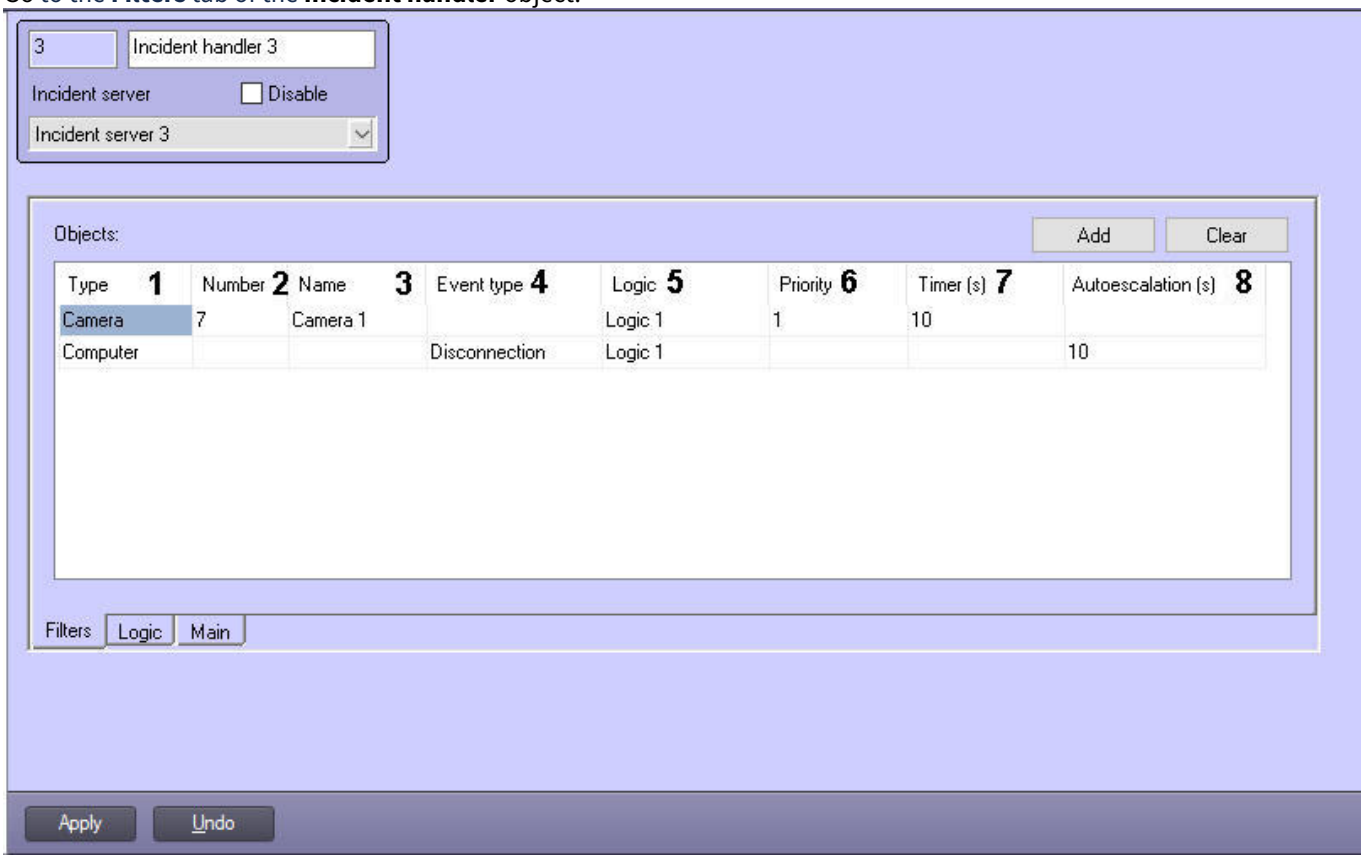
The **Incident handler** object is created.

23.3.22.3 Selecting events to display and handle

By default, no events are displayed in the **Incident manager**. It is necessary to explicitly specify the objects, the events from which should be received and processed.

This can be done in two ways: events can be selected as a group (this method is described in Displaying and handling events in bulk), or each event can be selected individually in the following way:

1. Go to the **Filters** tab of the **Incident handler** object.



2. In the **Objects** table, specify the objects, the events from which should be received and processed. If no objects are selected, no events will be displayed in the **Incident manager**.
   a. From the list in the **Type** column (**1**), select the object type.
   b. From the list in the **Number** column (**2**), select the object identification number. If the object number is not specified, events from all objects of the specified type will be logged. After you select the object type and number, the **Name** field (**3**) will be automatically filled in with the object name.
   c. From the list in the **Event type** column (**4**), select the events to be displayed in the **Incident manager**. If the event type is not specified, all events of the selected object will be sent to the module.
   d. In the **Logic** list (**5**), select the logic that will be used to process the events of the selected object. Logics are created and configured on the **Logic** tab (see Creating and configuring the logic of event handling).

      Attention!

      It is required to select the logic, otherwise the object's events will not be displayed.

   e. In the **Priority** drop-down list (**6**), select the priority level for the events of the selected object (see Setting the events priority). The priority can be used by the operator to sort the events. If no priority is selected, priority level **0** will be used.
   f. In the **Timer (s)** field (**7**), set the time in seconds from the moment the event occurred, after which the **Time is over** event will be generated. The timer will also count down the specified time in the interface in the **Time(sec)** column until it reaches zero.

      Note

      If grouping is enabled, then for groups the timer will apply to the last generated event with the specified timer.

   g. In the **Autoescalation (s)** field (**8**), specify the time in seconds from the moment the event occurs, after which the event will be automatically escalated. Autoescalation is performed within one **Incident handler** and works if the operator has the escalation rights (see Configuring user rights in Incident manager).

> **Note**
>
> If grouping is enabled, autoescalation is applied to each event separately.

3. Repeat the actions described in step 2 for all required objects.

> **Note**
>
> To add a row to the table, select the last row and press the ↓ key on the keyboard. To delete rows from the table, use the Ctrl + Del key combination.
> To clear the objects table, click the **Clear** button.

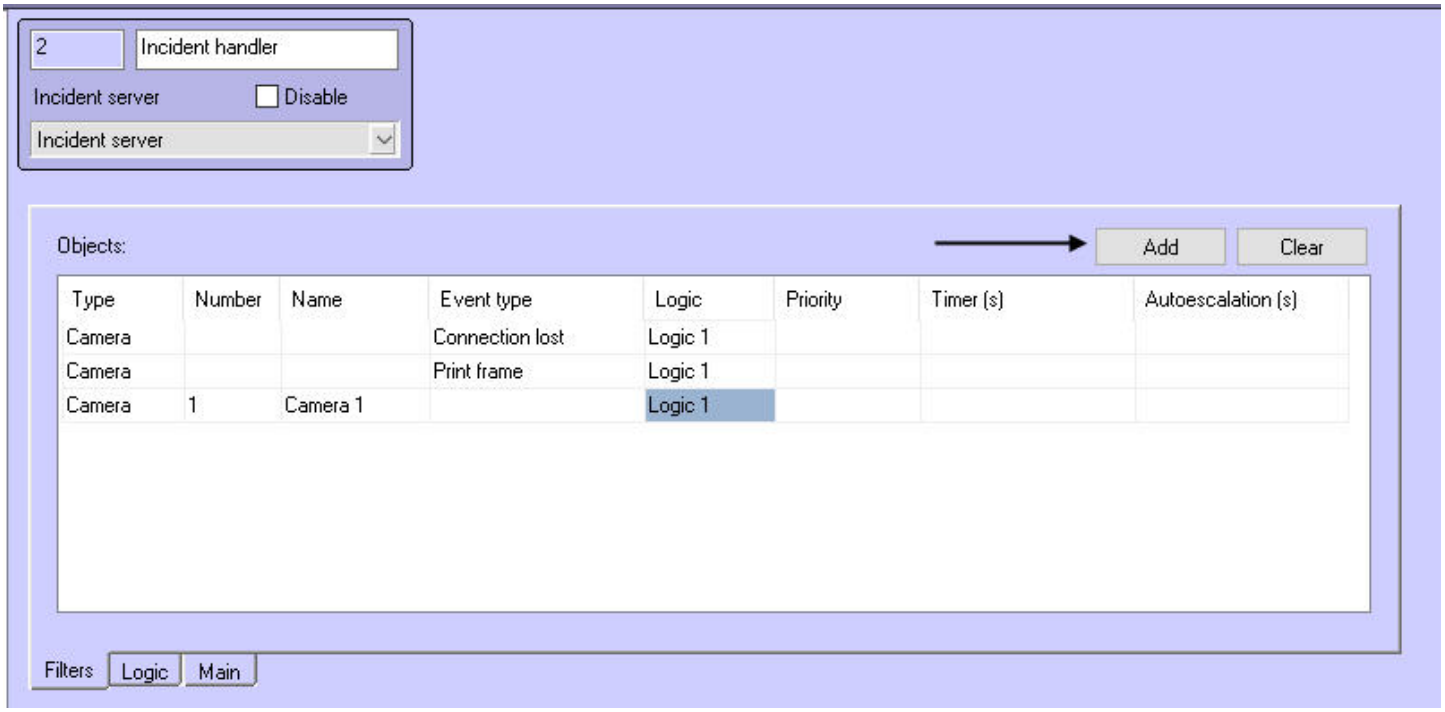
4. Click the **Apply** button.

As a result, the **Incident manager** will display the events from the objects that were selected on the **Filters** tab of the **Incident handler**.

23.3.22.3.1 Displaying and handling events in bulk

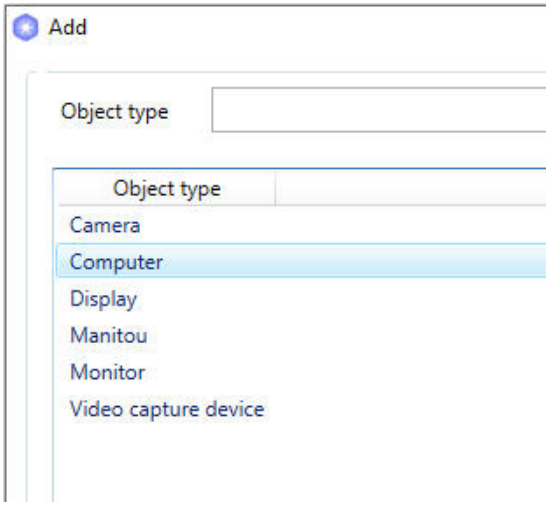
You can specify the objects from which you want to receive and handle events in the **Incident manager** in two ways: each event separately (this method is described in Selecting events to display and handle) or several events at once—this method is described below.

To add events as a group to the **Incident handler**, use the **Add** window that opens after clicking the **Add** button on the **Filters** tab of the **Incident handler** object:

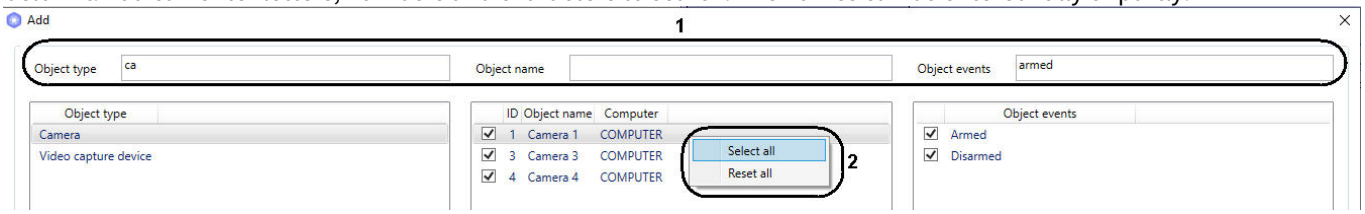


23.3.22.3.1.1 Functions used in this window

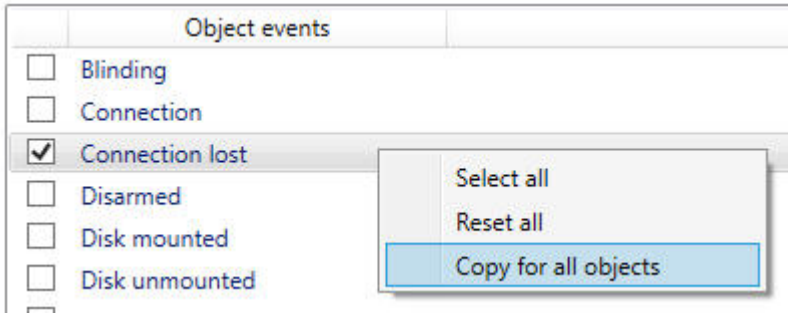
1. You can select only one of the specified object types (you cannot select several at once), because different events are used for different object types. All types of objects that are available in your *Intellect* software will be listed in the table:



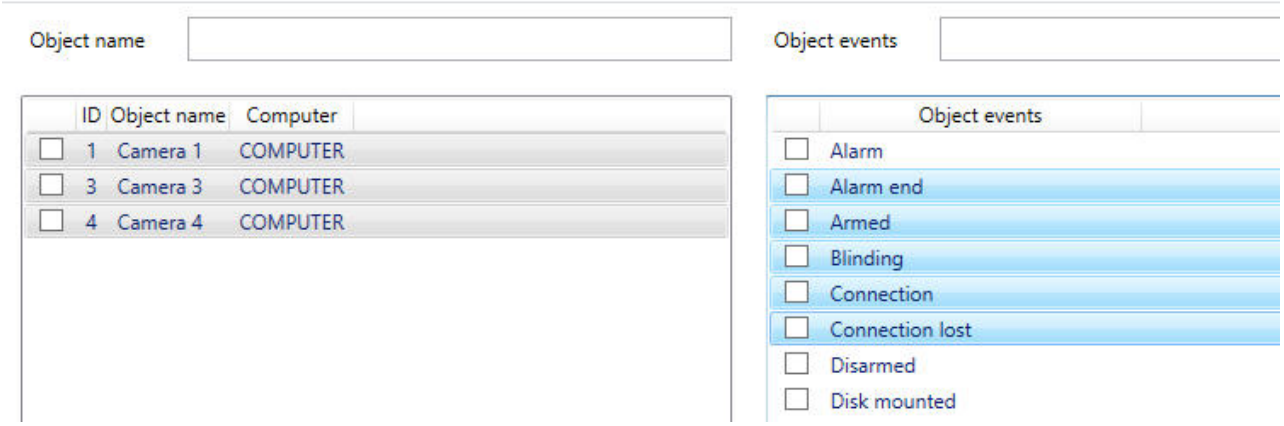
2. You can use the line with filters (**1**) to quickly find the required objects and events. Each filter applies only for the table below it. You can enter letters, numbers and characters to search. The names can be entered fully or partly.



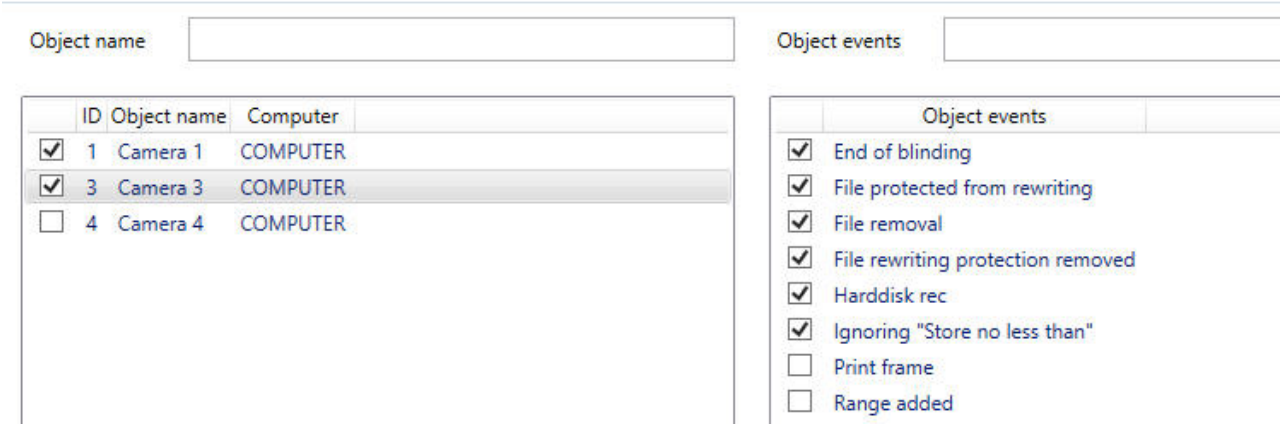
3. To set the checkboxes next to all names of objects of a particular type, right-click in any place of the **Object name** table, and in the context menu, click **Select all**. To clear all checkboxes, click **Reset all** (**2**).
4. To set/clear the checkboxes next to all events, you can click **Select all**/**Reset all** in the context menu of the **Object events** table. You can also select certain events for one object, and then copy the selection to other objects of this type. To do this, select **Copy for all objects** from the context menu. For example: **Camera 1** has the checkboxes set only next to the **Disarmed** and **Connection lost** events. After you click **Copy for all objects** in the context menu, only the checkboxes next to the **Disarmed** and **Connection lost** events will be set for all **cameras**.



5. You can select objects and events in two ways:
   a. Select them with the Ctrl key pressed. In this case, the lines of the selected objects and events will be highlighted in gray and blue:



b. Set the checkboxes next to the required objects and events:

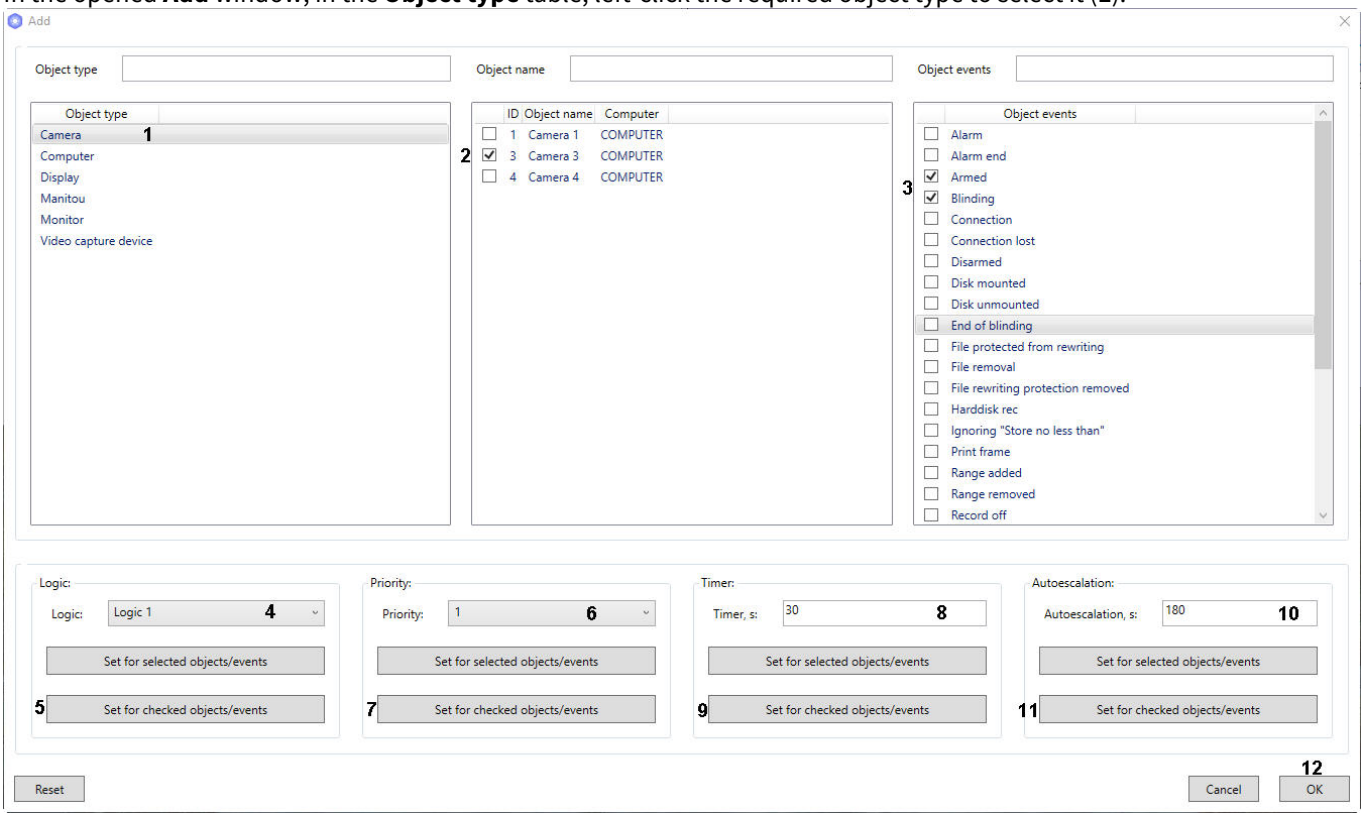


6. As a result, the buttons for setting **Logic**, **Priority**, **Timer**, and **Autoescalation** will be different:
   a. The Set for selected objects/events button applies the selected setting only for the objects and events that were selected with the Ctrl key pressed (regardless of the selection color—blue or gray);
   b. The Set for checked objects/events button applies the selected setting only for the objects and events next to which the checkboxes are set. ☐ The setting doesn't apply to objects and events highlighted in blue.
7. Depending on how you select the required **Object name**, the **Object events** table will display the following events:
   a. the events from the object selected by clicking its name. If several objects are selected in the **Object name** table, the events are displayed for the object that was selected first.
   b. the events from the object next to which the checkbox is set. If several checkboxes are set, the events from the object selected last will be displayed.
8. To clear all checkboxes in all tables, click the Reset button in the lower left corner. To exit without saving the changes, click the Cancel button.

23.3.22.3.1.2 Order of adding events to the Incident handler

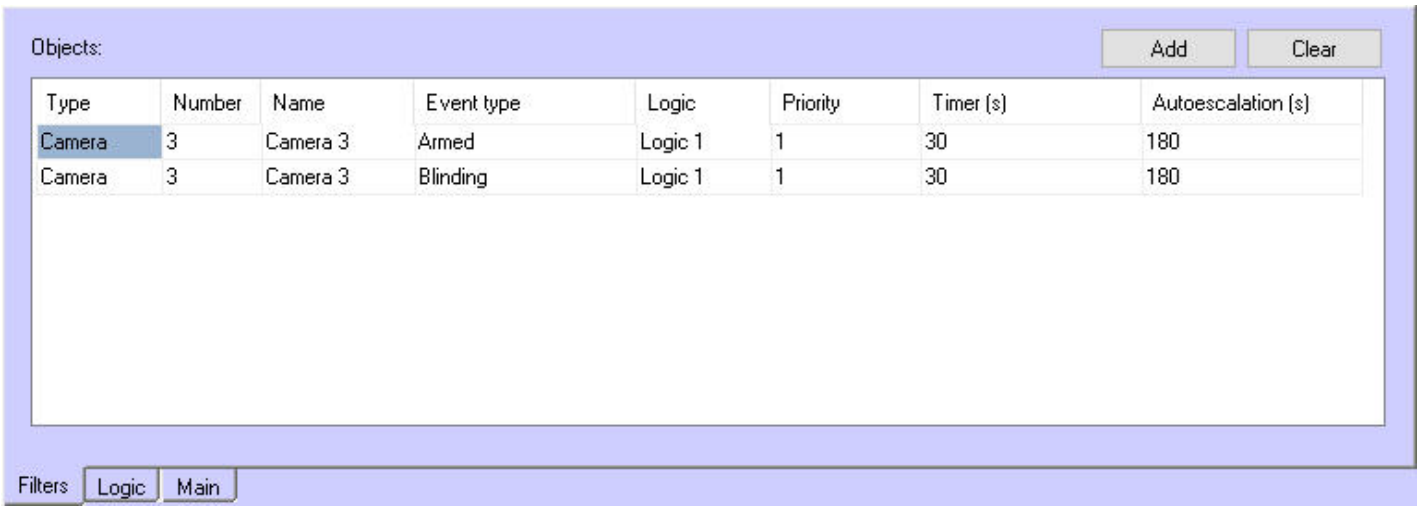
1. On the **Filters** tab of the **Incident handler** object, click the **Add** button.

2. In the opened **Add** window, in the **Object type** table, left-click the required object type to select it (**1**).



3. In the **Object name** table, set the checkbox next to the name of the object, the events from which you want to add (**2**).
4. The **Object events** table will display all possible events for this object. Select the events for displaying and handling by setting the checkboxes next to the necessary ones, without highlighting the line with color (**3**).
5. If necessary, set the **Logic** for the selected object events (the Logic must be created beforehand, see Creating and configuring the logic of event handling):
    a. Select the required **Logic** from the drop-down list (**4**);
    b. Click the **Set for checked objects/events** button (**5**).
6. If necessary, set the **Priority** (**6**, **7**), **Timer, s** (**8**, **9**), and **Autoescalation** (**10**, **11**), similar to **Logic**—see the previous step. The functionality and options for these settings are described in detail in Selecting events to display and handle.
7. Repeat steps 2-6 for all required objects.
8. Click the **OK** button (**12**).

As a result, the selected object events will be added to the **Filters** tab of the **Incident handler** with the specified logic, priority, timer and autoescalation settings. The example in the figure below shows the result after you click the **OK** button:



To save the result, click the Apply button.

Similarly, you can add events by selecting the required objects and events by clicking them (to select several at once—by clicking them with the Ctrl key pressed). In this case, to set the **Logic**, etc., the **Set for selected objects/events** button is used.

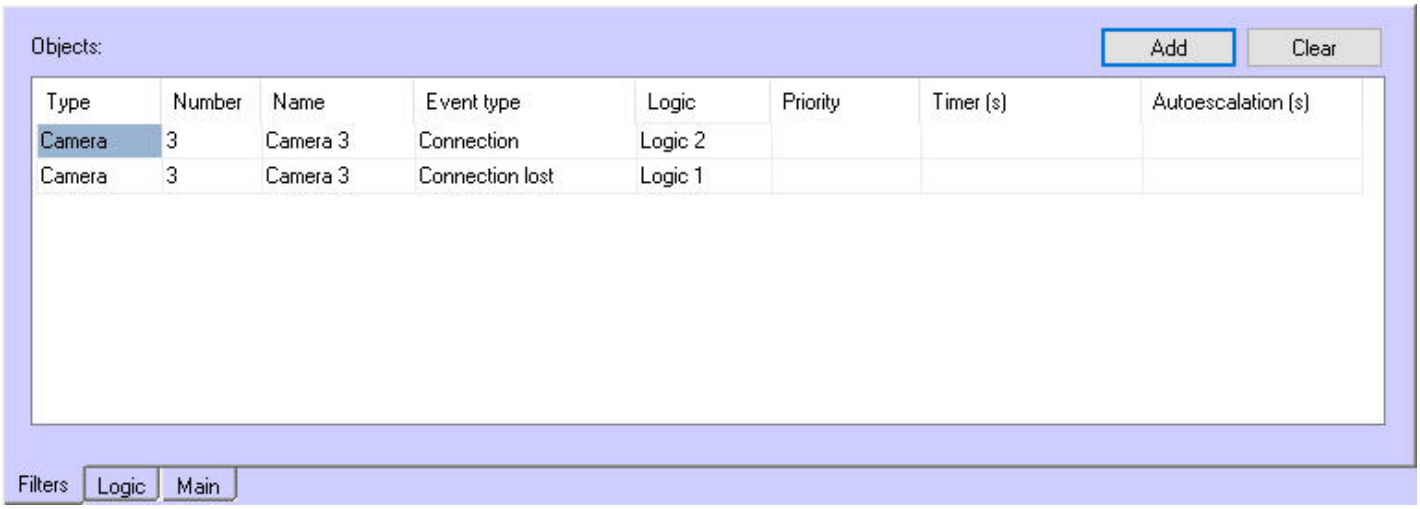
You can also combine checkboxes and object/event selection. Examples:

Task 1: Set different **Logics** (1 and 2) for the **Connection** and **Connection lost** events of the Camera 3.

Solution:

1. Select the **Camera** object type and select **Camera 3** object name by left-clicking.
2. Set the checkbox next to the **Connection lost** event.
3. Select **Logic 1** from the drop-down list and click the **Set for checked objects/events** button below it.
4. Set the checkbox next to the **Connection** event and highlight it with color by clicking it.
5. Select **Logic 2** from the drop-down list and click the **Set for selected objects/events** button below it.
6. Click the **OK** button.

The result:

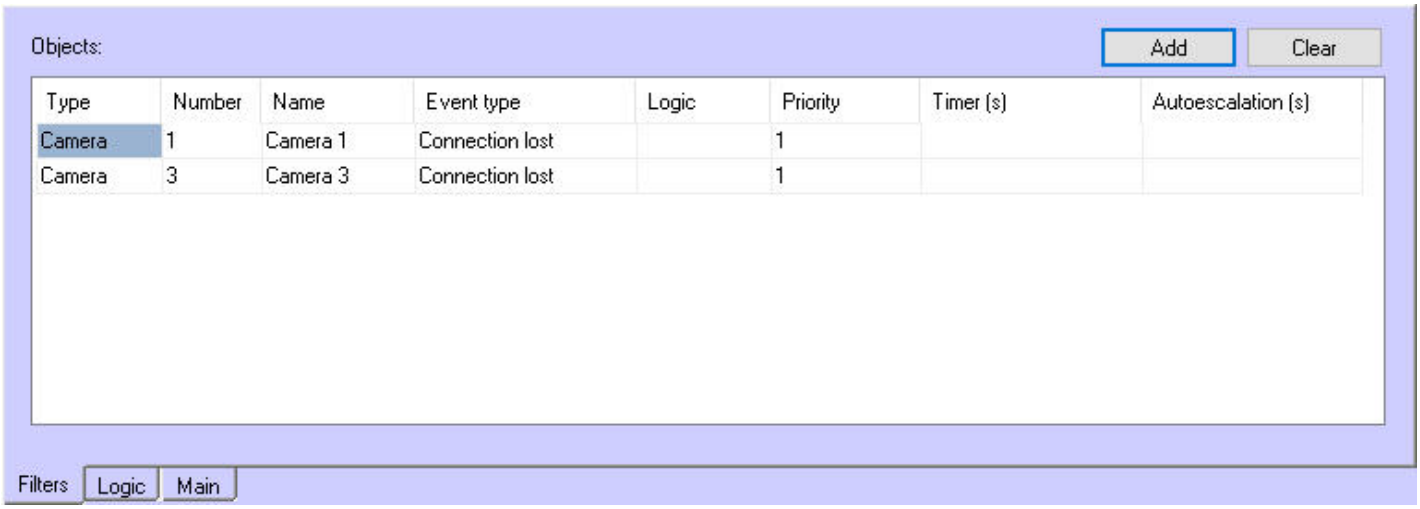


Task 2: Set the **Priority** "1" for the **Connection lost** event for all cameras that have this event selected.

Solution:

1. Select the **Camera** type and by clicking with the Ctrl key pressed, select **Camera 1** and **Camera 3** in the Object name table.
2. Set the checkbox next to the **Connection lost** event.
3. Select **Priority 1** from the drop-down list and click the **Set for checked objects/events** button below it.
4. Click the **OK** button.

The result:

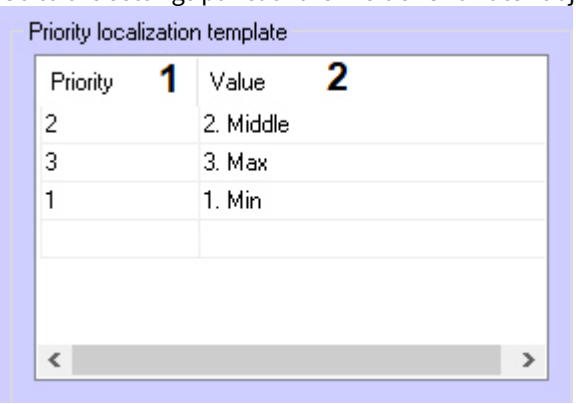


23.3.22.4 Setting the events priority

Each type of event in the **Incident handler** can be assigned a priority by which the operator can sort the events. By default, events have zero priority.

To do this:

1. Go to the settings panel of the **Incident handler** object and select the **Main** tab.



2. Add the required number of priorities to the **Priority localization template** table. To add a row to the table, select the last row and press the ↓ key on the keyboard. To delete rows from the table, use the Ctrl + Del key combination.
    a. The **Priority** column (**1**) is used to set the priority level.
    b. The **Value** column (**2**) is used to set the priority description. If the priority description is set, then it will be displayed in the **Incident handler**, otherwise the priority level will be displayed.

> **Note**
>
> Create zero priority only if it is necessary to set a description for it that will be displayed in the **Incident handler**.

3. For each type of event, set the level of the corresponding priority (see Selecting events to display and handle).
4. Click the **Apply** button.

23.3.22.5 Creating and configuring the logic of event handling

The logic of event handling is a sequence of actions that should be performed by an operator when processing an event in the **Incident manager**.

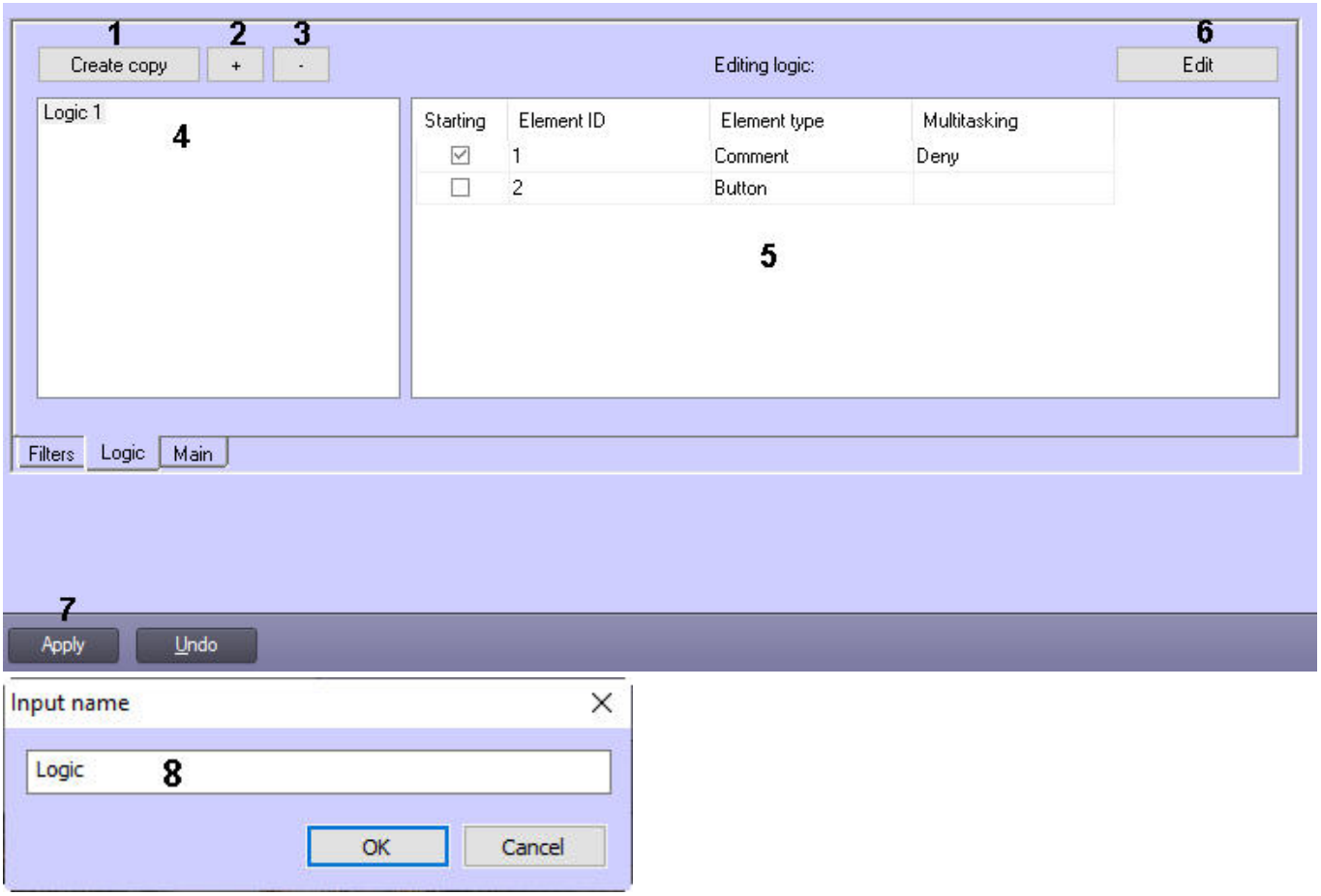
6 elements are used to perform the actions:

1. **Image**. The operator can add a frame from a video camera or an arbitrary image to the report. Images from maps or cameras can be added automatically.
2. **Button**. The button can be used to close the event handling interface and/or to open a report.
3. **Combobox**. The operator can select values from one or several lists.
4. **Comment**. The operator can add a comment while handling the event.
5. **Radio button**. The operator can choose one of the suggested values.
6. **Checkbox**. The operator can set one or more checkboxes.

The number of elements that can be used in the logic and the number of actions that the operator should perform are not limited. After the operator performed any action, the next action that should be performed is set in the element settings; a macro can be executed as well, if necessary. The sequence of actions can be determined by the operator's actions in the previous steps.

Create and configure the logic as follows:

1. Go to the **Logic** tab of the **Incident handler** object settings panel.
2. Click the **+** button (**2**) and in the appeared window enter the name for the new logic (**8**). You can also create a copy of an existing logic, for this it is necessary to select the logic in the list (**4**) and click **Create copy** (**1**). As a result, the new logic will appear in the list (**4**).



3. In the list of logics (**4**), select the logic to be configured.
4. Add the required number of elements to the logic (**5**). To add a row to the table, select the last row and press the ↓ key on the keyboard. To delete rows from the table, use the Ctrl + Del key combination.
5. In the **Element ID** column, enter the name of each element.
6. In the **Multitasking** column, set the ability to switch to processing other events when one event is processed while on the selected logic element:
   a. Select **Deny**, so that when this element appears, the operator cannot switch to processing another event until the operator moves to the element with the **Allow** value or completes processing the event (default);
   b. Select **Allow**, so that when this element appears, the operator can proceed to processing another event.
7. Select the element that will be displayed first for the operator when processing the event. To do this:
   a. Select an element in the table.
   b. Click the **Edit** button (**6**).
   c. In the **Starting element** drop-down list, select **Yes**.

   d. Click the **OK** button.
   As a result, a check mark will be displayed next to the selected element in the **Starting** column of the element table.

> **Note**
>
> If the starting element is not selected, then it will be the first element in the list.

8. Configure each element of logic and their correspondence (see Configuring the elements).

9. Repeat steps 3-7 for all added logics.
10. Click the **Apply** button (**7**).

The logic of event handling is configured. To delete a logic, select it in the list of logics (**4**) and click the **-** button (**3**).

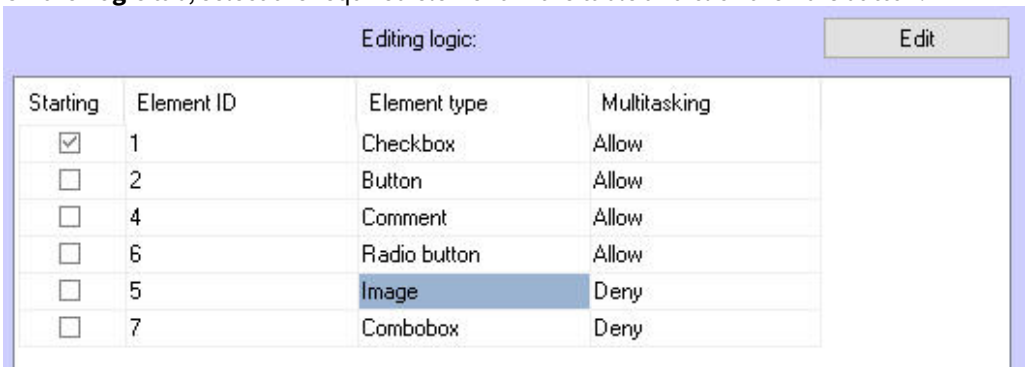
> **Note**
>
> The logic of event handling is applied to an event at the moment when the event gets into the Incident handler and is displayed in the Incident manager. Accordingly, if you change the logic, the updated logic will be applied to the events that occurred after it was changed. If a group processing of the events is enabled, the updated logic will be applied to a new group of the events after the existing group is closed.

23.3.22.5.1 Configuring the elements

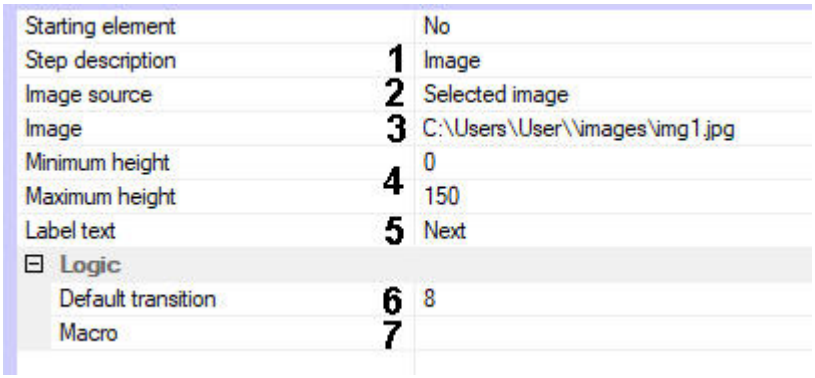
23.3.22.5.1.1 Configuring the image

Configure the image as follows:

1. On the **Logic** tab, select the required element in the table and click the **Edit** button.



2. If necessary, in the **Step description** field (**1**), enter the text that will be displayed in the column to the left opposite the element.



3. In the **Image source** drop-down list (**2**), select the image source:
   a. Images from cameras. When processing an event, images from cameras associated with the object that triggered the event will be displayed (see Connection of objects with cameras). If the event is triggered by a specific camera, then the image from it will be used.
   b. Images from maps: an image from the associated map will be used. If there are several layers on the map, then the image from the layer to which the object is attached will be used. If an object is attached to multiple layers, the layer on which the object was added earlier than other layers will be used.

      > **Note**
      >
      > To use the image from the map, the object should be added to the map and the map should be selected in the Incident manager settings (see Configuring the main parameters of the Incident manager).

   c. Images from Operator: Operator uploads images by himself.

d. Specified image: the image specified in the **Image** field (**3**) will be displayed. In this case, in the **Image** field, it is necessary to specify the path to the image, for example C:\Users\User1\Folder1\img1.png. The image can be in the following formats: jpg, bmp, png.

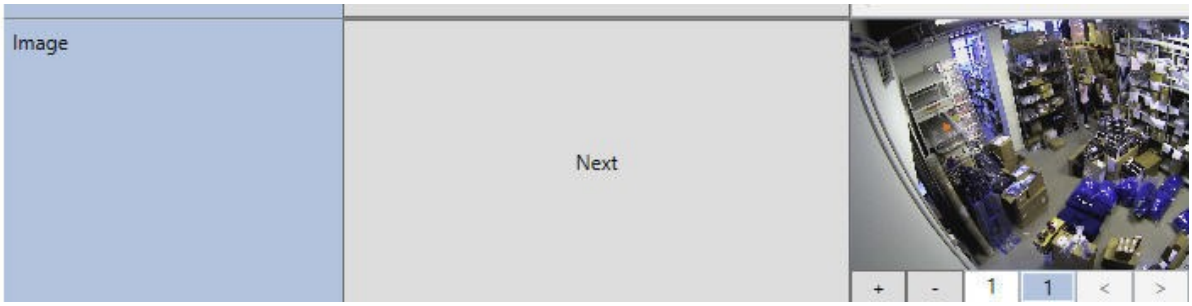
> **Note**
>
> The **Image** field (**3**) is displayed only if the **Specified image** value is selected.

4. In the **Minimum height** and **Maximum height** fields (**4**), enter the minimum and maximum image display height in pixels.
5. In the **Label text** field (**5**), enter the text that will be displayed on the button.

> **Note**
>
> If there are any event parameters, you can set them in the label text. To do this, in the **Label text** field, enter %<parameter name>%. For example, if you specify %time%, then the time of the event will be displayed on the button, if you specify %date% — the date will be displayed, if %user_id% — the user ID will be displayed (see Database tables reference guide for Intellect and vertical solutions).

6. In the **Default transition** field (**6**), select the element that should be displayed after clicking on the button.
7. If it is necessary to execute a macro command by clicking the button, select it from the **Macro** list (**7**).
8. Click **OK**.

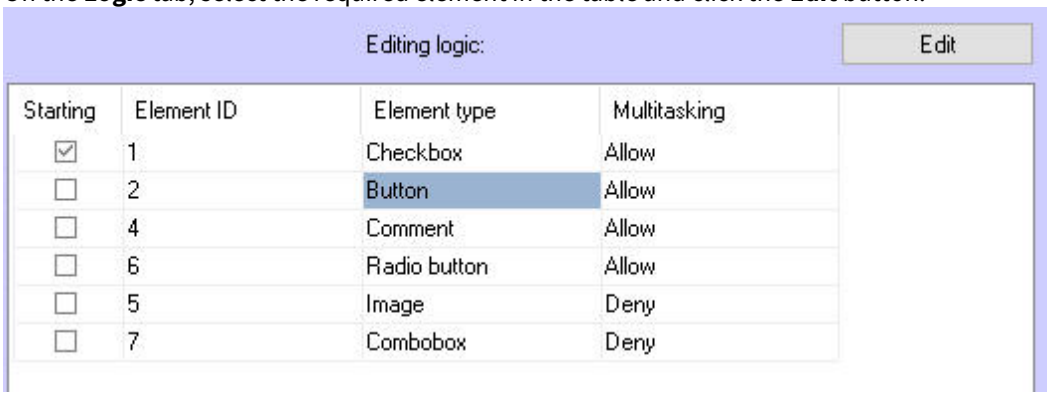
Example of displaying the **Image** element:



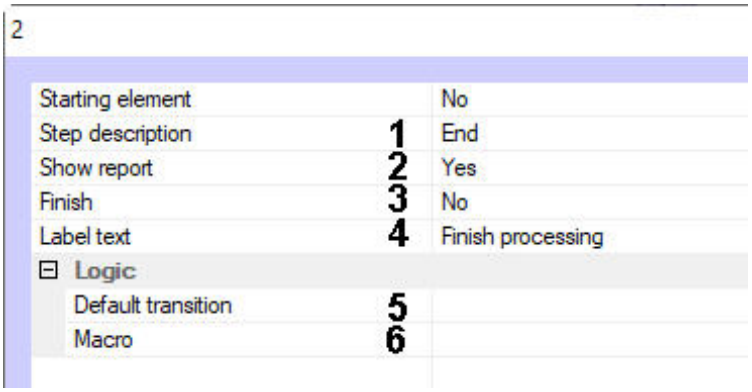
23.3.22.5.1.2 Configuring the button

Configure the button as follows:

1. On the **Logic** tab, select the required element in the table and click the **Edit** button.



2. If necessary, in the **Step description** field (**1**), enter the text that will be displayed in the column to the left opposite the element.

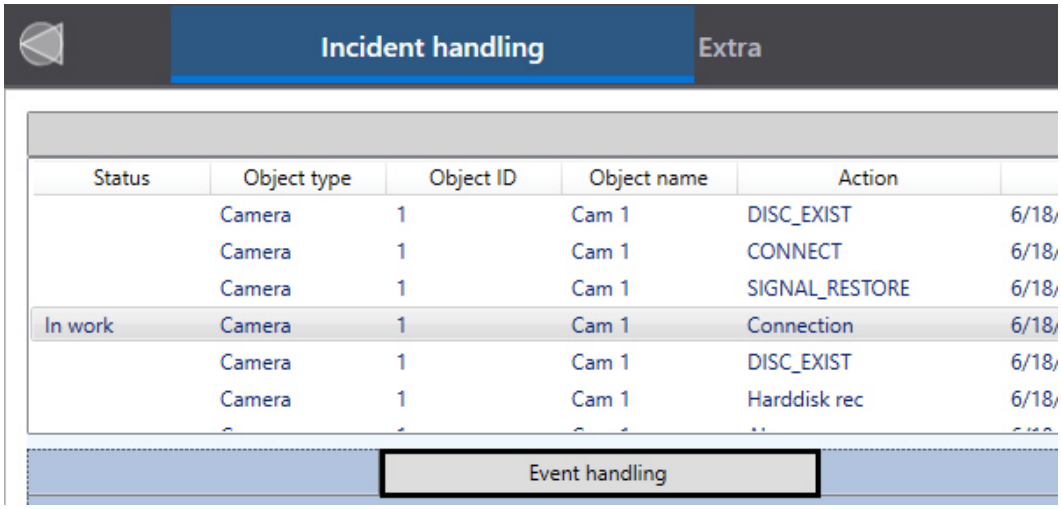


3. If it is necessary to open the report by clicking the button, select **True** in the **Show report** parameter (**2**).
4. If it is necessary to close the event handling interface after clicking the button, select **True** in the **Finish** parameter (**3**).
5. In the **Label text** field (**4**), enter the text that will be displayed on the button.

> **Note**
>
> If there are any event parameters, you can set them in the label text. To do this, in the **Label text** field, enter $<parameter name>$. For example, if you specify $time$, then the time of the event will be displayed on the button, if you specify $date$ — the date will be displayed, if $user_id$ — the user ID will be displayed (see Database tables reference guide for Intellect and vertical solutions).

6. In the **Default transition** field (**5**), select the element that should be displayed after clicking on the button (**4**). If the **Finish** parameter is set to **True,** the element cannot be selected.
7. If it is necessary to execute a macro command by clicking the button, select it from the **Macro** list (**6**).
8. Click **OK**.

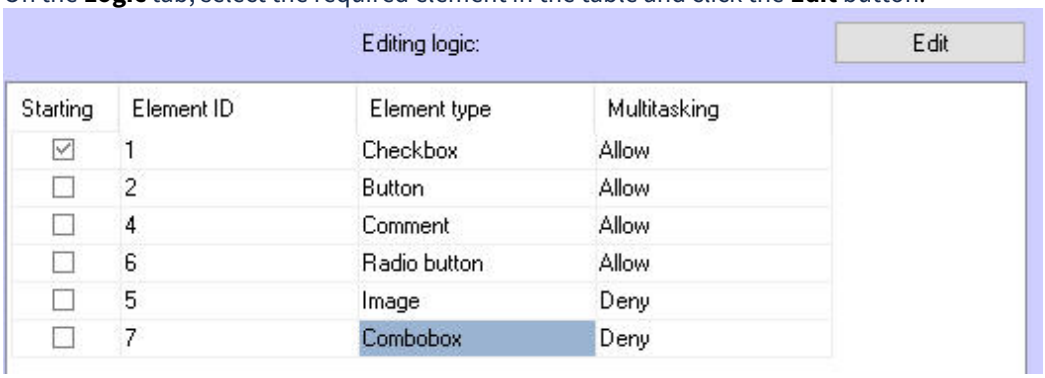
Example of displaying the **Button** element:



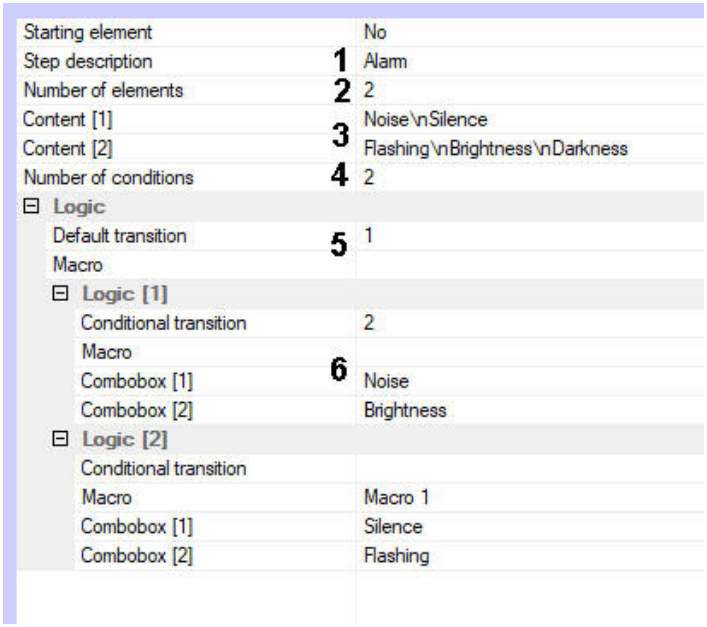
23.3.22.5.1.3 Configuring the combobox

Configure the combobox as follows:

1. On the **Logic** tab, select the required element in the table and click the **Edit** button.



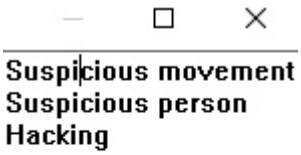
2. If necessary, in the **Step description** field (**1**), enter the text that will be displayed in the column to the left opposite the element.



3. From the **Number of elements** list (**2**), select the required number of drop-down lists.

> **Note**
>
> The maximum number of elements is determined by the possible number of columns when displaying the logic (see Configuring the display of logic).

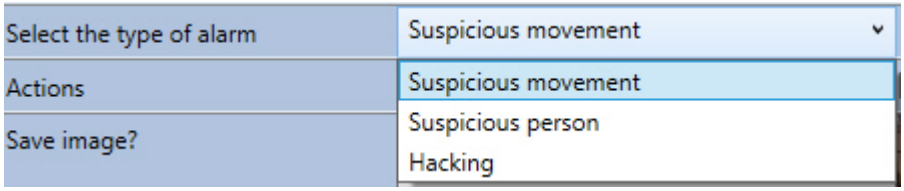
4. In the **Content** fields (**3**), click the ··· button and enter the values of each list. Each value should be entered on a new line.



To close this window, click ×.

5. From the **Number of conditions** list (**4**), select the number of different logics used for event handling. In this case, each logic implies a set of values that the operator selected from the lists. For each such set of values, it is possible to set the next element to display.
6. If it is necessary to display the same element for any selected values, then set up this element in the **Logic** group (**5**). If several logics are used, then set up each logic in the **Logic [N]** group (**6**), where N is the logic number. Do the following:
   a. In the **Conditional transition** field, select the element that should be displayed next.
   b. If at the same time it is necessary to execute a macro command, select it from the **Macro** list.
   c. Select values from the lists at which the above actions will be performed.
7. Click **OK**.

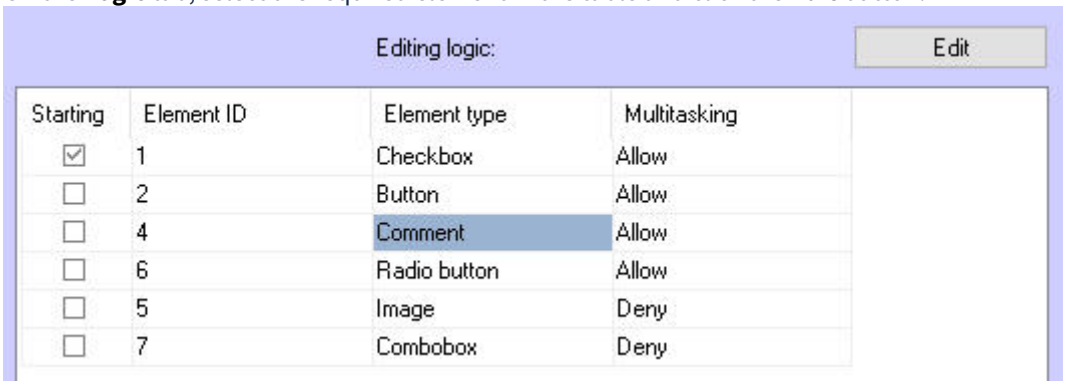
Example of displaying the **Combobox** element:



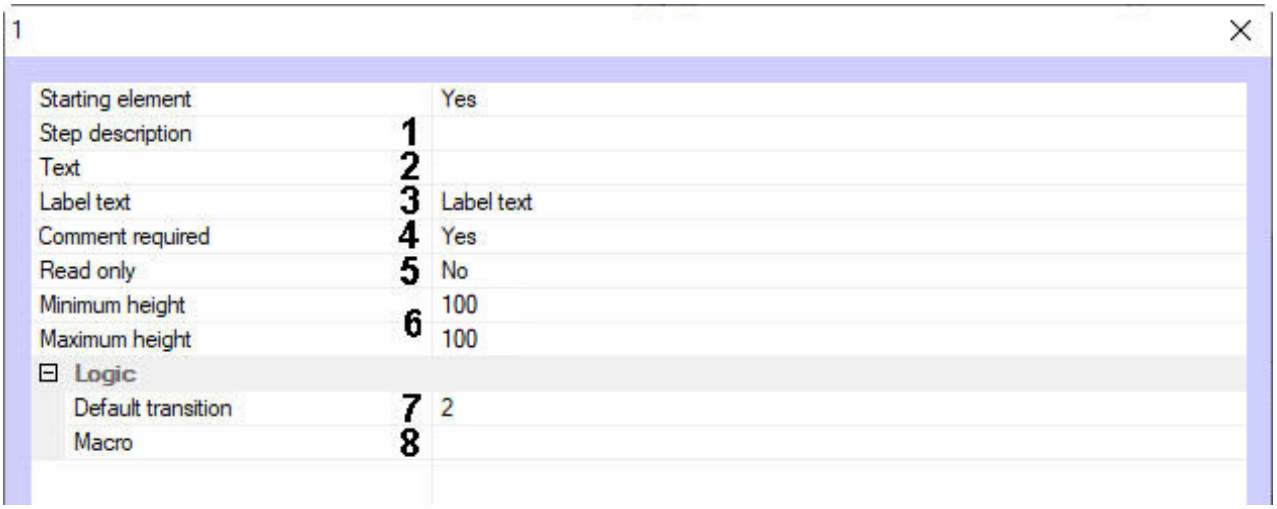
23.3.22.5.1.4 Configuring the comment

Configure the comment as follows:

1. On the **Logic** tab, select the required element in the table and click the **Edit** button.



2. If necessary, in the **Step description** field (**1**), enter the text that will be displayed in the column to the left opposite the element.



3. If necessary, in the **Text** field (**2**), enter the text that will be displayed in the comment input form.

> **Note**
>
> To display the current date and time in the input form, enter **%time%**. In this case, at the moment the Comment element is displayed, the date and time of the computer will be automatically recorded.

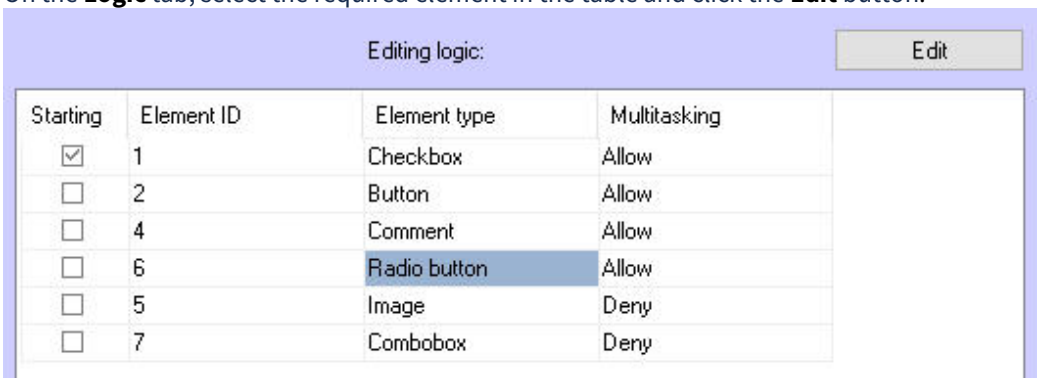
4. In the **Label text** field (**3**), enter the text that will be displayed on the button.
5. If the comment should be required, in the **Comment required** field (**4**) select **Yes**.
6. If it is necessary to block the ability to edit the comment by the Operator, in the **Read only** field (**5**) select **Yes**.
7. In the **Minimum height** and **Maximum height** fields (**6**), enter the minimum and maximum height of the comment input field in pixels. When the maximum value is exceeded, a scroll bar is displayed. The default value for both fields is 100.
8. In the **Default transition** field (**7**), select the element that should be displayed after clicking on the button.
9. If it is necessary to execute a macro command by clicking the button, select it from the **Macro** list (**8**).
10. Click **OK**.

Example of displaying the **Comment** element:

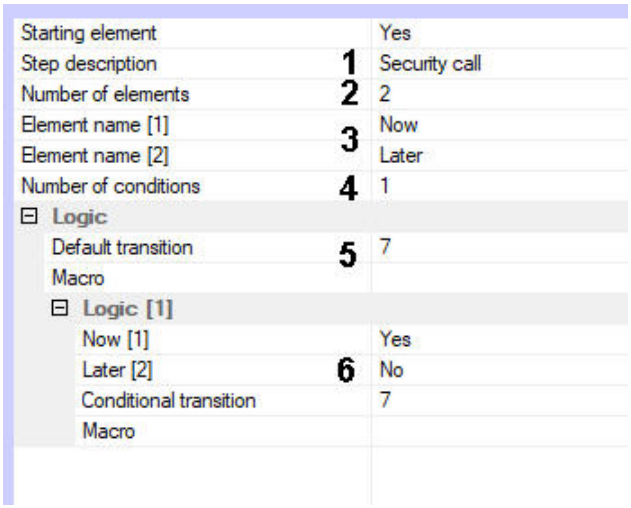
23.3.22.5.1.5 Configuring the radio button

Configure the radio button as follows:

1. On the **Logic** tab, select the required element in the table and click the **Edit** button.



2. If necessary, in the **Step description** field (**1**), enter the text that will be displayed in the column to the left opposite the element.



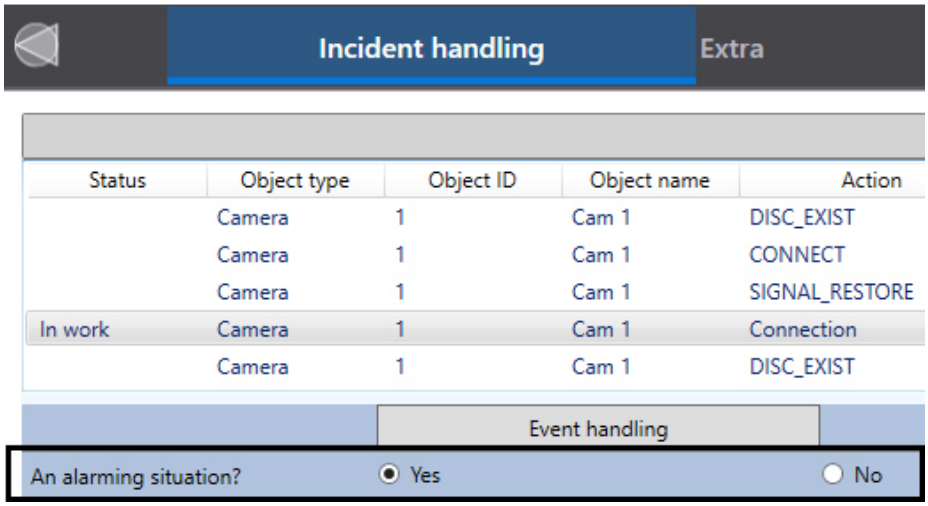
3. From the **Number of elements** list (**2**), select the required number of radio buttons.

> **Note**
>
> The maximum number of elements is determined by the possible number of columns when displaying the logic (see Configuring the display of logic).

4. In the **Element name** fields (**3**), enter the values of the radio buttons.
5. From the **Number of conditions** list (**4**), select the number of different logics used for event handling. In this case, each logic implies the value that the operator selected. For each value, it is possible to set the next element to display.

6. If it is necessary to display the same element for any selected value, then set up this element in the **Logic** group (**5**). If several logics are used, then set up each logic in the **Logic [N]** group (**6**), where N is the logic number. Do the following:
    a. In the **Conditional transition** field, select the element that should be displayed next.
    b. If at the same time it is necessary to execute a macro command, select it from the **Macro** list.
    c. Select the value of the radio button, at which the above actions will be performed.
7. Click **OK**.

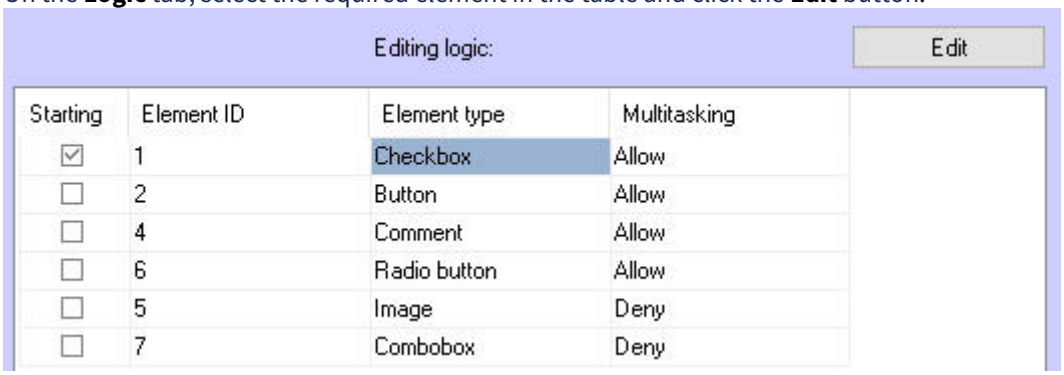
Example of displaying the **Radio button** element:



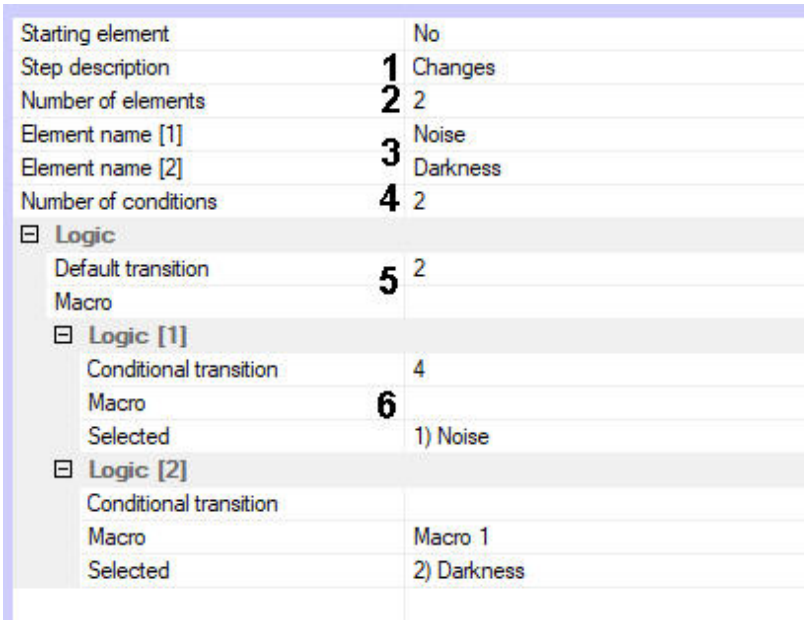
23.3.22.5.1.6 Configuring the checkbox

Configure the checkbox as follows:

1. On the **Logic** tab, select the required element in the table and click the **Edit** button.



2. If necessary, in the **Step description** field (**1**), enter the text that will be displayed in the column to the left opposite the element.

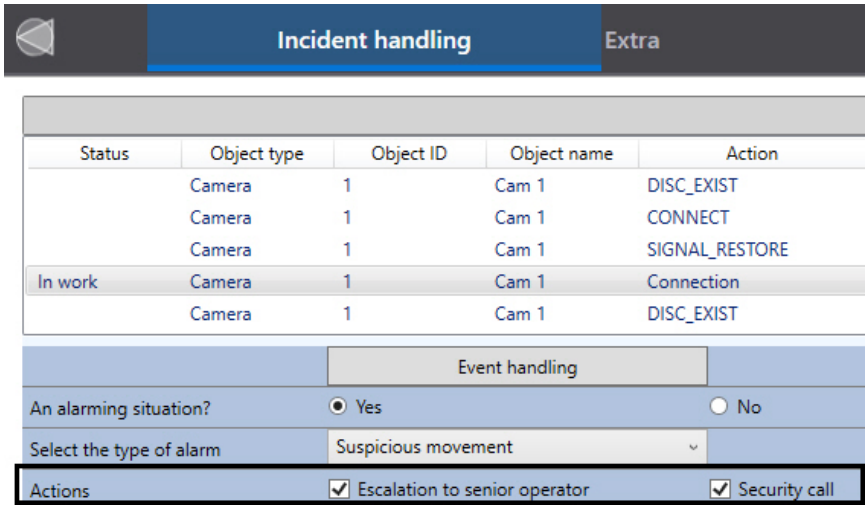


3. From the **Number of elements** list (**2**), select the required number of checkboxes.

> **Note**
>
> The maximum number of elements is determined by the possible number of columns when displaying the logic (see Configuring the display of logic).

4. In the **Element name** fields (**3**), enter the names of the checkboxes.
5. From the **Number of conditions** list (**4**), select the number of different logics used for event handling. In this case, each logic implies a certain set of checkboxes that the operator set. For each such set of checkboxes, it is possible to set the next element to display.
6. If it is necessary to display the same element for any possible values of the checkboxes, then set up this element in the **Logic** group (**5**). If several logics are used, then set up each logic in the **Logic [N]** group (**6**), where N is the logic number. Do the following:
   a. In the **Conditional transition** field, select the element that should be displayed next.
   b. If at the same time it is necessary to execute a macro command, select it from the **Macro** list.
   c. Select values of each checkbox, at which the above actions will be performed.
7. Click **OK**.

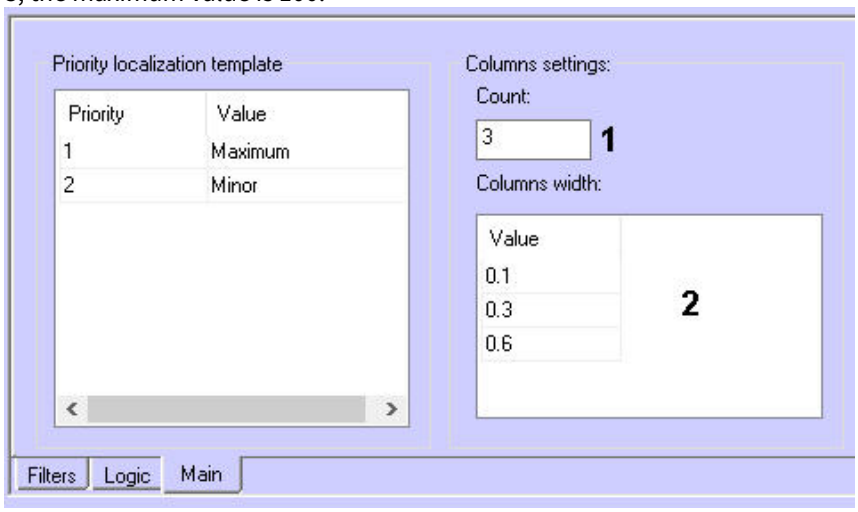
Example of displaying the **Checkbox** element:



23.3.22.6 Configuring the display of logic

In **Incident manager**, the logic of event handling is displayed as a number of columns and rows with logic steps. To configure the display of logic, do the following:

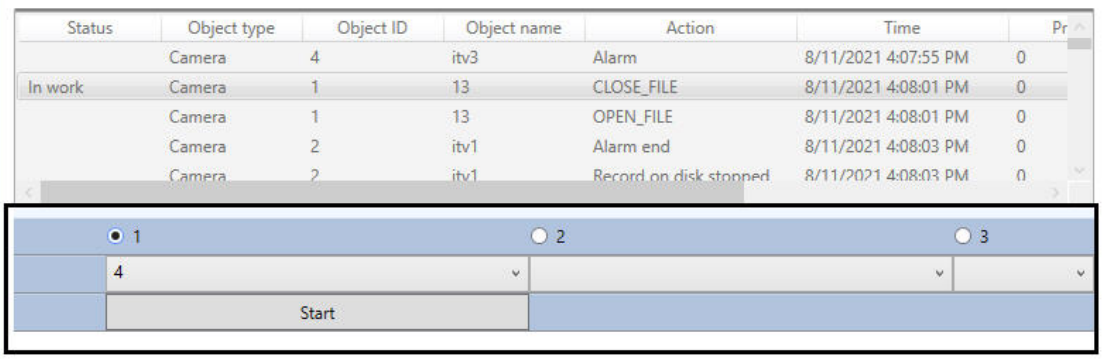
1. Go to the **Main** tab of the **Incident handler** object.
2. Specify the **Columns settings**:
   a. in the **Count** field (**1**), specify the number of columns required to display the logic of event handling. The default is 3, the maximum value is 100.



> **Note**
>
> The number of columns determines how many **Radiobutton**, **Checkbox**, and **Combobox** elements can be created (see Configuring the elements).
> If the logic of event handling is created, but the number of columns is not set, then it will be displayed incorrectly when the operator will take the event into processing.

   b. In the **Columns width** field (**2**), set the width of the columns when displaying the logic of event handling. The width is set in pixels or as a percentage of the entire width of the **Incident manager** interface. Percentage values should be set as fractions of 1, for example, 0.25. If you set a value greater than 1, then it will be considered as pixels. The default column width is 150 px.

> **Note**
>
> For example: **Count** — 4, **Columns width** — 100, 300, 300, 100.
> In this case, the logic of event handling is displayed as follows:



3. Click the **Apply** button.

The display of the logic of event handling is configured.

23.3.22.7 Configuring the use of an external database

By default, **Incident server** events are stored in the PROTOCOL_INC_SERVER table of the *Intellect* database.

If for the **Incident server** it is necessary to use a database that is different from the one used in *Intellect* by default, configure the connection as follows:

1. On the settings panel of the **Incident server** object, set the **Use** checkbox (**1**).

2. Configure the connection parameters in one of the following ways:
   a. Click the **Configure** button and set the parameters for connecting to an external database using the standard dialog box—see Configuring the connection to an external database in dialog mode (**2**).
   b. In the **Connection string**, manually enter the connection parameters separated by a semicolon without spaces (**3**).

Parameter	Possible values
Provider	**SQLOLEDB.1** when using MS SQL Server format database, **Microsoft.Jet.OLEDB.4.0** when using MS Access database
Integrated Security	**SSPI** when authenticating on MS SQL server using a Windows OS account. If MS SQL server is used and the parameter is missing, then username (login) and password will be used for authentication. When using a database in MS Access format, this parameter is not required
Persist Security Info	**True**—it is permitted to save the password for automatic connection to the database, **False**—it is prohibited to save the password for automatic connection to the database
Data Source	The name of the MS SQL server used to manage the database, or the path to the MDB file of the MS Access database

   All parameters, except for **Integrated Security**, are mandatory. Example:
   Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=True;Data Source=SQLEXPRESS2014
3. Click the **Apply** button (**4**).

As a result, the specified database will be used for the **Incident server**.

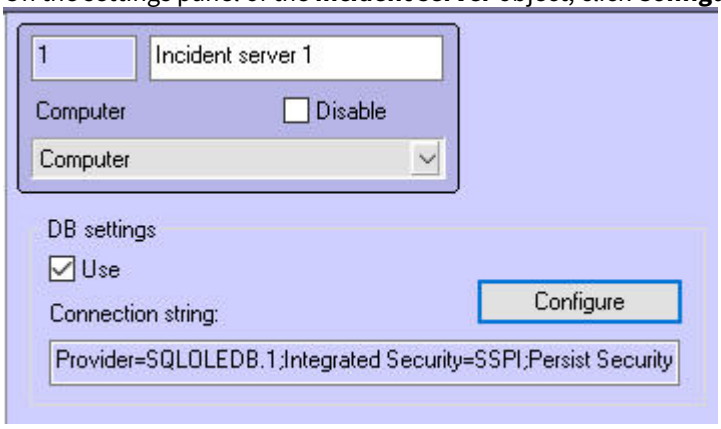
Note

The settings described above are required only for connection to an external database. If the default database is used, then there is no need to additionally configure the connection.

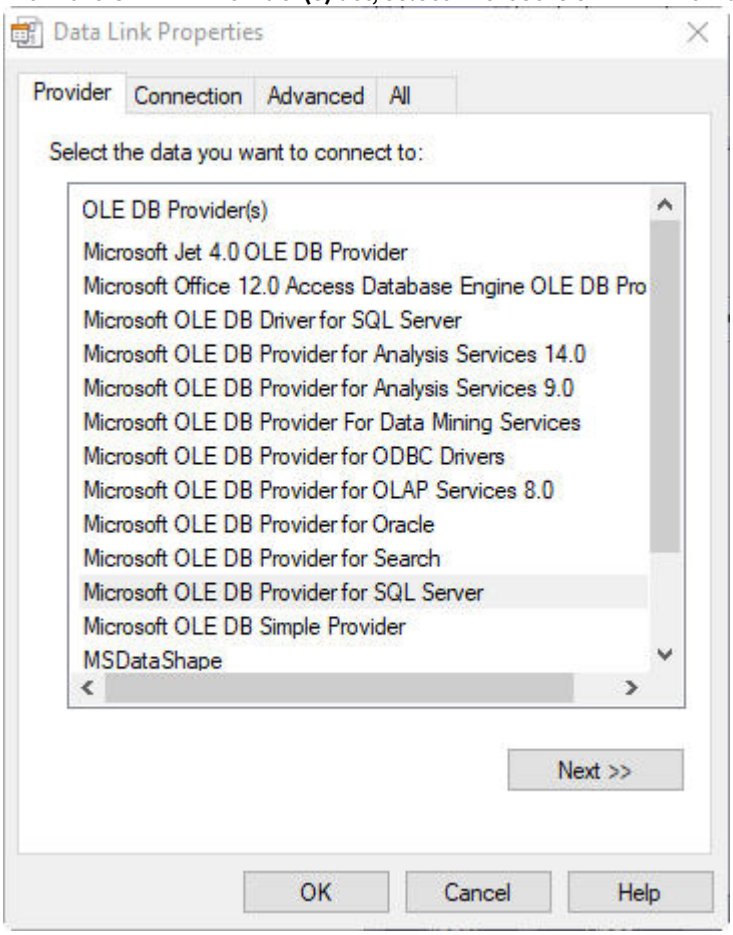
23.3.22.7.1 Configuring the connection to an external database in dialog mode

To configure the connection to an external database in dialog mode, do the following:

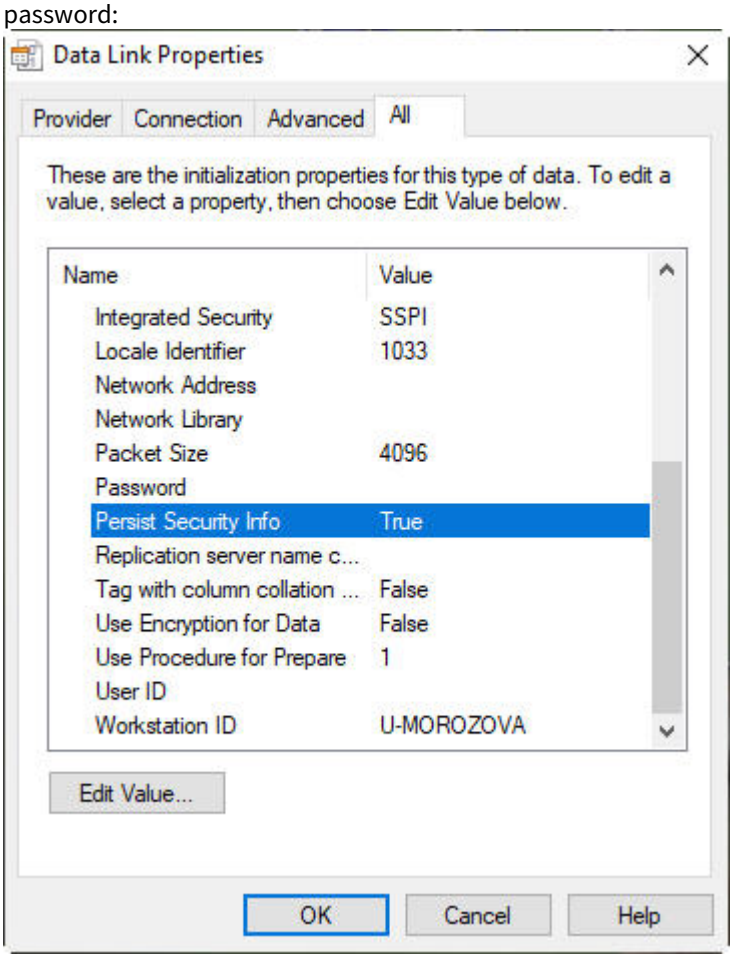
1. On the settings panel of the **Incident server** object, click **Configure**.



2. As a result, the **Data Link Properties** dialog box will open. Go to the **Provider** tab.
3. From the **OLE DB Provider(s)** list, select **Microsoft OLE DB Provider for SQL Server**.

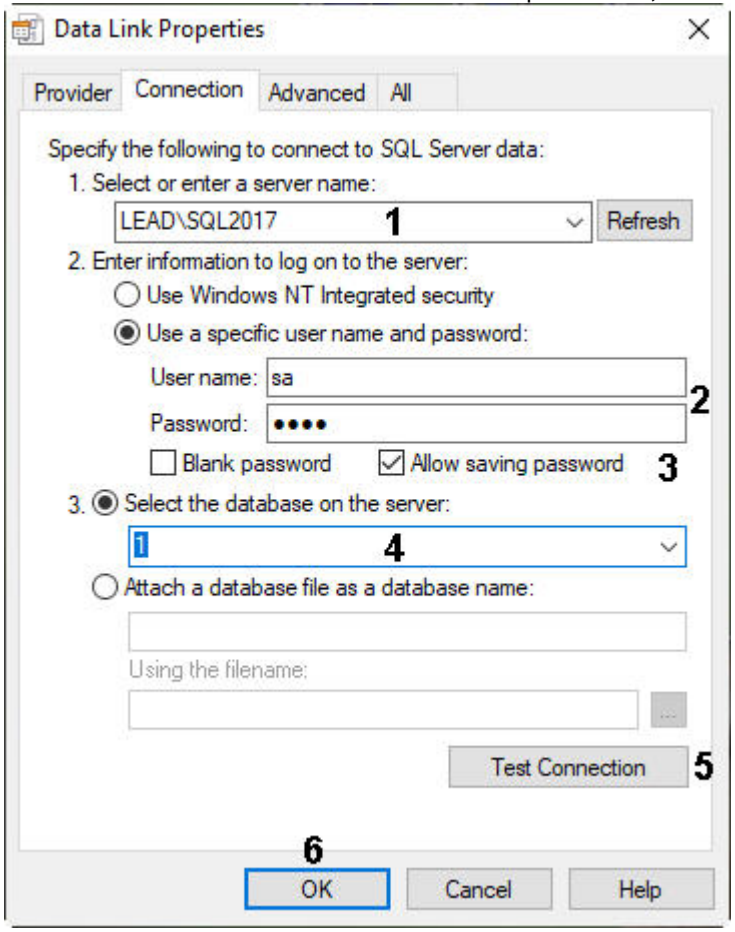


4. Go to the **All** tab and set the **Persist Security Info** parameter value to **True**. This is necessary to correctly save the user password:

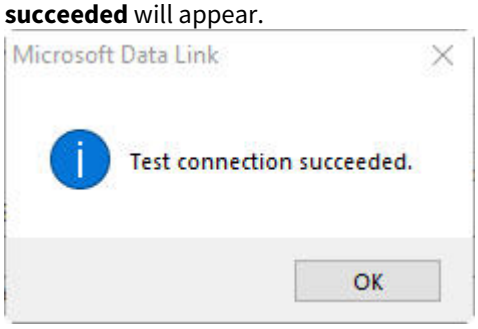


5. Go to the **Connection** tab:

a. From the **1. Select or enter a server name** drop-down list, select the server name (**1**).



b. In parameter **2. Enter information to log on to the server**, set the **Use a specific user name and password** checkbox and enter the username and password to access the server in the corresponding fields (**2**).
c. Set the **Allow saving password** checkbox (**3**).
d. From the **3. Select the database on the server** drop-down list, select the database to be used (**4**).
e. Click the **Test Connection** button (**5**).
f. If the connection to the MS SQL server is successfully established, a window with the message **Test connection succeeded** will appear.



g. Click the **OK** button on the message box, which will automatically close the window.

6. To apply the settings, click the **OK** button (**6**).
7. Click

.

As a result, the selected database will be used for the **Incident server**.

23.4 Configuration of interfaces

23.4.1 Intellect Software System's interface language

To change the interface language of the *Intellect* Software System, a language must be installed. This is done using a language pack. Language packs are available on the AxxonSoft website at https://www.axxonsoft.com/.

> **Note.**
>
> A language pack may be released later than the corresponding version of the Intellect Software System.

A language pack is collection of LP.msi files, each of which installs the localized product in one of the supported languages. Each file is located in a separate folder named using the ISO 639-1 two-letter code for the installer's language. Languages can be installed during the installation of the base product (see Installing INTELLECT™ software) or separately for each language (see Installing the language).

> **Important!**
>
> The operating system language must be the same as the language of the installed language pack. Otherwise, the *Intellect* settings and interfaces may be displayed incorrectly.

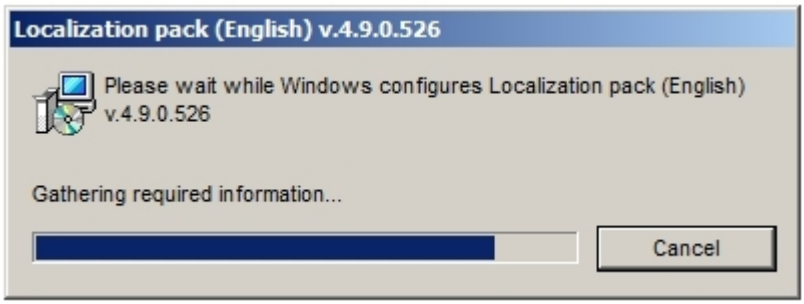
Installed languages are enabled in the *Intellect* Software System using the system's advance settings utility tweaki.exe (see Switching languages in the Intellect Software System).

> **Attention!**
>
> Localization files for Intellect-based vertical solution modules are not included into the language package.

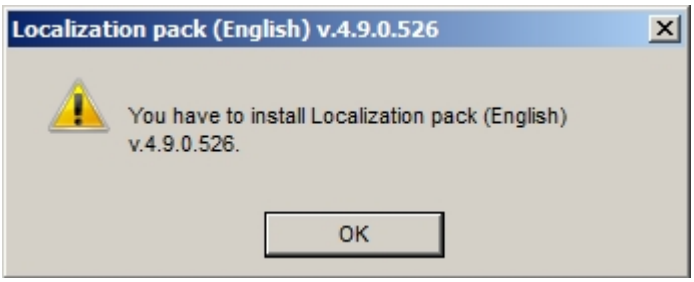
23.4.1.1 Installing the language

To install a new interface language for the *Intellect* Software System, do the following:

1. Download the latest version of the language pack from the AxxonSoft official website: https://www.axxonsoft.com/.
2. Unzip LP.zip in any directory, i.e. D:\LP\.
3. Go into the folder corresponding to the language you want to install, i.e. D:\LP\en to install English.
4. Launch LP.msi.
5. A window displaying the progress of the installation will be shown.



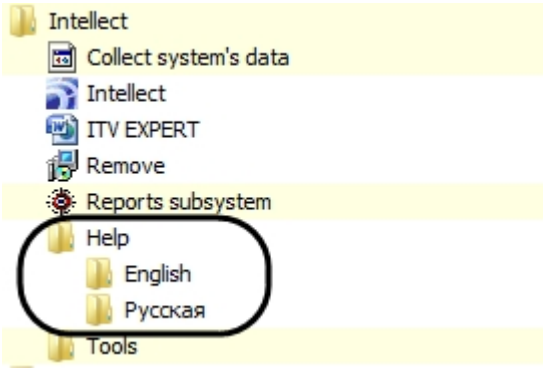
A language cannot be installed if the base product has not been installed. If the *Intellect* Software System has not been installed, a message indicating the need to install it will be shown.



Click **OK** to cancel the installation.

When the installation process is complete, a folder containing the required language files will be created in <*Intellect* installation directory>\Languages. Additionally, help files in the desired language will be placed in <*Intellect* installation directory>\Help.

Documentation in the installed language will also become available through **Start** –> **All Programs** –> **Intellect**–> **Documentation**.



Languages are uninstalled when the *Intellect* Software System is uninstalled.

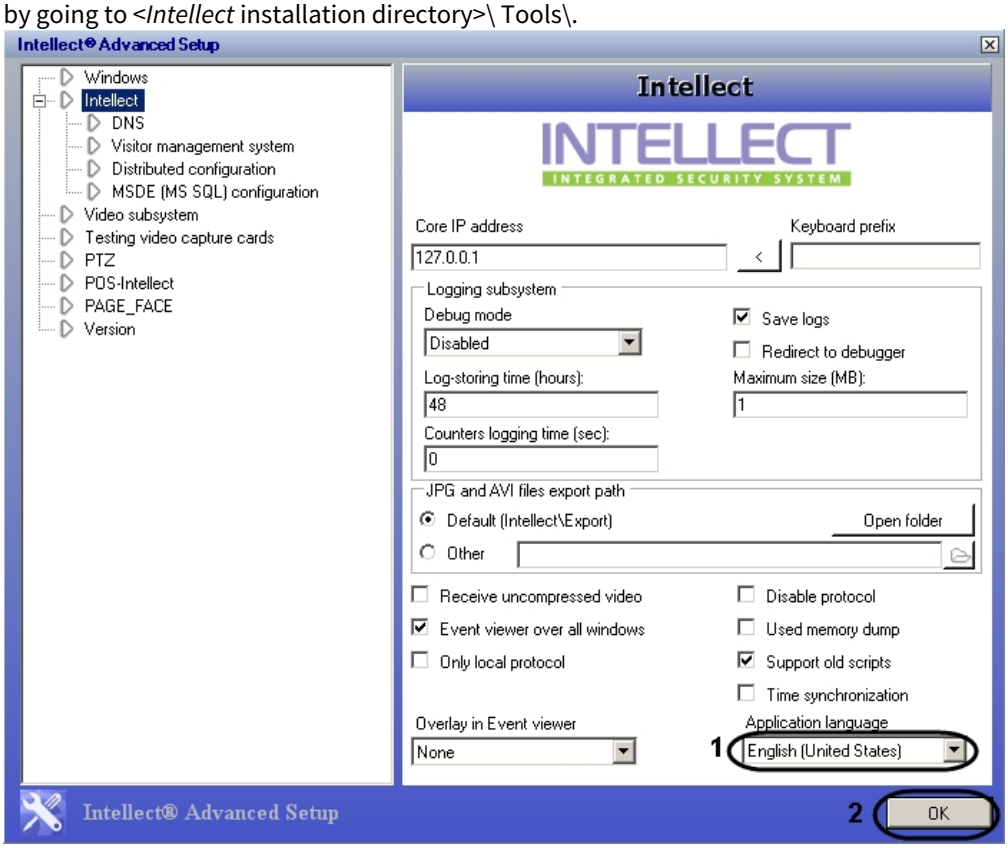
23.4.1.2 Switching languages in the Intellect Software System

Before switching languages, be sure the desired language has been installed (see Installing Intellect or Installing the language).

To switch the *Intellect* Software System's interface language, do the following:

1. Shut down the *Intellect* Software System.

2. Launch the system's advanced settings utility tweaki.exe. The utility is accessed through **Start** –> **Intellect** –> **Utilities**, or by going to <*Intellect* installation directory>\ Tools\.



3. From the **Application language** dropdown list, select the desired interface language for the *Intellect* Software System (1).
4. Click **OK** (2).
5. Launch the *Intellect* Software System.

This completes the process of switching languages.

23.4.2 Configuring the user interface

23.4.2.1 The user interface in the Intellect software

In the course of setting-up the video surveillance/audio monitoring system, the personal user interface is configured and personal (role-dependent) rights are assigned to each Operator for using the system functions and managing the system resources (see Configuration of users and permissions).

The user interface of the Intellect-based video surveillance system is built under the **Display** hierarchical object.

The **Display** object groups and sets the position of the UI components on the Operator's workstation monitor.

The **Display** object represents the whole visible area of the computer monitor showing all the interface components according to their settings.

The **Display** object includes the following interface components:

1. HTML Interface;
2. Audio player;
3. External window;
4. Map;
5. Live sound switch;
6. Monitor;
7. Intercom Control Monitor;
8. Telemetry control panel;
9. Panel of Backup archive;

10. Search by captions;
11. Configuration check;
12. Event Viewer;
13. Incident manager;
14. Operator protocol;
15. Scene.

The following windows are created on the base of the **Computer** object and pop up on the **Display**:

1. Alarm Message Window.
2. Operator query panel.

23.4.2.2 Setup procedure for the displays

Display creation is an important stage of the surveillance system design as it is the main working instrument of the Operator.

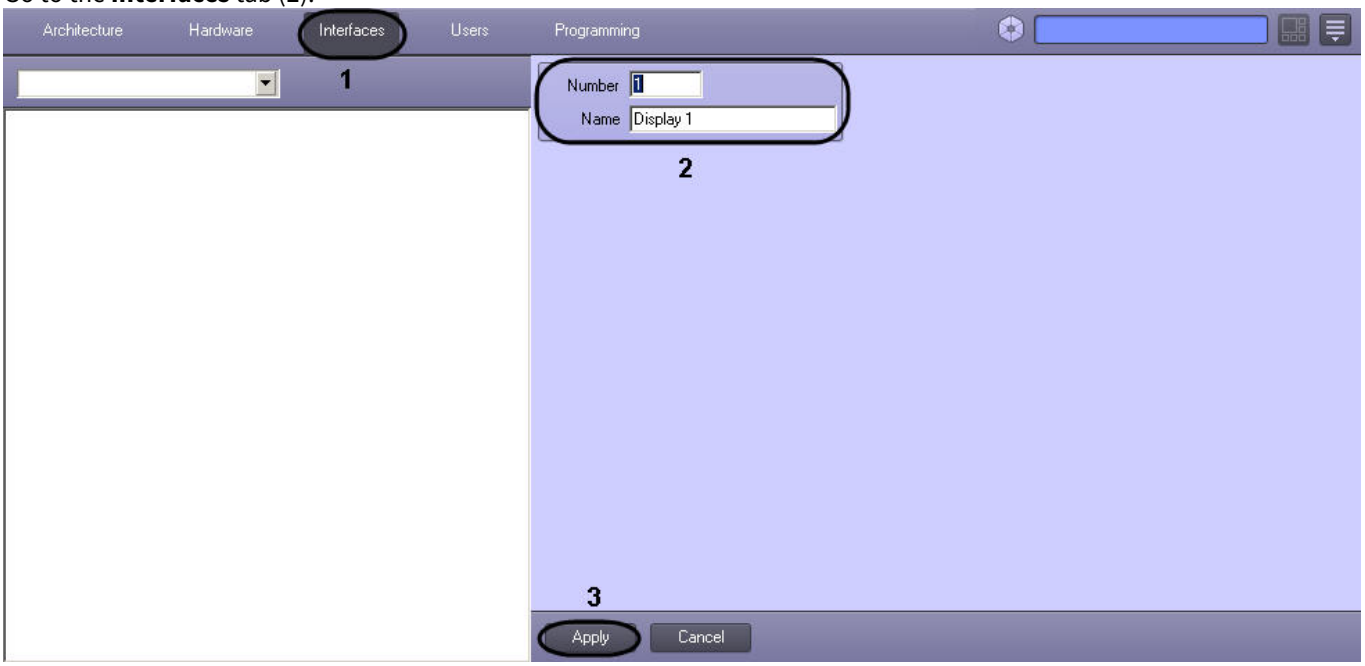
Display is created in the **Interfaces** tab and includes the following stages:

1. Creating **Display** objects.
2. Creating objects (interface components) on the base of the **Display** object in the **Interfaces** tab (see the list in the The user interface in the Intellect software section).
3. Placing the interface components on the screen in relation to each other.
4. Assigning the displays to the operator workstations.

23.4.2.3 Creating a Display object

The **Display** object is created on the **Interfaces** tab of the **System settings** dialog window. After the *Intellect* software is installed, no **Display** objects are created by default. To create the first **Display** object, do the following:

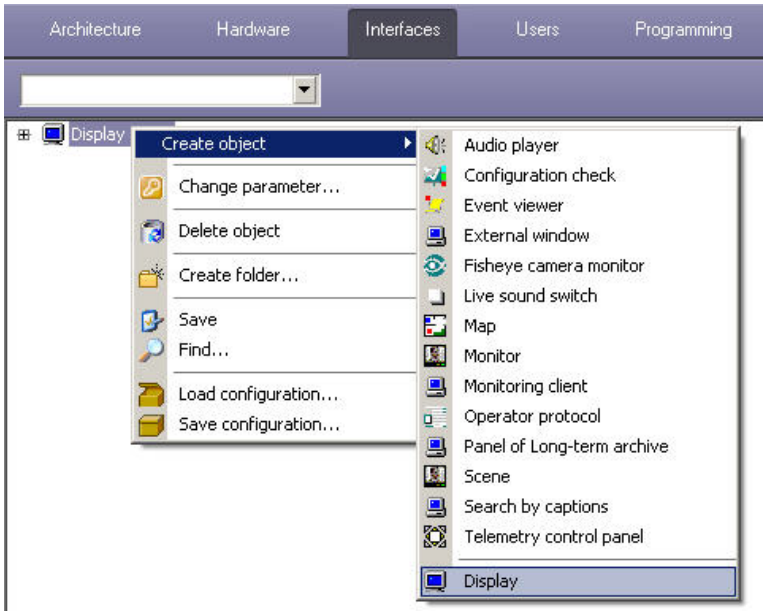
1. Go to the **Interfaces** tab (**1**).



2. Specify number and name of the **Display** object (**2**).
3. Click the **Apply** button (**3**).

Created object will be displayed in the objects tree:

After creating the first **Display** object the next **Display** objects are to be created on the basis of this or other **Display** objects. Right-click the **Display** object and select **Create object** → **Display** item in the functional menu.



Then follow the instruction presented above from the step 2.

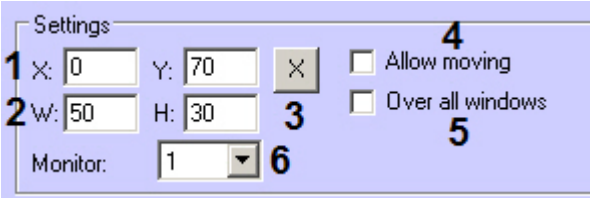
23.4.2.4 Placing the interface components on the screen

On this page:

- Window coordinates and size
- Moving a window and displaying on top of all windows
- Selecting a physical monitor for display
- Popup windows

23.4.2.4.1 Window coordinates and size

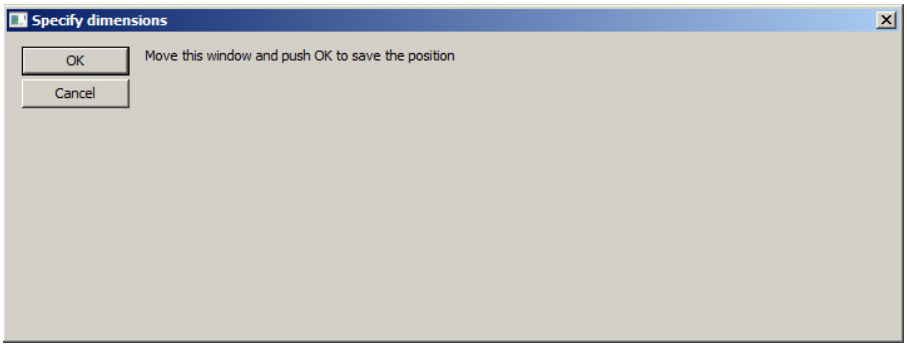
To place an interface component on the screen, its position coordinates **X** and **Y** (**1**) and window size **W** and **H** (**2**) are to be specified:



where

- **X** and **Y**—coordinates of the upper left corner of the window along the horizontal X axis and vertical Y axis;
- **W** and **H**—width and height of the window.

You may also set the interface window position and size with a template box. To do this, click X (**3**). The **Specify dimensions** box appears. Drag and resize it on the screen where the interface window should be, then click **OK**. The **X, Y, W, H** fields are automatically filled with values according to the **Specify dimensions** box position and size.



The size of some components (**Telemetry control panel**, etc.) is fixed. In this case the corresponding fields are not shown.

> **Note**
>
> The **Telemetry control panel** can also be half-transparent (see The Settings panel of the Telemetry control panel object).

23.4.2.4.2 Moving a window and displaying on top of all windows

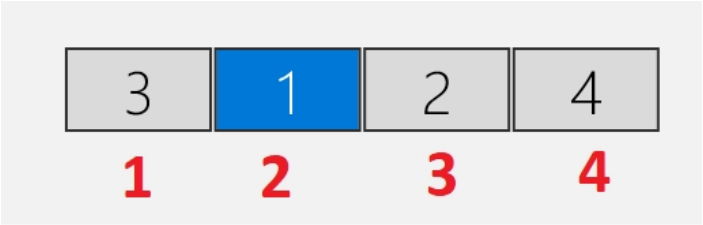
To enable the user to move the windows across the screen, set the **Allow moving** checkbox (**4**). Set the **Over all windows** to display the interface window always on top (**5**).

23.4.2.4.3 Selecting a physical monitor for display

When several monitors are connected to a computer, select from the **Monitor** drop-down list the identifier of monitor in the operating system, for displaying on which the object coordinates are set (**6**).

Monitors are numbered in physical order from left to right, top to bottom. So number 1 corresponds to the top left monitor, regardless of which monitor is considered primary or first in the operating system.

In the figure below, the monitor numbers in the operating system are gray, and *Intellect* monitors are red:



Consider this when choosing a physical monitor:

1. If there is no monitor selection for an object in the settings, then by default it will be displayed on Monitor 2 (2 in *Intellect* numeration), that is, on the same monitor where the *Intellect* settings window is displayed. An exception is the **Traffic Monitor** object in *Auto Intellect*, which is displayed on Monitor 1.

2. If there is no **Monitor** drop-down list on the object setting panel, you can adjust its position on non-primary monitor by specifying negative coordinates or coordinates greater than 100 depending on physical position of the monitor relative to the primary monitor. In this case it is strongly not recommended to set negative coordinates less than -200 (for example, -250, -300, etc.)
3. If you change the monitor numbering in the operating system settings while *Intellect* is running, then the interface objects will be placed in accordance with the OS monitor numbers configured at that moment. Linking to monitors will become correct again after restarting *Intellect*.

Note

Intellect supports NVIDIA® Mosaic™ multi-display technology when NVIDIA Quadro Sync is used additionally with it (see the related NVIDIA documentation). Without NVIDIA Quadro Sync there can be ~10-200 ms discrepancies in video playback time between monitors.

23.4.2.4.4 Popup windows

Popup windows (**Alarm notification window** and **Operator query panel**) have no position settings. They are displayed on top of other windows and can be moved to any place on the screen using the mouse.

For more details about the position settings for each interface object, refer to corresponding sections of Configuration of interfaces section, as well as the description of The Interfaces tab.

23.4.2.5 Assigning the displays to the operator workstations

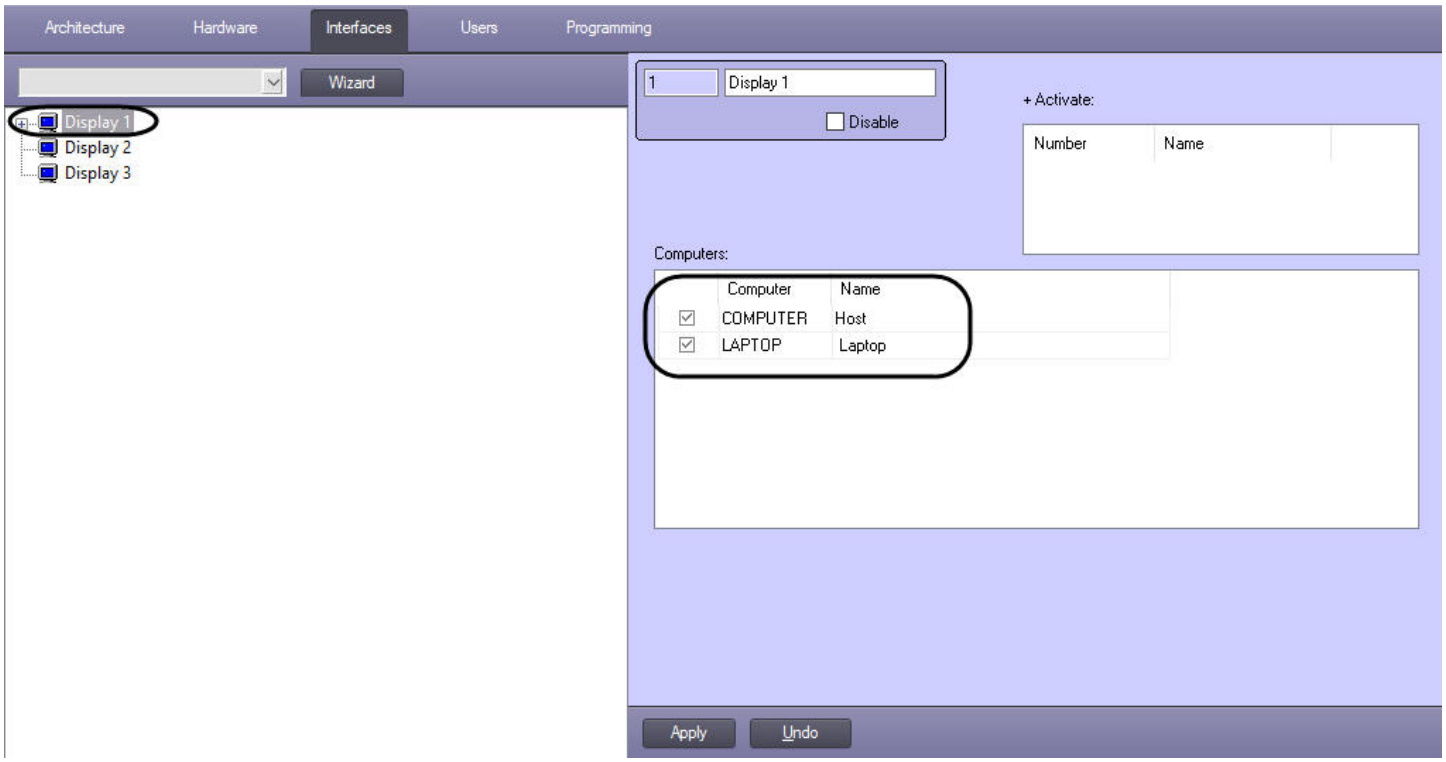
On the page:

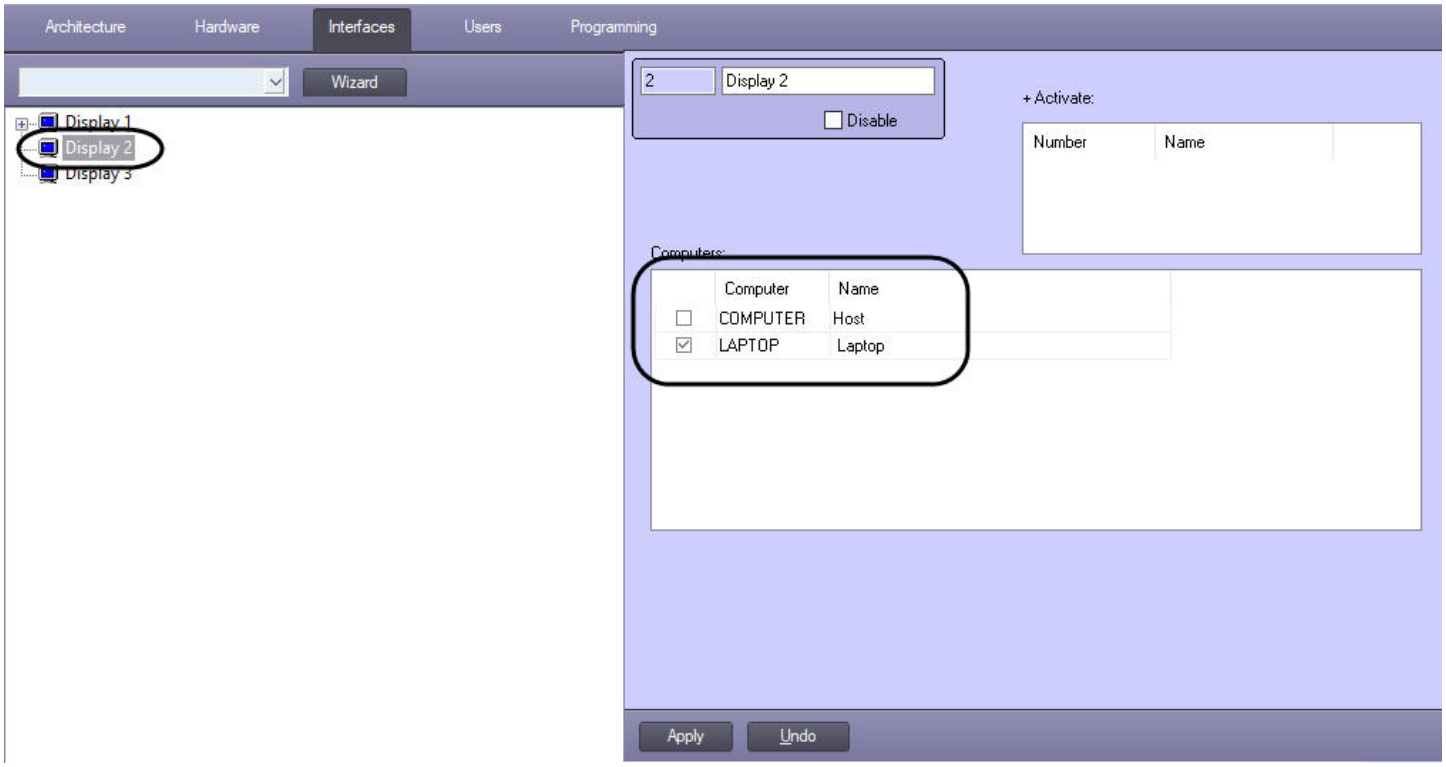
- Assigning displays manually
- Assigning displays via Wizard
- Assigning displays via display activation

To configure the access of several operator workstations to the same interfaces, the corresponding displays should be assigned to these workstations. This can be done manually for each display, via the display assigning Wizard or via the display activation.

23.4.2.5.1 Assigning displays manually

The displays can be assigned to the workstations on the settings panel of the **Display** object. The figure below shows the configuration of two objects: **Display 1** and **Display 2**. According to the configuration, the **Display 1** will be available to all computers of the video surveillance system, while the **Display 2** will be available only to the **LAPTOP** computer.





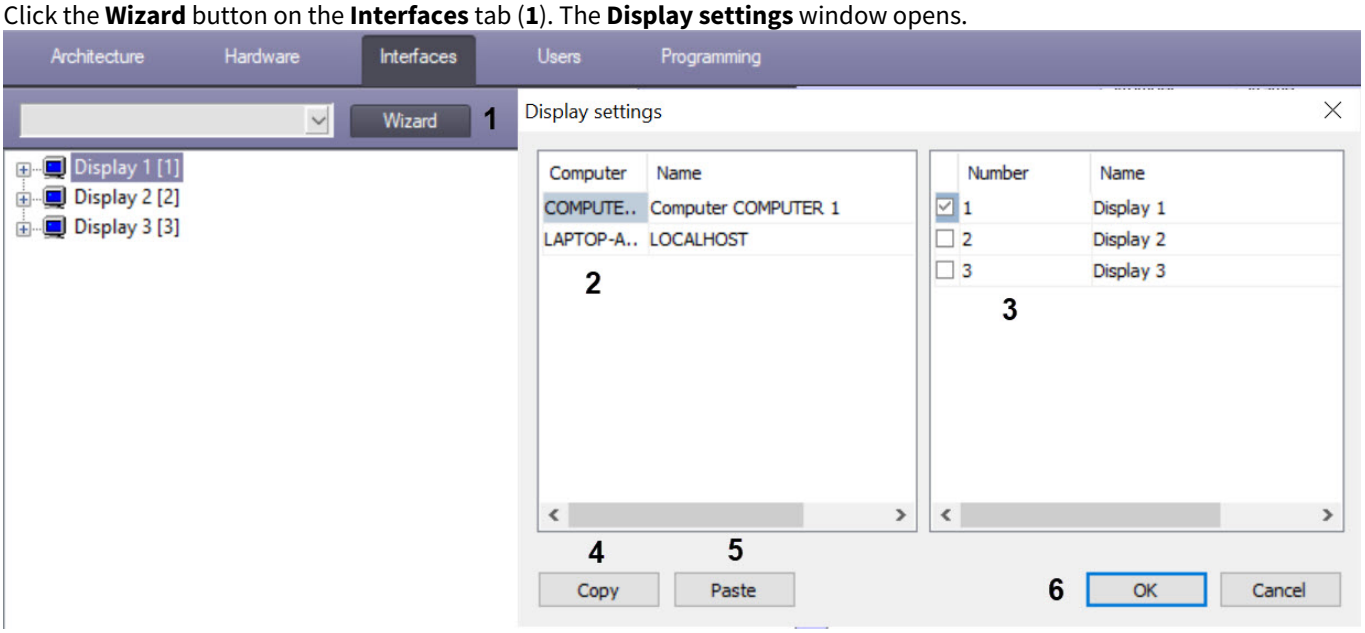
Note

If the display assigning is performed from the Server which is not connected with some Servers of the distributed system (the corresponding checkbox in the **Architecture** tab is not set — see Configuring the interaction of distributed system components), the data from this Server will not be displayed in the list of computers to which the current Display can be assigned. The settings of these Servers will not change after completing the display assignment.

23.4.2.5.2 Assigning displays via Wizard

To assign the displays via Wizard, do the following:

1. Click the **Wizard** button on the **Interfaces** tab (**1**). The **Display settings** window opens.



2. Select the computer in the **Computer** column (**2**).
3. Set the checkboxes next to the **Display** objects to assign them to the selected computer (**3**).
4. Repeat steps 2-3 for all required **Computer** objects.

> **Note**
>
> Use the **Copy** (**4**) and **Paste** (**5**) buttons to copy the display list. For example, to assign the same displays to the LAPTOP-A computer as those assigned to the COMPUTER 1 computer, do the following:
> 1. Select the COMPUTER 1 computer in the **Display settings** dialog box.
> 2. Click the **Copy** button (**4**).
> 3. Select the LAPTOP-A computer in the **Display settings** dialog box.
> 4. Click the **Paste** button (**5**).

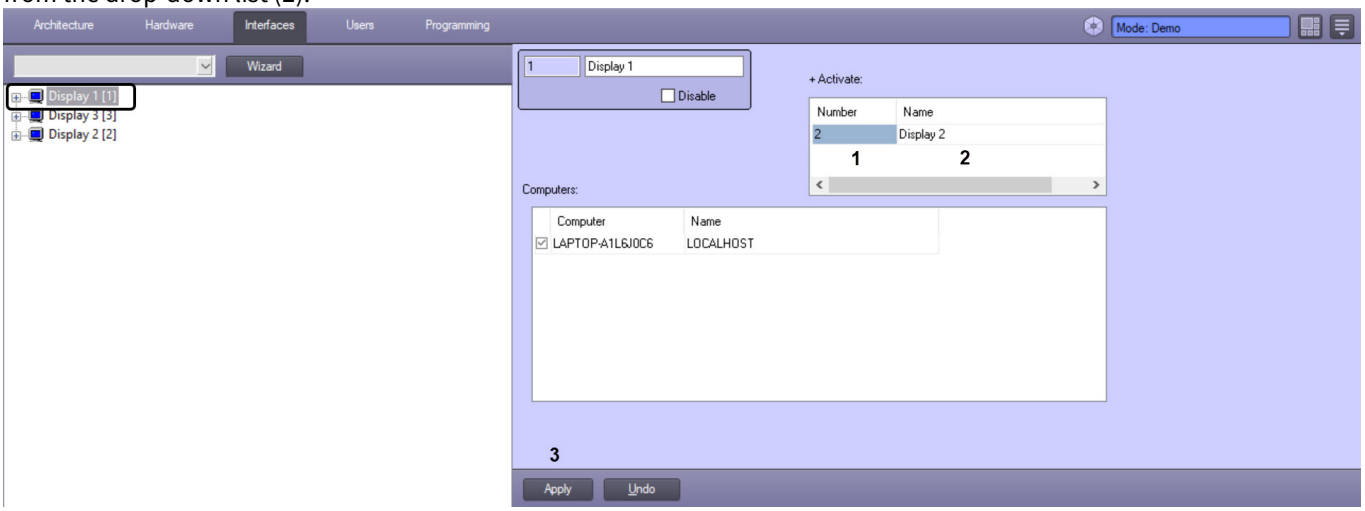
5. Click the **OK** button (**6**).

Assigning the displays via Wizard is now complete.

23.4.2.5.3 Assigning displays via display activation

Assigning the displays via the display activation allows displaying the objects of several displays simultaneously. Assign the displays via the display activation as follows:

1. Select the **Display** object on the **Interfaces** tab. In the **+Activate** table in the **Number** column, select the display number from the drop-down list (**1**).



2. In the **Name** column (**2**), select the display name from the drop-down list.
3. Click the **Apply** button (**3**).

According to this configuration, when the Display 1 is displayed, both the Display 1 and the Display 2 objects will be displayed.

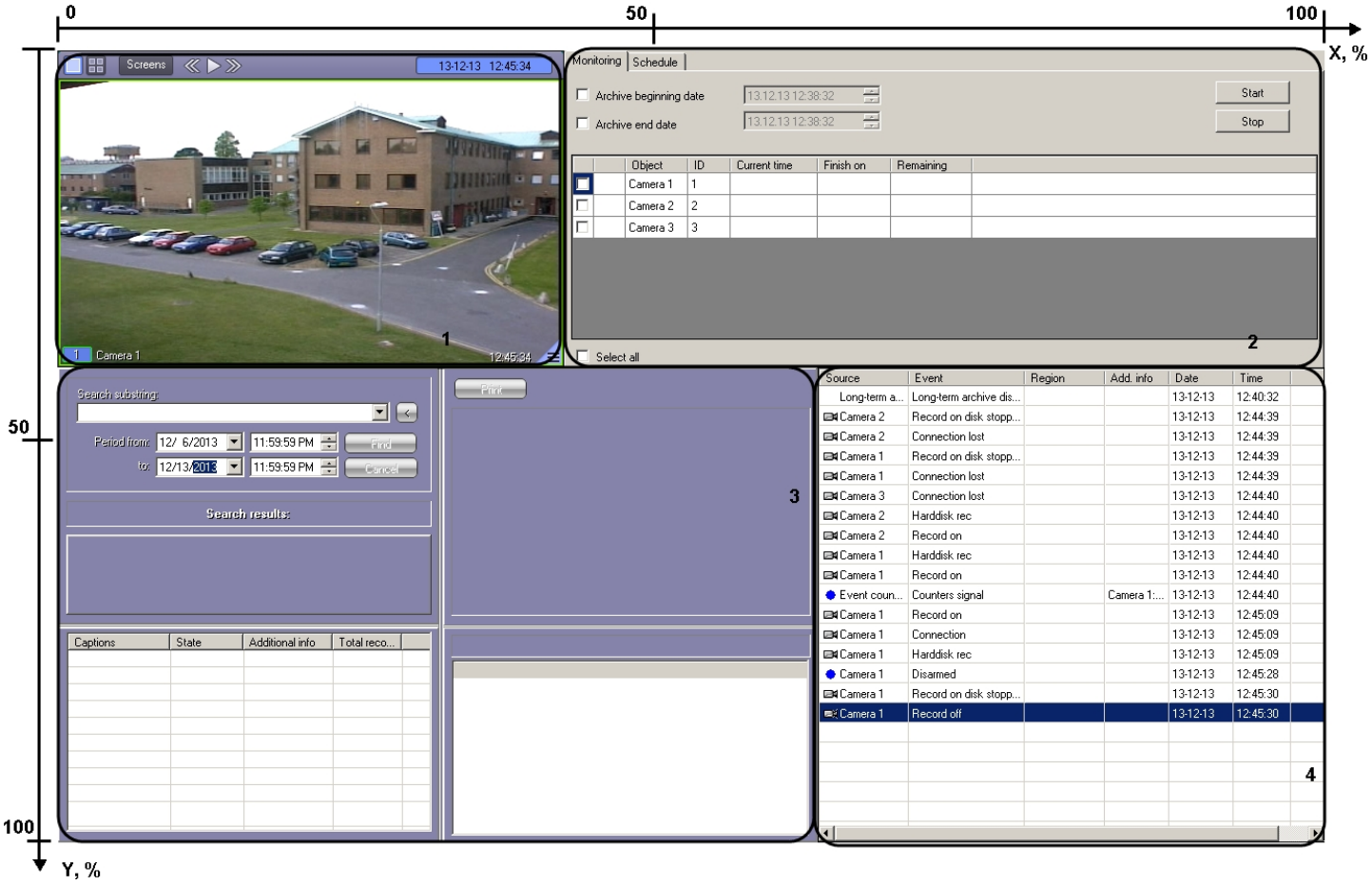
> **Note**
>
> To delete the display from the **+Activate** table, click on the corresponding line and press Ctrl+Del on the keyboard.

Assigning the displays via the display activation is now complete.

23.4.2.6 Examples of the user interface configuration

Figure below shows an example of the user interface components placed on the screen. Corresponding coordinates are given in the table.

	Interface component	**X, %**	**Y, %**	**W, %**	**H, %**
1	Monitor	0	0	40	40
2	Panel of Backup archive	40	0	41	60
3	Search by captions	0	40	60	60
4	Event Viewer	60	40	40	60



23.4.3 Configuration of video display

23.4.3.1 Configuring video display on Video Surveillance Monitor

23.4.3.1.1 General information on video signal displaying

With different video signal transmission modes, different video monitors are used:

1. Video server surveillance Monitor.
2. Video surveillance Monitor of the Remote Workstation, connected to the server via TCP/IP net.
3. Video monitor of the *Web-server*, displayed in web browsers on Remote Workstations, connected to the server via the web-server module over HTTP protocol.
4. Video monitor of the iOS or Android mobile client.

Video surveillance monitors on the server and Remote Workstations, connected to the videoserver via TCP/IP local net, are identical. Video surveillance monitors on the videoserver and on Remote Workstations are set up with the **System Setting** dialog box and is described below.

> **Important!**
>
> Specify the Server IP address (or DNS) while configuring the interaction between components in distributed architecture in order to transmit video to Video surveillance Monitors of the Remote Workstations – see Configuring the interaction of distributed system components.

To set up the video surveillance monitor of the Web-server module, Java-applet settings of its home page are changed (see the chapter Configuring the Web-server module).

The video monitor is used to:

1. display video signals;
2. play back the archives;
3. change the sequence of displaying video signals (surveillance windows layout, selection of video signals to be displayed in the surveillance windows, windows slide show, etc.);
4. process the displayed signals (deinterlacing, zooming, image sharpening and changing contrast);
5. export and hardcopy selected frames, export video and audio records;
6. control detectors, including camera alarm detectors (main motion detectors);
7. control video recording;
8. control PTZ devices and microphones.

Attention!

When you work with the Video Surveillance Monitor, it is not recommended to use automatic lock in Windows OS, because after each unlocking, the Server takes some time to restore the display of the video signal. Therefore, the more Displays, Video Surveillance Monitors and cameras are in your system, the longer the restore will take.

Video surveillance monitor operation

23.4.3.1.2 Setup procedure for the Monitor object

To configure the **Monitor** object, do the following:

1. Select the **Display** and create the **Monitor** object for it (see Creating the Monitor object).

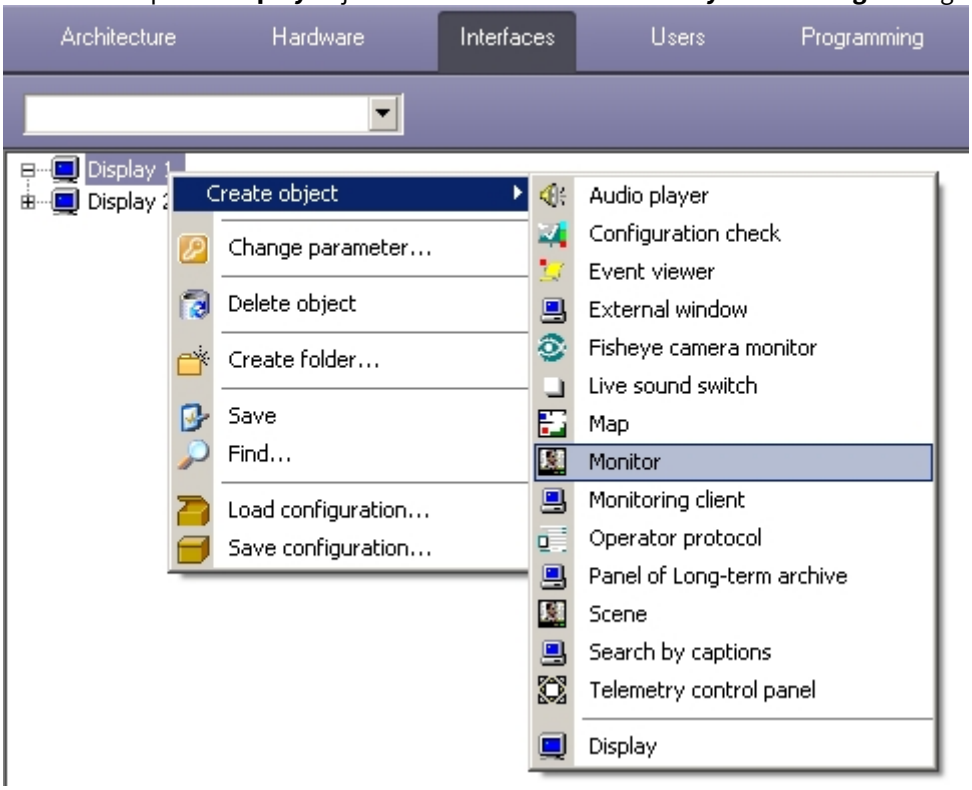
   Note

   The **Display** objects are created on the **Interfaces** tab of the **System setting** dialog box (see Creating a Display object).
2. Set the parameters of the **Monitor** interface box (see Setting the parameters of the Monitor interface box).
3. Select and configure cameras for displaying in the **Monitor** box (see Selecting and configuring video cameras or Selecting and configuring video cameras in bulk).
4. Configure an auto selection of video stream for displaying (see Configuring an auto select of video stream for displaying).
5. Configure the camera displaying mode (see Configuring the display mode of camera windows).
6. Select the video display mode (see Selecting the display mode).
7. Set the priority of PTZ device control (see Setting the Telemetry control priority using the Monitor object).
8. Configure the captions showing (see Configuring the captions showing).
9. Bind an Audio player to the Monitor (see Binding Audio player to the Monitor).
10. Configure a rotation angle of video image (see Configuring a rotation angle of video image).
11. Configure the interface of the Surveillance windows (see Configuring Video surveillance windows interface).
12. If necessary, enable and configure the display of Buttons (see Configuring buttons display on the Video surveillance monitor).

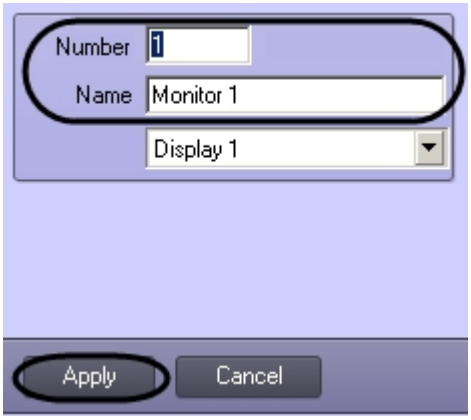
23.4.3.1.3 Creating the Monitor object

To create the **Monitor** object, do the following:

1. Select the required **Display** object in the Interfaces tab of the **System settings** dialog box.



2. Double-click the right mouse button upon the selected **Display** object and select **Create object > Monitor** in the contextual window.



3. Set the number and name of the **Monitor** object and click the **Apply** button. As a result the settings panel for the **Monitor** object will be displayed.

> **Important!**
>
> The **Monitor** object number should be a positive integer. You should not use numbers containing commas, dots or any other characters, otherwise the Monitor will become non-functional.

The **Monitor** object is now created.

23.4.3.1.4 Setting the parameters of the Monitor interface box

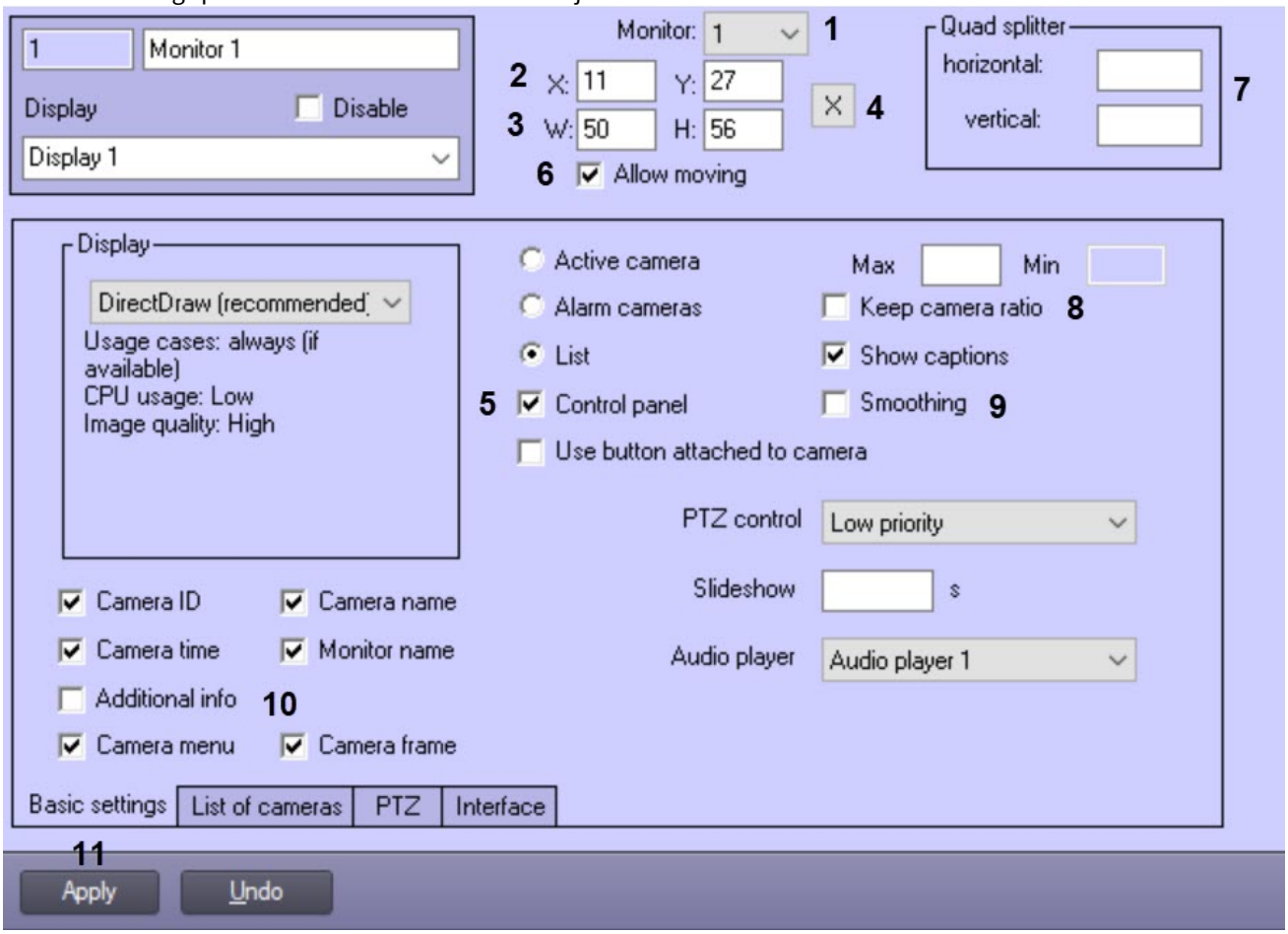
It is possible to set the following parameters of the **Monitor** interface box:

1. Window position.
2. Window size.
3. Toolbar (only in the List mode of camera's windows displaying—see Configuring the display mode of camera windows section).

4. Enable and disable displaying the number, name, time, menu and camera frame as well as additional info on the camera in the Surveillance window on the Video surveillance monitor.

To set the parameters of the **Monitor** interface box, do the following:

1. Go to the settings panel for the **Monitor** interface object.



2. In the **Monitor** drop-down list select the monitor number in the operating system for which coordinates are to be set further (**1**).
3. Set the position of the Monitor window in one of the following ways:
    a. Manually:
        i. Set coordinates of the left upper corner of the **Monitor** interface box: fields **X** (horizontal indent from the left edge of the image) and **Y** (vertical indent from the upper edge of the image) (**2**). Coordinates are set in percentage relative to the screen size horizontally and vertically correspondingly.
        ii. Set the dimensions of the Monitor interface box: **W** (window's width) and **H** (window's height) fields (**3**). Sizes are set in percentage relative to the screen size horizontally and vertically correspondingly.
        iii. To display a toolbar in the **Monitor** interface box the **List** group is to be switched in the **Basic settings** tab and the **Control panel** check box is to be set (**5**).

> **Note**
>
> If the toolbar is on, window's height **H** is automatically equal to the window's width **W**. The ability to set width less than 20% is also disabled in this case: such setting is saved but not applied.

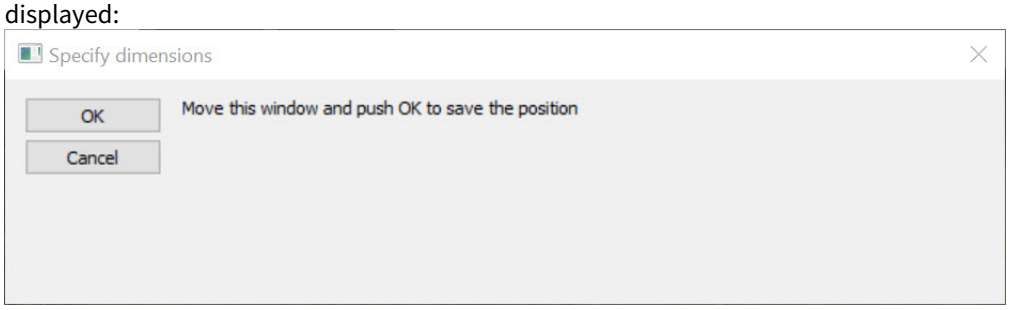
> **Note**

By manually setting the coordinates you can adjust the position of the **Monitor** interface box on several monitors at the same time. This can be used when setting up a video wall. For example, if it is necessary to stretch one **Monitor** window to two computer monitors, set **X**=0, **Y**=0, **W**=200, **H**=100. If it is necessary to stretch one **Monitor** window to four computer monitors, set **X**=0, **Y**=0, **W**=200, **H**=200.
Note that if there is one computer monitor, and **X** and **Y** coordinates are greater than 100 or width and height are greater than 100, the **Monitor** window will not be displayed on this single monitor or will be displayed incompletely.

Attention!

When configuring video wall using Windows, note that the load on video cards to which physical monitors for video wall are connected will be distributed unevenly and cannot be regulated by *Intellect*.
For an even load distribution on CPU and GPU, you should configure video wall using NVIDIA® Mosaic™ technology and NVIDIA Quadro Sync device (see NVIDIA documentation).

b. Using a test window:
   i. Click the **X** button (**4**).
   ii. Place the opened test window **Specify dimensions** in a position where the **Monitor** window should be displayed:



   iii. Click the **OK** button. As a result, the coordinates in the **X**, **Y**, **W**, **H** fields will be set in accordance with the size and position of the test window.

4. If moving the **Monitor** interface box is to be enabled, set the **Allow moving** checkbox (**6**).

Note

This setting is relevant only when the toolbar is in use.

5. In the **horizontal** and **vertical** fields of the **Quad splitter** group enter the number of video surveillance windows which will be displayed in the Monitor in horizontal and vertical directions correspondingly (**7**). If one of these values is not specified then default grid of video surveillance windows depending on the selected layout is displayed on the Monitor. The maximum number of video surveillance windows vertically and horizontally is 64 and 64, respectively.

Note

Fields in the **Quad splitter** group are inactive if the **Alarm cameras** mode is selected (see Configuring the display mode of camera windows).

Note

The **Quad splitter** settings will be ignored if the CycleByLayouts=1 key is set, which enables paging through layouts (see Registry keys reference guide).

6. If you want to save the ratio of the width and height of the video coming from the camera when displaying in the Surveillance window, then set the **Keep camera ratio** checkbox on the **Basic settings** tab (**8**). If the checkbox is set, there may be some empty space in the Surveillance window. If the checkbox is clear, the video fits the entire area of the Surveillance window while the ratio may be affected.

Note

Necessity to use other window proportions can occur while working with widescreen monitors, monitors of portrait orientation or in any other cases. The Monitor<monitor_id>_cw, monitor<monitor_id>_ch, monitor<monitor_id>_w43, monitor<monitor_id>_h43 registry keys are used in these cases. Detailed information about these registry keys is given in the Registry keys reference guide.

7. Set the **Smoothing** checkbox to display video with greater resolution on which the ladder effect appears while displaying in the small window (**9**).

Note

When using the smoothing function, the load on the CPU of the computer where the video is displayed increases significantly (up to 30%). As a result, if the computer does not have enough resources to use this function, the video display speed (fps) decreases, the response to telemetry commands slows down, etc. So, this setting is recommended only for displaying video from analog cameras or low-resolution video.
The function affects only displaying the video in the Video surveillance monitor. The original video stream from the camera is streamed to the archive and to detection tools.

Video image with the Smoothing function

Video image without the Smoothing function

8. By default, all elements of the Surveillance window (such as number, name, time, menu and camera frame, as well as the name of video surveillance monitor) are displayed except for additional info on the camera (see Additional information on camera). To disable displaying these elements set the corresponding checkboxes clear (**10**).

> **Note**
>
> These parameters were set using ShowName, ShowTime, ShowTitle, ShowBorder, ShowButtons and ShowID registry keys (see Registry keys reference guide) until *Intellect* version 4.10.1.
> The date can be displayed on the video next to the camera time if the ShowDate registry key is set.

9. To save all the changes, click the **Apply** button (**11**).

The parameters of the **Monitor** interface box are now set.

23.4.3.1.5 Selecting and configuring video cameras

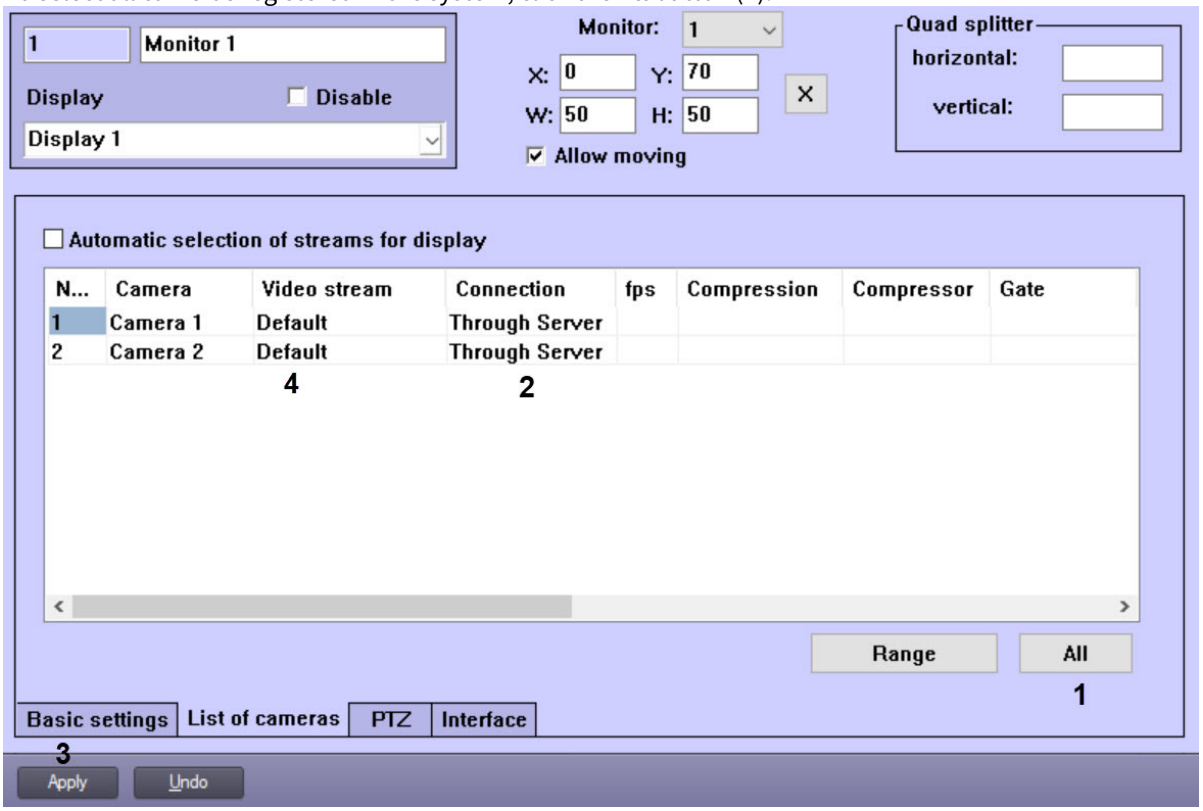
You can select and configure cameras for displaying in the **Monitor** interface window in two ways:

1. Separately. The settings panel of the **Monitor** object is used.
2. As a package. The **Add/Edit Camera Objects** dialog box is used.

> **Note**
>
> Order of selecting video cameras as a package to display in the **Monitor** interface box is described in Selecting and configuring video cameras in bulk.

To select video cameras on the settings panel of the **Monitor** object, do the following:

1. Go to the **List of cameras** tab.
2. To select all cameras registered in the system, click the **All** button (**1**).



3. To add a separate camera, configure the following settings in table (**2**):
   a. From the drop-down list in the **Number** column, select the number of the required camera.
   b. As a result, the name of the selected camera will be automatically displayed in the **Camera** column.

c. If multistream mode is enabled for the camera, in the **Video stream** drop-down list, select the number of the video stream that you want to display on the Monitor (**4**). If no stream is selected, the default stream is used.

> **Note**
>
> Configuration of the Server video streams is described in Configuration of multistream video. The selected video stream is requested when receiving a video signal both from the Server and via the Videogate.

d. By default, the Monitor receives a video stream through the Server. If it is necessary to get the video stream not through the Server, but directly from the camera, in the **Connection** drop-down list, select **Direct**.

e. If a video signal needs to be decimated for its transmission to the Client Monitor, select the required frame rate of the video signal from the drop-down list in the **fps** column.

> **Attention!**
>
> It is strongly not recommended to use additional decimation and/or compression of the video signals displayed on the Server Monitor, as it will lead to the additional spending of the Server resources and deterioration of the video quality.

> **Note**
>
> The selected FPS value should be less than the frame rate of the video digitising by a video capture card. Otherwise, the frame rate of the video signal will be the same as the FPS of digitising.

> **Note**
>
> For the correct decimation of a video stream compressed using the H.264 or MPEG4 codecs, the FPS value should be equal to the frame rate of the key frames specified in the device settings (IP cameras) or *Intellect* settings (see Key frame rate settings).

> **Note**
>
> Four streams for a chip are processed on SC300Q16 (FX4) video capture card. If the chip processes a stream without a signal (blue screen), then the total FPS is 10 (4 x 2,5 FPS) for one chip.

f. If video signal compression level needs to be changed for transmission to the Client Monitor, select the required level of video signal compression from the drop-down list in the **Compression** column. The compression level of the video signal increases from 0 (no compression) to 5 (maximum compression).

> **Note**
>
> If the compression level is set for the Client, the video signal on the Server needs to be pre-decompressed, which will result in a great load increase on the CPU of the Server.

g. To change the algorithm of the video signal compression for transmission to the Client Monitor, select the required algorithm of compression from the **Compressor** drop-down list. If the compressor is selected, the value in the **Compression** list is should be selected as well.

> **Note**
>
> Recompression of the video signal is performed on the Videogate side.

h. If the Monitor should receive live and archive video from the selected camera via the **Videogate** object, select the name of this object from the drop-down list in the **Gate** column.

i. If a video archive from the selected camera should be transmitted to the Monitor from the **Backup archive** object, select the name of this object from the drop-down list in the **Backup archive** column.

> **Note**
>
> In case the access to the Backup archive is performed through the Videogate, the specified value should coincide with the selected value for this video camera when configuring the **Videogate** object—see Selecting and configuring the cameras for the Videogate module.

j. If the selected video camera is used for video archive viewing from the edge storage, select the required **Edge storage** object from the **Edge storage** drop-down list.
k. If the tansmission from the **Backup archive** object is performed via the **Videogate** object, select the name of this object from the drop-down list in the **Videogate for Backup archive** column.
l. To enable smart search in the archive of the corresponding camera, select the **VMDA metadata storage** object corresponding to the VMDA tracks database intended to be used for smart search from the **VMDA metadata storage** drop-down list.
m. If there is a fisheye or a panomorph lens on the camera (see Configuring fisheye cameras), in the **Display type** drop-down list, select the type of displaying video from the camera in the Surveillance window: virtual telemetry or panorama.

> **Note**
>
> Conversion is enabled in the Video surveillance monitor when zooming-in (see Mouse PTZ control) or in the function menu of the Surveillance window (see Enabling fisheye).

> **Note**
>
> **This feature won't work if:**
>
> - **only alarm cameras are displayed on the monitor (see** Configuring the display mode of camera windows**);**
> - **PTZ control on the Video surveillance monitor is forbidden (see** Setting the Telemetry control priority using the Monitor object**).**

n. If it is necessary to start macros from the camera function menu in the Surveillance window, select the corresponding **Macro** objects from the **Macro 1** and **Macro 2** lists. See also Creating and using macros.
o. The **Guid** column will automatically display the unique identifier of the selected camera. This value cannot be changed, it depends on the camera number.
p. Repeat steps a-n for all required video cameras.

4. To save all changes, click the **Apply** button (**3**).

Video cameras on the settings panel of the **Monitor** object are now selected.

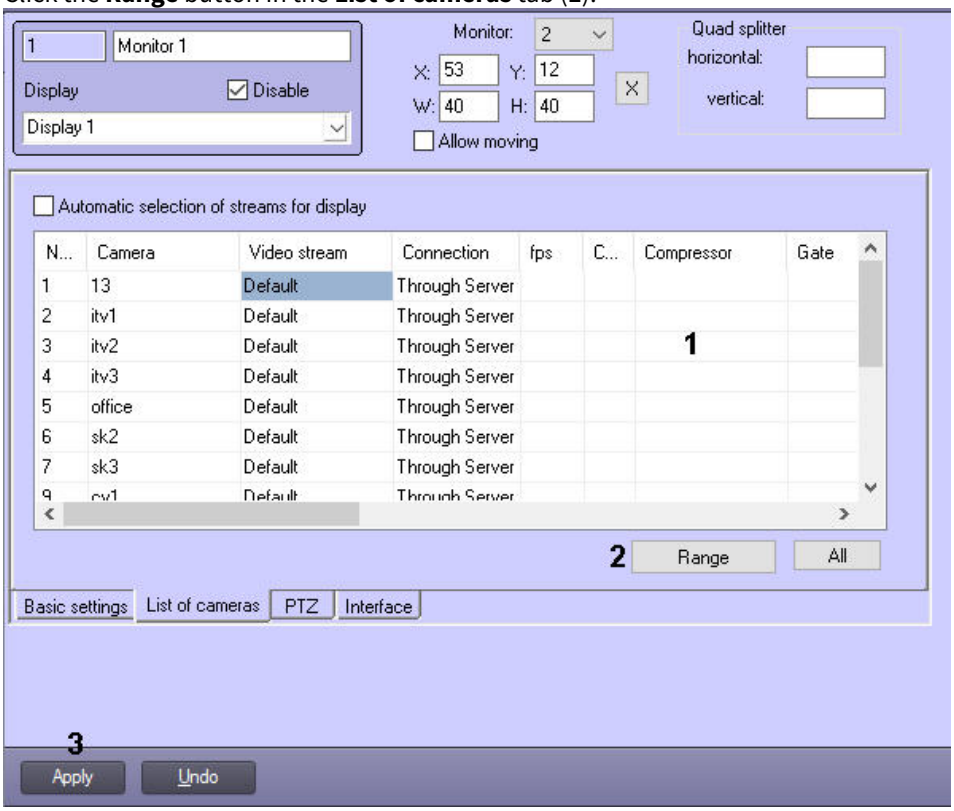
23.4.3.1.6 Selecting and configuring video cameras in bulk

You can select several cameras at once and edit their parameters to display them in the **Monitor** interface box.

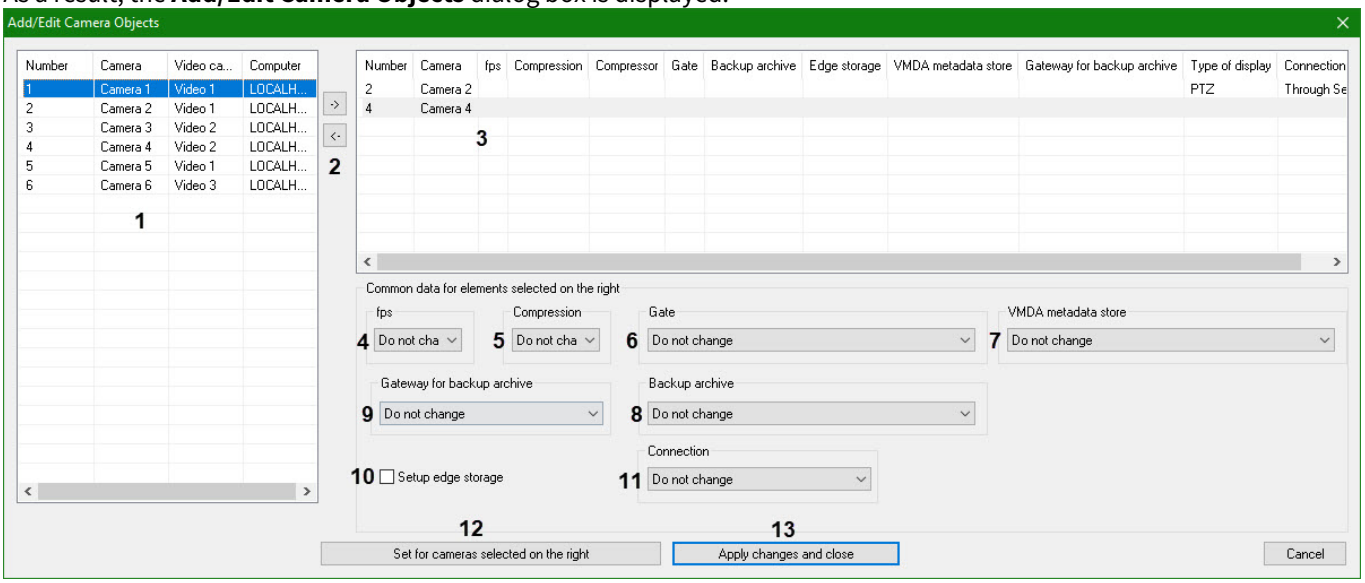
To select video cameras in bulk, do the following:

1. Go to the settings panel for the **Monitor** interface object.

2. Click the **Range** button in the **List of cameras** tab (**1**).



3. As a result, the **Add/Edit Camera Objects** dialog box is displayed.



4. Select the required cameras in the left list of the **Add/Edit Camera Objects** box (**1**).
5. Move the selected cameras to the right list by clicking the button (**2**).

> **Note**
>
> The right list is the list of cameras selected for displaying in the **Monitor** interface box.
>
> The button is used for inverse action, i.e. for moving the selected video cameras from the right list to the left one (**2**).
> In both lists, you can change the sorting by clicking on the column names to make it easier to find the required cameras and their settings.

6. As a result, the selected cameras will be displayed in the list on the right of the **Add/Edit Camera Objects** box (**3**).

7. If it is necessary, select the names of required cameras in the right list for complex editing of their parameters (**3**).

   Attention!

   The same parameters will be set for all selected cameras.

8. To enable decimation of a video signal for transmitting to the Monitor of the Client, select the required frame rate of a video signal in the **fps** drop-down list (**4**).

   Attention!

   It is strongly discouraged to set additional grooming and/or compression for video signals displayed on the Server Monitor: this will result in unnecessary consumption of the Server resources while the video image quality deteriorates.

   Note

   The selected fps value must be less than the frame rate of the video signal digitized by the video capture device. Otherwise, the frame rate of the video signal will be equal to the frame rate of the digitization.
   The **fps**, **Compression**, **Gate**, **Backup archive** and **Gateway for backup archive** settings are in the **Common data for elements selected on the right** group.
   For correct grooming of a video stream compressed with the help of H.264 or MPEG4 codecs, the fps value is to be equal to keyframe rate specified in the device (IP-camera) or *Intellect* settings (see Configuring video compression section).

9. If video compression level is to be changed for transmitting to the Monitor of the Client, select the required level of video signal compression in the drop-down list of the **Compression** column (**5**). Compression level is increased from 0 (no compression) to 5 (maximum compression).

   Note

   If the compression level is set for the Client, a video signal on the Server is to be preliminary decompressed, that results in a great load increase on CPU of the Server.

10. If the Monitor is to receive live and archive video from the selected cameras via the **Gate** object, then select the name of this object in the **Gate** drop-down list (**6**).
11. To enable smart search in the archive of the selected cameras, select the **VMDA metadata storage object** corresponding to the VMDA trajectories database intended to use for smart search from the **VMDA metadata storage** drop-down list (**7**).
12. If a video archive from the selected camera is to be transmitted to the Monitor from the **Backup archive** object, then select the name of this object in the **Backup archive** drop-down list (**8**).
13. If the transmission from the **Backup archive** object is performed via the **Gate** object, then select the name of this object in the **Gateway for backup archive** drop-down list (**9**).
14. If cameras are used to view video archive from external storage, set the **Setup edge storage** check box (**10**). As a result, for each selected camera, the external storage available to it will be applied.
15. By default, the Video Surveillance Monitor receives a video stream through the Server. If it is necessary to get the video stream not through a Server, but from cameras directly, in the **Connection** drop-down list select **Direct** (**11**).
16. To save the set parameters, click the **Set for cameras selected on the right** button (**12**).
17. As a result set parameters will be displayed in the list on the right of the **Add/Edit Camera Objects** box (**3**).
18. Repeat steps 6-12 for complex editing of all required cameras.
19. To save all the changes and close the **Add/Edit Camera Objects** box, click the **Apply changes and close** button (**13**).
20. Set camera settings will be displayed in the **List** table on the settings panel of the **Monitor** object (**2**).
21. To save all the changes click the **Apply** button (**3**).

Video cameras are now selected in bulk.

23.4.3.1.7 Configuring an auto select of video stream for displaying

In *Intellect* it is possible to use scaling while video signal displaying on the Video surveillance monitor. This function allows choosing the optimal stream depending on the size of the video image. For example, if many cameras are simultaneously

displayed on the Video surveillance monitor, it is not needed to receive the video from them in high resolution. Increasing the video image the video stream should be requested in a higher resolution.

Video stream properties can be specified through the *Intellect* interface (see the section Configuration of multistream video) or through a camera's web interface.

For automatic video stream selection to work, the **Video stream setting** check box must be selected in the configuration panel of the **Camera** object (see the section Configuration of multistream video) and more than one video stream from the camera must be integrated (refer to the list of IP devices integrated with *Intellect*, on the Drivers Pack documentation page).

If the function of video stream auto select is enabled, *Intellec*t selects video stream the following way:

1. The streams indicated on the **Advanced settings** tab of the **Camera** object are selected (all streams that are not disabled).
2. From the streams chosen during the previous step, the streams that have a resolution greater than the resolution requested by the Client are selected. If no such streams exist, the streams with the highest resolution are selected.
3. From the streams chosen during the previous step, the streams that have a frame rate higher than the frame rate requested by the Client are selected. If no such streams exist, the streams with the highest frame rate are selected.

   Note

   The requested frame rate is specified during selection and configuration of cameras for the **Monitor** interface object, in the **fps** column on the **List of cameras** tab (see the section Selecting and configuring video cameras).
4. If multiple streams were selected during the previous steps, the stream among these that has the highest bitrate is selected.

If a stream is selected because it has the highest bitrate, another stream will be selected only if the new stream's bitrate is higher than the current bitrate by more than 5% (to avoid constant back-and-forth switching when bitrates are approximately equal). When video stream properties change, a decision to display a different stream is made only if confirmation for making a change is received within 35 seconds. This feature is also designed to avoid constant back-and-forth switching between video streams.

If automatic stream selection is enabled, selection will be performed for the cameras for which the **Default** video stream has been selected.

Any stream can be forbidden for display using the block_stream registry key (see Registry keys reference guide).

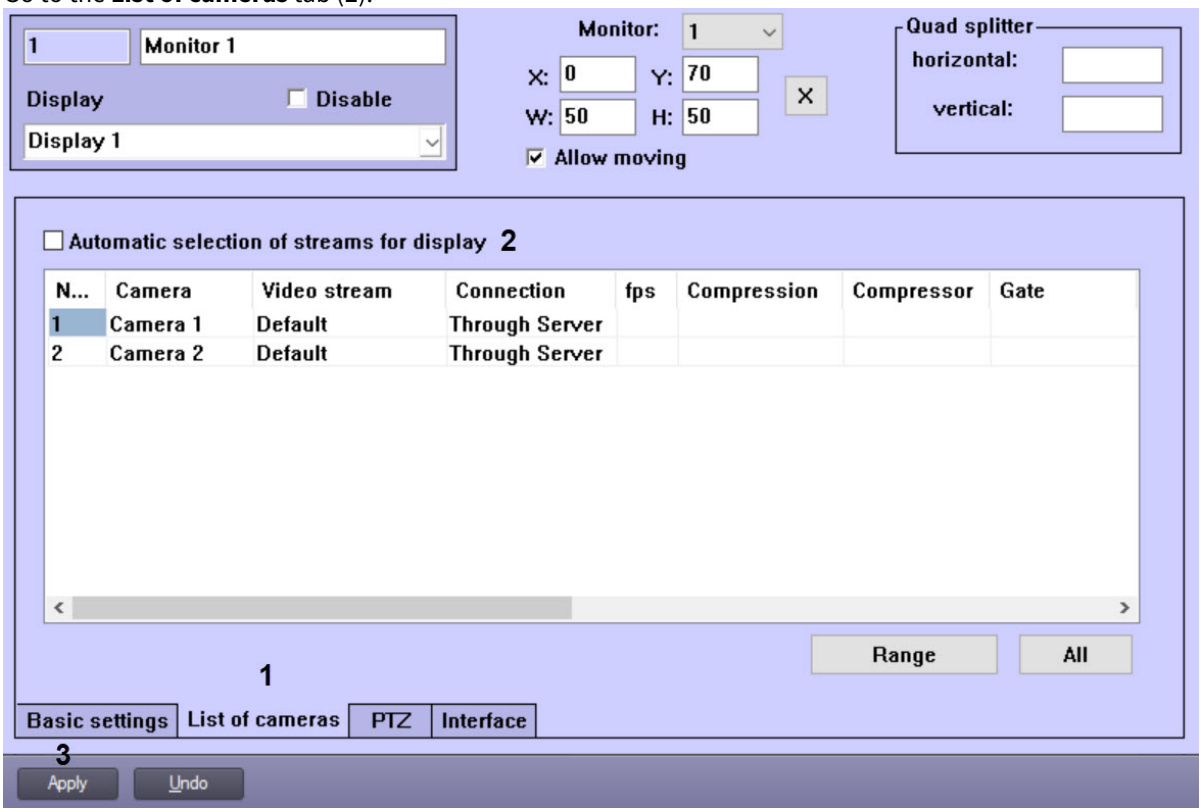
Note

When the layout of a viewing tile is changed in the Video Surveillance Monitor, the width of the viewing tile may change, causing another stream to be selected for display.

To enable the function of auto select of video stream for displaying, do the following:

1. Go to the settings panel of the **Monitor** interface object.

2. Go to the **List of cameras** tab (**1**).



3. Set the **Automatic selection of streams for display** checkbox (**2**).
4. Click the **Apply** button (**3**).

Configuring an auto select of video stream for displaying is completed.

23.4.3.1.8 Configuring the display mode of camera windows

To display camera windows (windows with video images) one of the following modes is used:

1. The **Active camera** mode. Only the active camera window is displayed in the **Monitor** interface window.

> **Note**
>
> To make the camera window active, left-click it. A camera window is switched to the active mode using another **Video surveillance monitor**. So, when the **Active camera** display mode is used, more than one **Monitor** object should be created in the system. If only one **Monitor** object is created and the **Active camera** display mode is selected for it, then surveillance windows won't be displayed on the monitor.
> Video from the camera selected on the Map or Operator protocol created on the basis of the same **Display** object as the **Video surveillance monitor** object is also displayed on the **Video surveillance monitor** in the **Active camera** mode.

2. The **Alarm cameras** mode. The windows of the alarm cameras are displayed in the **Monitor** interface window.
3. The **List** mode. Camera windows are displayed in the **Monitor** window according to the selected layout.

Functions available in the **List** mode:

1. Toolbar (see Setting the parameters of the Monitor interface box);
2. Slideshow.

The **toolbar** is displayed in the **Monitor** interface window and enables the following operations:

1. Select the number of the displayed cameras;
2. Set and use the layouts of cameras;
3. Control the slideshow.

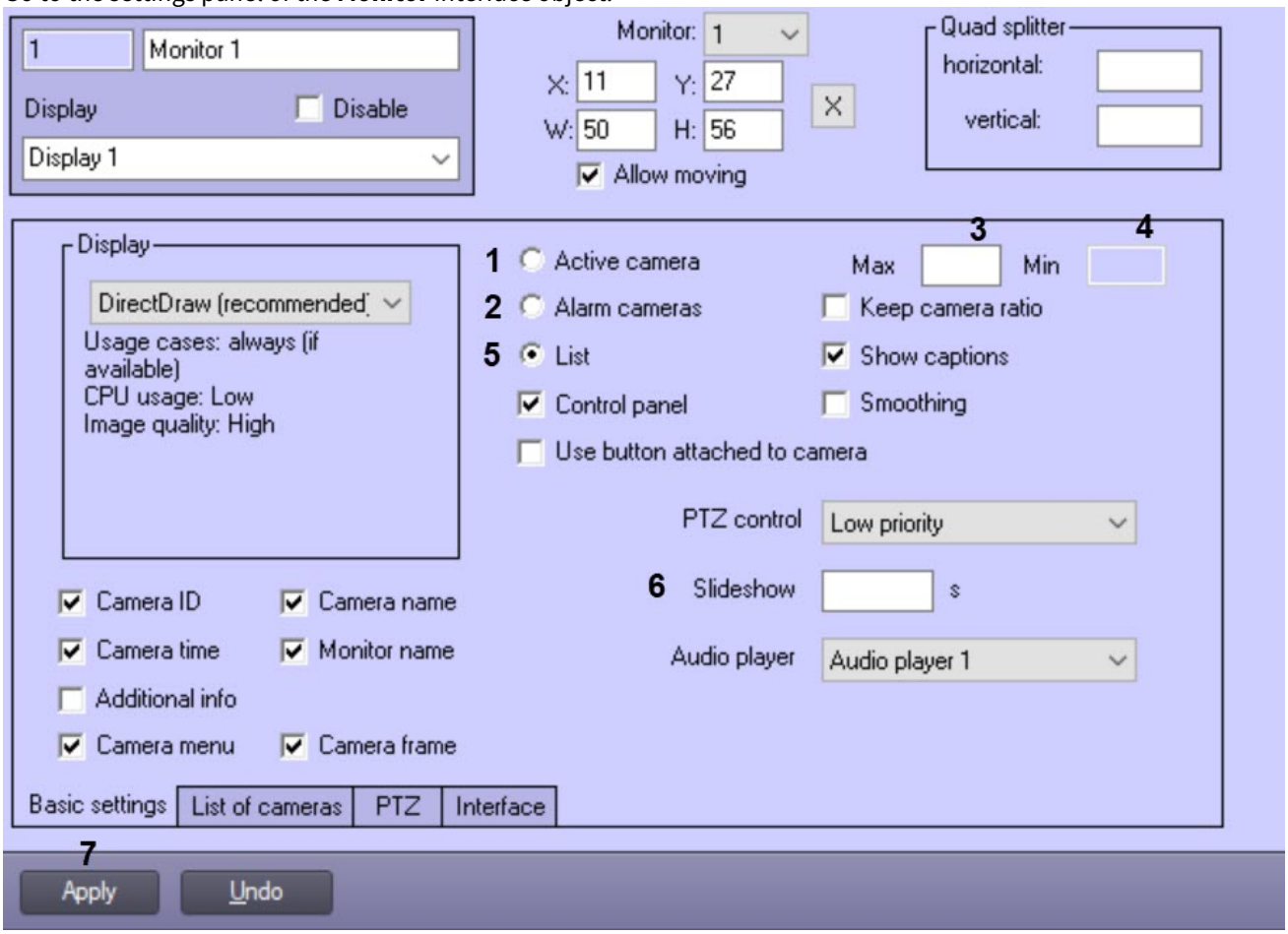
Current date and time are also displayed on the toolbar.

The **slideshow** is used for a successive close-up display of camera windows on the **Monitor.** Slideshow is performed with the help of the buttons on the toolbar of the **Monitor** in two ways:

1. Manually. Buttons for switching to the previous or next camera window are used.
2. Automatically. Switching to the next camera window is performed automatically in a set period of time.

To set the display mode for camera windows, do the following:

1. Go to the settings panel of the **Monitor** interface object.



2. To enable the **Active camera** mode, set the **Active camera** radio button in the **Basic settings** tab (**1**).
3. To enable the **Alarm cameras** mode, set the **Alarm cameras** radio button in the **Basic settings** tab (**2**). As a result, the **Min** field will be available.
4. In the **Max** field, specify the required maximum number of camera windows that should be displayed on the **Monitor** in the **Alarm cameras** or **List** mode (**3**). If the number of alarm cameras exceeds the maximum number, then the display of the camera windows, the alarms on which were registered earlier, is stopped.

> **Example**
>
> The **Monitor** object is set for operation with the maximum number of alarm cameras, equal to five. The windows of four alarm cameras are displayed in the **Monitor** window. Alarm events on these cameras were registered in the following sequence: Camera 1, Camera 2, Camera 3 and Camera 4. When alarm is registered on three more cameras, seven cameras are alarmed at the same time. This exceeds the maximum acceptable number, so the display of Camera 1 and Camera 2 windows is stopped.

If the number of cameras is less than the maximum or not specified, then camera windows fill the maximum available space of the **Monitor.**

> **Note**

In order for the camera windows in the **Monitor** to be displayed as symmetrical folds (1, 2x2, 3x3, 4x4, etc.), it is necessary to add the **TrySquareLayout** registry key (see Registry keys reference guide).

5. If the **Alarm cameras** mode is selected, then in the **Min** field, specify the required minimum number of cameras to be displayed on the layout of the **Video surveillance monitor** (**4**). If the number of the alarm cameras is less than the minimum number, the **Monitor** will display fewer cameras than specified in the **Min** field. The fold of the **Monitor** will correspond to the **Min** field. The following folds (number of camera windows) are available: 1, 4, 9, etc.
If there is no alarm, and if the default value of 0 (zero) is set for the **Min** parameter, the camera windows are not displayed in the **Monitor** window. By default, the **Min** field is empty.

   Example

   The **Monitor** object is set for operation with the minimum number of alarm cameras, equal to three. Windows of five alarm cameras are displayed in the **Monitor** window. When the alarm on four cameras is stopped in the sequence: Camera 1, Camera 2, Camera 3 and Camera 4, one camera is in the alarm mode. This is less than the minimum number, so Camera 5 will be displayed on the **Monitor**, and the **Monitor** will switch to the four-fold display.

6. To enable the **List** mode, set the **List** radio button in the **Basic settings** tab (**5**).
7. If necessary, specify the required value (in seconds) of automatic slideshow of the camera windows in the **Slideshow** field (**6**). The default camera windows scroll interval is 3 second. If you enter 0 in the field, the default value will be applied. The maximum possible value is 600 seconds.

   Note

   This setting is relevant only in the **List** mode when the toolbar is used.
   Instead of camera windows slideshow, you can enable layouts slideshow using the CycleByLayouts registry key (see Registry keys reference guide).

8. To save all the changes, click the **Apply** button (**7**).

The display mode of camera windows is now configured.

23.4.3.1.9 Selecting the display mode

Intellect allows you to select the video image processing mode prior to displaying it using the video card resources and DirectX libraries.

The video image processing improves the quality of the displayed image due to optimization of the color settings, spatial smoothing, and other processes of the graphics optimization. At the same time, the CPU load is reduced, as the video image is processed with the resources of the video card.

When selecting a display mode, consider if it is supported by the installed video card. If you select a mode that is not supported by the video card, the video signal will not be displayed correctly on the **Video surveillance monitor** (with a strong slowdown).

There are three display modes in *Intellect*:

1. **Direct3D** is a recommended mode and selected by default. This mode uses the most advanced Windows graphics libraries for rendering 2D and 3D graphics. It is necessary to use this mode when displaying a video signal from fisheye cameras or a signal decoded with the Intel QuickSync technology.

   Note

   If the fisheye camera added to the Monitor has the corresponding settings described on the Configuring fisheye cameras page, the Monitor switches to the Direct3D mode automatically.

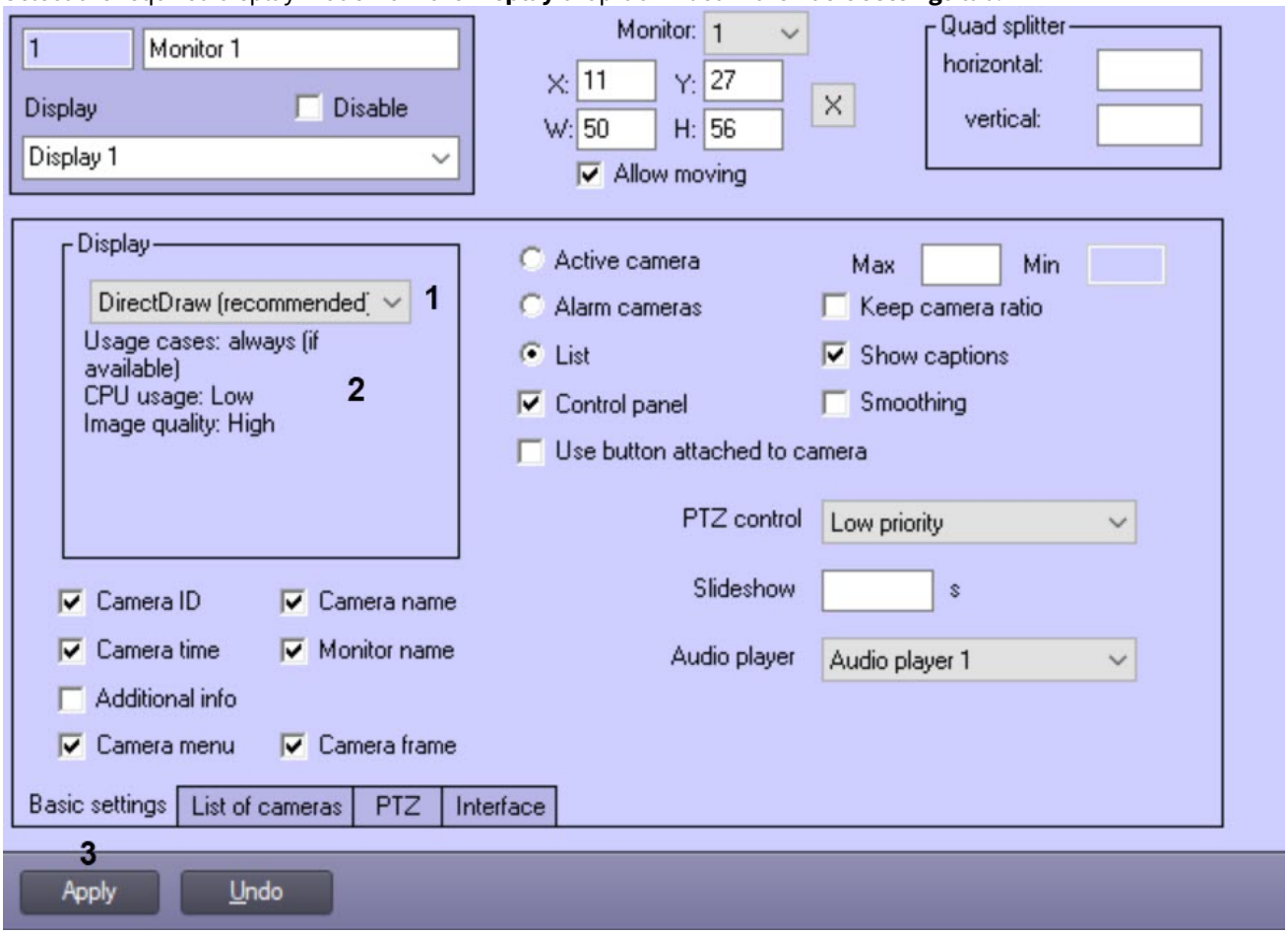
2. **DirectDraw** is a deprecated version of DirectX for processing 2D graphics. The mode should be used if the capacity of the video card is not enough to process in the **Direct3D** mode.
3. **Programmed**. Video signals from cameras are not processed by a video card. This mode should be used if *Intellect* is installed on a virtual platform (for example, VMware).

Note

For correct display mode operation in *Intellect*, installed as a Service, set the 0 value for the NoDesktop text parameter in the *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer* registry section. This parameter is responsible for displaying icons on the user's desktop.

To select a display mode, do the following:

1. Go to the settings panel for the **Monitor** interface object.
2. Select the required display mode from the **Display** drop-down list in the **Basic settings** tab.



Note

There is a description of the selected display mode in the field below the **Display** drop-down list.

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

The display mode is now selected.

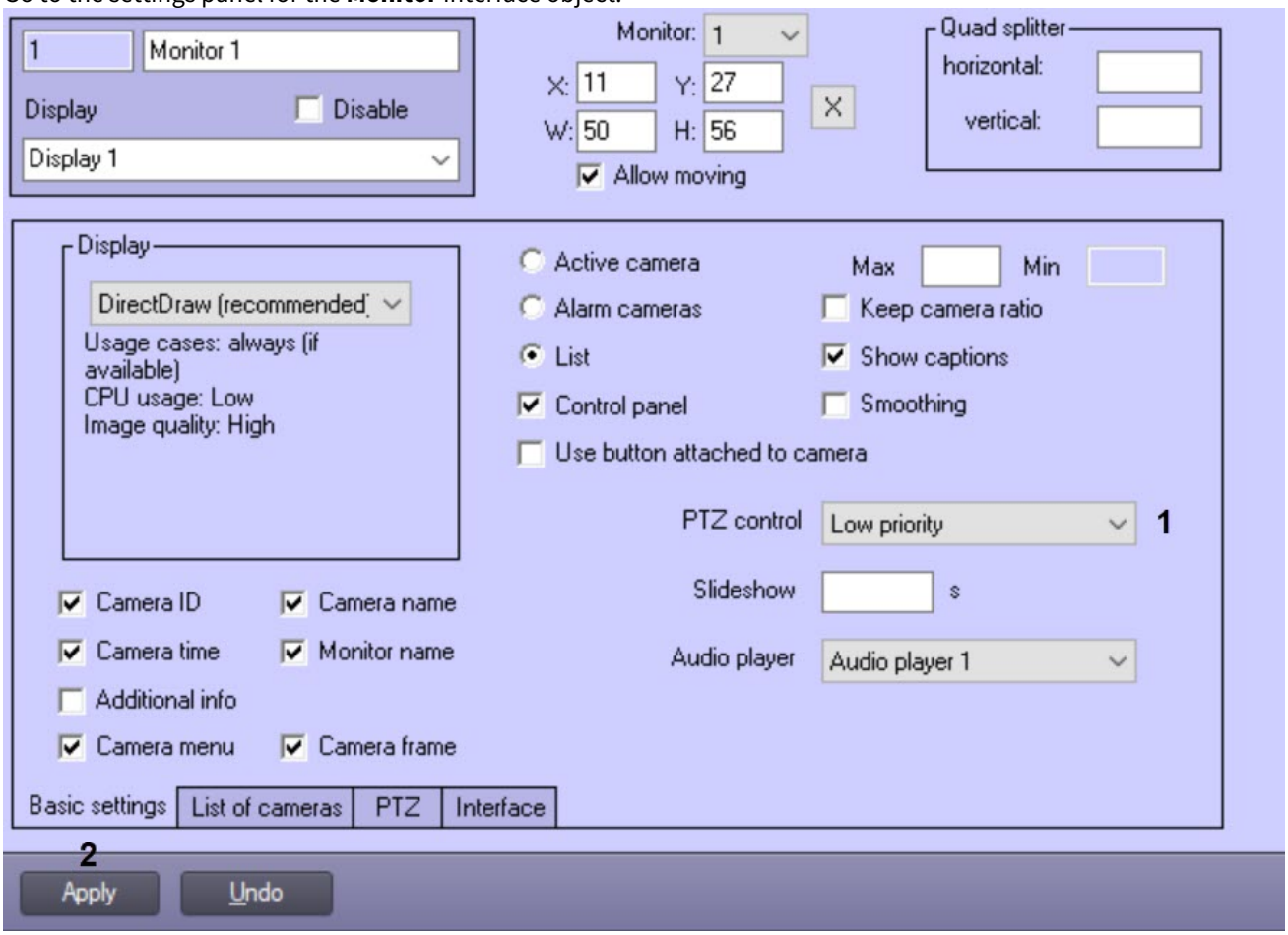
23.4.3.1.10 Setting the Telemetry control priority using the Monitor object

Intellect has an option of Telemetry control using the **Monitor** object. The control is performed with the help of a mouse or joystick.

By default, the **Telemetry control** option with the use of the **Monitor** object is disabled. To enable the **Telemetry control** option, the control priority is to be set for the **Monitor** object (see Installing and configuring security system components guide).

To set **Telemetry control** priority using the **Monitor** object, do the following:

1. Go to the settings panel for the **Monitor** interface object.



2. Select the required Telemetry control priority in the **PTZ control** drop-down list in the **Basic settings** tab (**1**).

> **Note**
>
> To disable **PTZ control** option using the **Monitor** object, select the **Forbidden** value.

3. To save all the changes, click the **Apply** button (**2**).

Telemetry control priority using the **Monitor** object is now set.

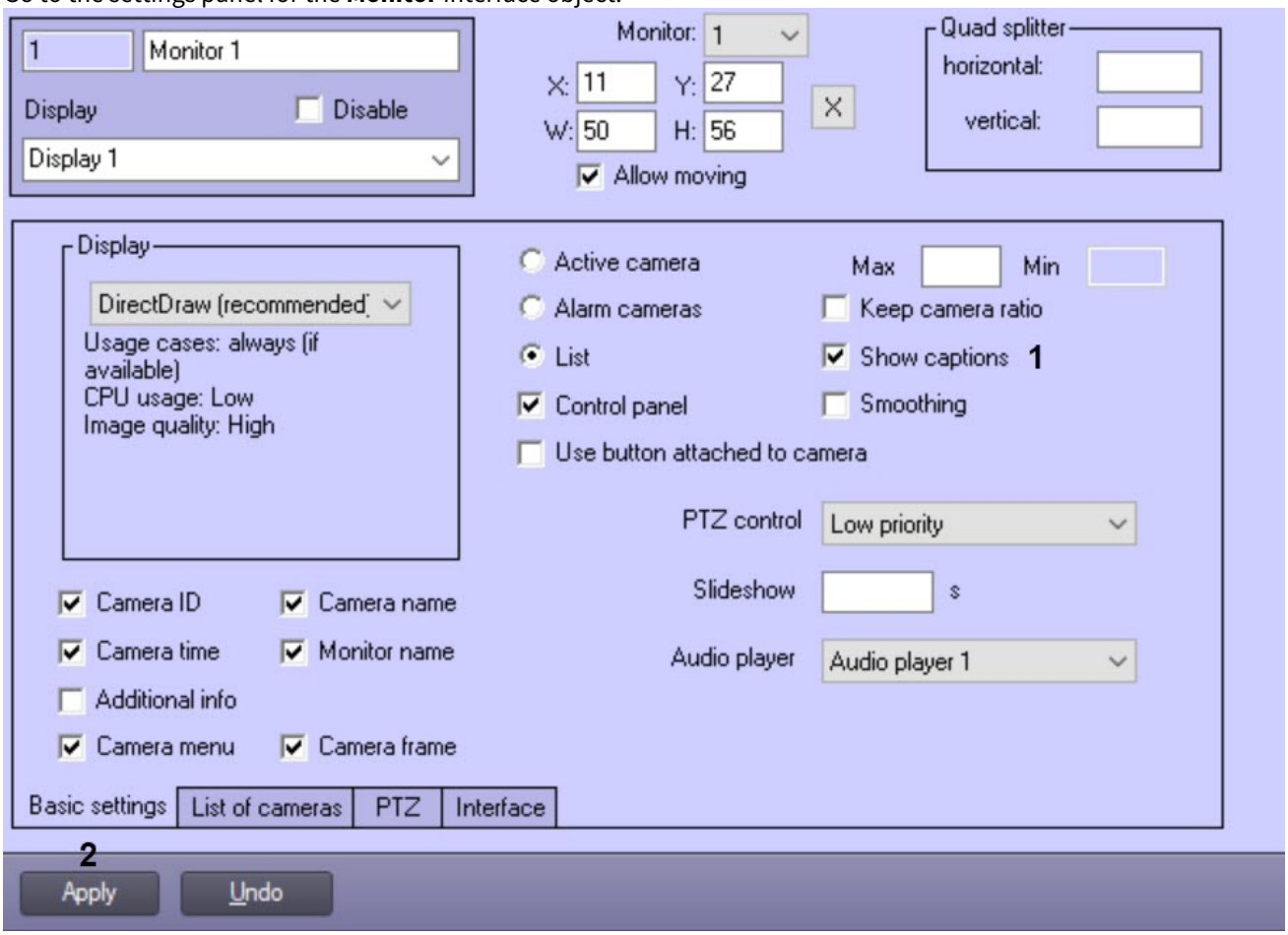
23.4.3.1.11 Configuring the captions showing

23.4.3.1.11.1 Enabling the captions showing

Intellect has the option of showing captions for a list of cameras that are displayed in the **Monitor** interface box. This option is enabled by default. In large distributed systems, it is recommended to disable captions on those monitors where captions are not planned to be shown in order to decrease the number of redundant events.

To disable the option of captions showing, do the following:

1. Go to the settings panel for the **Monitor** interface object.



2. To disable the titles showing menu, clear the **Show captions** checkbox in the **Basic settings** tab (**1**).
3. Click the **Apply** button to save the changes (**2**).

The option of captions showing is disabled.

23.4.3.1.11.2 Configuring captions display on a video image

The **Captioner** object is a child object of the **Camera** system object. It is designed for configuring titles display on a video recording and maintaining titles database.

This object allows setting the limits of titles output, font parameters and color of words. Titles are output into the field on a video recording from a camera.

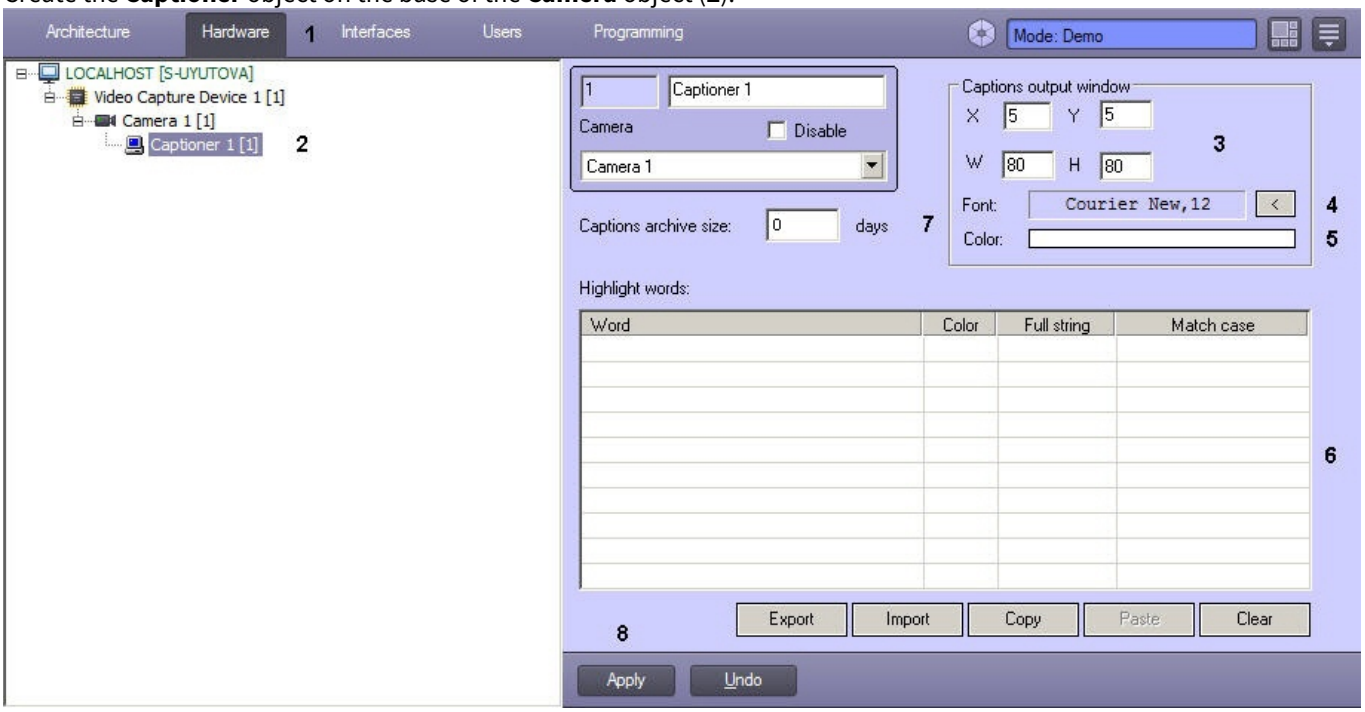
If the **Captioner** object is not created in the system, then titles are not displayed.

> **Note.**
>
> Titling on a video recording can be performed, for instance, using the scripts or programs in INTELLECT™ embedded language (see The Script object. Programming using the JScript language).

To configure the **Captioner** object, do the following:

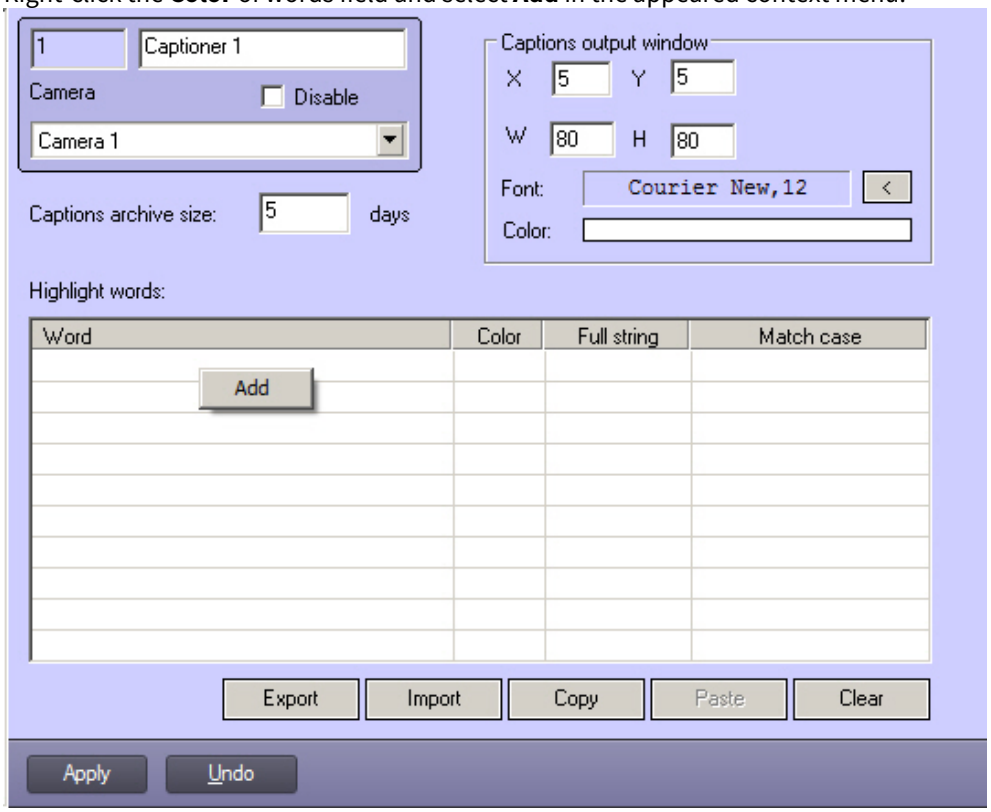
1. Go to the **Hardware** tab of the **System settings** dialog box (**1**)

2. Create the **Captioner** object on the base of the **Camera** object (**2**).

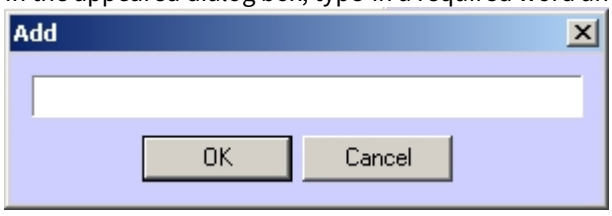


3. Specify the parameters of the titles output window (**3**):
   a. Set coordinates of the upper left corner of the titles output window: **X** (horizontal indent from left border of screen) and **Y** (vertical indent from top border of screen) fields.
   b. Set measurement of the titles output window: **W** (width of the titles output window) and **H** (height of the titles output window) fields.
4. Specify the parameters of font used for titles output:
   a. Click the < button (**4**).
   b. In the appeared Windows dialog box, specify font parameters and click **OK.**
   c. Double left-click the **Color** field (**5**)
   d. In the appeared Windows dialog box, select color and click **OK.**
5. Specify the parameters for words highlighting (**6**):

a. Right-click the **Color** of words field and select **Add** in the appeared context menu.



b. In the appeared dialog box, type-in a required word and click **OK**. The word is added to the **Color** of words table.



c. Specify the color with which the word will be highlighted by double left-clicking the **Color** field next to the specified word. In the appeared Windows dialog box, select color and click **OK.**
d. If the full string with a word is to be highlighted, then set the **Full string** checkbox.
e. If the case of word characters is to be matched, then set the **Match case** checkbox.
f. Repeat steps 5.1-5.5 for all required words.

> **Note.**
>
> Use the context menu for operations with words in the table (right-click a word). If the table is to be cleared, then click **Clear**.

6. If necessary, specify the maximum number of days as the difference between the newest and the oldest entry in the titles database for the given captioner in the **Captions archive size__days** field (**7**). Entries which were added earlier than the specified number of days before the most recent entry will be automatically deleted "in a loop". If the **0** (default) value is specified, the entries are deleted "in a loop" together with the video archive.

> **Example**
>
> For example, the titles archive size is 1 day. On Friday, the titles from the Captioner 1 were added to the titles database. On Saturday and Sunday the camera was turned off, and the titles were not recorded. On Monday the camera was turned on, and the titles from the Captioner 1 from Friday remained in the titles database until the new record was added to the titles database of the Captioner 1. In 3 minutes after the new record was made on Monday, the captions from Friday were deleted.

7. Click the **Apply** button (**8**).

The **Captioner** object is now configured.

> **Note.**
>
> Use the **Copy** and **Paste** buttons to import all settings from one **Captioner** object to another.
> The **Color of words** table can be saved and imported from a file. The **Export** and **Import** buttons are used to save and import the table.

23.4.3.1.12 Configuring buttons display on the Video surveillance monitor

23.4.3.1.12.1 Enable buttons display on the Monitor

In *Intellect,* you can add **Buttons** that will be displayed in the interface window of the **Video surveillance monitor**.

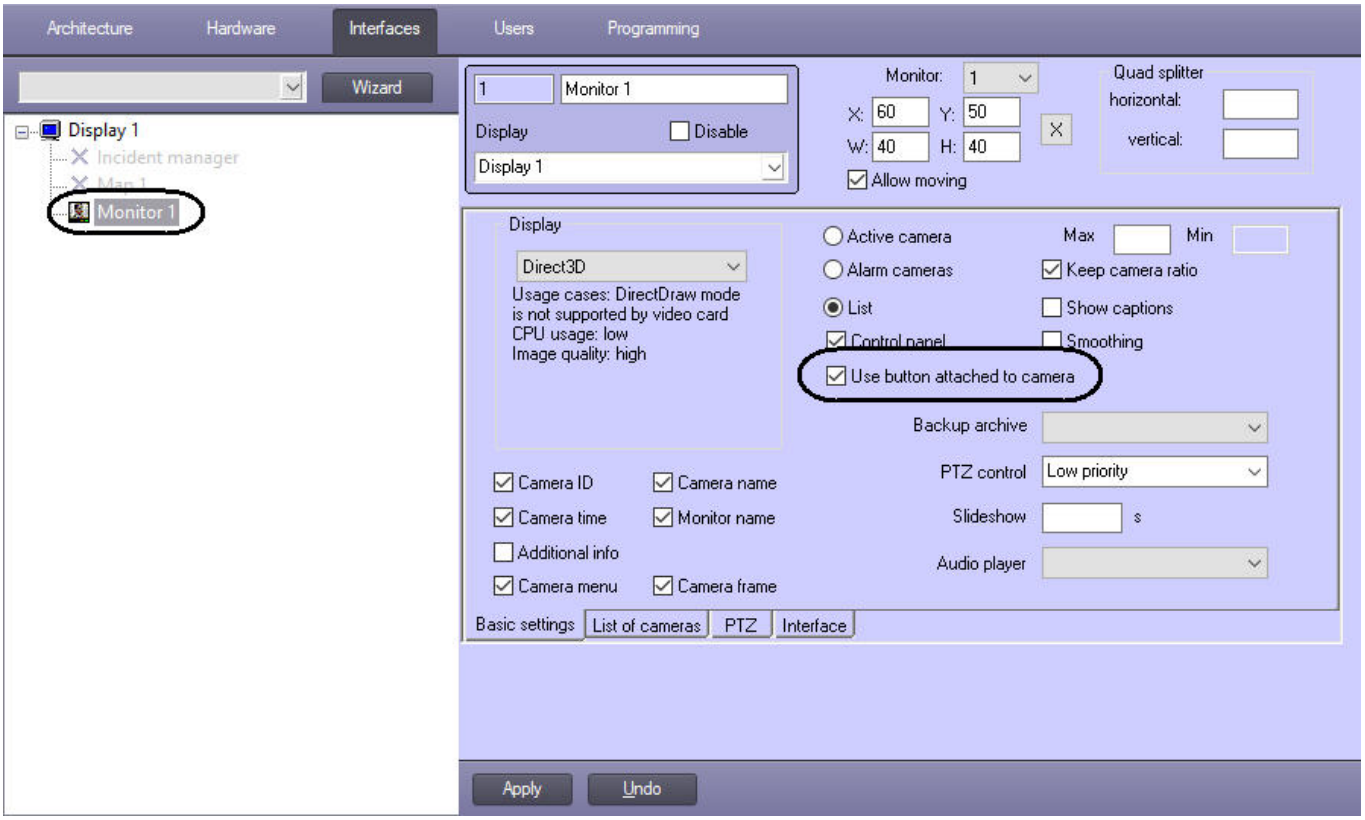
The actions when clicking such a **Button** are the following:

- switching to another camera;
- running a macro.

The **Button** can also perform no actions. The number of **Buttons** is unlimited. By default, the **Buttons** display is disabled.

To enable the **Buttons** display, do the following:

1. Go to the settings panel of the **Monitor** interface object.
2. Set the **Use button attached to camera** checkbox.



3. Click the **Apply** button.

As a result, the **Buttons** will be displayed in the **Monitor** over the video from the cameras for which the Buttons were created (see Configuring a button to display on the Monitor).

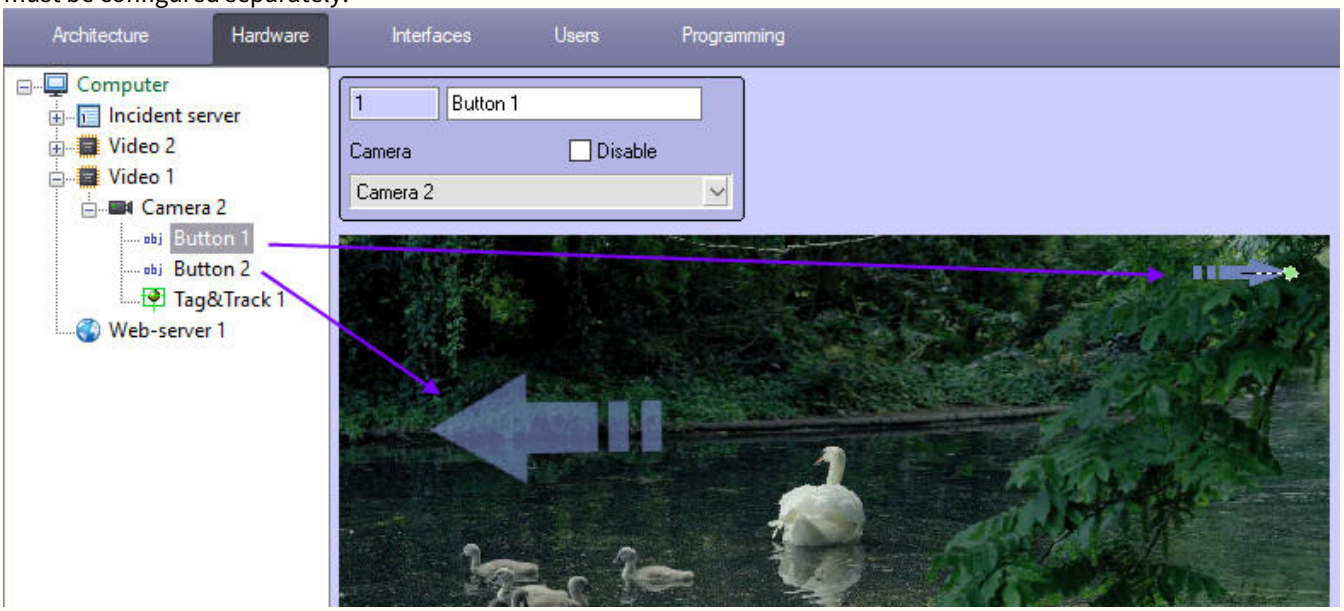
23.4.3.1.12.2 Configuring a button to display on the Monitor

The **Button** object is a child object of the **Camera** system object and is used to display the **Button** over the video image received from the parent camera. This page describes how to configure the appearance of a **Button**, as well as how to choose the action that will occur when the **Button** is clicked.

The **Buttons** display in the **Video surveillance monitor** must be enabled beforehand. If no **Button** objects are created in the system, they are not displayed.

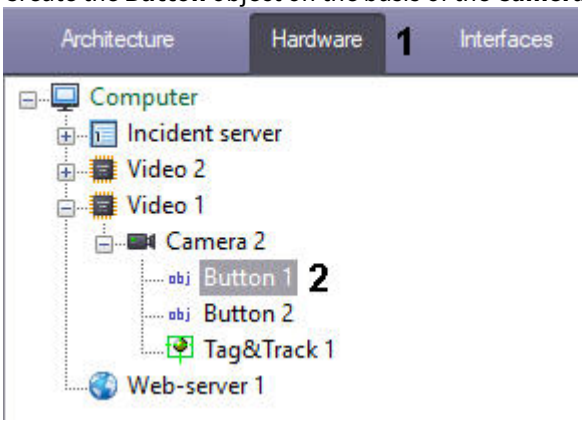
Attention!

Several **Buttons** can be created for the **Camera.** In this case, the preview window will display all created **Buttons**, and the setting described below will be applied only to the current (selected in the objects tree) **Button**, i.e., each **Button** must be configured separately.

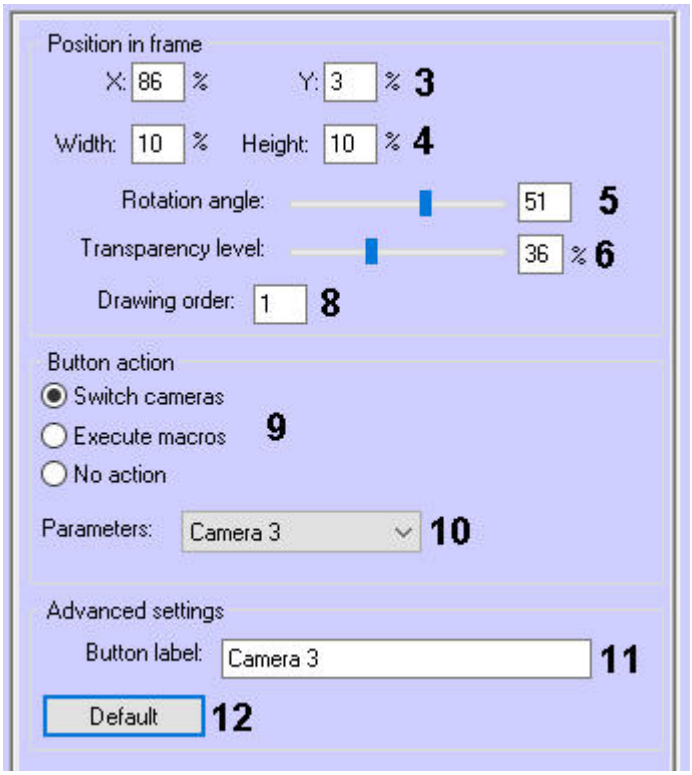


To configure the **Button** object, do the following:

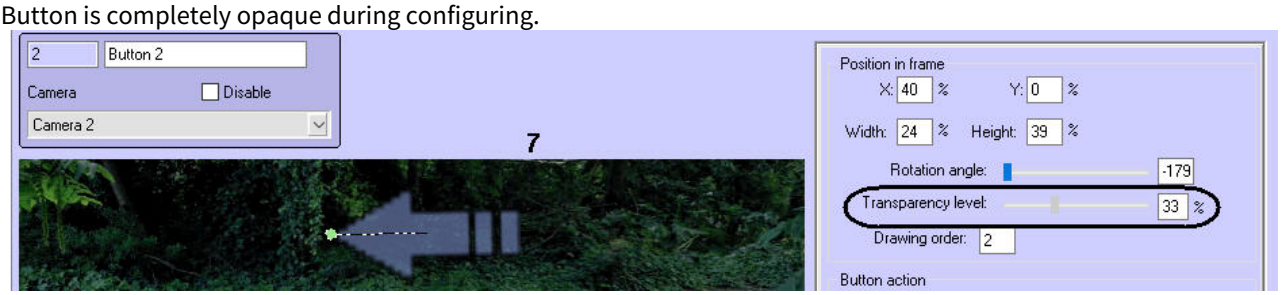
1. Go to the **Hardware** tab of the **System settings** dialog window (**1**).
2. Create the **Button** object on the basis of the **Camera** object (**2**).



3. Configure the position and display of the **Button** in the **Surveillance window**:
   a. the position of the top left corner of the Button is set by the **X** and **Y** fields (**3**). **X** is the horizontal indent from the left border as a percentage, **Y** is the vertical indent from the top border as a percentage. For example, if you set 50 and 50, then the left top corner of the Button will be in the middle of the Surveillance window.



b. in the **Width** and **Height** fields (**4**), set the size of the button as a percentage of the size of the Surveillance window.
c. set the **Rotation angle** of the Button in degrees from -180 to 180. By default, it is assumed that the button isn't rotated, the angle is zero (**5**).
d. set the **Transparency level** of the Button as a percentage (**6**). The feature of this setting: the real transparency will be displayed in the preview area (**7**) only when transparency is being edited with the slider. The rest of the time, the Button is completely opaque during configuring.



> **Note**
>
> You can configure the size and position of the Button not only by entering values, but also manually. To do this, in the preview area, after clicking the Button, you can:
> - drag the Button with the mouse;
> - stretch or shrink the Button, and rotate it, using the green anchor points on its perimeter.
>
> You can fine-tune the Button size and rotation angle manually: when Shift is pressed and when you drag the green circle with the mouse, the Button will change only its size. When Ctrl is pressed, the Button will change only its angle. When Shift+Ctrl are pressed, the Button won't change.

e. set the **Drawing order** of the configured Button in the corresponding field if several Buttons are created for one **Camera** (**8**). The setting determines the order in which the Buttons are drawn in the Surveillance window.

4. Select the **Button action**—what will happen when the Operator clicks the **Button** in the **Monitor** (**9**):
   a. Switch between the video images of the cameras. The cameras that will be controlled by the Button must be added to the Monitor (see Selecting and configuring video cameras), otherwise you won't be able to switch between the video images when you click the Button.
   b. Execute macros. The macros must be created beforehand (see Creating and using macros).
   c. No action.

5. From the **Parameters** drop-down list (**10**), select a specific action when clicking the **Button**. Possible values are determined by what action was selected in the previous step: it can be both available macros and the list of cameras between which you can switch.
6. If necessary, set the **Button label** in the corresponding field (**11**). To display a default label for the **Button** depending on the selected action, click the **Default** button (**12**). In this case, the label will contain the name of the camera, macro or current object.

> **Note**
>
> In the **Video surveillance monitor** interface, the label is displayed only as a tooltip when you hover the cursor over the **Button**.

7. Click the Apply button.

As a result, the **Monitor** will display the **Button** over the video image received from the **Camera** on the basis of which this **Button** was created.

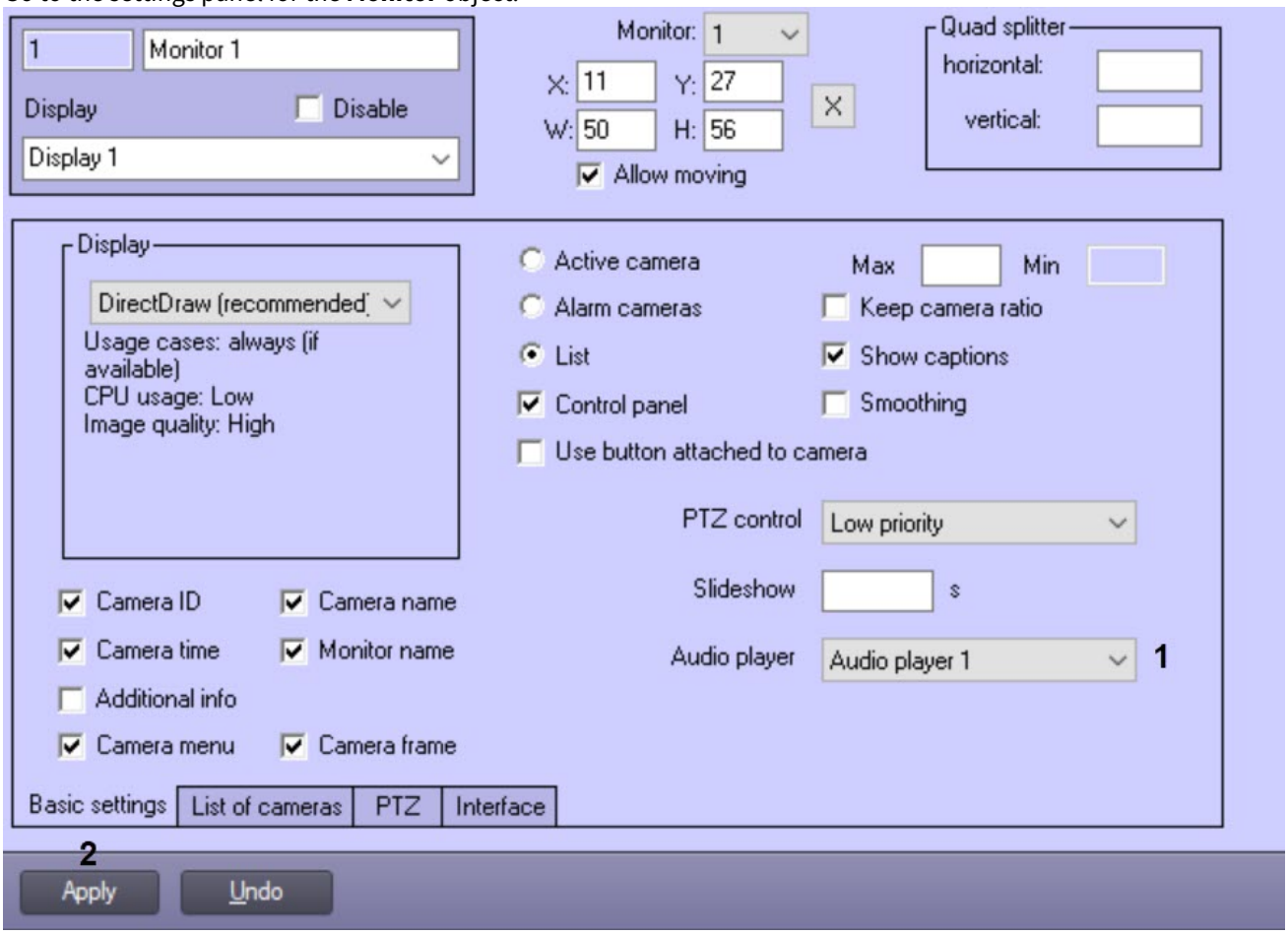
23.4.3.1.13 Binding Audio player to the Monitor

Audio player binding to the video surveillance monitor is for playback and export video with audio from the **Monitor** interface. Bind the Audio player, configured to playback audio received from microphones bound to cameras on which the playback and export are to be performed, to the video monitor.

Information on how to create and configure the **Audio player** object is given in Configuring audio signals playback using the Audio player object.

To bind the Audio player to the video surveillance monitor, do the following:

1. Go to the settings panel for the **Monitor** object.



2. In the **Audio player** drop-down list, select the previously created **Audio player** object that is to be used for playback and export of video with sound from the Monitor interface (**1**).
3. Click the **Apply** button (**2**).

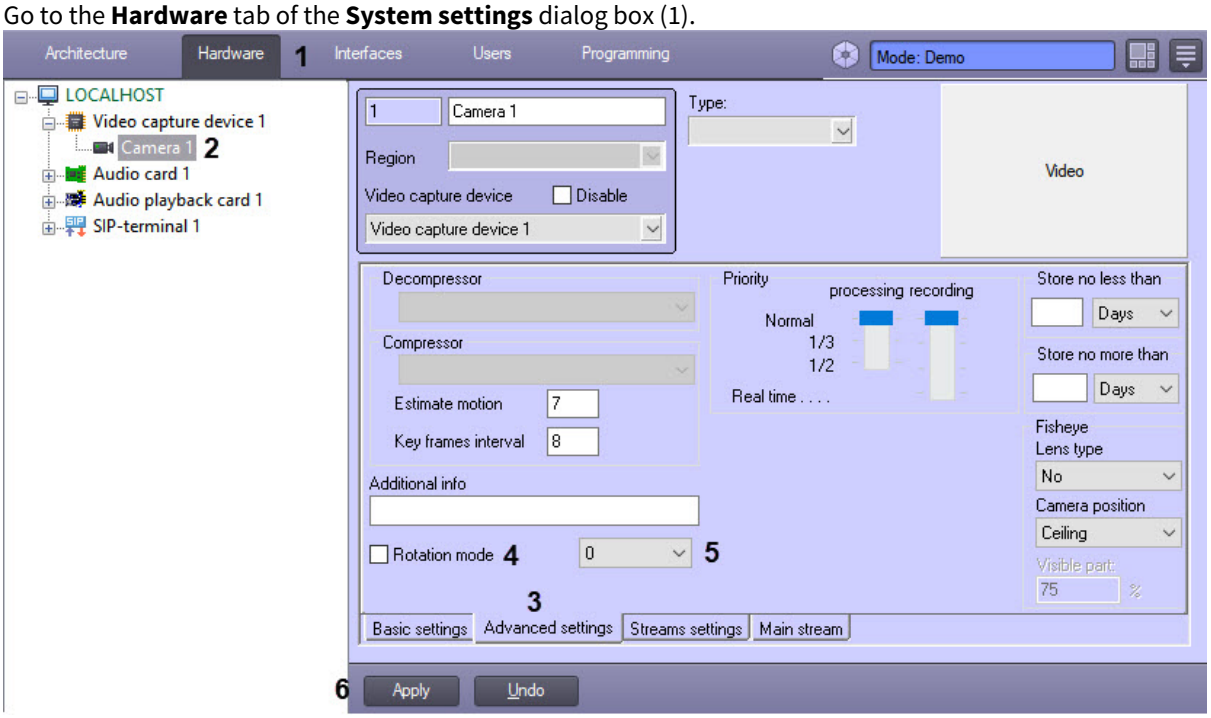
The Audio player is now bound to the Monitor.

23.4.3.1.14 Configuring a rotation angle of video image

In the Intellect software the image from the video camera can be panned while displaying it on the Video surveillance monitor and viewing the video archive. Available rotation angles are 90, 180 and 270 degrees.

To configure the rotation angle do the following:

1. Go to the **Hardware** tab of the **System settings** dialog box (1).



2. Select the **Camera** object corresponding to the video camera from which the video image is to be rotated while displaying (2).
3. Go to the **Advanced settings** tab (3).
4. Set the **Rotation mode** checkbox to activate the rotation function (4).
5. From the drop-down list select the rotation angle (5).
6. To save settings in the Intellect software click the **Apply** button (6).

> **Note.**
>
> On default the video signal is displayed in the Video surveillance window in initial non-rotated state. To rotate the video image select the **Pan** function in the **Processing** sub-menu of the Video surveillance window – see the Operator's Guide document.

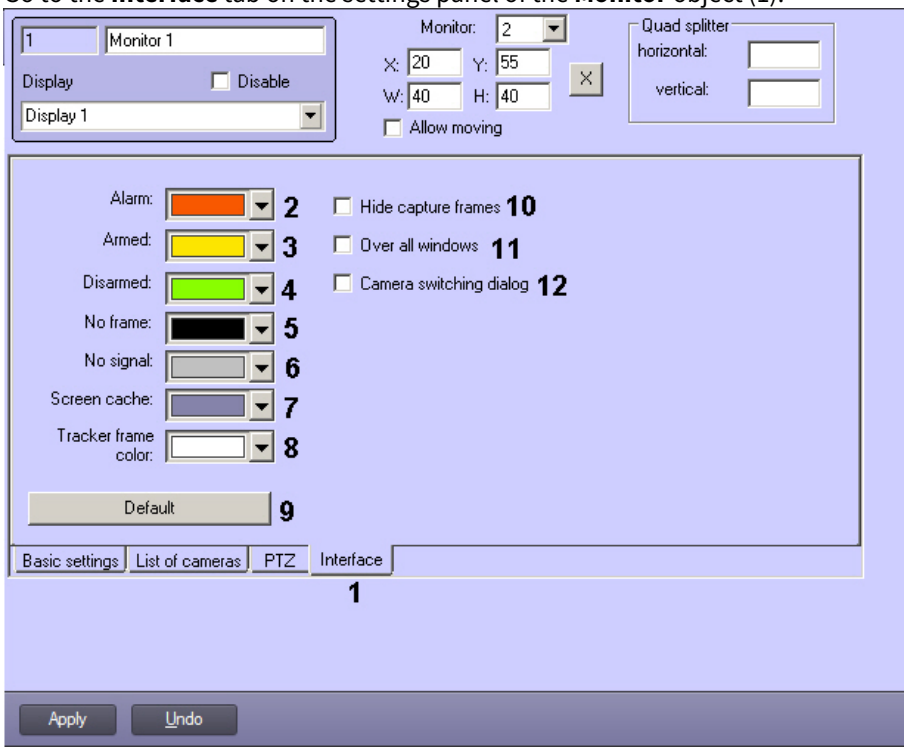
Configuring a rotation angle of the video image is completed.

23.4.3.1.15 Configuring Video surveillance windows interface

In the *Intellect* software package, it is possible to configure the interface of the Video surveillance window: the camera frame color in various states (alarm, armed, disarmed, no frame, no signal), displaying the frames of the Face Detection tool, and also displaying the Video Surveillance Monitor window on top of all windows.

Configuring the interface of the Video surveillance window as follows:

1. Go to the **Interface** tab on the settings panel of the **Monitor** object (1).



2. In the **Alarm** dropdown list select the Viewing tile frame color if there is an alarm on the camera (2). By default it is red.
3. In the **Armed** dropdown list select the Viewing tile frame color when the camera is armed and there are no alarms (3). By default it is yellow.
4. In the **Disarmed** dropdown list select the Viewing tile frame color when the camera is disarmed (4). By default it is green.
5. In the **No frame** dropdown list select the Viewing tile frame color when there is no frame from the camera in the Viewing tile (5). By default it is black.
6. In the **No signal** dropdown list select the Viewing tile frame color when there is no signal from the camera (6). By default it is grey.
7. In the **Screen cache** dropdown list select the Viewing tile background color that is displayed when the video from the camera does not overlay the Viewing tile, for instance, when the camera proportions are kept (7).
8. In the **Tracker frame color** dropdown list select the color of the frame highlighting the tracking objects detected by smart detection tools on the video image (8). See also Configuring smart video detection tools. In addition, the DrawDetectorColors registry key can be set to enable the frame color calculation depending on the background it is displayed on (see Registry keys reference guide).
9. Click the **Default** button to restore the default settings (9).
10. If frames shown by Face detection tool are not to be displayed, set the **Hide capture frames** checkbox (10). See also Configuring Face detection tool.
11. In order to show the Video Surveillance Monitor on top of all windows, set the **Over all windows** checkbox (11).
12. To enable a special dialog for selecting cameras to display in the Video surveillance window, set the **Camera switching dialog** checkbox (12). See also Selecting camera to display in Surveillance window.
13. Click the **Apply** button to save the changes.

The Viewing tile frame color is now configured.

23.4.3.2 Configuring object's panoramic view by means of the Scene object

Panoramic view window is designed for creating and using the panoramic image, composed from several cameras' view fields. Setting up the panoramic view window is performed by **Scene** object settings panel.

The **Scene** object setup is performed in the following way:

1. Select a screen and create the **Scene** object.
2. Set the parameters of the **Scene** interface box.
3. Select and setup cameras for displaying in the **Scene** window.

Note.

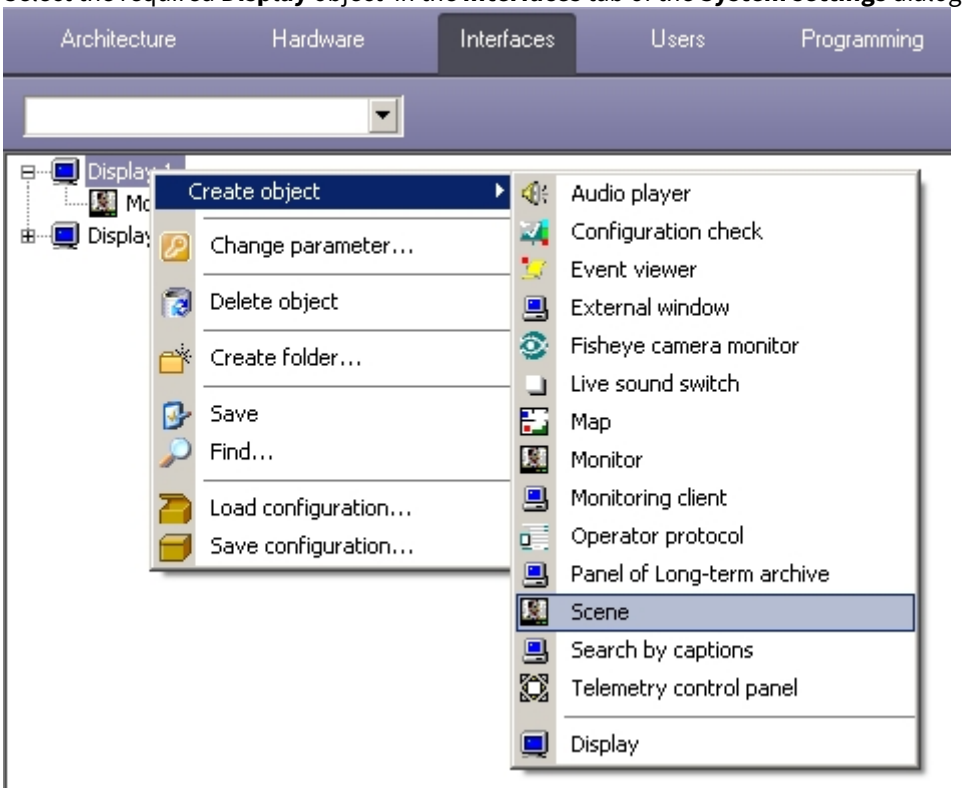
Working with Panoramic view window is described in detail in Operator's Guide.

Working with panoramic video surveilance window

23.4.3.2.1 Creating the Scene object

To create the **Scene** object, do the following:

1. Select the required **Display** object in the **Interfaces** tab of the **System settings** dialog box.



2. Make a right mouse click upon the selected **Display** object and select **Create object -> Scene** in the appeared context menu.
3. Set the name and number of the **Scene** object in the appeared window and then click the **Apply** button.

   Note.

   The settings panel for the **Scene** object will be displayed as a result.

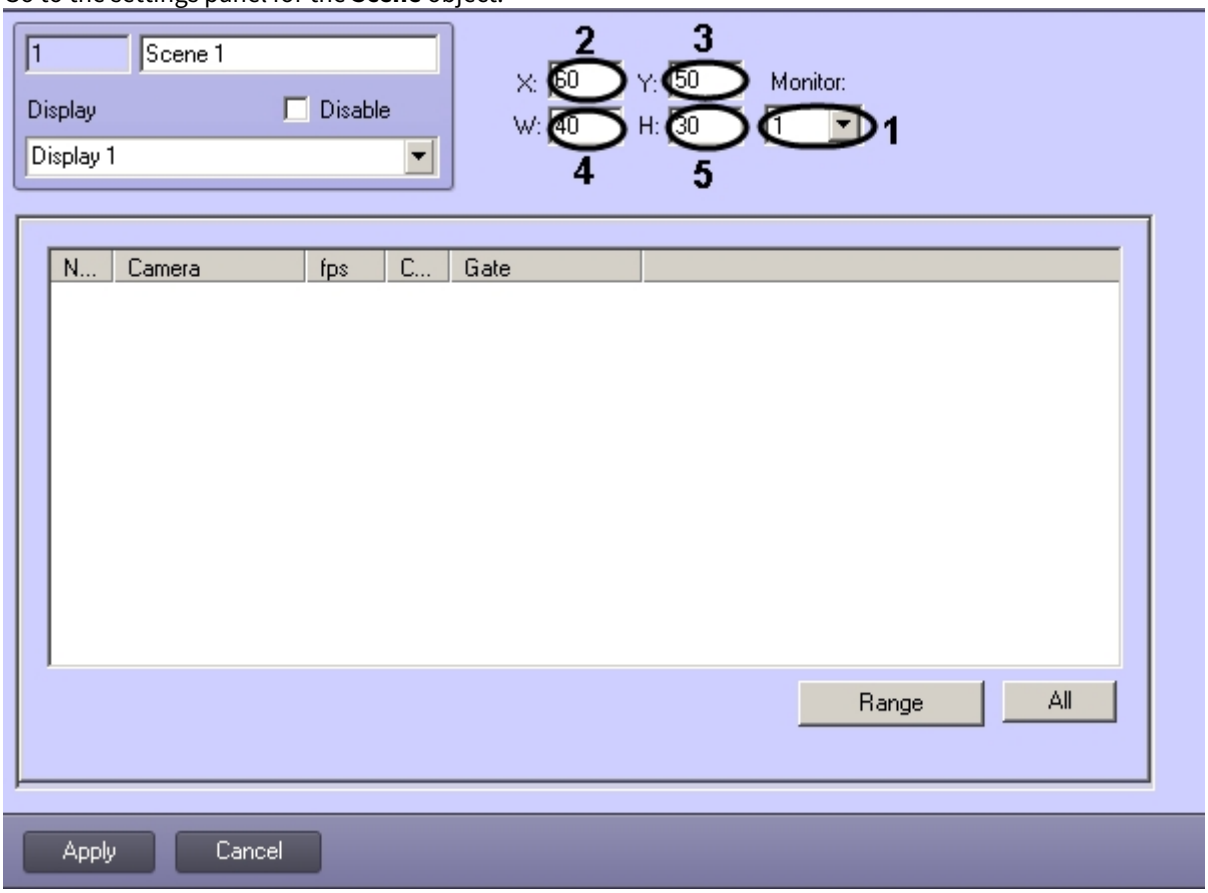
4. Repeat steps 1-3 for all required **Display** and **Scene** objects.

The **Scene** object is now created.

23.4.3.2.2 Setting the parameters of the Scene interface box

Setting the parameters of the **Scene** interface box is done in the following way:

1. Go to the settings panel for the **Scene** object.



2. Select the number of physical monitor on which screen there will be displayed the panoramic view from the **Monitor** dropdown list (1).
3. Set the coordinates of the left upper corner in the **Scene** interface box: fields **X** (horizontal shift from the left image border) and **Y** (vertical shift from the upper image border) – see 2-3. The coordinates are given in percentage according to vertical and horizontal screen size.
4. Set the sizes of the **Scene** interface box: fields **W** (window's width) and **H** (window's height) – 4-5. The sizes are given in percentage according to vertical and horizontal screen size.
5. Click the **Apply** button to save the changes.

Parameters of the **Scene** interface box are now set.

23.4.3.2.3 Selecting and configuring cameras for the Scene object

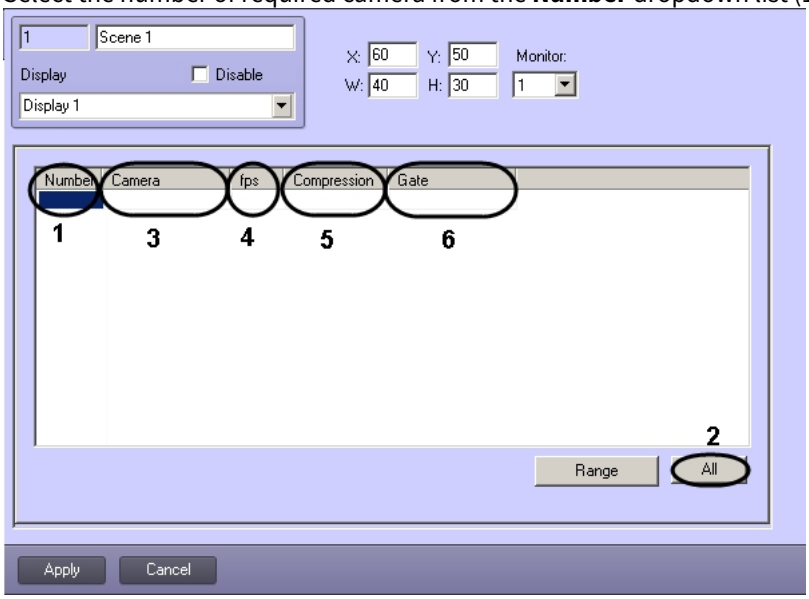
One can select and configure cameras for displaying in the interface box in two ways:

1. Separately. The settings panel of the **Scene** object is used.
2. In a complex way. The **Add/edit cameras** dialog box is used.

To select a camera on the settings panel of the **Scene** object, do the following:

1. Go to the settings panel of the **Scene** object.

2. Select the number of required camera from the **Number** dropdown list (1).



> **Note.**
>
> To select all the cameras, registered in the system, click the **All** button (2).

3. The name of selected camera will automatically be displayed in the **Camera** column (3)
4. If a signal is to be groomed, the required fps is to be selected from the fps dropdown list (4).

> **Note.**
>
> It's not recommended to change **fps** value while using H.264 codec

5. If a compression level of video signal is to be changed, the required compression level is to be selected from the **Compression** dropdown list (5). The compression level increases from 0 (no compression) to 5 (maximum compression).
6. If the archive from the selected camera is to be received via the **Gate** object, then select the name of this object from the **Gate** dropdown list (6)
7. Repeat steps 2-6 for all the required cameras.

> **Note.**
>
> To add a new camera, go to the last line in the selected cameras list and press "down" on the keyboard.

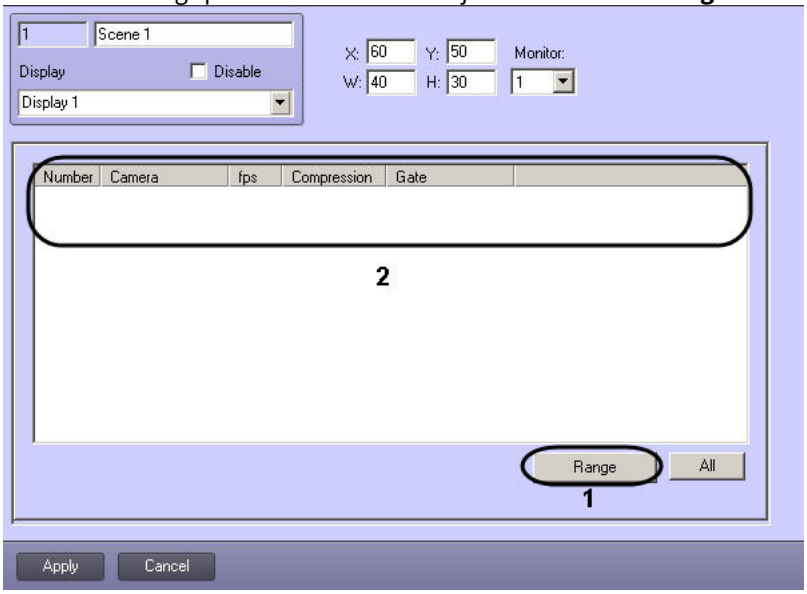
8. Click the **Apply** button to save the changes.

Cameras selection on the settings panel of the **Scene** object is completed.

There is possibility to select and edit parameters of cameras for displaying in the **Scene** interface box in a complex way.

Complex cameras selection is performed in the following way:

1. Go to the settings panel for the **Scene** object and click the **Range** button (1)



2. The **Add/edit cameras** dialog box will open as a result.

> **Note.**
>
> The **Add/edit cameras** dialog box is described in the Selecting and configuring video cameras in bulk section.

3. Cameras settings, set in the **Add/edit cameras** dialog box will be displayed on the settings panel of the **Scene** object (2).
4. Click the **Apply** button to save the changes.

Complex cameras selection is completed.

23.4.3.3 Configuring video transmission to Remote Workstations

INTELLECT™ software supports transmitting the digital video signal from the Server to the Remote Workstations for remote video surveillance, archiving, routing via the video gate, transmitting via the Web-server by HTTP protocol (Internet), to a mobile device with iOS or Android operation system. Both real-time and archive video signals may be transmitted to the Remote Workstations.

Real-time video signals are transmitted by Remote Workstation demand for displaying, archiving, routing via the video gate or transmitting via the Web-server by HTTP protocol (Internet), to a mobile device with iOS operation system. By default, transmitted video signals have the same parameters (resolution, color depth, frame rate etc.) as they have during digitizing and processing by the video capture card or IP-device.

Prior to transmitting to Remote Workstations, video signals are compressed. By default, video signals, transmitted to the TCP/IP place via local net, and archived video signals are compressed at the same rate. For the setup procedure of video signal compression rate, see Configuring video compression section.

Real-time video displaying may lag if the connection is unstable and/or transmitting rate via network connection is low. To eliminate or minimize this effect, use the following registry keys:

- AcsStdLimit – the registry key used for setting the upper frame sequence limit in MJPEG format. It possesses the values from 1 to 30.
- AcsMpegLimit – the registry key used for setting the upper frame sequence limit in H.264/MPEG4 format. It possesses the values from 1 to 30.

If sequence of frames transmitted to a Remote Workstation rises to the value specified in the registry key, then grooming is enabled.

> **Note.**

Keys are to be created in the HKEY_LOCAL_MACHINE\SOFTWARE\ITV\INTELLECT\Video for 32-bit system (HKEY_LOCAL_MACHINE\Software\Wow6432Node\ITV\INTELLECT\Video for 64-bit system) registry section on the Server.The process of key creation is described in Working with Windows OS registry section.

When video signals are transmitted to Remote Workstations for displaying, archiving and routing with video gate, it is possible to reduce their frame rate and to increase their compression rate.

When video signals are transmitted to Remote Workstations for displaying, their frame rate reduction and their compression rate increase are set on the settings panel of the Monitor object for each camera individually.

When video signals are transmitted to Remote Workstations for archiving, their frame rate reduction and compression rate increase are set on the settings panel of the **Backup archive** object for each camera individually.

When video signals are transmitted to the video gate, their frame rate is reduced and compression rate is increased on the settings panel of the **Video gate** object for each camera individually.

When video signals are transmitted via a web-server by HTTP protocol to a Remote Workstation, a mobile device with iOS or Android operation system, its compression rate is set on the settings panel of the **Web-server** object that corresponds to the Web-server module. For the setup procedure of the video signal compression rate, see the chapters on Web-server or the documentation on the mobile clients.

23.4.4 Configuration of audio

23.4.4.1 Configuring audio signals playback using the video monitor

The video monitor has the facility to play back audio signals only from the microphones that have been set to synchro video and audio recording. INTELLECT™ software provides an audio playback option for real-time audio signal and for audio signals, archived in the synchro recording mode.

To enable the option of audio signals playback by the video monitor, do the following:

1. Configure synchro video and audio recording with a camera - see Configuring audio and video synchro recording.
2. Bind the **Audio player** object to the **Monitor**. The configuration of binding is described in Binding Audio player to the Monitor section.

This option is deactivated automatically, when the synchro video and audio recording option is disabled for the selected camera and microphone or when the Audio player binding to the video surveillance monitor is disabled.

Synchronous playback of video and audio recordings

23.4.4.2 Configuring audio signals playback using the Audio player object

23.4.4.2.1 Audio player setup sequence

Audio player object is a subclass of the **Display** interface object and is designed for implementing the following functions:

1. Perform recording of sound activated audio signals;
2. Record audio signals by Operator command;
3. Play back input audio signals;
4. Play back audio signals, recorded by sound level or by Operator command;
5. Perform voice notification.

To set the **Audio player** object, do the following:

1. Select the screen and create for it the **Audio player** object.
2. Set the parameters of the **Audio player** interface object.
3. Set the recording and playback of audio signals from microphones.
4. Set the voice notification during alarms registration by cameras' motion detectors (see Setting up the voice notification using Audio player object).

Note

Setup sequence of **Audio player** object for transmission of audio signals to IP-device is described in Setting up the transmission of audio signals to IP devices.

Note

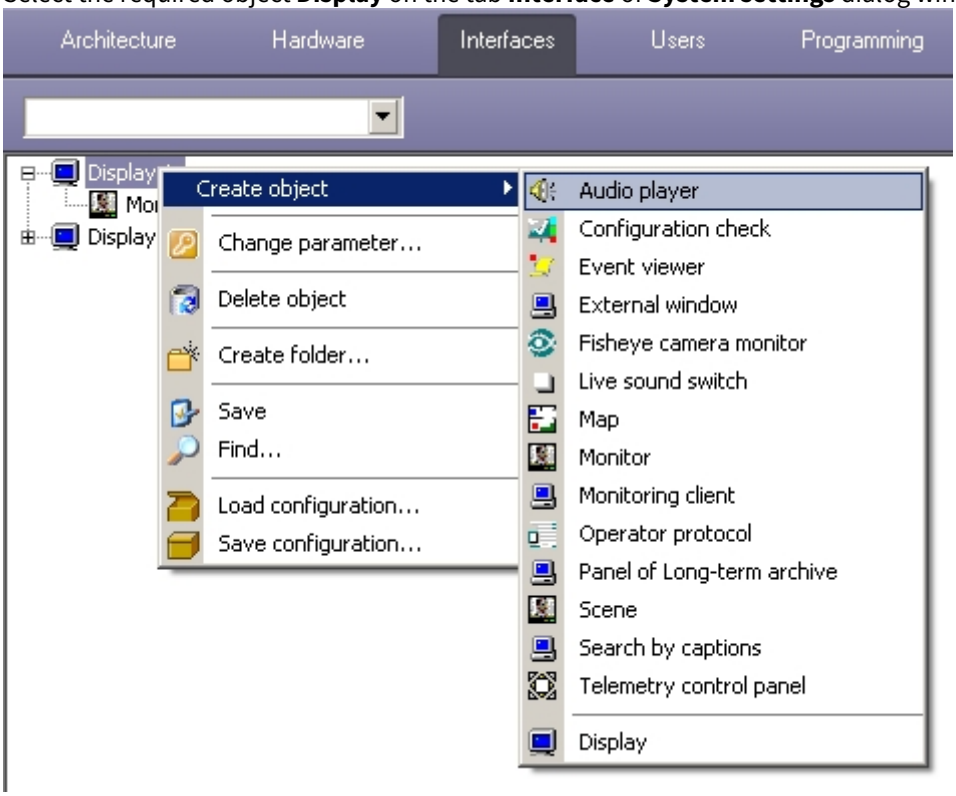
The Audio player uses PCM (preferrable) or GSM (legacy) codecs. The codec is selected automatically.
Audio bitrate does not change when played back via the Audio player.

Audio player operation

23.4.4.2.2 Creating the Audio player object

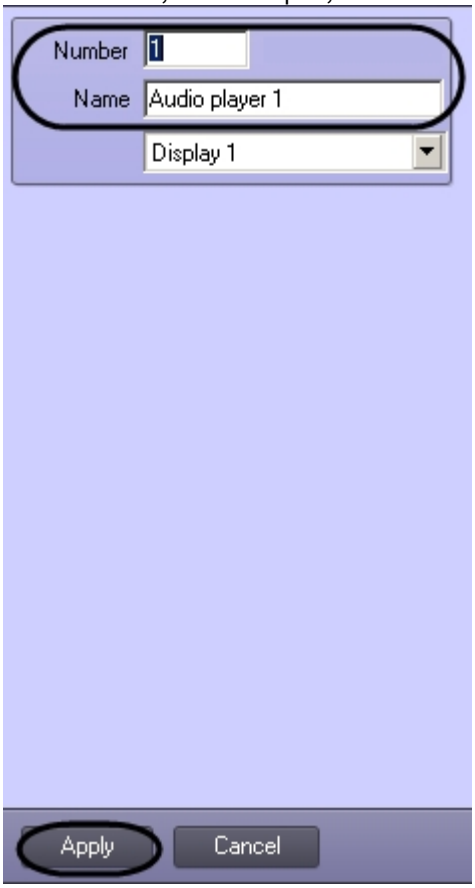
To create the **Audio player** object do the following:

1. Select the required object **Display** on the tab **Interface** of **System settings** dialog window.



2. Click with the right mouse button upon the selected object **Display** and in the contextual menu, that will open, select **Create object -> Audio player** (1).

3. In the window, that will open, set the name and number of the object **Audio player** and then click **Apply** button.



> **Note.**
>
> In result Settings panel of **Audio player** object will be shown.

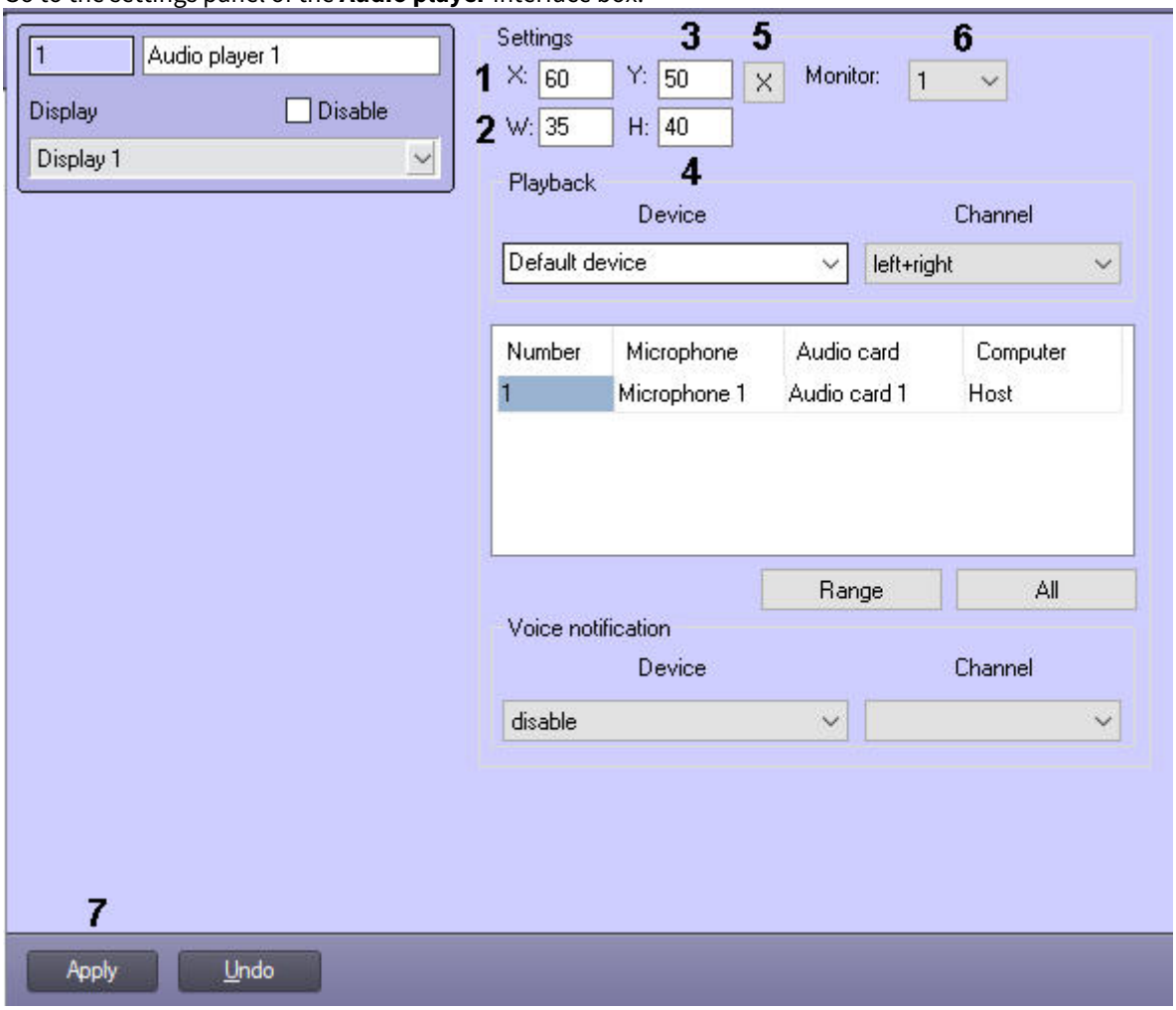
4. Repeat steps 1-3 for all the required objects **Display** and **Audio player.**

Creation of **Audio player** object is over.

23.4.4.2.3 Setting the parameters of the Audio player interface box

To set the parameters of the **Audio player** interface box, do the following:

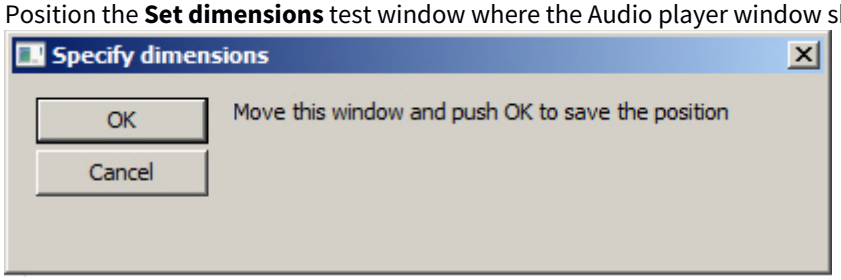
1. Go to the settings panel of the **Audio player** interface box.



2. Set the **Audio player** interface box position in one of the following ways:
   a. Manually:
      i. Set the coordinates of **Audio player** window's left upper corner: fields **X** (horizontal indent from the left image border) and **Y** (vertical indent from the upper image border - 1 and 2. Coordinates are given in percentage in relation to screen size horizontally and vertically.
      ii. Set the dimensions of the **Audio player** interface box: fields **W** (window's width) and **H** (window's height) – 3 and 4. Dimensions are given in percentage in relation to screen size horizontally and vertically.

> **Note.**
>
> Minimal allowed value of parameter **W** is 35%, **H** – 40%. With lesser value displayed width or height of the window will correspond to minimal allowed value.

   b. With a test window:
      i. Click **X** (5).
      ii. Position the **Set dimensions** test window where the Audio player window should be displayed.



      iii. Click **OK**. As a result, the coordinates in the fields **X, Y, W, H** will be set in accordance with the size and position of the test window.

3. From the **Monitor** drop-down list select the number of monitor for which coordinates are specifying (6).

> **Note.**
>
> The monitors are numbered from left to right, from top to bottom, i.e. the 1st monitor is the one in the upper left corner regardless of which monitor is assigned as main or what number the monitor has in OS.

4. Click **Apply** button to save all the changes (7).

Setting the parameters of the **Audio player** interface box is completed.

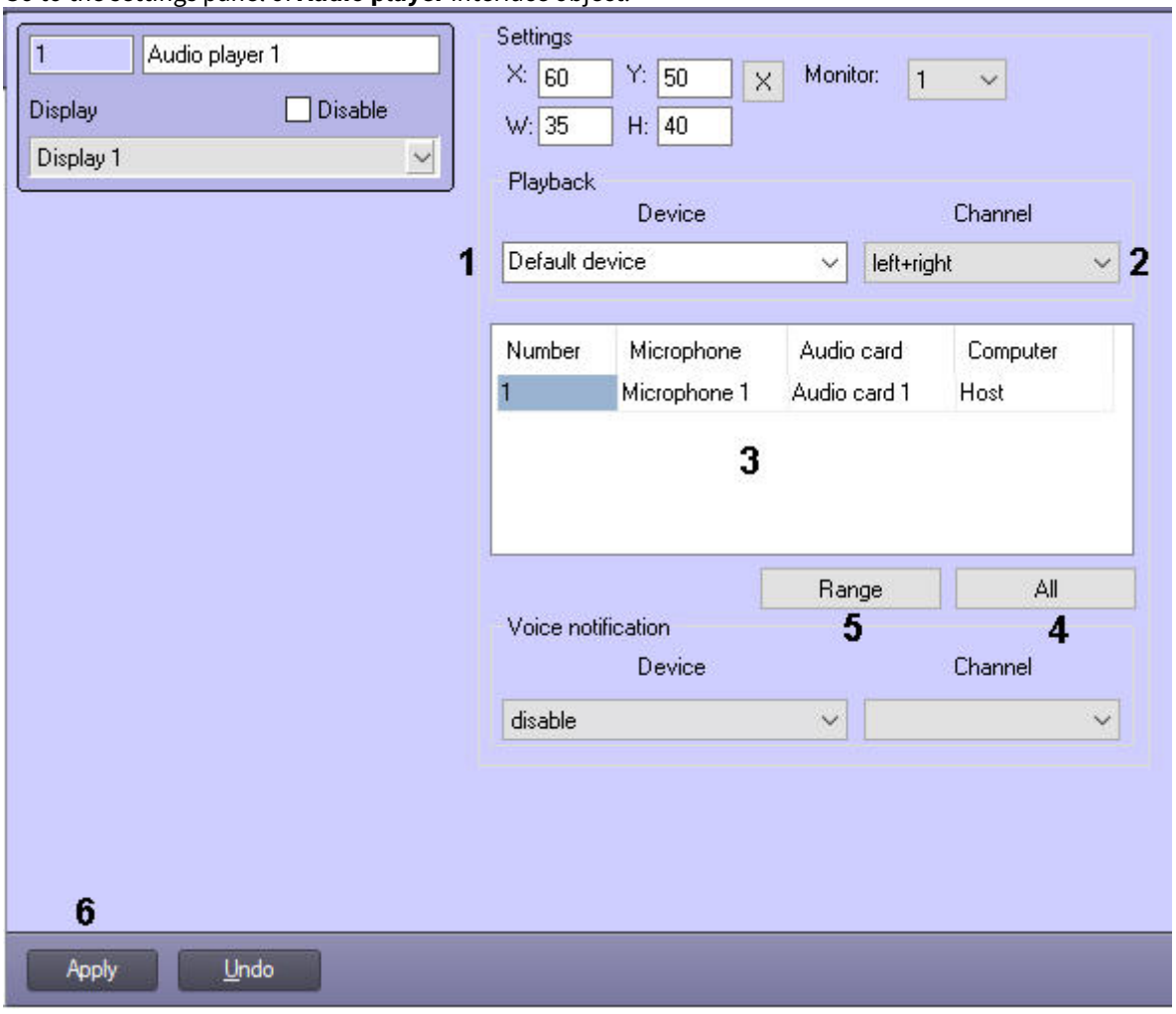
23.4.4.2.4 Setting up the recording and audio signals' playback

With the help of **Microphone** object the following opportunities of **Audio player** object are realized:

1. Playback of audio signals from the microphones.
2. Recording of audio signals by sound level or by Operator command.

To set up the recording and playback of audio signals from the microphones do the following way:

1. Go to the settings panel of **Audio player** interface object.



2. From the dropdown list **Device** of **Playback** group select the required device of audio signals backup (1).

> **Note.**
>
> Standard sound map corresponds to to the value **Default device**.

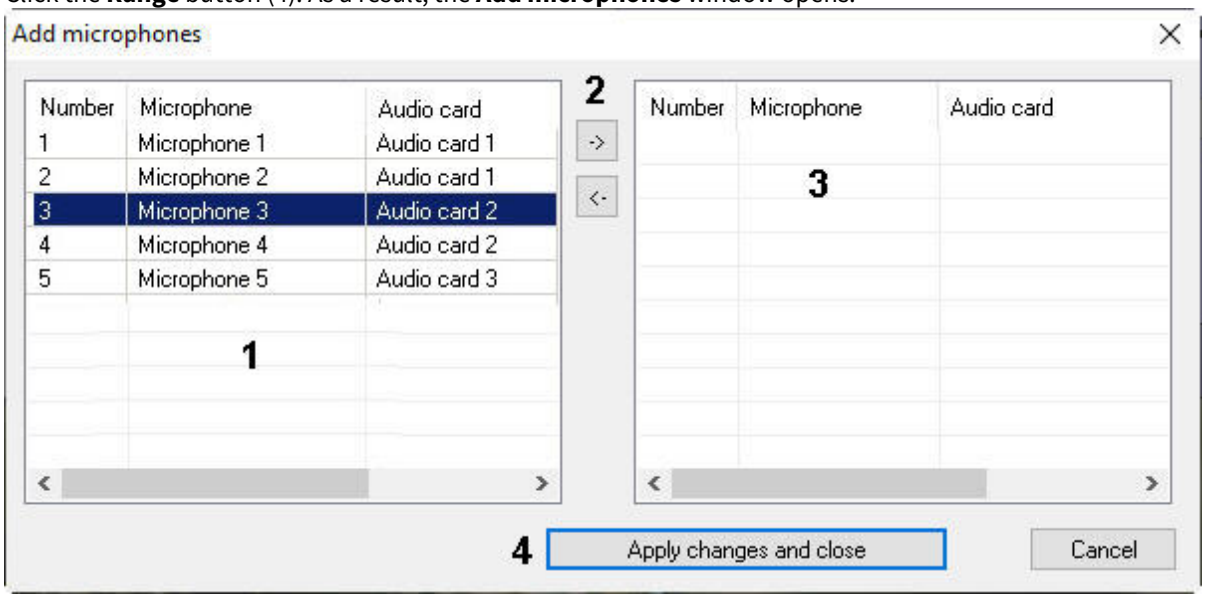
3. From the dropdown list **Channel** of **Playback** group select the required channel of audio signals backup (2).

> **Important.**
>
> The **Device** and **Channel** settings are available only if the **Display** with this Audio Player is assigned to one computer in the distributed system (see Assigning the displays to the operator workstations). If the Display is assigned to multiple computers, these settings cannot be changed and only the **Default device** can be used.

4. Add microphones for recording and playing back audio from in one of the following ways:
   a. One by one:
      i. Form the dropdown lit in the column **Name** select the name of **Microphone** object, which audio signals are suggested to be recorded/played back (3).
      ii. Repeat step 4 for all the required **Microphone** objects.

      > **Note.**
      >
      > Use "down" arrow on a keyboard to add a line to the table. Press Ctrl+Del after selecting a line to delete it.

   b. All microphones created in the hardware tree: click on the **All** button (3).
   c. Several microphones from the list:
      i. Click the **Range** button (4). As a result, the **Add microphones** window opens.



      ii. In the list on the left, select the necessary microphones to add (1). To select several lines, left-click them while holding the Ctrl key on the keyboard.
      iii. Move the microphones to the list on the right (3) using the **->** button (2).
      iv. Click **Apply changes button and close** (4).
      v. As a result, the selected microphones are added to the list on the settings panel of the **Audio player** object.
5. Click **Apply** button to save all the changes (6).

Setting up the recording and playback of audio signals from the microphones is completed.

23.4.4.3 Features of audio signals export using the video monitor

The video monitor has the facility to export audio signals only from the microphones that have been set to synchro video and audio recording.

In order to provide synhro audio export when a video recording is exported from the video monitor interface, the **Audio player** object is to be bound to the **Monitor**. The configuration of binding is described in Binding Audio player to the Monitor section. If audio player is not bound, then video from the **Monitor** interface will be exported without sound even if the archive is recorded with sound. Information on how to create and configure the **Audio player** object is given in the Configuring audio signals playback using the Audio player object section of this manual.

Detailed information on how to export video recordings from the video monitor interface is given in the Export of video recording with sound section.

23.4.4.4 Setting up the audio signal transmission to Remote Workstations and servers

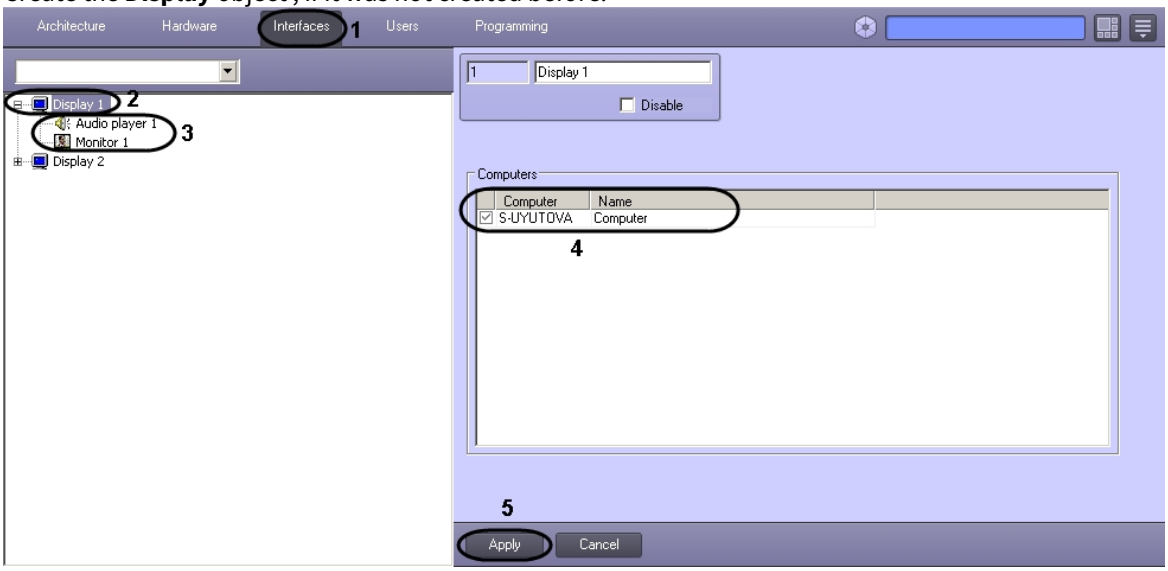
INTELLECT™ software has the facility to transmit audio signals both from microphones and from the archive to Remote Workstations and servers.

Audio signal transmission to Remote Workplaces and servers, connected by the TCP/IP net, is performed only via **Video surveillance monitor** or **Audio player** interface objects.

The video monitor has the facility to transmit only audio signals from the microphones that have been set to synchro video and audio recording. The Audio player may be configured to transmit audio signals from all video surveillance system microphones to the Remote Workstations and servers.

To enable audio signal transmission to Remote Workplaces and servers, follow the steps:

1. Go to the **Interfaces** tab in the **System Settings** dialog box.
2. Create the **Display** object , if it was not created before.



3. Set the checkmarks in the **Computers** table for those Remote Workplaces and servers, where audio signals should be transmitted.
4. Click the **Apply** button.
5. Create and set up **Monitor** and/or **Audio player** objects (for description of setting up these objects see the relevant sections).

Setup of audio signal transmission to Remote Workplaces and servers is completed.

23.4.5 Configuring the interactive map for object state indication and controlling the objects

23.4.5.1 General information on the structure of the interactive map of the protected facility

The interactive map of the *Intellect* system uses graphical diagrams of the protected territory to navigate among the surveillance system components. The interactive map allows controlling the objects from the context menus of the graphical symbols on the map showing the states of the corresponding objects.

The interactive map can be comprised of a set of plans (layers) with one of the following background:

1. Images: photographs, maps, diagrams, drawings in bmp, gif, jpeg, jpg, png, tiff, emf, or svg format. The size and resolution of the images is not limited, however, please note that a large image may not fit into the screen, or the objects shown on it may look indiscernible.

> **Note**
>
> We recommend creating the images in third-party graphical software packages (Microsoft Paint, Adobe Photoshop, etc.), as the standard delivery configuration of *Intellect* software does not include tools for image editing.

2. Solid background of a given color.
3. External maps, for example, OpenStreetMap, Google Maps, Yandex Maps, etc. The use of external maps may be charged. In this case, please contact the map provider to pay for its use.

Working with the Map

23.4.5.2 Configuring the interactive map

23.4.5.2.1 Setup procedure for the interactive map

To configure interactive map do the following:

1. Create and set the **Map** interface object (see Setting up the position of the Map on the screen).
2. Create and set objects Layer on the basis of interface object **Map** (see Creating the layers of the interactive map).
3. Attach required objects to the Layers of interactive map (see Attaching objects to the layers of interactive map).
4. Place the object symbols of the assigned objects on the map's layers (see Operations with objects in the Map editor utility).
5. Set up the links between the layers, to be used for interactive card navigation (see Linking the layers of the interactive map).
6. Configure object ID displaying (see Configuring object ID is displaying).

23.4.5.2.2 Setting up the position of the Map on the screen

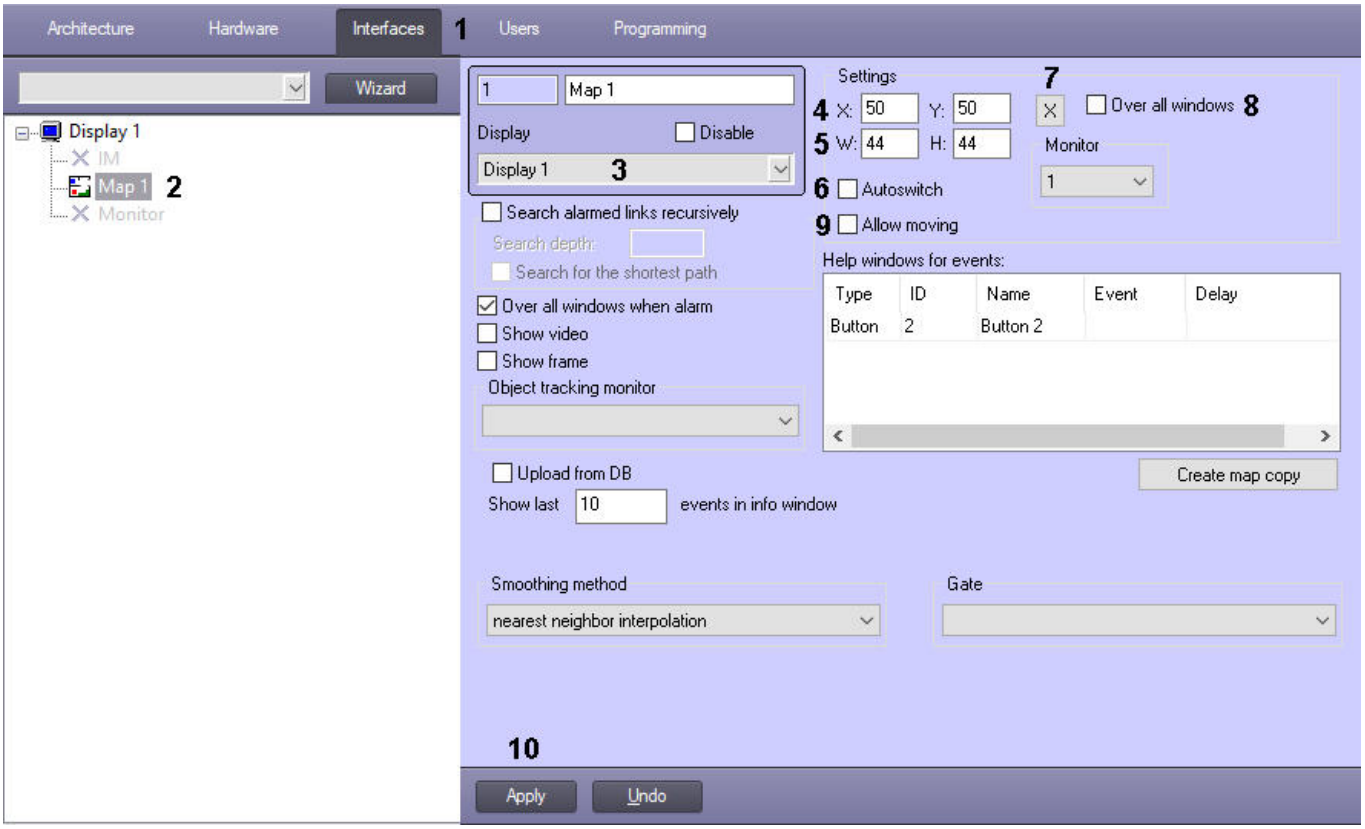
To register the interactive map in *Intellect*, create the **Map** interface object.

When setting up the **Map** object, specify the position of the **Map** interactive window on the screen.

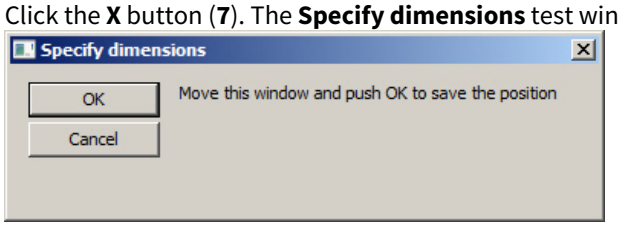
To register the **Map** and specify its position on the screen, do the following:

1. Go to the **Interfaces** tab of the **System Settings** window (**1**).

2. Create a **Map** object (**2**) on the basis of the **Display** object, or select the corresponding object in the object tree on the **Interfaces** tab.



3. When creating a **Map** object, specify the ID and the name for the object, and select the **Display** object on the basis of which the **Map** object is created (**3**).
4. Set the **Map** window position on screen in one of the following ways:
    a. Manually:
        i. Set the coordinates of the position of the interactive **Map** window by changing the values in the **X** and **Y** fields (**4**). The values in the **X** and **Y** fields correspond to the coordinates of the top left corner of the interactive **Map** window on the screen and are expressed as a percentage of the horizontal and vertical screen dimensions, respectively.
        ii. Set the width and the height of the interactive **Map** window displayed on the screen (**5**). The values in the **W** and **H** fields are expressed as a percentage of the horizontal and vertical screen dimensions, respectively.
        iii. From the **Monitor** drop-down list (**6**), select the number of the monitor in the system for which the coordinates are set.
    b. Using the test window:
        i. Click the **X** button (**7**). The **Specify dimensions** test window opens.



        ii. Position the test window on screen, set the required size.
        iii. Click the **OK** button. As a result, the coordinates in the **X, Y, W, H** and **Monitor** fields will be set according to the dimensions and position of the test window.
5. Set the **Over all windows** checkbox (**8**), if the **Map** window should always be displayed over all windows.
6. Set the **Allow moving** checkbox (**9**), if you want to change the position and the size of the **Map** manually.
7. Click the **Apply** button (**10**) to save the changes.

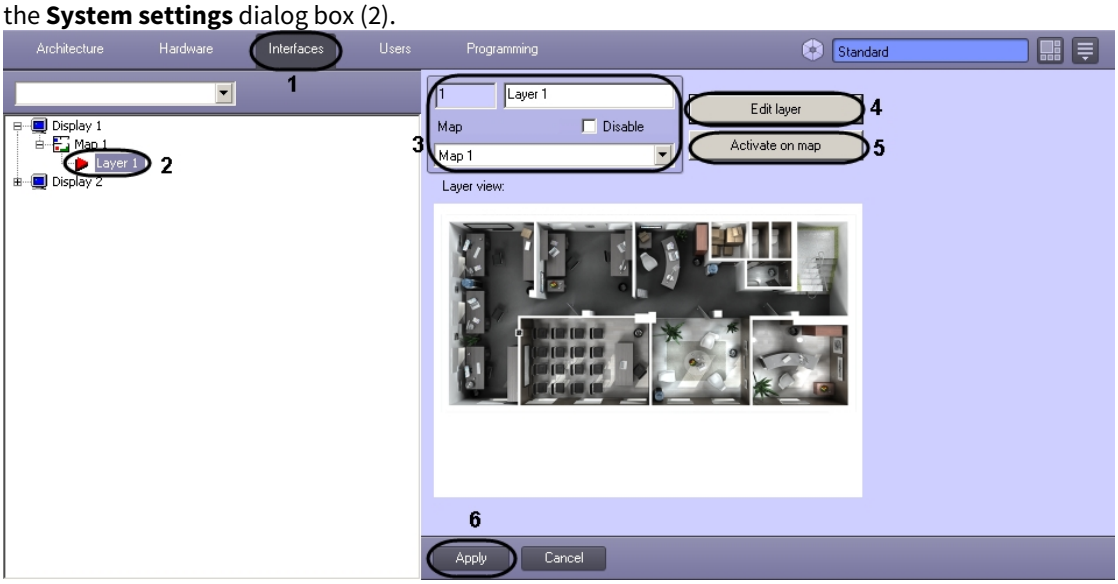
Setting up the position of the **Map** on the screen is complete.

23.4.5.2.3 Creating the layers of the interactive map

You can locate several graphical plans of guarded objects on one interactive Map. Each graphical plan is represented by a Layer object.

Create and configure the **Layer** object as follows:

1. Go to the **Interfaces** tab of the **System settings** dialog box (1).
2. Create a **Layer** object under the **Map** object or select the existing **Layer** object in the objects tree in the **Interfaces** tab of the **System settings** dialog box (2).



3. Specify the ID and name for the **Layer** object, and select the **Map** object to become the parent of the **Layer** object (3).
4. To edit the image represented by the **Layer**, click the **Edit layer** button (4). The **Map editor** utility will open allowing the graphical image to be edited.

> **Note**
>
> When the *Map editor* utility is started, then the **System settings** dialog box is inactive. Close the **Map editor** utility to continue working with the **System settings** dialog box.
> You cannot start the *Map editor* utility for several layers.

5. To display this layer on top of all other layers, click the **Activate on map** button (5).
6. To save all the changes click the **Apply** button (6).

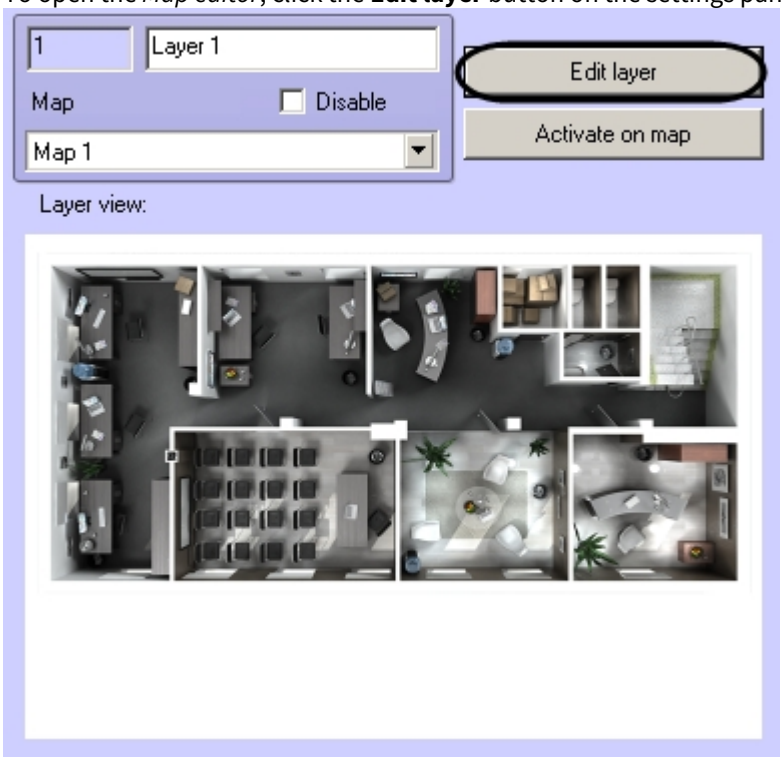
After a new layer is created and configured, a graphical image of the area is to be attached to it, or the layer background color is to be selected, or the map server is to be selected to use external map as a background. These types of background are mutually exclusive, i.e. only one of them can be in use in one time. For example, if the file or external map is selected, then the background color will not be applied.

Attach the image or select the background color as follows:

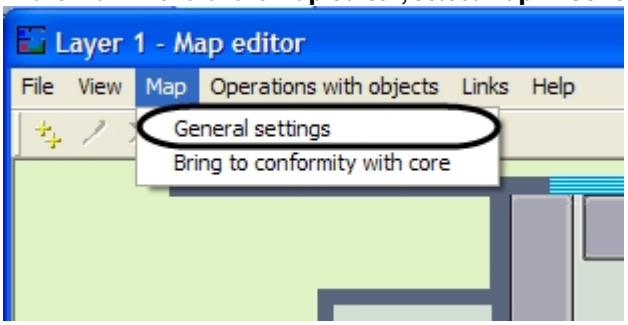
1. Go to the settings panel of the **Layer** object.
2. Open the *Map editor* application.

> **Note**
>
> The *Map editor* application allows selecting the plan of guarded area, creating the devices icons and placing them on the map, as well as other settings.

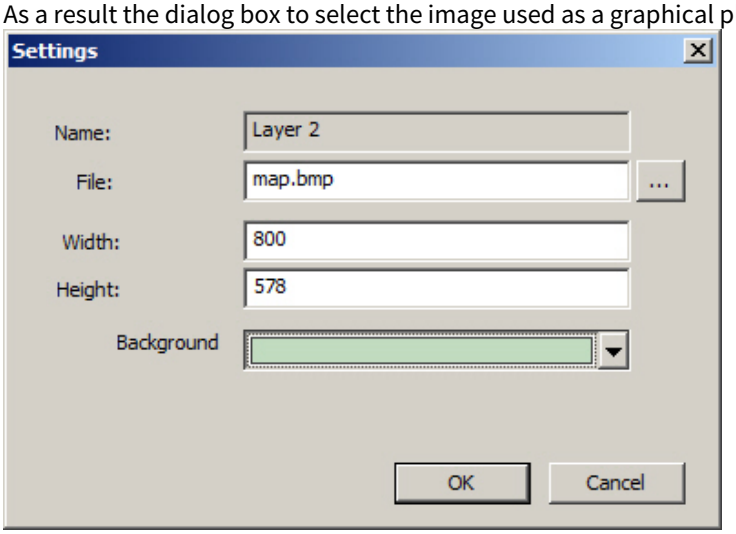
To open the *Map editor*, click the **Edit layer** button on the settings panel of the **Layer** object.



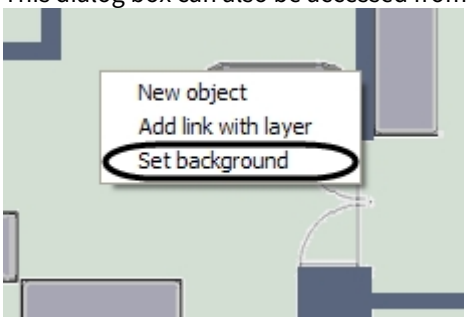
3. In the main menu of the **Map editor**, select **Map** -> **General settings**.



As a result the dialog box to select the image used as a graphical plan of the guarded area will open.

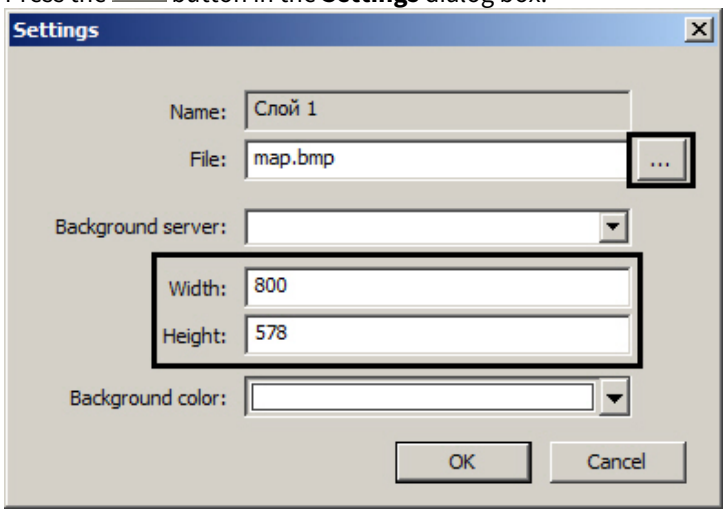


This dialog box can also be accessed from the **Set background** item of the context menu of the map area.



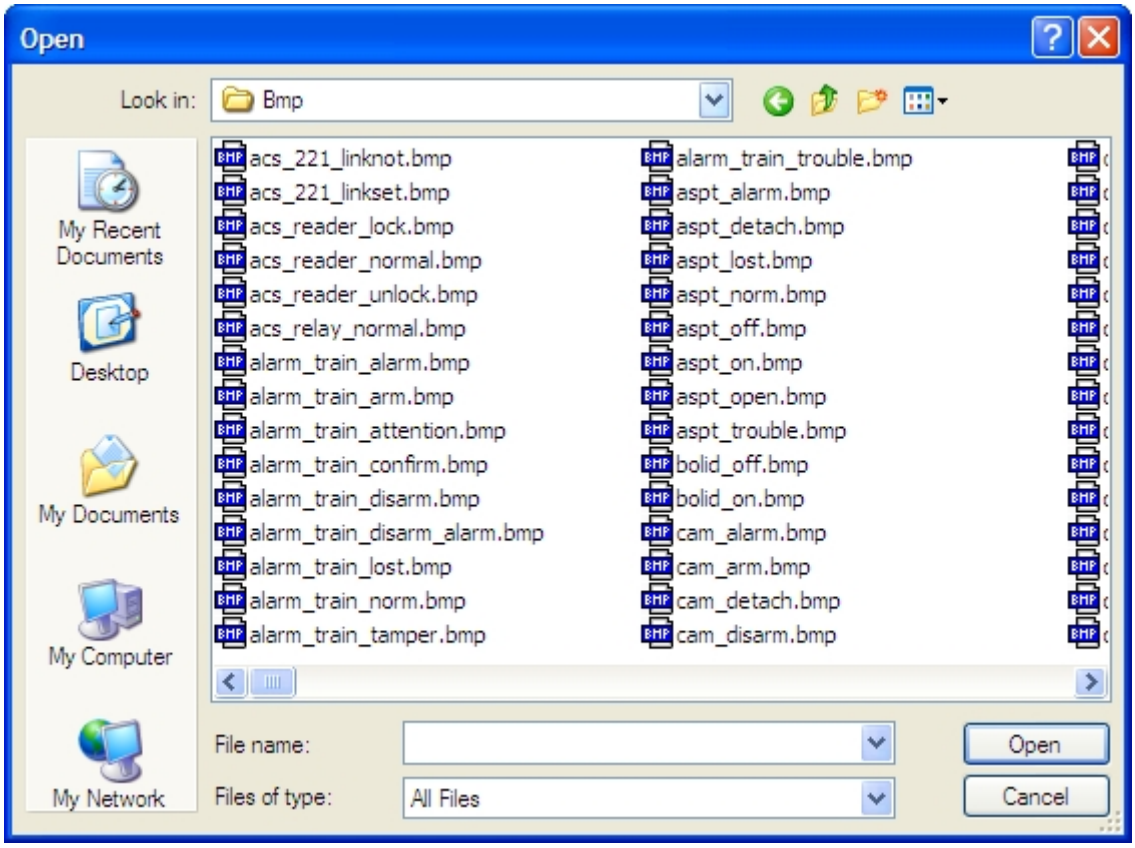
4. Select the background file as follows:

   a. Press the ... button in the **Settings** dialog box.



   As a result the standard dialog box to select the image used as a graphical plan of the guarded area will open.

> **Note**
>
> The graphical area plan should be saved as a bmp, gif, jpeg, jpg, png, tiff, emf or svg image file.



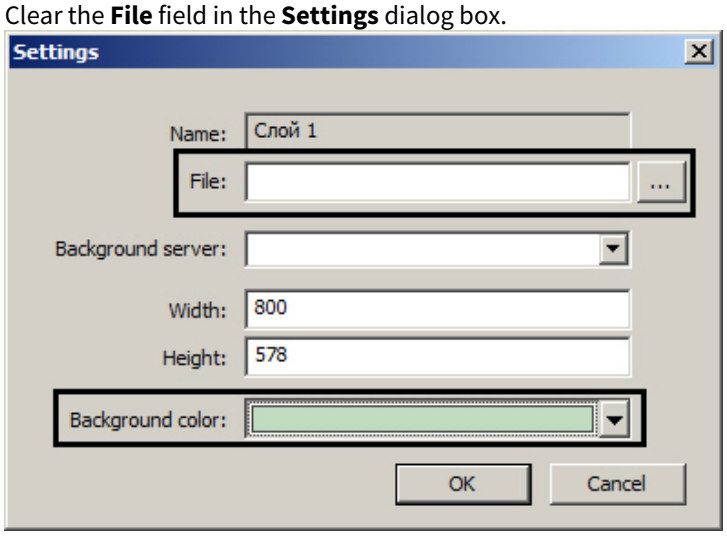
Open the .bmp file and click the **Open** button.
When the layer file is selected, it is copied to the **Bmp** folder in INTELLECT™ installation folder.

> **Attention!**
>
> For proper operation of the interactive map in the distributed configuration, the **Bmp** folders are to be synchronized on all computers in the distributed system. The folders are synchronized automatically - start the Client under the Administrator.

b. In the **Width** and **Height** fields specify the resolution of the image used as a graphical plan of the guarded area. The values specified in the **Width** and **Height** fields are to match real resolution of the image file.

5. Set the layer background as follows:

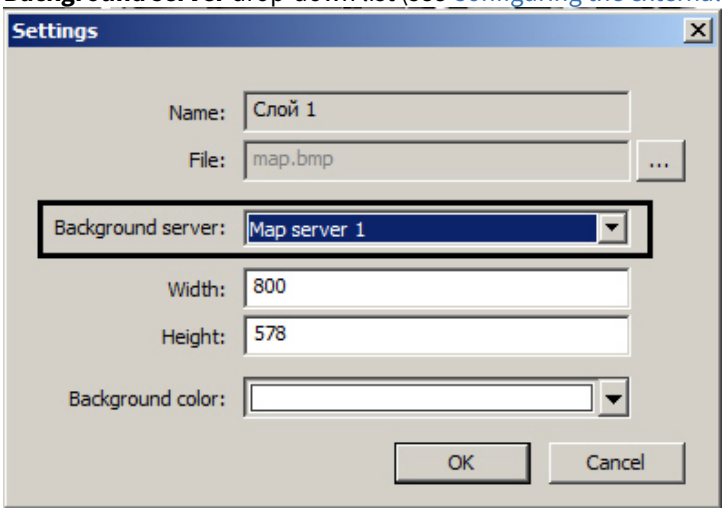
a. Clear the **File** field in the **Settings** dialog box.



b. Select the required background color in the **Background** dropdown list.

> **Note**
>
> The background color will be applied only after shutting down the *Map editor* utility and opening it once again.

6. To select an external map as a background, select the previously created and configured **Map Server** object from the **Background server** drop-down list (see Configuring the external Map server).



> **Note.**
>
> If an external map is selected as a backgroung, the layer is automatically binded to geographical coordinates – see also Configuring map binding to coordinate grid.

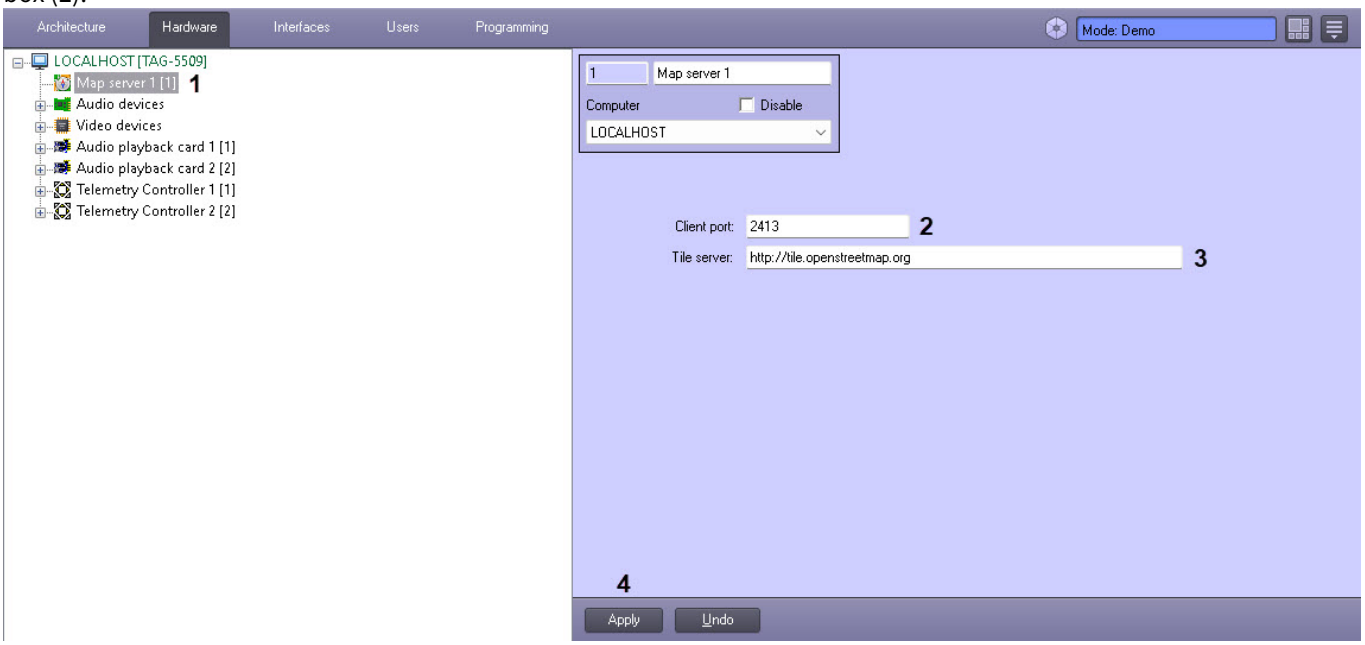
7. To apply all the changes click the **OK** button in the **Settings** dialog box.
The *Map editor* will display the new graphical plan of the guarded area.

23.4.5.2.3.1 Configuring the external Map server

The external Map server corresponds to the source from which the *Intellect* Map layer receives images for the layer background.

Configure the external Map server as follows:

1. Create the **Map server** object on the basis of the **Computer** object on the **Hardware** tab of the **System settings** dialog box (**1**).



2. In the **Client port** field (**2**), enter the port value. By default, the port value is 2413.
3. In the **Tile server** field (**3**), enter a link to the external map. By default, a link to the OpenStreetMap free map is set http://tile.openstreetmap.org.
4. Click the **Apply** button (**4**).

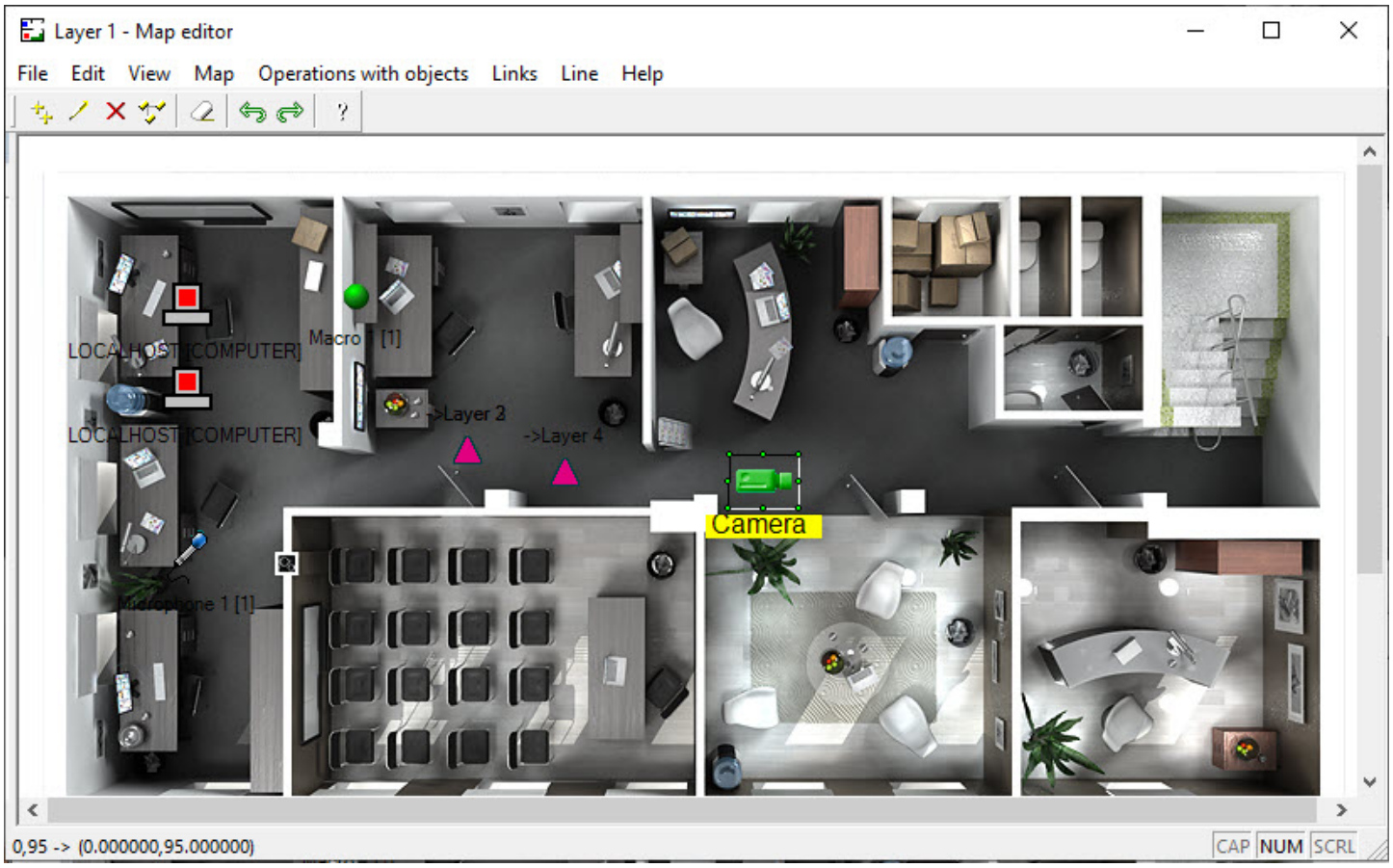
When creating a layer, select the Map server as the background – see Creating the layers of the interactive map.

The external Map server configuration is complete.

23.4.5.2.4 Attaching objects to the layers of interactive map

You can attach the objects to a layer of the interactive map using the *Map editor* utility.

> **Note**
>
> To open the *Map editor* utility window, click the **Edit layer** button on the settings panel of the **Layer** object (see Creating the layers of the interactive map).



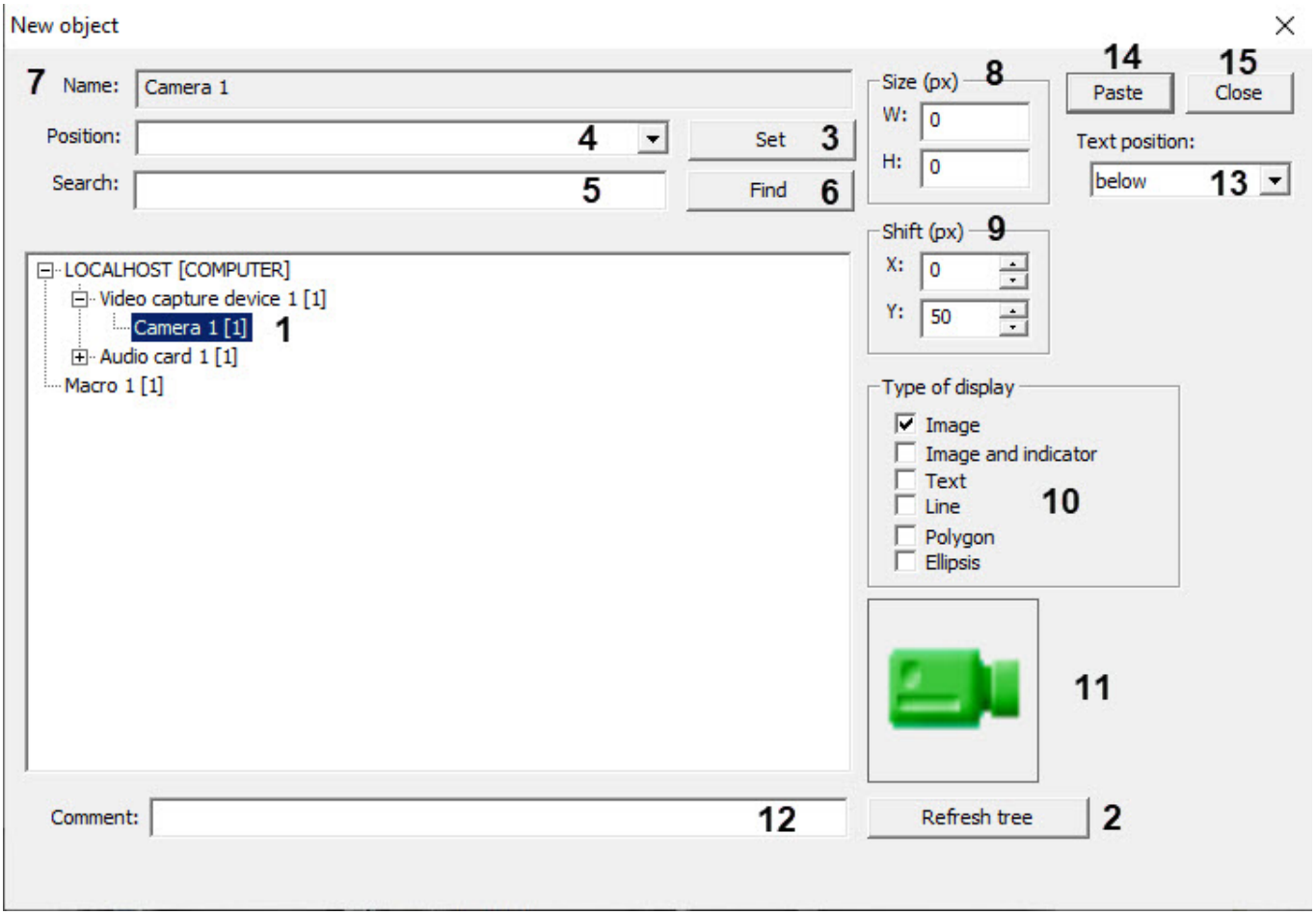
Attach the objects to the layers of the interactive map as follows:

1. Open the **New object** dialog window of the *Map editor* utility in one of three possible ways:
   a. Execute the main menu command **Objects operations** -> **New object**.
   b. Click the button on the toolbar.
   c. Execute the context menu command **New object** (to open it, right-click anywhere on the graphic layout).
2. Select the required object in the objects tree of the **New object** dialog box (**1**). The objects tree displays only the objects that can be added to a layer, or objects whose child objects can be added to a layer.

> **Note**
>
> To refresh the objects tree, click the **Refresh tree** button (**2**).

> **Note**
>
> Click the **Set** button (**3**) to put in bold the objects in the object tree which were already added to any layer of any map. If you put the object in bold in the object tree, the layers and the maps to which this object is added, will be displayed in the **Position** drop-down list (**4**).

> **Note**
>
> To search the object by the name or a part of the name, enter it in the **Search** field (**5**) and click the **Find** button (**6**). If you leave the search field blank and click the **Find** button, then the top object in the object tree will be selected. You can use the **Find** button to move through the object tree, including the child objects.



3. As a result, the name of the selected object will be automatically displayed in the **Name** field (**7**).
4. Enter the object icon size in the **W** (icon width) and **H** (icon height) fields (**8**). The size is specified in pixels. If 0 is set for **W** and **H**, the icon is displayed in the original scale.
5. Enter the icon shift along the **X** and **Y** axes in pixels (**9**). The first icon is added in such a way that the upper left corner of its rectangle is the point of the last mouse click. The subsequent icons are added with the specified shift.

> **Note**
>
> If 0 value is specified in the **X** and **Y** fields, the object icons are displayed on top of one another.

6. In the **Type of display** group (**10**), set the checkboxes next to the required types of display. If several types are selected, then several separate icons of the selected object will be simultaneously added to the map. These icons can then be removed and edited independently of one another.

Type of display item	Object icon display type	Usage
Image	Object schematic view	Objects of base configuration
Image and indicator	Object schematic view and indicator of object state	SCADA objects
Text	Object name and text defined by the script (see the Examples of scripts in the JScript language section of the The Script object. Programming using the JScript language). The icons with the **Text** type of display can be used to place a comment on the map (descriptions, notes, additional information). The text of the comment can be specified after adding the object using the **Text information** parameter on the **Properties** panel (see Editing object properties using the Properties panel).	SCADA objects

Type of display item	Object icon display type	Usage
	*Note. If the **Text** type of display is selected, the object value will be displayed on the map as "Value = <value>". In order for an object value to be displayed without "Value =", it is necessary to change the **HideAnalogName** parameter value in the Windows OS registry to **1** (see Registry keys reference guide)*	
Line	Object images in the form of a straight line or a polyline	SCADA objects
Polygon	Object representation as the polygon with the specified color and transparency with arbitrary number of apexes	SCADA objects
Ellipsis	Object representation as the ellipse with the specified color and transparency	SCADA objects

Note

If the **Image and indicator** or **Text** type of display is selected, the object values and states will be saved after *Intellect* restarts only if the object receives new values/states during the Map operation. If no new values/states were received before *Intellect* closing, they are not saved.

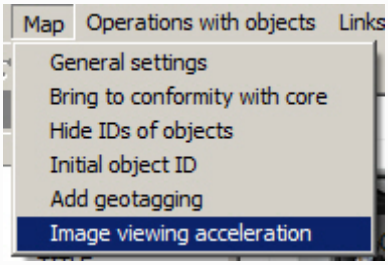
Note

The object icon is automatically displayed in the **Preview** field (**11**) in accordance with the selected type of display.

7. In the **Comment** field (**12**) enter the additional information about the object if necessary.
8. From the **Text position** drop-down list (**13**), select the object name display position relative to the icon: none (i.e. only icon without the name is displayed), above, to the right, below, to the left.
9. Click the **Paste** button (**14**) or press **Insert** on the keyboard to attach the object to the layer of the interactive map.
10. Repeat steps 2-8 for all required objects.
11. Click the **Close** button (**15**) to close the **New object** dialog window.

Note

If many objects (1-2 thousand) are attached to a layer, there may be problems when they are displayed in the interactive map window due to operating system limitations. In this case, enable the **Image viewing acceleration** in the **Map** menu.



If even more objects are attached to the layer, increase the values of the following registry keys to improve their display: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\GDIProcessHandleQuota and USERProcessHandleQuota.
However, it is not recommended to attach more than a thousand objects to a layer.

Attaching the objects to the layers of the interactive map is complete.

23.4.5.2.5 Operations with objects in the Map editor utility

On the page:

- Operations with the objects, added to the layer
- Editing the additional data and type of icon display
- Editing the font, color, background or frame size of object name
- Editing the object size
- Editing the position of object
  - Using the Position of object dialog window
  - Using the mouse
  - Using the Properties panel
- Changing the camera angle display
- Editing color and transparency (polygon and ellipsis)
- Editing the line thickness
- Adding or removing apexes of polygon or polyline
- Setting the order of displaying objects on map
- Configuring the objects states display (polygon and ellipsis)

23.4.5.2.5.1 Operations with the objects, added to the layer

The *Map editor* utility toolbar is shown on the figure:

The *Map editor* utility enables to perform the following operations with the objects, added to the layer.

Description of operation	Operation call			Note
	In the Operations with objects main menu	In the context menu	On the toolbar	
Deletes the selected object	Delete object	Delete	The 1 button	-
Copies the selected object. The copy is placed above the original	Copy object	Make a copy	The 2 button	-

Description of operation	Operation call			Note
	In the Operations with objects main menu	**In the context menu**	**On the toolbar**	
Edits additional data and type of displaying the icon for the selected object	Edit object	Edit	The 3 button	Performed in the **Edit object** dialog box
Set the displaying of the selected objects on the Map only in alarmed state (when there is no alarm, the objects are hidden)	Hide the selected	Hide	-	-
Cancels the hiding of the selected objects	Show the selected	Unhide	-	-
Edits the font for the selected object name	Set the font	-	-	Performed in the **Font** standard Windows dialog box
Restores the deleted name of the selected object	Restores the title object	-	-	-
Edits the size of the selected object	Objects size	-	-	Performed in the **Object size** dialog box
Edits the position of the selected object	Object position	Object position	-	Performed in the **Object position** dialog box or with the help of the mouse
Selects objects of one group	-	Selects all the similar	-	Example: all the **Camera** objects are selected
Selects all the identical objects within a group	-	Selects all the identical	-	Example: all the **Sensor** objects of the **Gerkon** type are selected

The *Map editor* utility enables to perform operations with a group of objects. To select several objects, hold down the Ctrl key on the keyboard.

Note

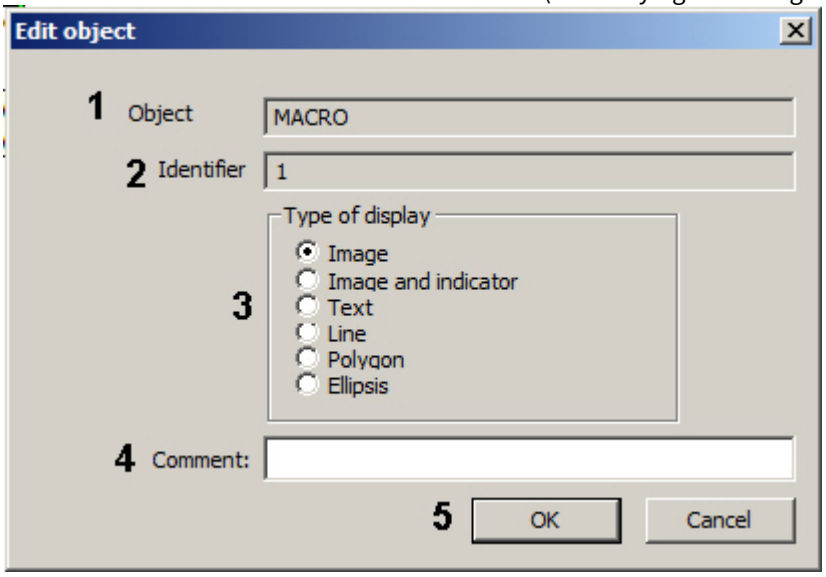
The **Object position** operation is not performed with a group of objects.

23.4.5.2.5.2 Editing the additional data and type of icon display

Edit the additional data and type of object icon display as follows:

1. Select an object that should be edited. Green-pointed frame will appear around the image as a result.
2. Call for the **Edit object** dialog window of the *Map editor* utility in one of the three ways:
   a. Perform the command of the main menu **Operations with objects -> Edit object**;
   b. Click the button on the toolbar;

c. Perform the **Edit** command of the context menu (called by right-clicking the object image).



3. The type of the selected object is automatically displayed in the **Object** field (**1**).
4. ID of the selected object is automatically displayed in the **Identifier** field (**2**).
5. If necessary, change the type of object icon display with the help of the **Type of display** switch (**3**).

The Type of display switch position	Type of object icon display	Note
Image	Schematic object image	Basic configuration objects, SCADA objects
Image and indicator	Schematic image and identifier of object state	SCADA objects
Text	Object name and text defined on the **Properties** panel or by script (see Editing object properties using the Properties panel or Examples of scripts in the JScript language in the The Script object. Programming using the JScript language)	SCADA objects
Line	Displaying object in the form of a straight line	SCADA objects
Polygon	Displaying object in the form of a polygon	Basic configuration objects, SCADA objects
Ellipsis	Displaying object in the form of an ellipsis	Basic configuration objects, SCADA objects

Note

Line object transformed to text will no longer be displayed on the Map, if **Text info** property is empty (see Editing object properties using the Properties panel).

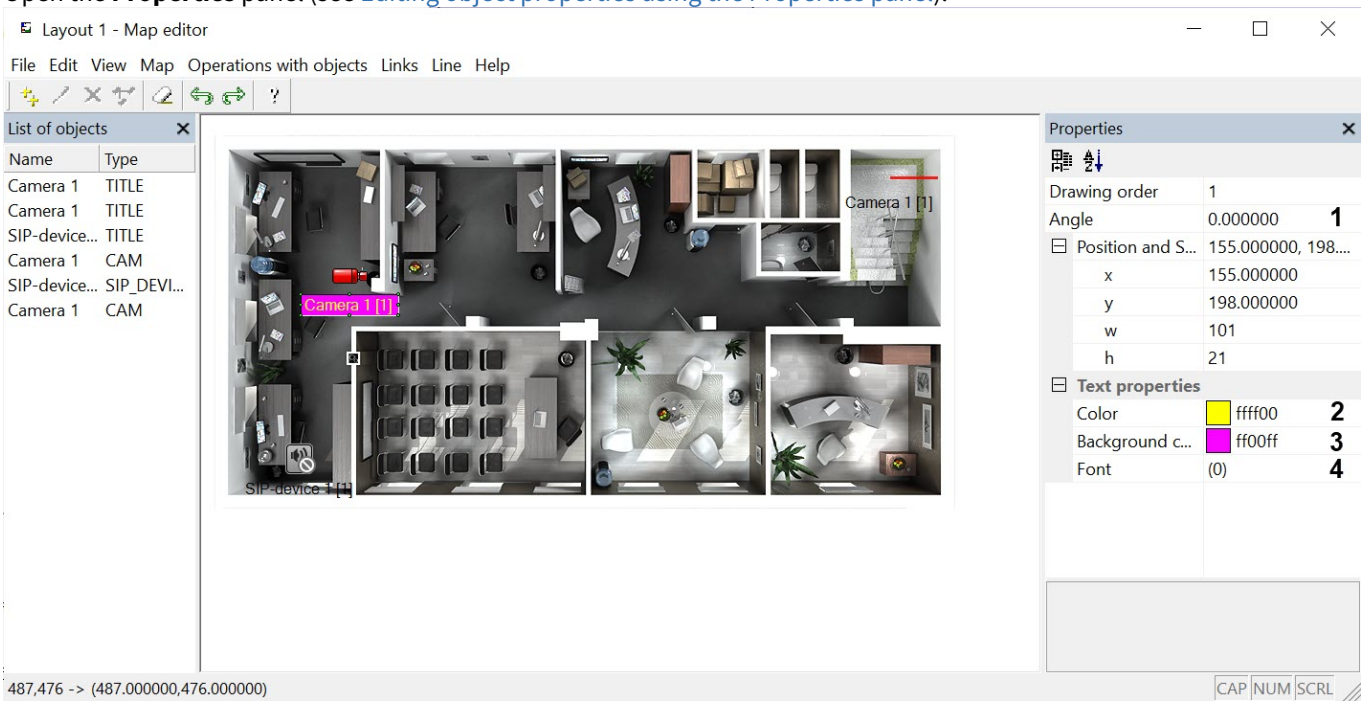
6. If necessary, change the object additional data in the **Comment** field (**4**).
7. To save the changes, click the **OK** button (**5**).

Editing the additional data and type of object icon display is completed.

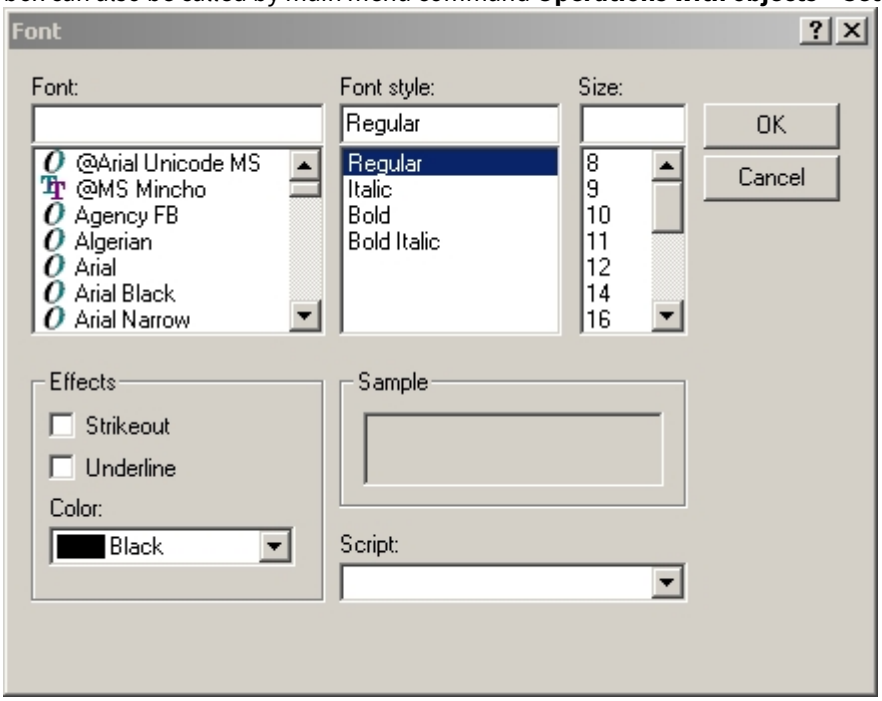
23.4.5.2.5.3 Editing the font, color, background or frame size of object name

Edit the font, color, background or frame size of object name as follows:

1. Select the name of the object, which font, color or background should be edited. Green-pointed frame will appear around the image as a result.
2. Open the **Properties** panel (see Editing object properties using the Properties panel).



3. Set **X** and **Y** coordinates of the left upper corner of the text frame, as well as frame height and width (**w** and **h**) and clockwise rotation **Angle** (**1**).
4. In the **Color** field, select the object name font color (**2**).
5. In the **Background color** field, select the object name background color (**3**).
6. Click ... in the **Font** field (**4**). The standard Windows dialog window **Font** of the **Map editor** utility is opened. This dialog box can also be called by main menu command **Operations with objects > Set the font**



7. In the opened dialog window, set the required font or color parameters.
8. Click the **OK** button to save the changes.

Editing the font, color or background of object name is complete.

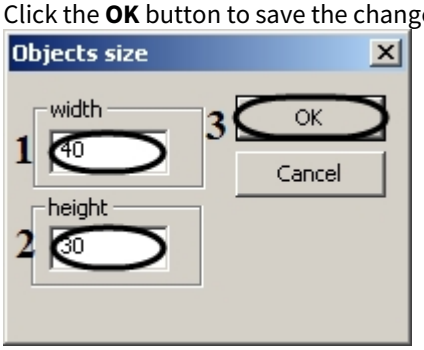
23.4.5.2.5.4 Editing the object size

Edit the object size as follows:

1. Select the object, the size of which should be edited. Green-pointed frame will appear around the image as a result.
2. Call for the **Objects size** dialog window of the *Map editor* utility by the main menu command **Operations with objects** > **Objects size**.
3. Specify the size of the image: **Width** (icon width) and **Height** (icon height) fields (**1**, **2**). Icon size is expressed in pixels.

> **Note**
>
> If 0 value is entered in the **Width** and **Height** fields, object icon will be displayed in the original size.

4. Click the **OK** button to save the changes (**3**).

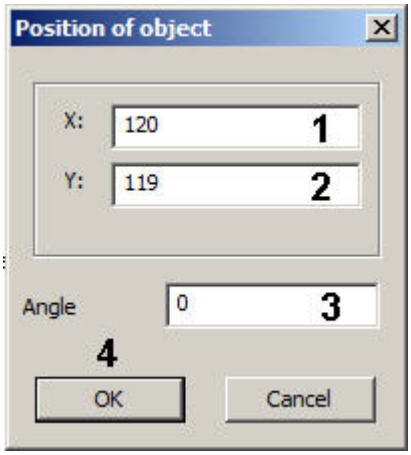


Editing the object size is complete.

23.4.5.2.5.5 Editing the position of object

Using the Position of object dialog window
Edit the position of object with the help of the **Position of object** dialog window as follows:

1. Select the object, the position of which should be edited.
2. Call for the **Position of object** dialog window of the *Map editor* utility in one of two ways:
   a. Perform the command of the main menu **Operations with objects > Position of object**;
   b. Perform the command of the context menu **Position of object** (called by right-clicking the object image).



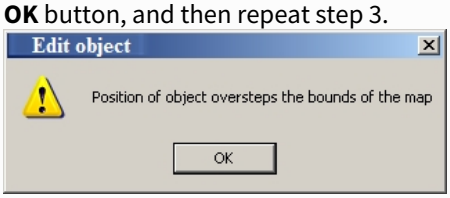
3. Set the coordinates of the object center: **X** (horizontal indent from the left border of graphic plan) and **Z** (horizontal indent from the bottom border of graphic plan) fields (**1**, **2**).

> **Note**
>
> The **In Meters** switch position is relevant when real parameters of the protected facility are set, to which this layer corresponds (see Creating the layers of the interactive map).

4. Enter the angle in degrees of object image turn in the **Angle** field. The angle is set counterclockwise from the contour line (**3**).
5. To save the changes, click the **OK** button (**4**).

Note

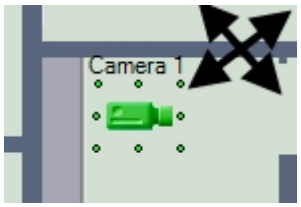
In case when at least one coordinate oversteps the bounds of the map, the message window will be displayed. Click the **OK** button, and then repeat step 3.



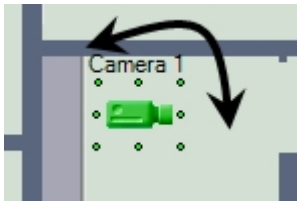
Editing the object position with the help of **Position of object** dialog window is completed.

Using the mouse
The *Map editor* utility also enables to edit the object position with the help of the mouse.

To set the position of the icon on the map, hover the mouse cursor over it and left-click it. Holding the left mouse button, place the icon on the place on the map that corresponds to its real location on the territory of the protected facility.

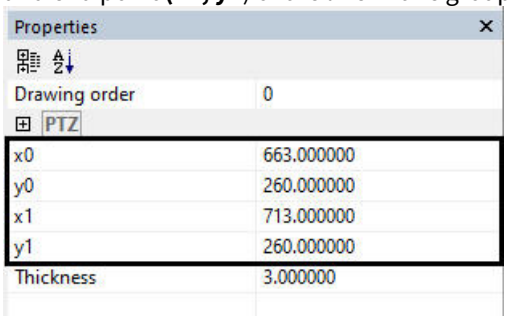


To rotate the icon, hover the mouse cursor over it and left-click it. Green-pointed frame will appear around the icon as a result. Point at one of the corner dots. A bended arrow will appear. Move the mouse in the required direction to rotate the icon.

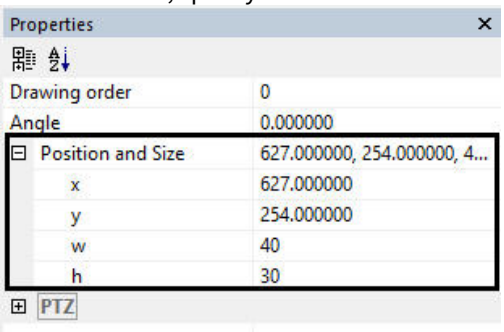


Using the Properties panel
You can also change the coordinates, rotation angle and the icon size of the **Line**, **Image**, **Image and indicator** and **Text** object types using the **Properties** panel:

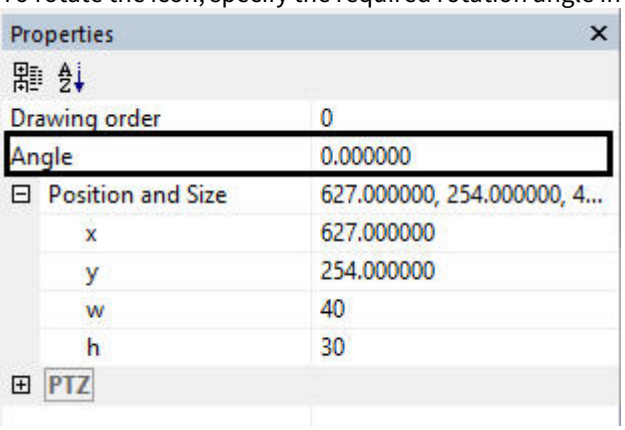
1. Open the **Properties** panel for the required object (see Editing object properties using the Properties panel).
2. Expand the **Position and Size** settings group. For the **Line** icon type, specify the coordinates of the initial point (**x0, y0**) and end point **(x1, y1**) of the line in this group.



3. For other icons, specify the coordinates of the upper left corner (**x, y**), width (**w**) and height (**h**).



4. To rotate the icon, specify the required rotation angle in degrees in the **Angle** field.

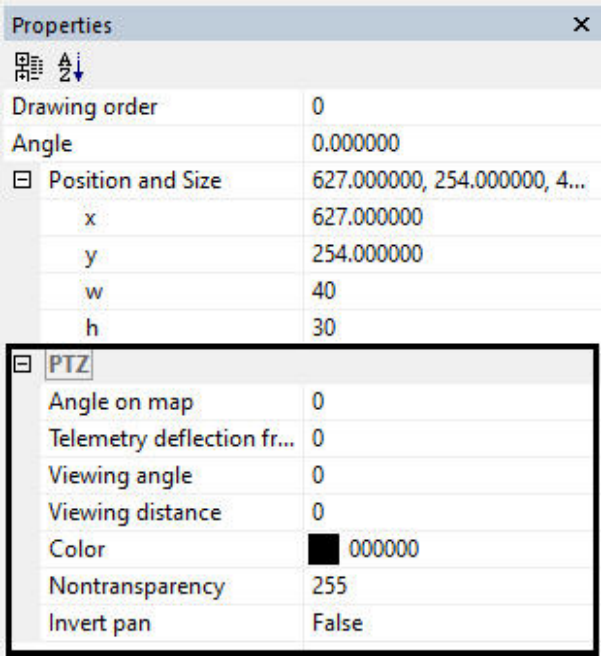


Editing the object position using the **Properties** panel is complete.

23.4.5.2.5.6 Changing the camera angle display

To display the camera angle on the map, do the following:

1. Select the object for which it is necessary to display the viewing angle. As a result, the object name will be highlighted with a border of green dots.
2. Open the **Properties** panel for the required object (see Editing object properties using the Properties panel) and expand the **PTZ** settings group.



3. Set the required field values:

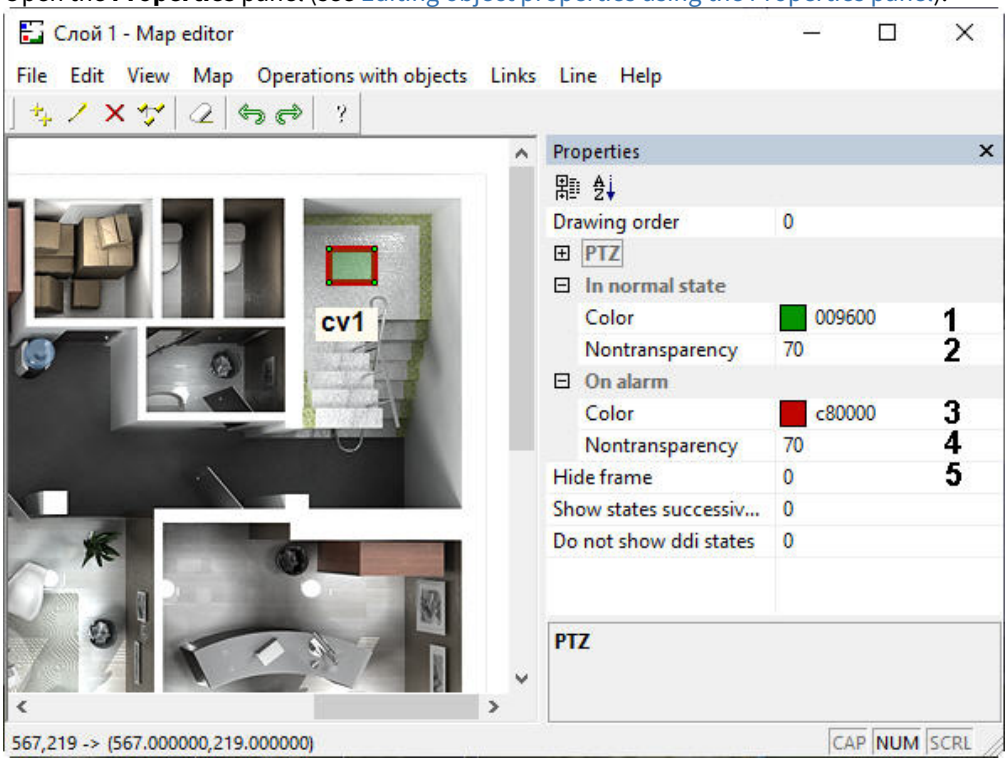
a. **Angle on map**—the direction of the display vector on the map. A value of 0 is the actual position of the camera at the time of setting the parameters.
b. **Telemetry deflection from zero**—the actual offset of the camera.
c. **Viewing angle**—the angle of the view display vector.
d. **Viewing distance**—the size of the the view display vector.
e. **Color**—the color of the view display vector.
f. **Nontransparency**—the transparency of the view display vector.
g. **Invert pan**—select **True** in the drop-down list if it is necessary to invert the camera rotation.

Changing the camera angle display is complete.

23.4.5.2.5.7 Editing color and transparency (polygon and ellipsis)

Edit the color and transparency of objects added to the map as polygons and ellipsis as follows:

1. Open the **Properties** panel (see Editing object properties using the Properties panel).



2. From the drop-down list, select the fill color of the polygon or ellipsis (**1**).
3. Set the degree of transparency of the polygon or ellipsis in the normal state (**2**). The smaller the number, the higher the degree of transparency. 0 corresponds to full transparency, 255 — full opacity.
4. From the drop-down list, select the fill color of the polygon or ellipsis in case of alarm (**3**).
5. Set the degree of transparency of the polygon or ellipsis in the alarm state (**4**). The smaller the number, the higher the degree of transparency. 0 corresponds to full transparency, 255 — full opacity.
6. If the frame framing the polygon should be hidden, then set the value to **1** in the **Hide frame** field (**5**).

23.4.5.2.5.8 Editing the line thickness

To edit the thickness of the object icons added to the map in the form of a line, do the following:

1. Select the object for which it is necessary to edit the line thickness. Green-pointed frame will appear around the image as a result.

2. In the *Map editor* utility dialog box, select **Line -> Thickness**.

3. In the **Thickness** dialog box, specify the line thickness.

4. Click the **OK** button.

Editing the object line thickness is complete.

> **Note**
>
> You can edit the thickness, as well other other display parameters of several object icons in the form of a line simultaneously. To do this, select the required icons with left mouse button, while holding down the Ctrl key on the keyboard.

23.4.5.2.5.9 Adding or removing apexes of polygon or polyline

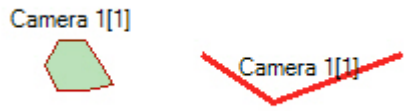
To add apexes to an object icon in the form of a polygon or polyline, do the following:

> **Note**
>
> Maximum number of apexes in the polygon is 51.

1. Call the context menu of the object icon by right-clicking and holding down the Ctrl key in the polygon area or on the polyline.

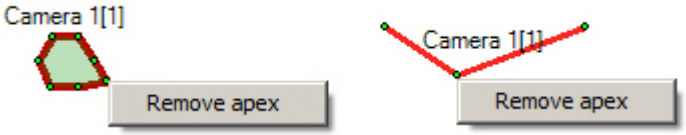
2. Select **Add apex**.
3. Select the required position of a new apex and left-click.

4. The apex will be added to the polygon or the polyline.



Adding apexes to an object icon in the form of a polygon or polyline is complete.

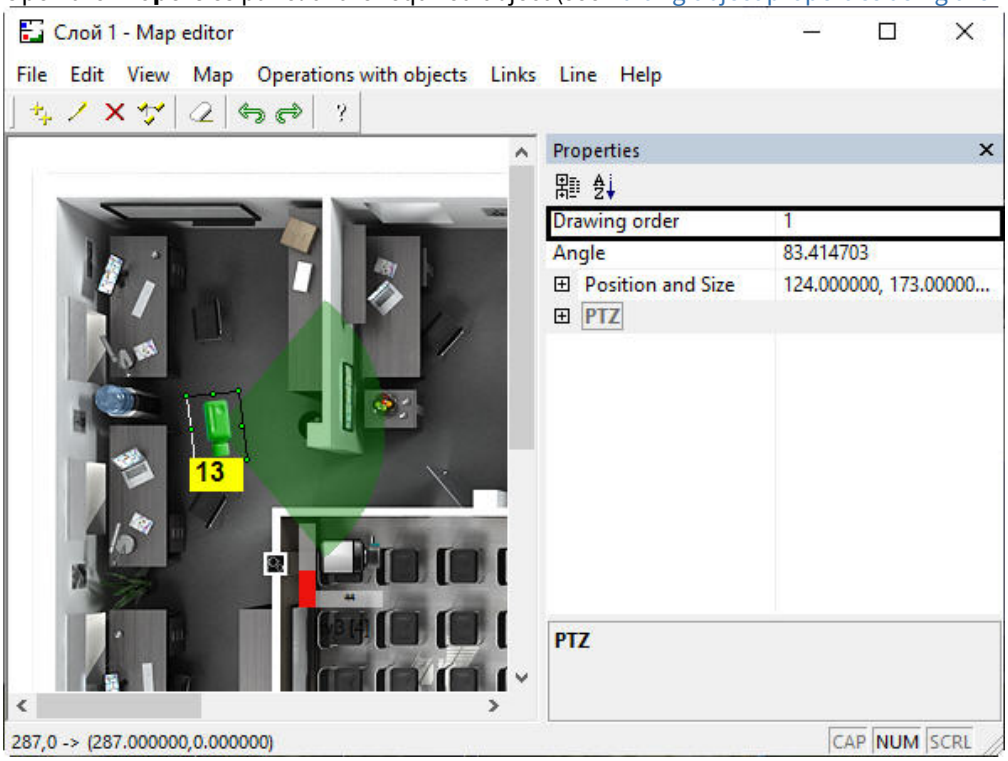
To remove the apex, right-click it holding down the Ctrl key and select **Remove apex**.



23.4.5.2.5.10 Setting the order of displaying objects on map

You can set the order of object icons display when they overlay. To do this, do the following:

1. Open the **Properties** panel of the required object (see Editing object properties using the Properties panel).



2. Set the value of the **Drawing order** parameter. The icons with higher value of this parameter will be displayed over the icons with lower value.

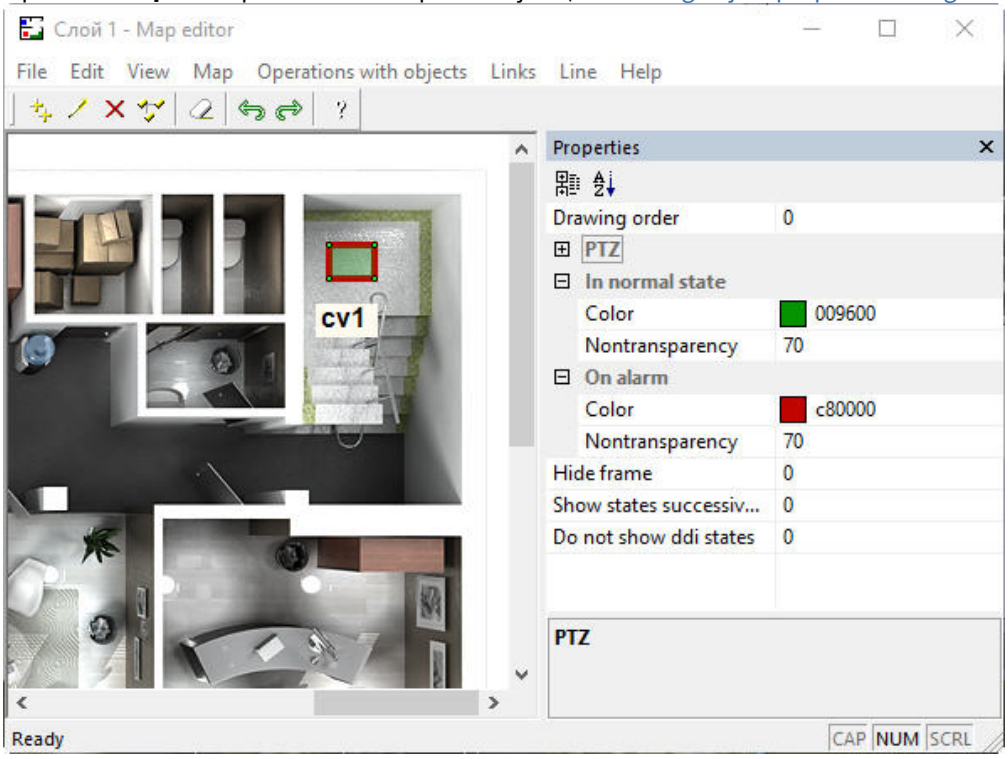
Setting the order of object icons display is complete.

23.4.5.2.5.11 Configuring the objects states display (polygon and ellipsis)

By default, if the object is in several states at the same time, the device icon changes according to these states in a short time, and when the object is selected on the map all its states are displayed as the thumbnails next to it (see Graphic objects on the Map).

It is possible to disable displaying states thumbnails. To do this, do the following:

1. Open the **Properties** panel for the required object (see Editing object properties using the Properties panel).



2. To disable the display of the thumbnails, select the **1** value from the **Show states successively** drop-down list. To enable their display, select the **0** value from this drop-down list.

Configuring the display of the objects states is complete.

23.4.5.2.6 Linking the layers of the interactive map

Intellect system allows creating multilevel maps comprised of several layers.

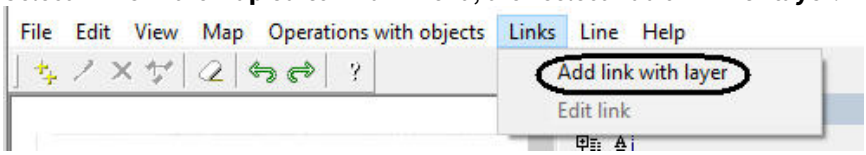
In case of multiple layers, the links should be established between the layers. These links help move to other layers for operative control and viewing of the device objects located on them.

The links are created in the **Map editor**. To run the **Map editor**, click **Edit selected layer** in the settings panel of the **Layer** object. When a link is established, a special symbol appears on the map. Clicking on this symbol takes the operator from the current layer to another layer.

> **Note.**
>
> The link symbols also notify the operator about alarms coming from devices located on the linked layer.

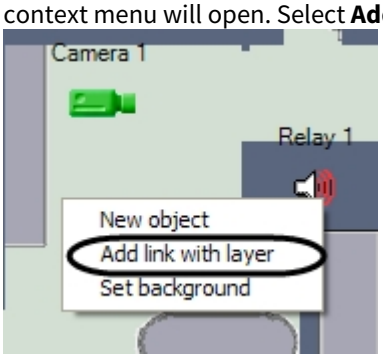
To create a new link from the current layer to another, do the following:

1. Select **Links** in the **Map editor** main menu, then select **Add link with layer**.



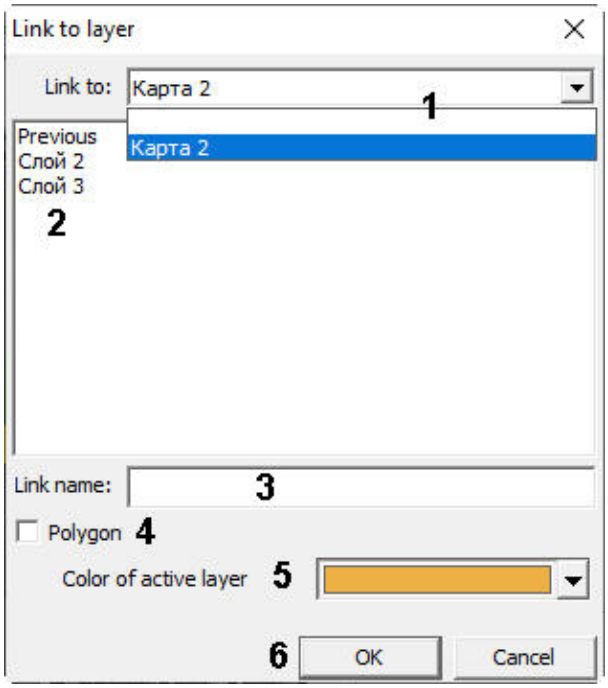
The **Link to layer** window opens, allowing to choose the layer to link to.
There is another way of opening the **Link to layer** window. In the **Map editor,** click anywhere on the layer map. The

context menu will open. Select **Add link with layer** from this menu.



2. Do the following in the **Link to layer** window:
   a. If the switch to the layer of another map is to be performed, then select the required **Map** object in the **Link** dropdown list (1). If the switch to the layer of the same map is to be performed, then select an empty value in the dropdown list.

> **Note.**
>
> The layer of another map is opened in this map box and not in the box where there is the layer the switch is performed from.

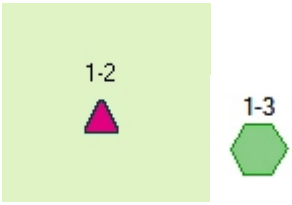


   b. Select a layer the switch is to be performed to (2).
   c. Enter the name for this link in the **Link name** field (3).
   d. If the link on the map is to be displayed as a polygon, set the **Polygon** checkbox checked (4).

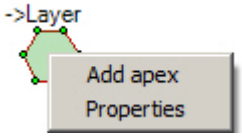
> **Note.**
>
> The color and shape of the polygon are set after adding it to the layer. By default, the link is represented by a green hexagon.

   e. If the selected layer the switch will be performed to, is on another map, then in the **Color of active layer** dropdown list select the color the link will be marked when this layer is active on the map (5).
   f. Click the **OK** button to create the link (6).

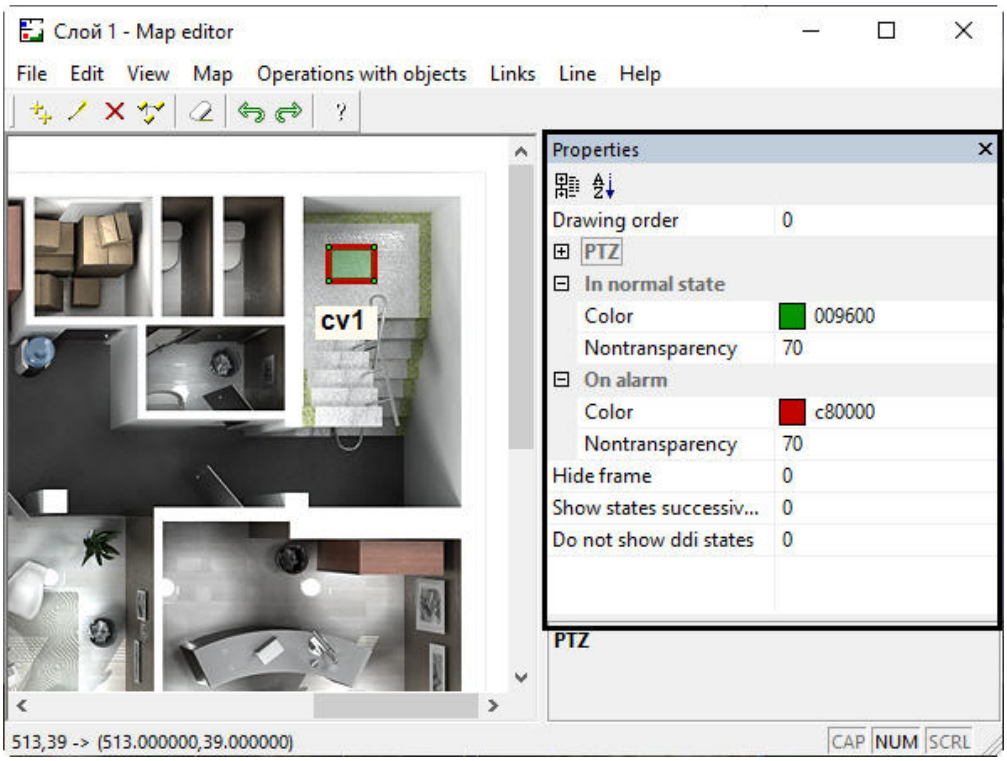
A symbol will appear on the map representing the link. The icon of the link is represented by a red triangle or a polygon if the **Polygon** checkbox was checked (see step 2.d):



The feature menu appears when right clicking the polygon holding down the Ctrl key. The following features are available:



1. **Add apex** – add a new apex to the polygon. A new apex appears when selecting this menu item. One is to locate it left clicking on the map.
2. **Properties** – display the properties panel of the icon on the right of the **Map editor**. Using this panel one can set the color and opacity of the normal and alarm states of the layer icon, as well as configure whether to hide frame limiting the polygon.



By default the symbol of connection with this layer starts to flash if alarm is detected on the layer. If additional indication is required it is possible to configure alarm symbol of connection with layer. To do this place the file link_alarm.bmp containing some image characterizing alarm on the layer to the <*Intellect* installation directory>/Bmp folder. If such file is in the Bmp folder then symbol of connection with this layer will changed to image from the link_alarm.bmp file and start to flash while alarm on this layer.

Note.

If the link with the layer is represented by the polygon, then it starts changing its color (blinking) when there is an alarm on the layer.

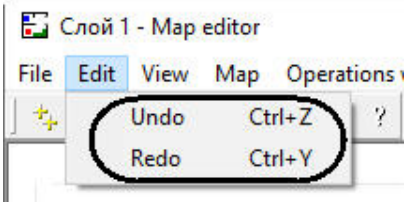
Switching between layers of the Map

23.4.5.2.7 Cancelling the last action in Map editor

While configuring interactive map in the *Map editor* utility it's possible to cancel the last action and redo the last cancelled action in one of the following ways:

1. Using the corresponding buttons on the toolbar of the *Map editor* utility.

2. Using combination of Ctrl+Z and Ctrl+Y buttons.
3. Using the corresponding commands in the **Edit** menu.

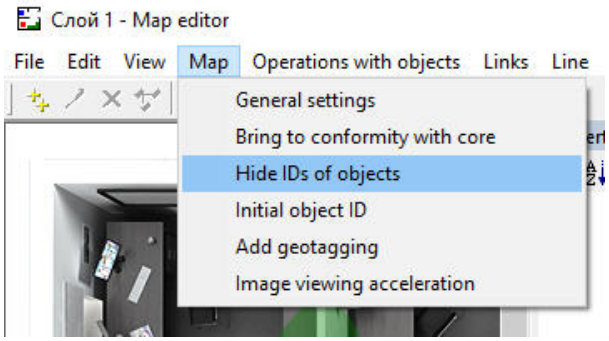


It is possible to cancel not more than 30 actions.

23.4.5.2.8 Configuring object ID is displaying

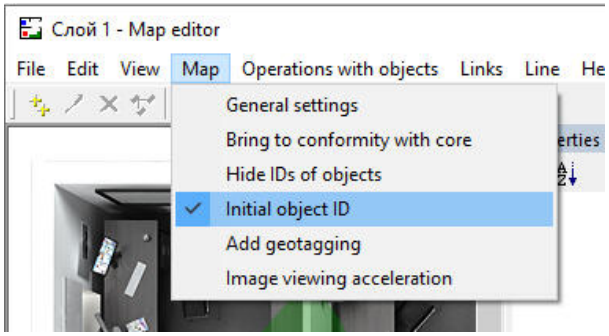
By default the object ID is displayed in square brackets next to the object name on the interactive map.

One can hide object IDs on each layer of the interactive map. For this set the **Hide object ID** checkbox checked in the **Map** menu of *Map editor*.



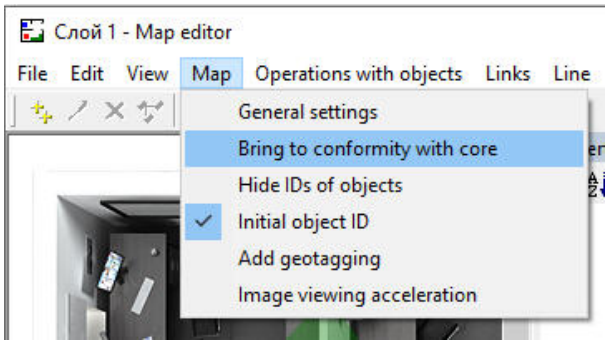
As a result object IDs are hidden on the layer that being edited on the interactive map.

Object ID can also be configured to display before object's name. For this set the **Initial object ID** checkbox checked in the **Map** menu of *Map editor*.



If no space is displayed between object name and object ID, or the "]" symbol is not displayed after ID, select **Bring to conformity with core** in the **Map** menu. This will bring the text field to a standard size in case is it was somehow reduced or enlarged earlier.

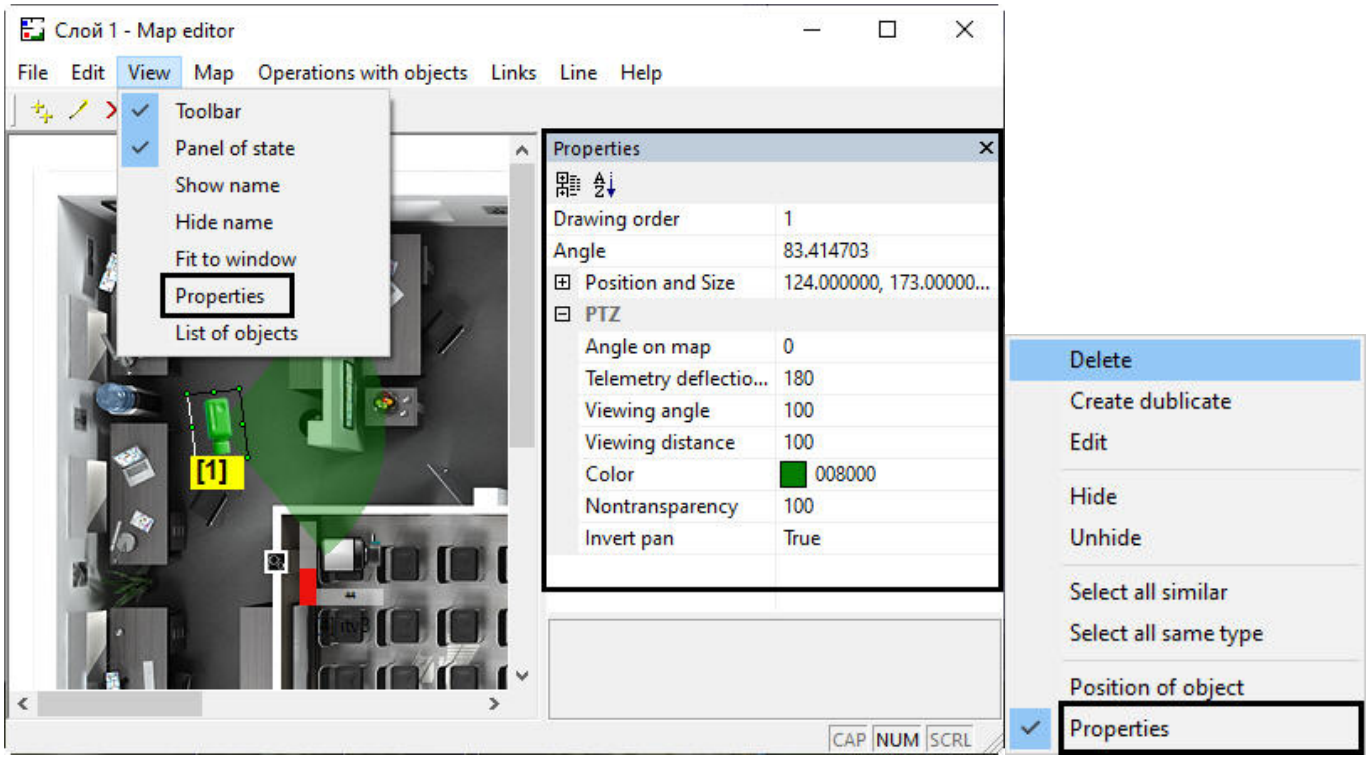
> **Note.**
>
> This will also delete icons of non-existing objects from the layer.



23.4.5.2.9 Editing object properties using the Properties panel

The **Properties** panel is displayed on the right side of the **Map editor** utility dialog box when you select **View -> Properties**.

This panel can also be opened by selecting the **Properties** item in the context menu of any object.



When selecting an object on the layer of the interactive map, the list of the object parameters is displayed on the **Properties** panel. These parameters can also be edited with the help of this panel.

For example, using this panel, you can set the color and the font of the object caption, as well as the color and other parameters of the object icon in the form of polygon.

When selecting an object on the **Properties** panel, you can control the display of this object parameter list by using the following buttons:

— expands the object parameters tree.

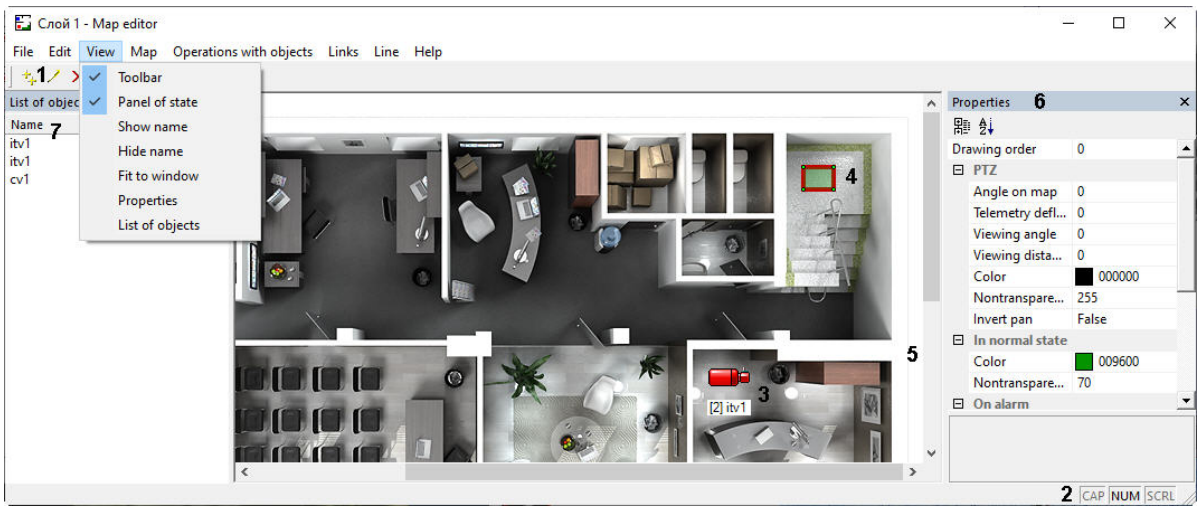
— sorts the parameters in alphabetical order.

To edit the display parameters of several similar object icons simultaneously, select the icons with the left mouse button while holding down the Ctrl key on the keyboard. Further editing of the parameters is performed in the same way as for a single object.

If several different object icons are selected (for example, image and line, or polygon and text), then group editing of their properties is not available.

23.4.5.2.10 Configuring viewing Map editor utility

Configuration of viewing the *Map editor* window is performed using the **View** menu.



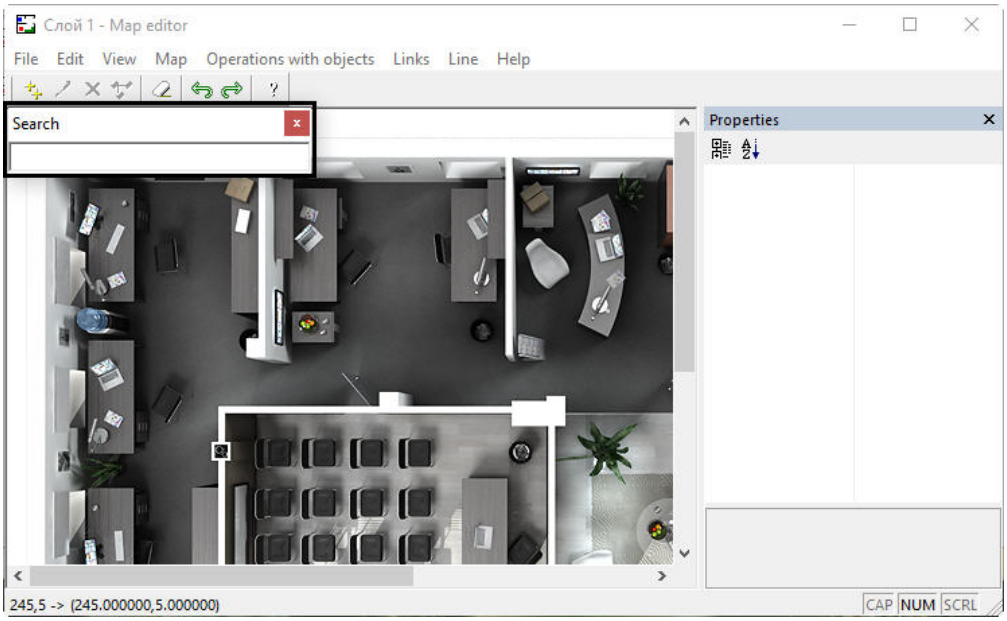
Find the description of menu items in the table.

Menu item	**Function**
Tools panel	Show and hide the tools panel (1).
State panel	Show and hide the state panel (2).
Show name	Enable showing the name of selected object (3).
Hide name	Disable showing the name of selected object (4).
Fit the window	To change the image scale this way set the checkbox unchecked. Set a scale at which the image of the Map fits perfectly into the window of the *Map editor* utility (5). If this checkbox is set checked, the scale of the map image cannot be changed by scrolling with the Ctrl key held down on the keyboard. The checkbox is to be set unchecked to change the scale this way. *Note 1. Setting this checkbox checked does not affect the scale of the Map image in the Map window. This scale is set independently.*

	*Note 2. If this checkbox was previously set for any layer, it is automatically set for all other layers. To disable the automatic activation of the **Fit the window** checkbox, it is necessary to set the **0** value for the **InscribeEditor** key (see Registry keys reference guide, for details about working with the registry, see Working with Windows OS registry).*
Properties	Displaying the Properties panel (6).
List of objects	Displaying the list of objects added to the map (7).

23.4.5.2.11 Searching object in the Map editor utility by its name and ID

To search for an object in the *Map editor* utility by its name or ID, press Ctrl+F on the keyboard. The **Search** box is displayed in the upper-left corner of the **Map editor** window.



Specify the name or ID of the object and press Enter. If an object ID is specified for the search, then the search is performed both by the ID and by name. Press F3 on the keyboard to show the next search result, press Shift+F3 to show the previous result.
The found objects are outlined with green dots, while the icon of the object is positioned in the center of the **Map editor** window. After the object is found, its icon flashes for a few seconds.

23.4.5.3 Configuring the mechanism for searching and processing alarm signals on multilayer maps

On this page:

- Displaying the Map over all windows
- Autoswitch to a layer with an alarm signal
- Recursive search for a layer with an alarm signal

When using multilayer interactive maps in *Intellect*, it is possible to set rules for moving to the layers that have objects that triggered an **Alarm**.

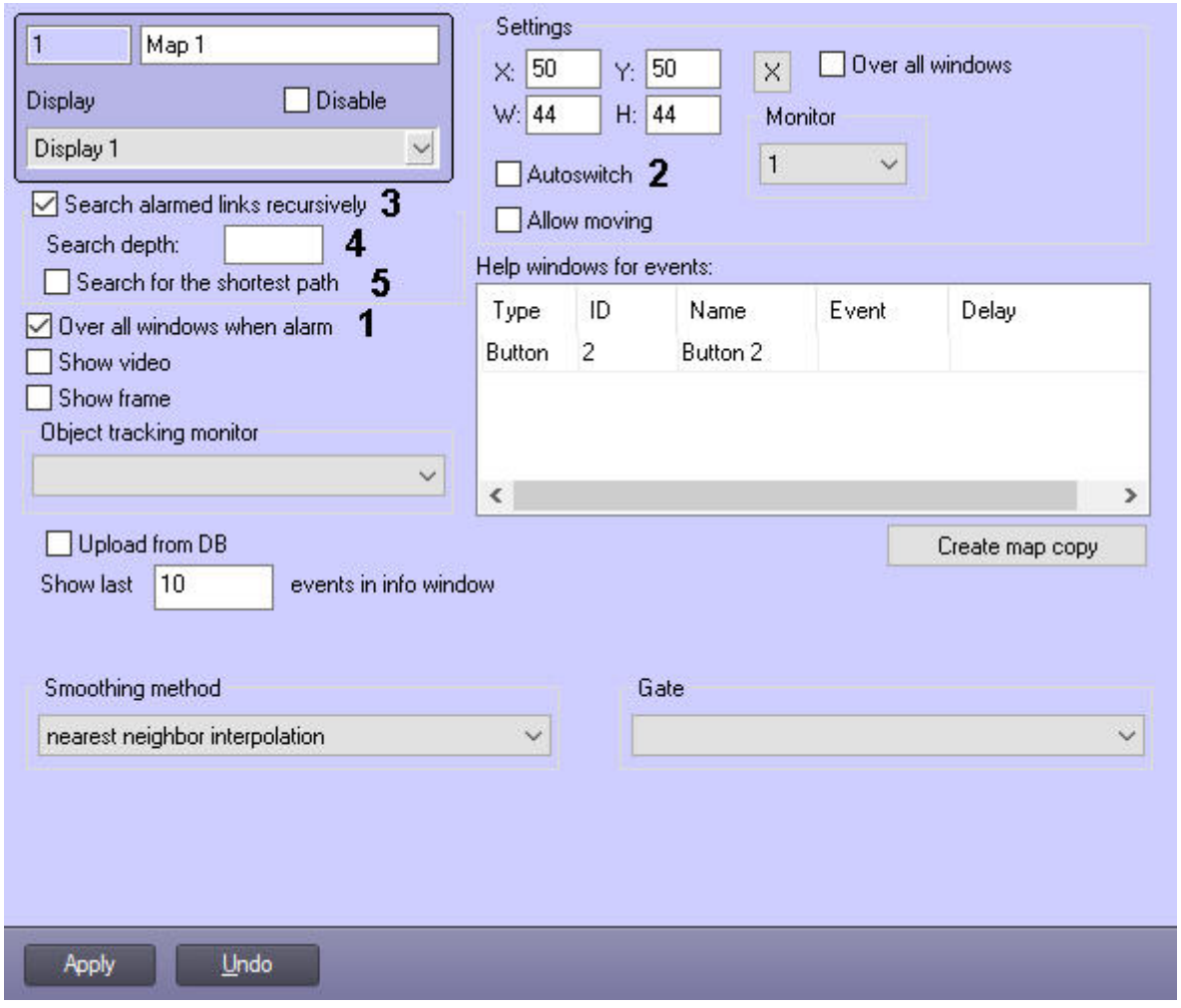
The following ways of displaying the layer with an alarm signal exist in *Intellect*:

1. When an **Alarm** occurs, the interactive Map window opens above all other active windows showing the layer with an alarm, including the objects and their corresponding symbols on the layer.
2. The layer with a registered **Alarm** displays automatically.
3. The links recursively lead to the layer with an alarm signal.

23.4.5.3.1 Displaying the Map over all windows

To open the Map window above all other windows, set the **Over all windows when alarm** checkbox (**1**) and click the **Apply** button in the settings panel of the **Map** object. The **Map** window will now open on top of other windows in case of alarm registration.

> **Note**
>
> If the Map has multiple layers, this setting will only work for the active layer.
> Example 1: Layer 1 is active, alarm signal is on Layer 2. The Map will not be displayed over all windows.
> Example 2: Layer 2 is active, alarm signal is on Layer 2. The Map will be displayed over all windows.
> In order to display the Map over all windows regardless of the active layer, you should enable **Autoswitch** (described below).



23.4.5.3.2 Autoswitch to a layer with an alarm signal

In order to automatically switch to the layer with an **Alarm** signal, set the **Autoswitch** checkbox (**2**) and click the **Apply** button. As a result, the layer with an alarm signal will be activated when an Alarm occurs.

23.4.5.3.3 Recursive search for a layer with an alarm signal

To make it possible to move from the current layer to any other layer on multilayer maps, the sequential links to other layers should be specified. If the links recursively connect all layers of the map, the recursive links can be used for registering an Alarm on one of the layers. To enable recursive search of a layer with a registered Alarm, set the **Search alarmed links recursively** checkbox (**3**) and click the **Apply** button in the settings panel of the **Map** object. If there are many layers, then you can limit the **Search depth** for links across layers by setting the required value in field (**4**):

- empty field—search across layers is not limited;
- 0—related layers are not taken into account during search, that is, in case of alarm, only the layer on which the alarm occurred will blink;
- >0—indicates the number of layers through which the search will be performed. For example, the Map has 6 interconnected layers and the alarm appeared on the 3rd layer. If the key value=1, the alarm will blink on layer 3, as well as on layers 2 and 4.

Note

The **Search depth** parameter in the interface is similar to the **AlarmLinkSearchDepthKey** registry key (see Registry keys reference guide): if the key was created earlier than the interface parameter was set, then the field is filled in based on the key value.
If the key is created on the Remote Client, then the value from the key will be used on the Remote Client, regardless of the **Search depth** parameter value specified on the Server. If a key is not created on the Remote Client, then the Server **Search depth** is used everywhere.
Examples:

1. The **Search depth** is set to 1 on the Server; the key is not created on the Remote Client. Result: on the Server and on the Remote Client, the search depth is 1.
2. The **Search depth** is set to 1 on the Server, the **AlarmLinkSearchDepthKey** with the value 2 is created on the Remote Client. Result: the search depth on the Server is 1, on the Remote Client it is 2.

The recursive search of objects on the Map is a type of search when it is possible to switch to a layer with an alarm from a layer where the link is located by sequential transitions to adjacent layers, using sequential links. If the **Search for the shortest path** checkbox is set (**5**), the shortest possible path to the layer with an alarm will be automatically selected.

Example

The 1st layer contains the link to the 2nd layer, and the 2nd layer contains the link to the 3rd layer. The 1st layer is currently active. An alarm is triggered on the 3rd layer. If the recursive search is on, the link from the 1st to the 2nd layer will blink, and the link from the 2nd to the 3rd layer will blink. If the recursive search is off, only the link from the 2nd to the 3rd layer will blink, not allowing the operator to see the alarm if the 1st layer is active.

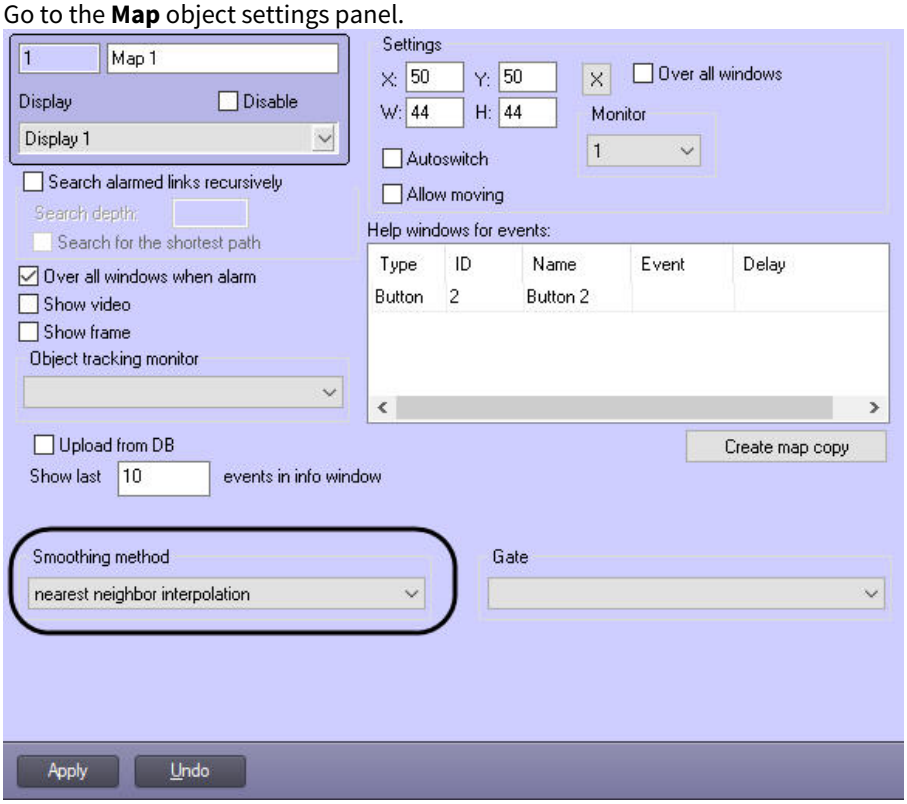
Example

The 1st layer contains the links to the 2nd and the 3d layers, and the 2nd layer contains the link to the 3d layer (i.e. there are two ways to reach the 3d layer: directly or via the 2nd layer). Let the 1st layer be currently active. An **Alarm** comes from the 3d layer. If recursive search is on and the **Search for the shortest path** checkbox is set on the 1st (active) layer, the link to the 3rd layer will blink. If the **Search for the shortest path** checkbox is not set, the links to the 2nd and 3rd layer will blink on the 1st layer.

23.4.5.4 Configuring the smoothing method of the Map when scaling

To configure the smoothing method of the Map when scaling, do the following:

1. Go to the **Map** object settings panel.



2. From the **Smoothing method** drop-down list, select the necessary smoothing method:
   - low quality
   - high quality
   - bilinear interpolation
   - bicubic interpolation
   - nearest neighbor method
   - high quality bilinear interpolation
   - high quality bicubic interpolation

> **Note**
>
> Smoothing minimizes the ragged diagonal edges of the image and creates the impression of softer image borders and higher resolution.

3. Click the **Apply** button.

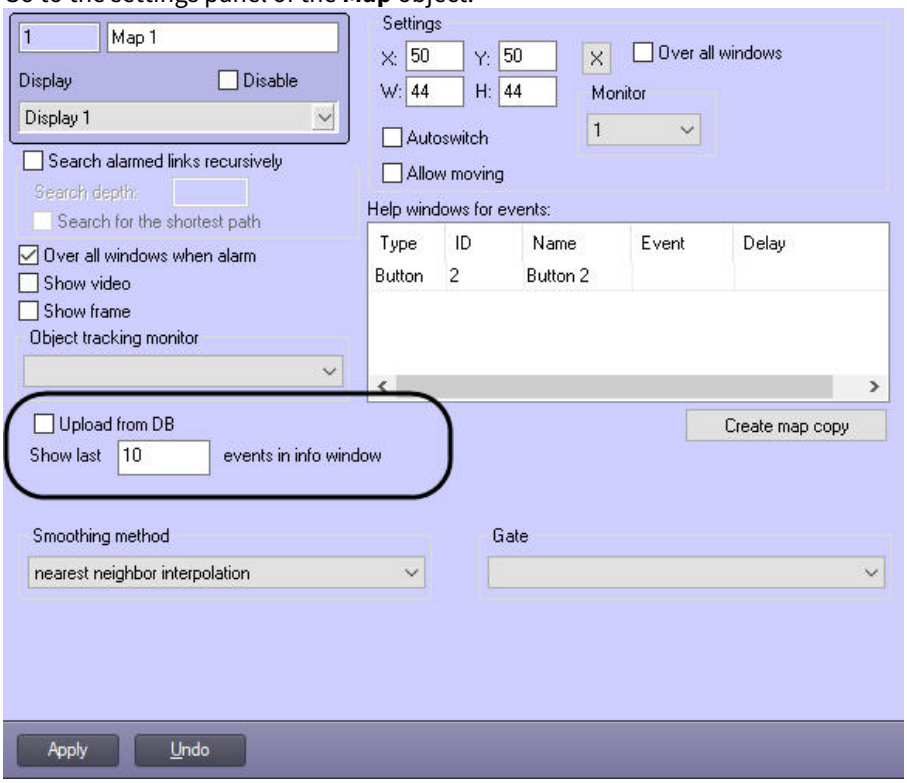
The smoothing method of the Map when scaling is configured.

23.4.5.5 Configuring the number of events displayed in the Map window

Several recent events of the selected object can be displayed in the Map window (see Viewing last object events on the map).

Configure the number of events to be displayed as follows:

1. Go to the settings panel of the **Map** object.



2. In the **Show last ____ events in info window** field specify the number of events that should be displayed in the info window on the Map. The value must be strictly less than 100.
3. Set the **Upload from DB** checkbox in order to upload last events from database on the *Intellect* startup to display in the Map window. If the checkbox is cleared, only events registered after the *Intellect* start are displayed.
4. Click the **Apply** button.

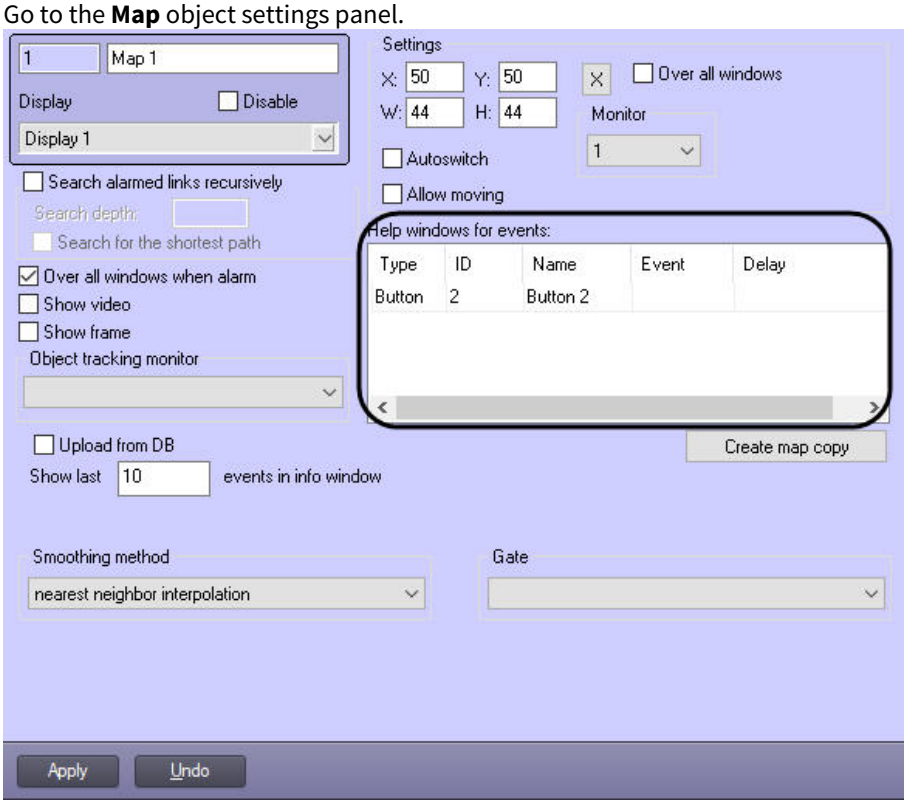
The number of events to be displayed in the Map window is now configured.

23.4.5.6 Configuring the event tooltips

The map allows you to set a list of events. When these events come in, the tooltip with the event name is displayed for a certain time above the corresponding object.

To configure the event tooltips, do the following:

1. Go to the **Map** object settings panel.



2. From the **Type** drop-down list, select the object type from which the required event come .
3. From the **id** drop-down list, select the object identifier. If no identifier is selected, the event tooltips will be displayed above all objects of the selected type.
4. After the type and identifier are selected, the **Name** field will be filled automatically.
5. From the **Event** drop-down list, select the event name. When the event incomes from the object name specified in this parameter, the tooltip with the name of the event is displayed. If no event is selected, the event tooltips will be displayed for all events which come in from the selected object(s).
6. In the **Delay** field, enter the time period in seconds during which the tooltip will be displayed after registering the event. If another event which should also be displayed on the tooltip comes in from the object within the specified time interval, the newer event will be displayed, and the older one will be hidden.
7. Click the **Apply** button.

The event tooltips are configured.

23.4.5.7 Configuring the order of reactions in the object menu

The object management on the map is performed using the feature menu (see Graphic objects on the Map section in Operator's Guide). If one needs to put the most frequently used commands (reactions) at the top of the menu for ease of use, then it is possible to customize the sorting of commands. For this use the **map_react_sort.ini** file created in the *Intellect* installation directory when the Map is started.

> **Important!**
>
> Reactions are ordered as specified in **map_react_sort.ini** file only on the computer where this file is. To show the same order of reactions place **map_react_sort.ini** file onto all computers that will use the **Map** interface (Servers, AWS, Clients).

Initially, this file contains an unsorted list of reactions:

```
[CAM]
REC_STOP=0
MUX1=1
```

```
ARM=2
REC=3
SIP_DISCONNECT=4
DISARM=5
SIP_CONNECT=6
```

The number after the "=" sign indicates the command number in the feature menu.

Change the order of commands in the menu as follows:
1. Shut down *Intellect*.
2. Number the reactions in the **map_react_sort.ini** file as required. The smaller the number, the higher the command will be in the list. If there are two identical values, the corresponding commands will follow one another.
3. Save the changes in the **map_react_sort.ini** file.
4. Start *Intellect*.

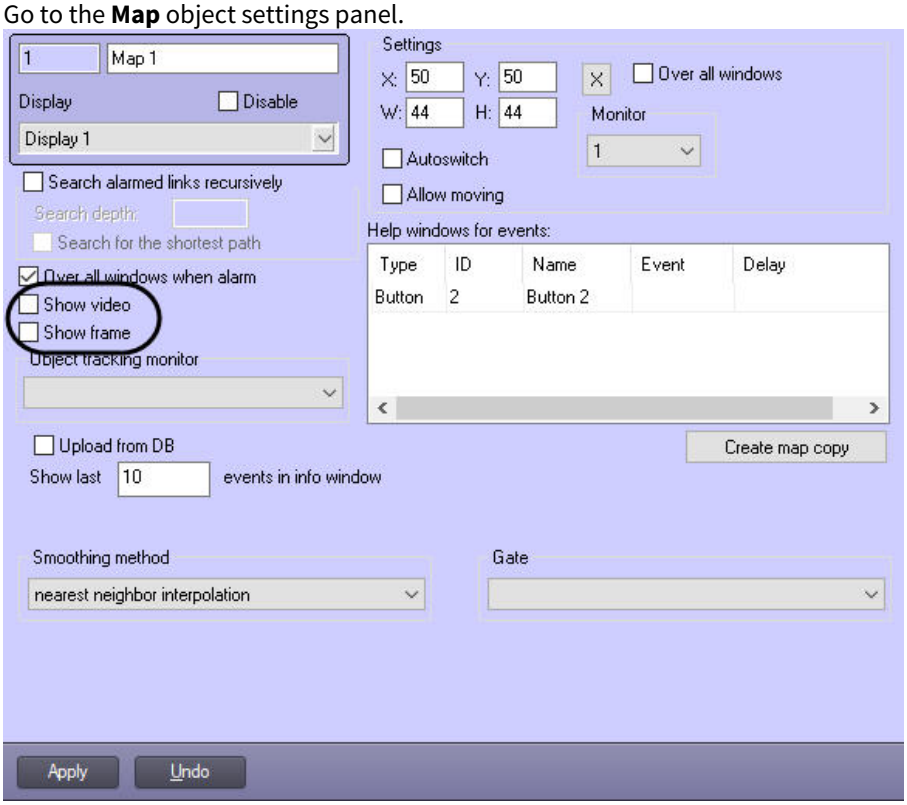
After starting the Map, this file will be rewritten: the reactions will be numbered according to sorting, starting with 0, the same numbers will be eliminated.

23.4.5.8 Enabling the frame or video request function

Intellect allows to request frames as well as live and archive video from cameras and for object linked to cameras (see Connection of objects with cameras for details on linking object with cameras). See Operator's Guide for details on operation of the frame/ video request function.

The frame and video request functions are disabled by default. To enable them, proceed as follows:

1. Go to the **Map** object settings panel.



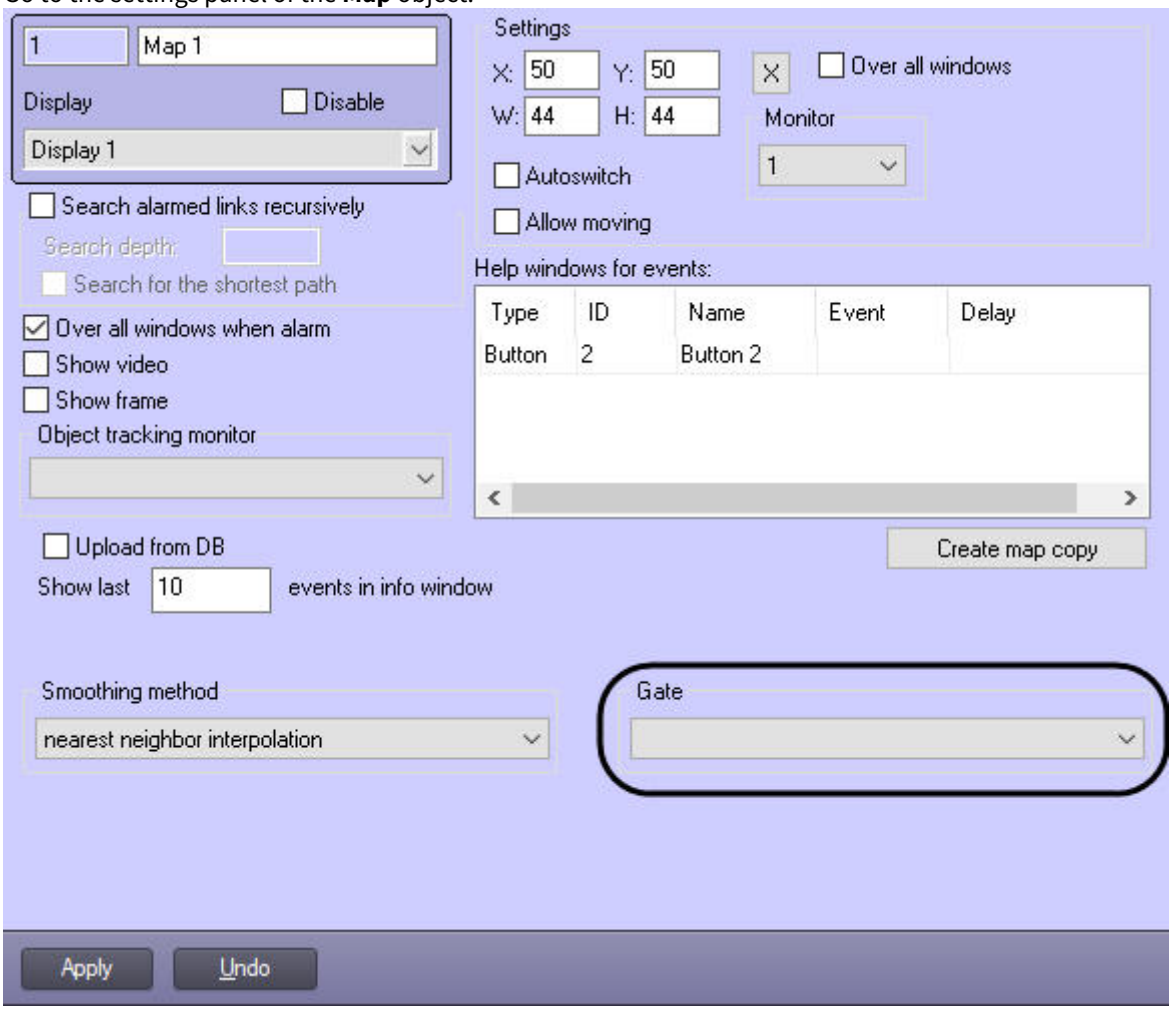
2. Set the **Show video** checkbox in order to enable live and archive video request.
3. Set the **Show frame** checkbox in order to enable frame request.
4. Click **Apply**.

Enabling frame and video request functions is completed.

23.4.5.9 Selecting a Video Gate to display video on the map

To select the Video gateway through which the video will be displayed on the map (see Configuring the Videogate module), do the following:

1. Go to the settings panel of the **Map** object.



2. From the **Gate** drop-down list, select the required Videogate.
3. Click the **Apply** button.

The Video gateway is now selected.

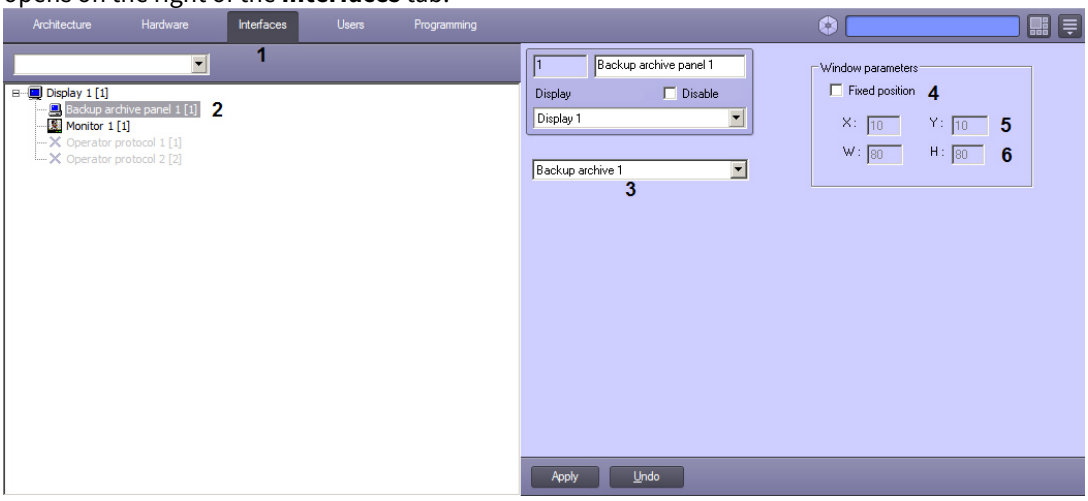
23.4.6 Configuring the Backup archive panel object

The **Backup archive panel** interface object is designed for configuring the Backup archive panel, which is used for starting the backup archiving, changing its parameters and monitoring the backup process.

To configure the main parameters of the **Backup archive panel** object, do the following:

1. Go to the **Interfaces** tab in the **System Settings** dialog box (1)

2. Select the **Backup archive panel** object in the objects tree of the **Interfaces** tab (2). The settings panel for this object opens on the right of the **Interfaces** tab.



3. In the object list, select that **Backup archive** object for which this panel is to be created (3).
4. To set the exact position of the **Backup archive panel** box on the screen, set the **Fixed position** checkbox (4). As a result the **X, Y, W** and **H** fields are available for editing.
5. Specify **X** and **Y** coordinates of the upper left corner of the box, in percentage of the corresponding screen dimensions (5).
6. Specify the width (**W**) and height (**H**) of the window, in percentage of the corresponding dimensions of the screen (6).
7. Click the **Apply** button (7).

The **Backup archive panel** interface object is now configured.

Copying video sequence to the Backup archive
Configuring backup archiving

23.4.7 Configuring the Operator protocol interface object

The **Operator protocol** object is for processing events from security system objects and searching in an event archive.

The **Operator protocol** object performs the following features:

1. Displaying the events registered by the security system objects in the interface box.
2. Assigning a status (type) to a registered event.
3. Adding a comment to an event.
4. Recording events to an archive.
5. Searching events in an archive.
6. Viewing video of an event.
7. Escalating non-processed events to an operator protocol of a higher level.

Configuration procedure for the **Operator protocol** object is as follows:

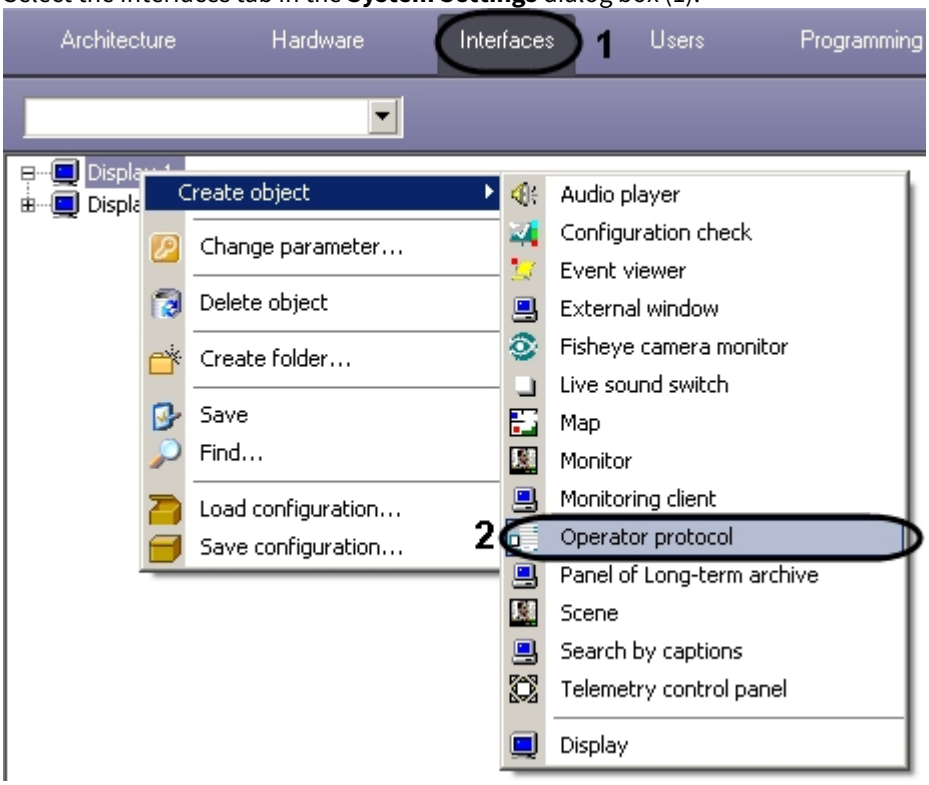
1. Creating the Operator protocol object.
2. Configuring the position of the Operator protocol object.
3. Setting up the event filter for the Operator protocol.
4. Setting the options for handling events in the Operator protocol.
5. Optional: Configuring the checklist.
6. Optional: Configuring the Operator protocol interface.
7. Optional: Connecting external DBs.

Event processing using the Operator protocol

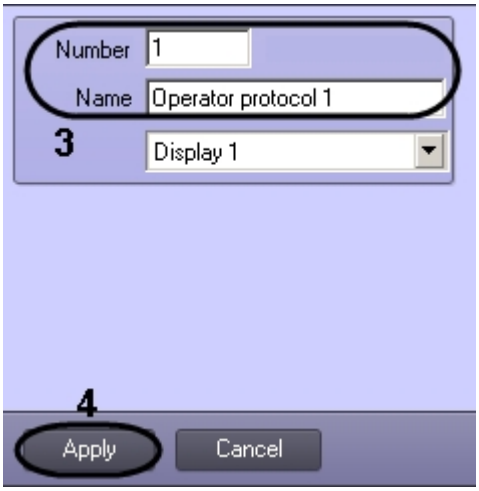
23.4.7.1 Creating the Operator protocol object

To create the **Operator protocol** object, do the following:

1. Select the Interfaces tab in the **System Settings** dialog box (1).



2. In the context menu of the **Display** object on which the created object is to be based, select the **Operator protocol** item in the **Create** object submenu (2).
3. Set the number and name of the created object (3).



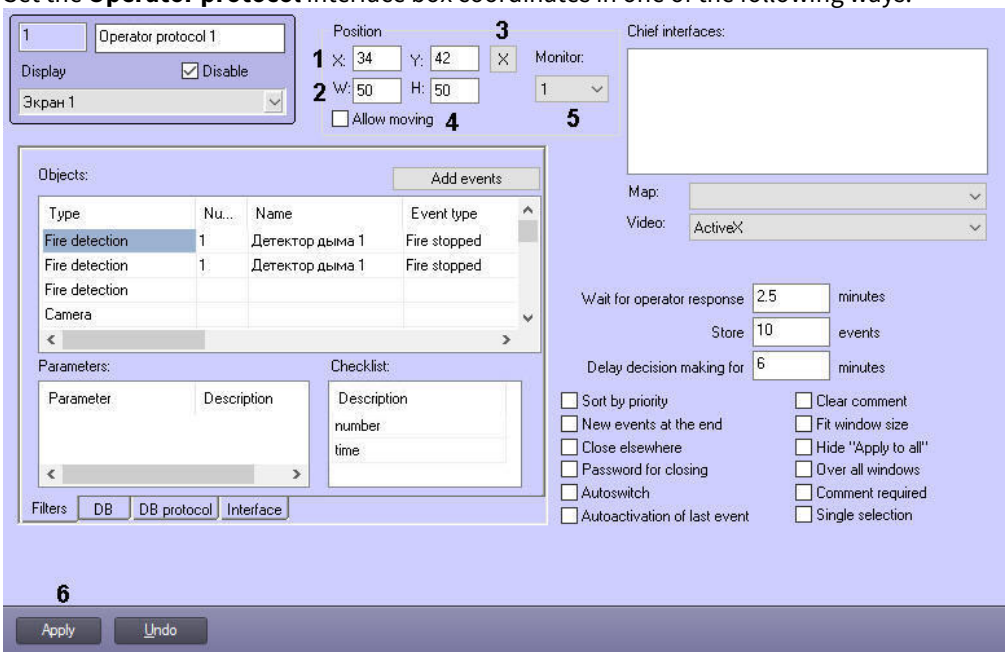
4. To create an object, click the **Apply** button (4).

As a result the settings panel for the Operator protocol is displayed.

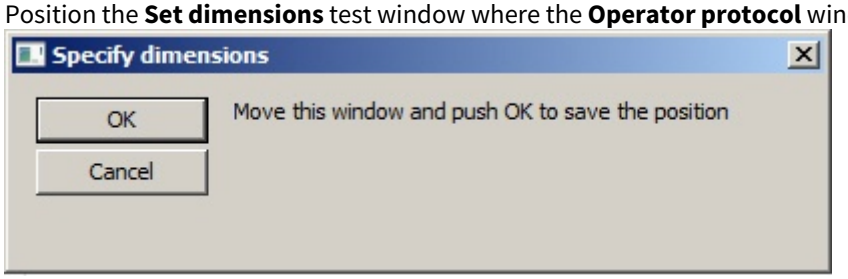
23.4.7.2 Configuring the position of the Operator protocol object

To configure the **Operator protocol** object position, do the following on the settings panel of the object:

1. Set the **Operator protocol** interface box coordinates in one of the following ways.



   a. Manually:
      i. Set the **X** (horizontally indented from screen's left border) and **Y** (vertically indented from screen's upper border) coordinates of the upper left corner of the **Operator protocol** interface box. Coordinates are set as a percentage of the corresponding screen dimensions horizontally and vertically as follows (1).
      ii. Set the dimensions of the **Operator protocol** interface box: window's width «**W**» and window's height «**H**». Dimensions are set as a percentage of the corresponding screen dimensions horizontally and vertically as follows (2).
   b. With a test window:
      i. Click **X** (3).
      ii. Position the **Set dimensions** test window where the **Operator protocol** window should be displayed.



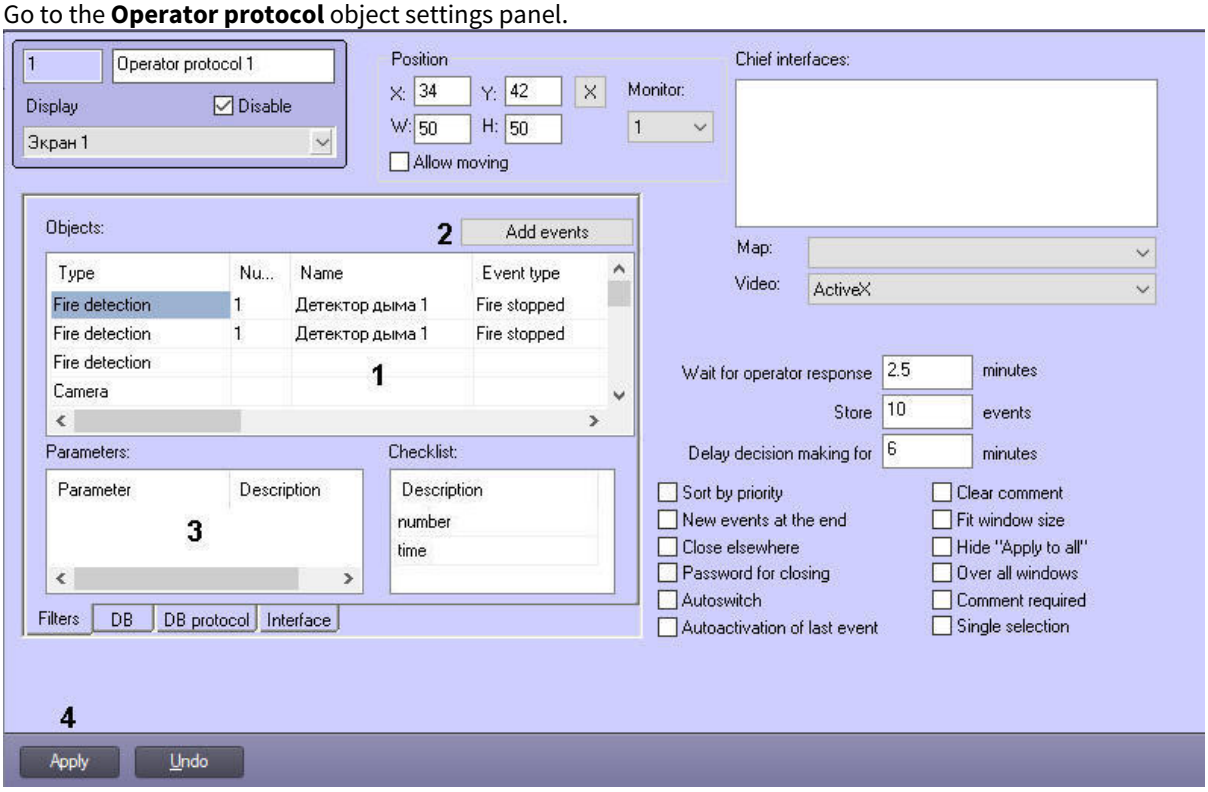
      iii. Click **OK**. As a result, the coordinates in the fields **X, Y, W, H** will be set in accordance with the size and position of the test window.
2. Set the **Allow moving** checkbox if the position and size of the **Operator protocol** interface box are to be changed manually (4).
3. In the **Monitor** dropdown list select the the system ID of a monitor for which the coordinates are set and on which the **Operator protocol** interface box is to be displayed (5).
4. Click **Apply** (6).

The **Operator protocol** object position is now configured.

23.4.7.3 Setting up the event filter for the Operator protocol

To display the events in the Operator Protocol, it is necessary to explicitly specify the objects the events from which are to be received and processed:

1. Go to the **Operator protocol** object settings panel.



2. Specify the objects the events from which are to be received and processed in the Objects table (1):

> **Attention!**
>
> Events are not displayed in the **Operator protocol** if not any objects selected.

   a. Select the object type in the list of the **Type** column.

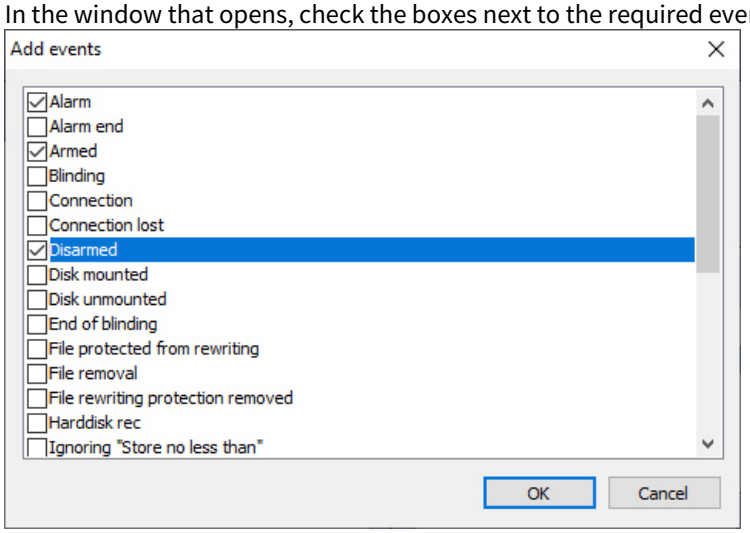
   > **Note.**
   >
   > Only objects for which the "INFORMATION" or "ALARM" value is selected in the **Processing messages** column on the **Events** tab in the ddi.exe utility are available for selection (see The Events tab section).

   b. In the list of the **Number** column select the object id. The object name will be set automatically. If the object number is not specified, then events from all objects of selected type will get to the protocol. After you select the type and number, the **Name** field will be automatically filled with the object name.
   c. In the list of the **Event type** column select events that are to be displayed in the protocol box. If the event type is not specified, then all events registered by the selected object will get to the protocol.
   d. If the processing of an event is to be confirmed with a password, select the **Yes** value in the **Request password** dropdown list. If there is no need to confirm the processing with a password, select the **No** value in this dropdown list.

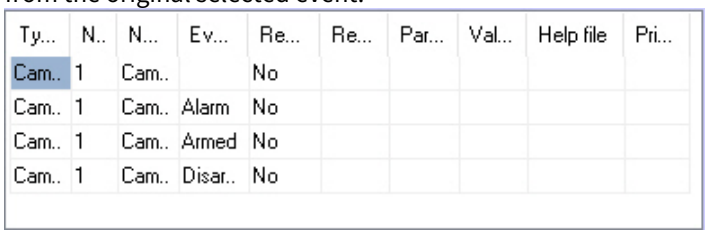
   > **Note.**
   >
   > If the processing of all events is to be confirmed with a password, set the **Password for closing** checkbox checked (see Setting the options for handling events in the Operator protocol).

   e. In the **Region** dropdown list select the **Section** object corresponding to the object.
   f. If an event of specified type is to be received and processed only when its specific parameter has a specific value, then set the parameter and value in the **Parameter** and **Value** fields respectively.
   g. If it is necessary to display the helping guide about the event processing, in the **Help file** field specify the full path to the text file in pdf, doc, docx, txt or other format which contains the required information. The Operator will be able to access the helping guide upon request. The installed application for viewing the files of the corresponding type is required to open the helping guide.

h. In the **Priority** list, select the priority of events of the selected type, which is used when sorting by importance (see Setting the options for handling events in the Operator protocol).
i. If it is necessary to add one or more events from the same object, do the following:
   i. Select a line in which at least the type of object has already been selected.
   ii. Click the **Add events** button (2).
   iii. In the window that opens, check the boxes next to the required events.



   iv. Click **OK**.
   v. As a result, rows corresponding to the selected events are added to the table. All event settings are copied from the original selected event.



Ty...	N..	N...	Ev...	Re...	Re...	Par...	Val...	Help file	Pri...
Cam..	1	Cam..		No					
Cam..	1	Cam..	Alarm	No					
Cam..	1	Cam..	Armed	No					
Cam..	1	Cam..	Disar..	No					

3. Repeat actions described in step 2 for all required objects. To add a line go to the last line of the table and click the ↓ key.

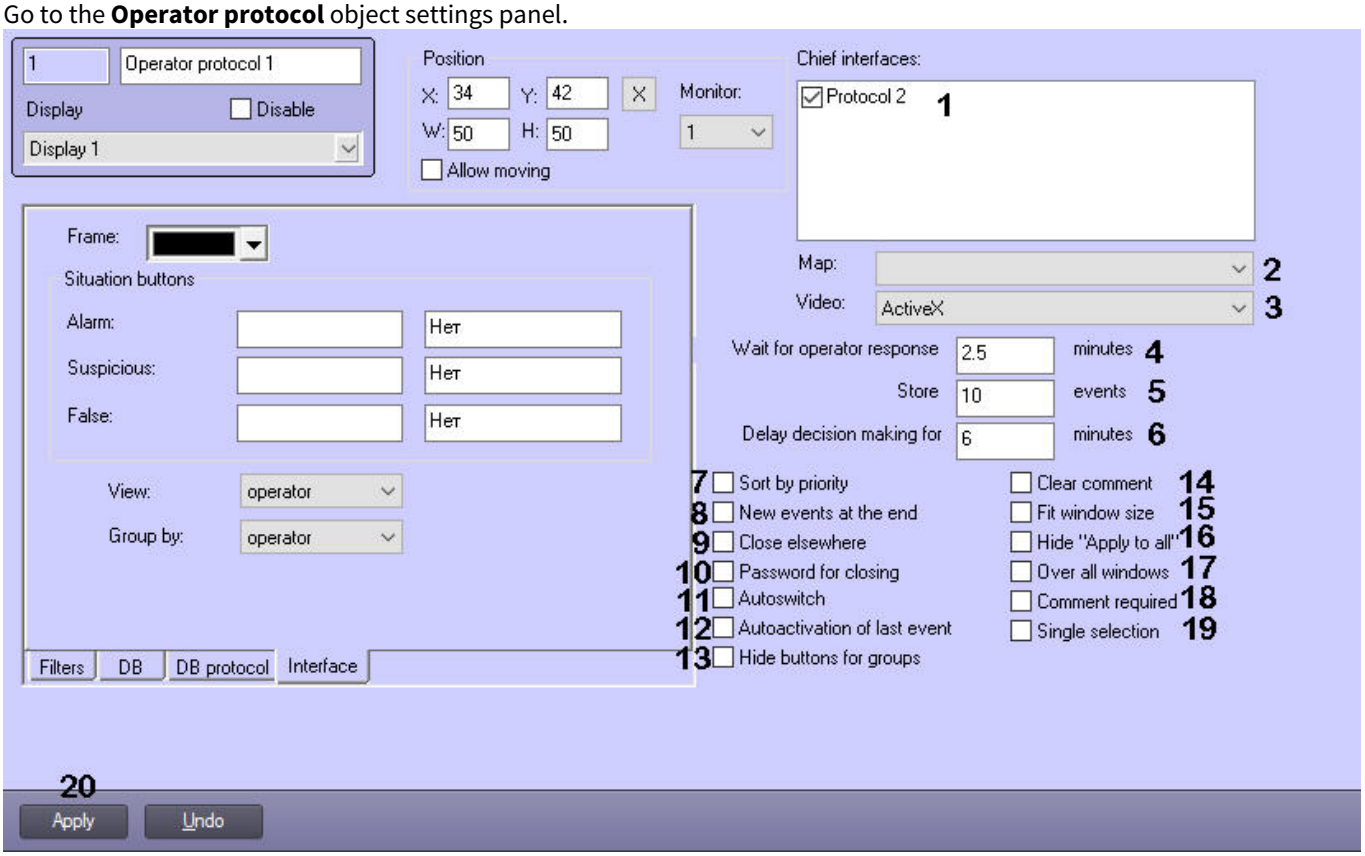
> **Note.**
>
> To add a row to the table, select the last row and press the ↓ button on the keyboard. To remove the lines from the table use the Ctrl + Del key combination.

4. In the **Parameters** table, specify additional settings for an object event. These settings are to be displayed in the **Operator protocol** interface box (3).
   a. In the **Parameter** field, set the parameter name. To specify the parameters sent by the event use a debug box or a ddi file.
   b. In the **Description** field, set a short description of the parameter.
5. Click **Apply** (4).

23.4.7.4 Setting the options for handling events in the Operator protocol

Configure the options for handling events in the Operator protocol as follows:

1. Go to the **Operator protocol** object settings panel.



2. In the **Chief interfaces** list (**1**) set the checkboxes checked next to **Operator protocol** objects to which events are to be sent when the specified time period expires.
3. In the **Map** drop-down list (**2**) select the previously created **Map** object for event monitoring.
4. From the **Video** drop-down list (**3**), select the method of the video displaying from the operator's protocol:
   a. **ActiveX** – archive and live video will open in a separate window.
   b. **Monitor** – archive and live video will open on the selected Video Surveillance Monitor. In this case the Video Surveillance Monitor will operate in **Active camera** mode regardless of the corresponding setting – see Configuring the display mode of camera windows.
5. In the **Wait for the operator response___minutes** field (**4**) specify the time period at the end of which an event will have the **Non-processed** event type or it will be escalated. Time period is set in minutes – non-integer values can be set (use the decimal point to separate integer and fractional parts). For instance, specify 0.5 to set the waiting period for response equal to 30 seconds. The maximum period is 10000 minutes.
6. In the **Store___events** field (**5**), set the maximum of events displayed in the Operator protocol interface box.

> **Important!**
>
> The number of events displayed in the Operator protocol interface box affects the main memory capacity. If 100 non-processed events are displayed in the interface box, then the **Operator protocol** module can use up to 200 Mb of main memory. When the value of the **Store___events** parameter is increased, the main memory capacity is increased too.

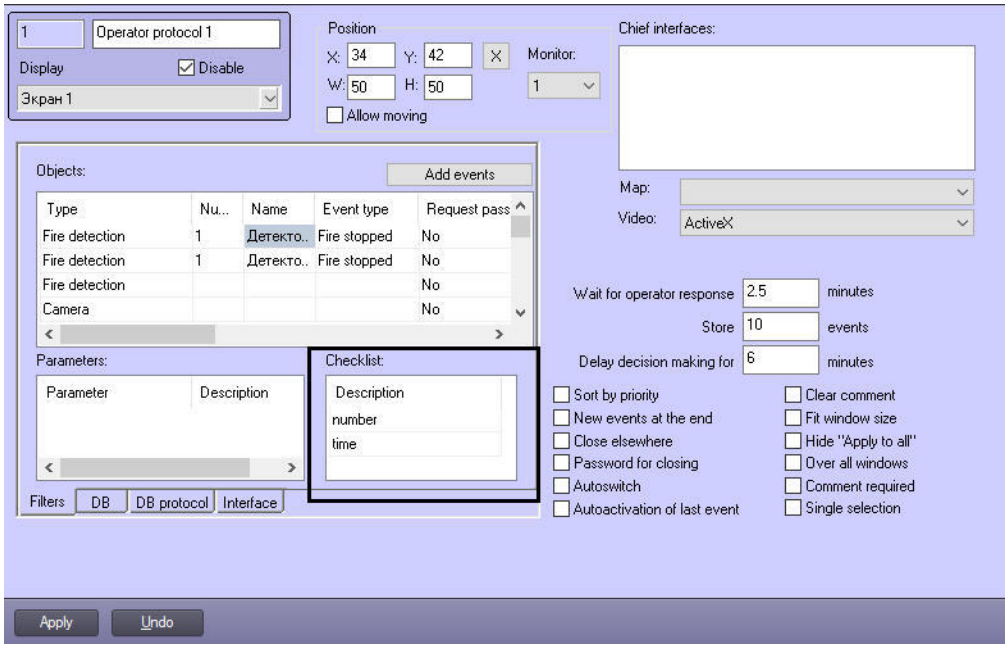
7. If the decision on the event classification is to be delayed once for the operator, then in the **Delay decision making for___minutes** field (**6**) specify the time period (in minutes) for which the event procession will be delayed. The time period is specified in minutes, though non-integer values can be set - in this case the dot is used to separate integer and non-integer parts of the number. For instance, to delay decision making for 15 seconds 0.25 is to be specified in the field.
8. If events are to be sorted by priority (not by time they are received) in the Operator protocol, then set the **Sort by priority** checkbox (**7**). The descending sorting is performed in this order: Escalated, Alarm, Information and Standard (three latest event parameters can be set in the DDI file - see The Events tab). Inside these groups the sorting is performed according to the priority assigned in the **Objects** table (see 18.h).
9. Set the **New events at the end** checkbox (**8**) if new events are to be added to the end of the list of current events.

10. If after processing an event in one of Operator protocols it is to be removed from other Operator protocols, then set the **Close elsewhere** checkbox (**9**).
11. If the processing of all events is to be confirmed with a password, set the **Password for closing** checkbox (**10**).
12. If autoswitch to the **Current events** tab when a new event occurs is to be performed in the Operator protocol, then set the **Autoswitch** checkbox (**11**).
13. If it is necessary to automatically activate the last received event, set the **Autoactivation of last event** checkbox (**12**).
14. If it is necessary to hide the buttons for handling events when selecting a group of events, set the **Hide buttons for groups** checkbox (**13**).
15. By default, the comment entered by the operator when assigning a type to an event, is not deleted. If it is necessary to clear the comment field after processing the event, set the **Clear comment** checkbox (**14**).
16. By default, the alarms are displayed in the Operator Protocol window as the tiles of a specified size. If it is necessary to enlarge the alarm tile to the entire window size (except for the event control panel), set the **Fit window size** checkbox (**15**).
17. If it is necessary to prohibit the Operator from processing all alarms at once, set the **Hide "Apply to all"** checkbox (**16**).
18. If the Operator protocol interface window is to be displayed on top of all other windows, set the **Over all windows** checkbox (**17**).
19. To prevent the Operator from processing the event without entering a comment, set the **Comment required** checkbox (**18**). The buttons for classifying events (**Alarm situation**, **Suspicious situation**, **False alarm**) will not appear until the **Comment** field is filled if this checkbox is set.
20. If it is necessary to prohibit the Operator from selecting multiple events using the Shift and Ctrl keys, set the **Single selection** checkbox (**19**).
21. Click **Apply** to save changes (**20**).

The options for handling events in the Operator protocol are now configured.

23.4.7.5 Configuring the checklist

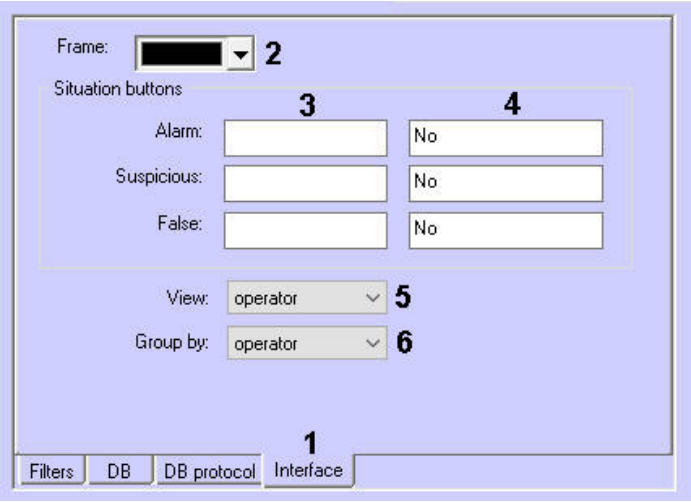
When configuring the Operator protocol, it is possible to set a checklist of the actions that the operator must perform when processing an event. For that, enter the description of the actions that the operator must perform before assigning the status to an event in the **Checklist** table. These actions will be displayed in a special field in the Operator Protocol interface, and the Operator will be able to mark their completion.



23.4.7.6 Configuring the Operator protocol interface

To configure the Operator protocol interface, do the following:

1. Go to the **Interface** tab on the **Operator protocol** object settings panel (**1**).



2. From the **Frame** drop-down list, select the frame color of the active event tile (**2**).
3. If it is necessary to set the custom names for the alarm processing buttons, enter the button names in the left fields of the **Situation buttons** group (**3**).
4. If it is necessary to assign the hot keys for the alarm events processing, set the cursor in the right field of the **Situation buttons** group (**4**) and press the required key combination. It is allowed to combine the Ctrl, Alt and Shift keys with any other keys on the keyboard. For example, the Ctrl+Shift+Alt+A or the Ctrl+A shortcuts are allowed, but the D+A or D+Ins shortcuts are not allowed, etc.
5. From the **View** drop-down list select a way of displaying events on the **Current events** tab (**5**):
    a. **operator**: the operator can choose a full or simple view;
    b. **full**: the events are displayed as cells with screenshots;
    c. **simple**: the events are displayed as strings without screenshots.
6. From the **Group by** drop-down list select a way of grouping events on the **Current events** tab (**6**):
    a. **operator**: the operator can choose the grouping options;
    b. **default**: the event grouping is disabled;
    c. **object**: the events are grouped by object;
    d. **event**: the events are grouped by event type;
    e. **region**: the events are grouped by region.
7. Click the **Apply** button to save the settings.

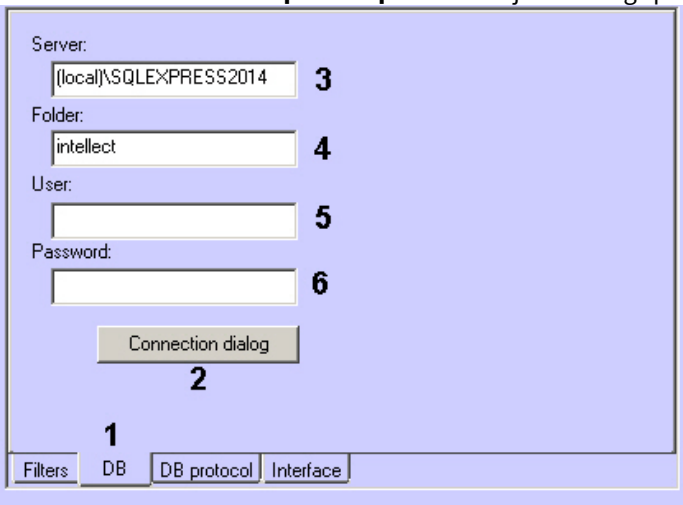
The Operator protocol interface is now configured.

23.4.7.7 Connecting external DBs

23.4.7.7.1 Connecting an external configuration database

If the Operator protocol should use an external database that is different from the one used in Intellect, configure the connection to the database server as follows:

1. Go to the **DB** tab on the **Operator protocol** object settings panel (1).



> **Note.**
>
> Parameters set at INTELLECT ™ software installation are used by default to connect to the database server.

2. Set the connection parameters in one of the following ways:
   a. Click **Connection dialog** and set parameters for connecting to an external database using the standard dialog box – see Configuring the database server connection in a dialog mode (2).
   b. Set connection parameters manually:
      i. In the **Server** field set the name of the database server to connect to (3).

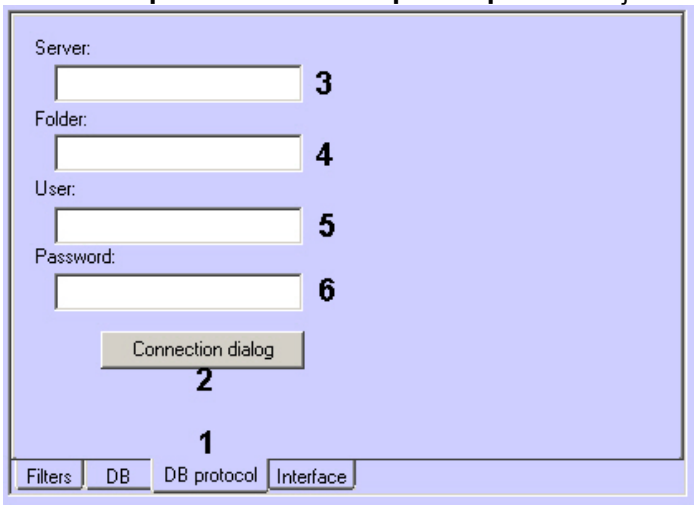
> **Note.**
>
> Working in the distributed configuration it is needed to enter the name of computer without the (local) value where the database is stored. For example, "WS1\SQLEXPRESS", where WS1 is the name of computer on which the database is stored.

      ii. In the **Folder** field set the name of the database to store events (4).
      iii. In the **User** field set the username for the authorization on the database server (5).
      iv. In the **Password** field set the password for the authorization on the database server (6).
3. Click **Apply**.

23.4.7.7.2 Connecting an external Event protocol database

If the Event protocol database is extracted to a separate database (see Extracting event protocol into an individual database), configure the connection to the Event protocol database server as follows:

1. Go to the **DB protocol** tab on the **Operator protocol** object settings panel (1).



2. Set the connection parameters in one of the following ways:
   a. Click **Connection dialog** and set parameters for connecting to an external database using the standard dialog box – see Configuring the database server connection in a dialog mode (2).
   b. Set connection parameters manually:
      i. In the **Server** field set the name of the database server to connect to (3).

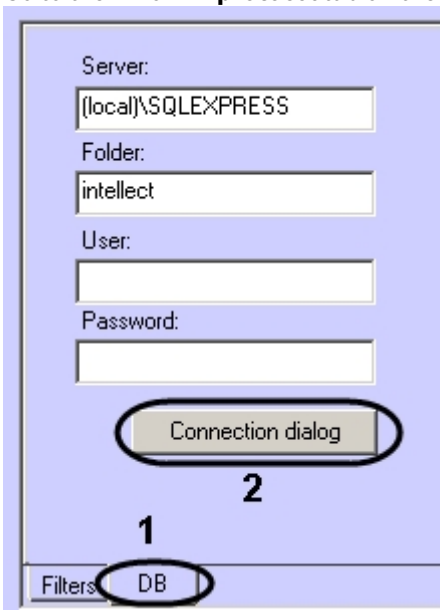
> **Note.**
>
> Working in the distributed configuration it is needed to enter the name of computer without the (local) value where the database is stored. For example, "WS1\SQLEXPRESS", where WS1 is the name of computer on which the database is stored.

      ii. In the **Folder** field set the name of the database to store events (4).
      iii. In the **User** field set the username for the authorization on the database server (5).
      iv. In the **Password** field set the password for the authorization on the database server (6).
3. Click **Apply**.

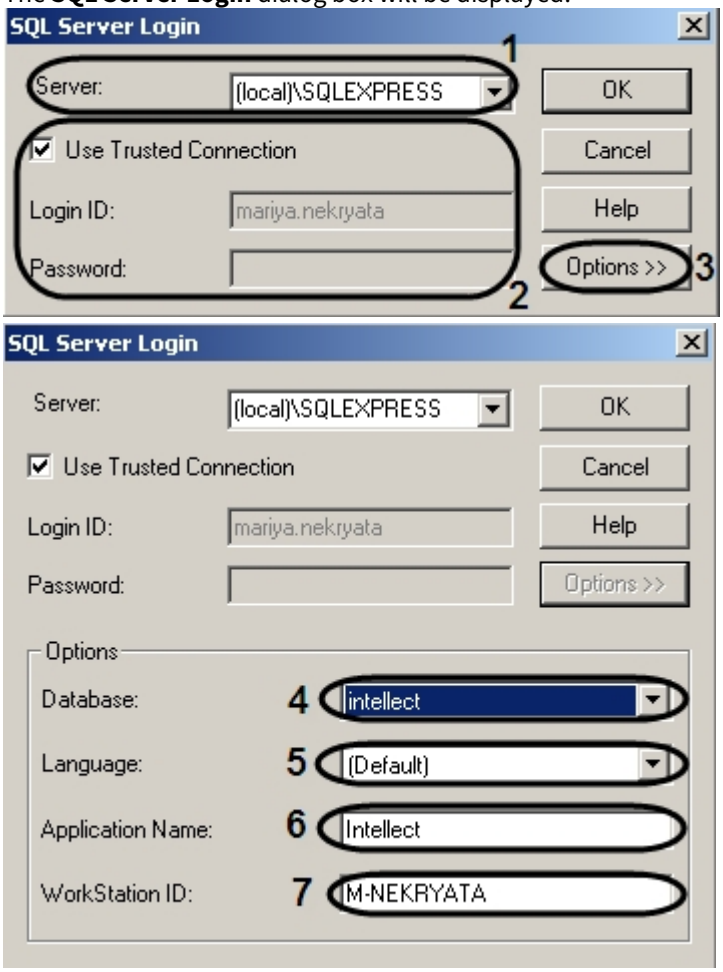
23.4.7.7.3 Configuring the database server connection in a dialog mode

To configure the database server connection in an dialog mode, do the following:

1. Go to the **DB** or **DB protocol** tab on the settings panel of the **Operator protocol** object (1).



2. Click the **Connecting dialog** button (2).
   The **SQL Server Login** dialog box will be displayed.



3. In the **Server** list, specify the SQL Server to connect to (1).

> **Note.**
>
> If the required SQL Server is in the **Server** list, then there is no need to further configure the connection.

> **Note.**
>
> Working in the distributed configuration it is needed to enter the name of computer without the (local) value where the database is stored. For example, "WS1\SQLEXPRESS", where WS1 – the name of computer on which the database is stored.

4. If you need to specify the login and password to authorize the SQL Server, then set the **Use Trusted Connection** checkbox unchecked (2). As a result the **Login ID** and **Password** fields are available for editing.

> **Note.**
>
> If the **Use Trusted Connection** checkbox is set, then the authorization on the SQL Server will be provided using Windows account information.

5. To set advanced connection options, click the **Options >>** button (3).
   a. In the **Database** drop-down list, select the database to store events (4).
   b. In the **Language** list, select the language of SQL system messages 5).
   c. In the **Application Name** field, set the application name (Intellect by default) (6).
      In the **WorkStation ID** field, set the computer name (WindowsID by default) (7).
6. To save the settings, click **OK.**

Note.

To view the supplemental information about the **SQL Server Login** dialog box, click the Help button.

The database server connection is now configured.

23.4.8 Configuring the Event Viewer interface object

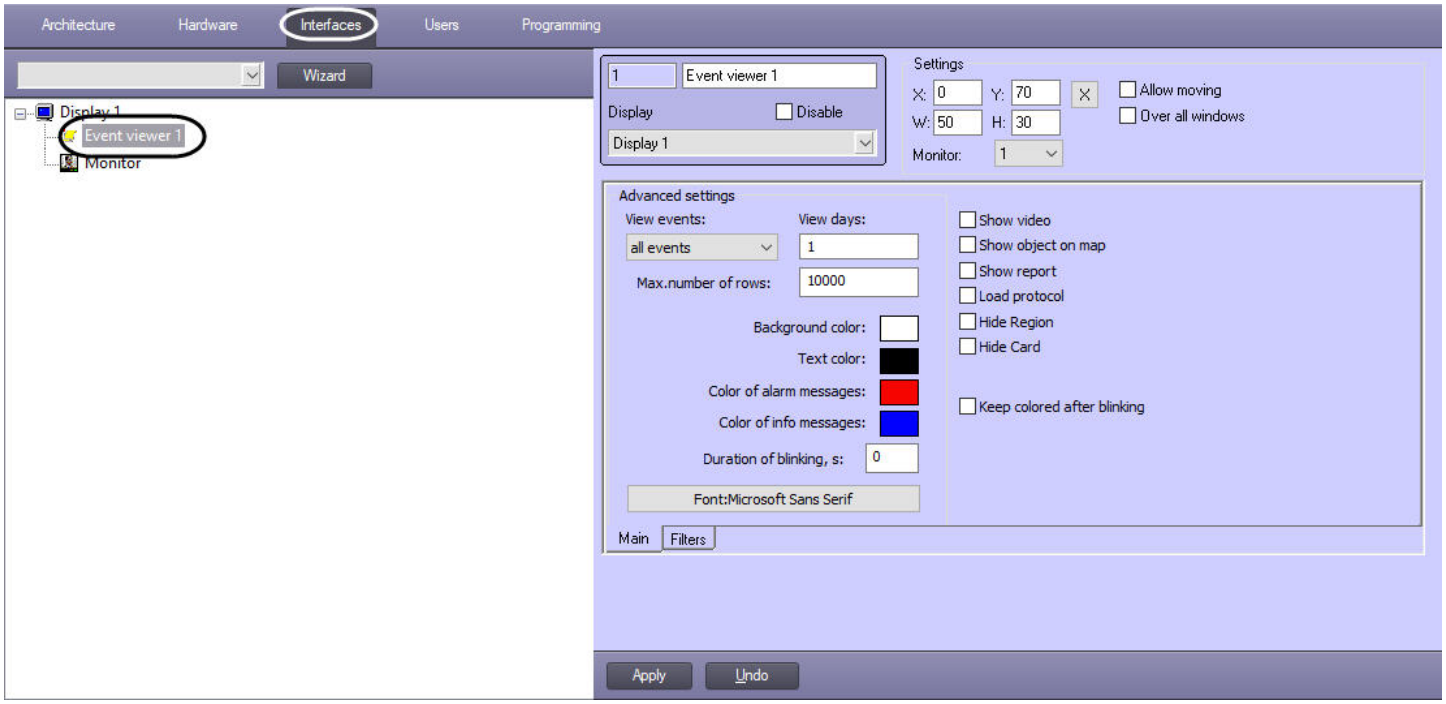
23.4.8.1 Order of configuring the Event Viewer interface object

The **Event viewer** object is a child-object of the **Display** interface object and is used for displaying information about registered events in the interface box. Events may be registered both locally and on the computers in the distributed system.

Note.

Events transmission among computers is set in the Architecture tab in the Systems settings dialog box (see the Configuring the interaction of distributed system components section).

The **Event viewer** interface object is created and configured in the **Interfaces** tab of the **System settings** dialog box.



To configure the **Event viewer** interface object, do the following:

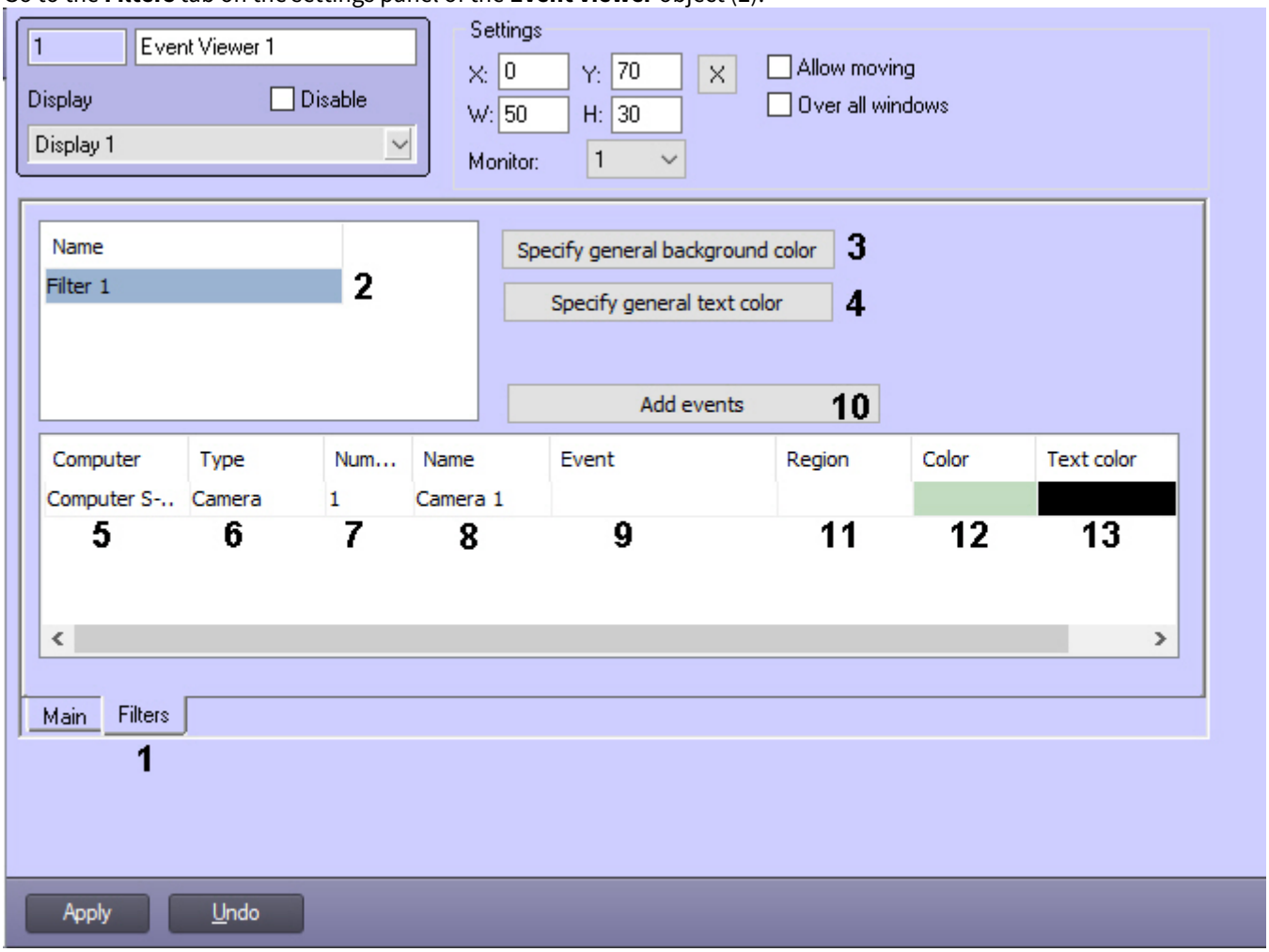
1. Choose the events, information on which should be logged to the **Events viewer** interface object in case of its registration in the system (see Configuring event filters for displaying in the Event viewer).
2. Set the parameters of the event viewer (see Event viewer parameters).
3. Configure the displaying of the **Event viewer** interface box (see Parameters of displaying the Event Viewer interface box).

Event control via Event viewer

23.4.8.2 Configuring event filters for displaying in the Event viewer

To select the events that are to be logged in the **Events viewer** interface object, do the following:

1. Go to the **Filters** tab on the settings panel of the **Event viewer** object (**1**).



2. Set filter name in the **Name** field (**2**). By default **Filter1**, **Filter2**, etc. are created. To add a new filter select the end line in the list of filters and click the “down” key on the keyboard.

> **Note**
>
> The created filters can be copied by selecting the filter name, using Ctrl + C and Ctrl + V

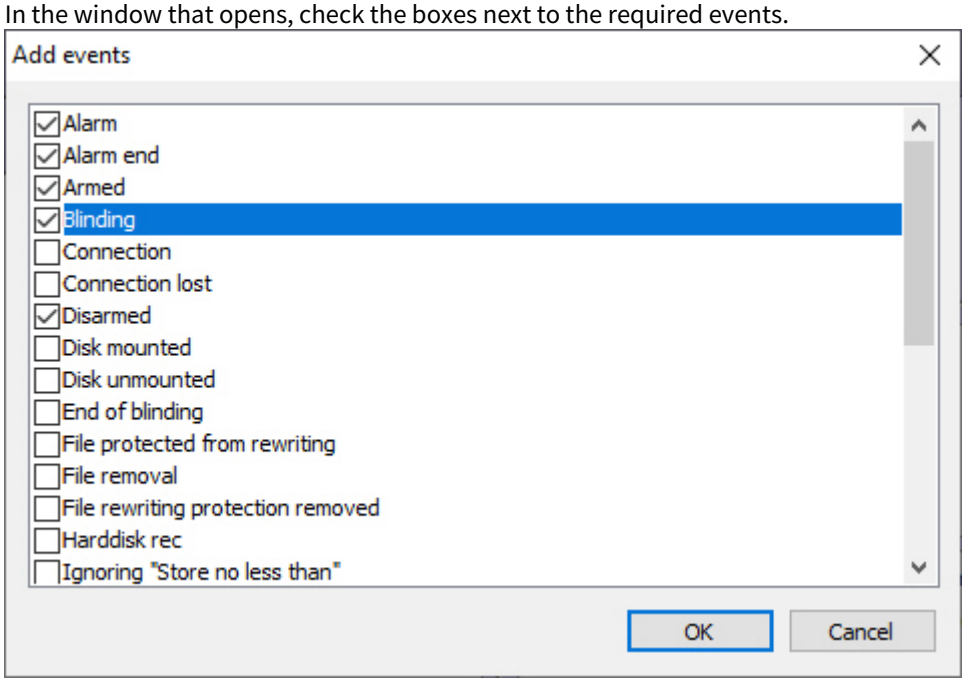
> **Attention!**
>
> A blank filter (i.e. filter with blank columns) should be created in order to display all events for all objects in the system in the Event viewer. All events are also displayed in the Event viewer when there is no filter at all.
> If you delete all previously created filters, an empty filter will be left. When selected, it will display all events.

3. To set the background color that will be used by default for all filter events, click the **Specify general background color** (**3**) button and select the required color in the standard dialog box. The default background color is white.
4. To set the text color that will be used by default for all filter events, click the **Specify general text color** (**4**) button and select the required color in the standard dialog box. The default text color is black.
5. In the **Computer** drop-down list, select the **Computer** object under which the objects included in the filter are to be created (**5**). If filtering by computer is not required or the required object is created not under the Computer object, then the empty value is to be selected in this drop-down list.
6. In the drop-down list of the **Type** column in the **Objects** tab, select the type of an object for which the required event may be logged (**6**). If the field is empty, the Events viewer will display all the events for all the objects in the system.

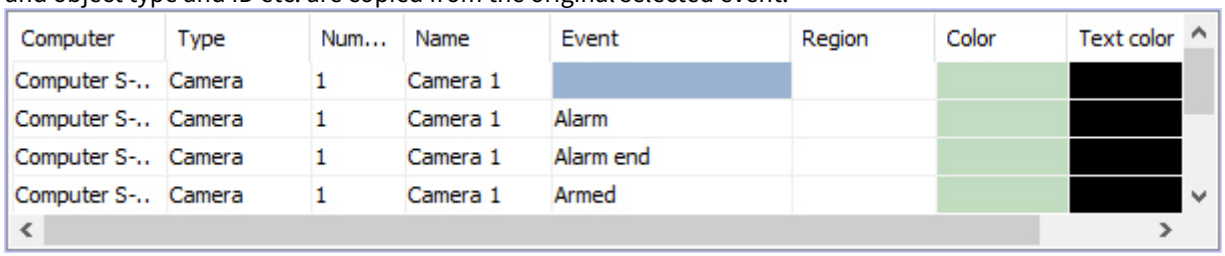
> **Note**

To activate the drop-down list in the **Objects** tab and in the **Areas** list, left-click on the corresponding cell. Detailed description of actions with tabs and lists is in the Object settings panel.

7. In the drop-down list of the Number column in the **Objects** tab, specify the ID for an object of the type selected in step 1 (**7**). If the field is empty, the interface **Events viewer** will log all the events of the specified type.
8. Object name is set automatically on the basis of the values selected in step 1-2 and displayed in the Number column of the **Objects** tab (**8**). You can not edit the **Name** column.
9. In the drop-down list of the **Event** column of the **Objects** tab, specify the required event for the selected object in step 1-2 (**9**). If the field is empty, the interface **Events viewer** will log all the events of the specified type.
10. To add one or more events from the same object, proceed as follows:
    a. Select a line in which at least the type of object has already been selected.
    b. Click the **Add events** button (**10**).
    c. In the window that opens, check the boxes next to the required events.



    d. Click the **OK** button.
    e. As a result, rows corresponding to the selected events are added to the table. All event settings including colors and object type and ID etc. are copied from the original selected event.



11. In the **Areas** table select the region which object's events are to be logged (**11**). If the objects are identified (see step 7) or no region is set, then the events are logged without object's belonging to any region.
12. In the **Color** drop-down list select the background color for the message about event in the Event viewer (**12**).
13. In the **Text color** drop-down list select the text color of the event message in the Event Viewer (**13**).
14. Repeat steps 3-9 for all required objects and sections in the filter.
15. Repeat steps 2-10 for all required objects and regions.
16. Click the **Apply** button to save all the changes.

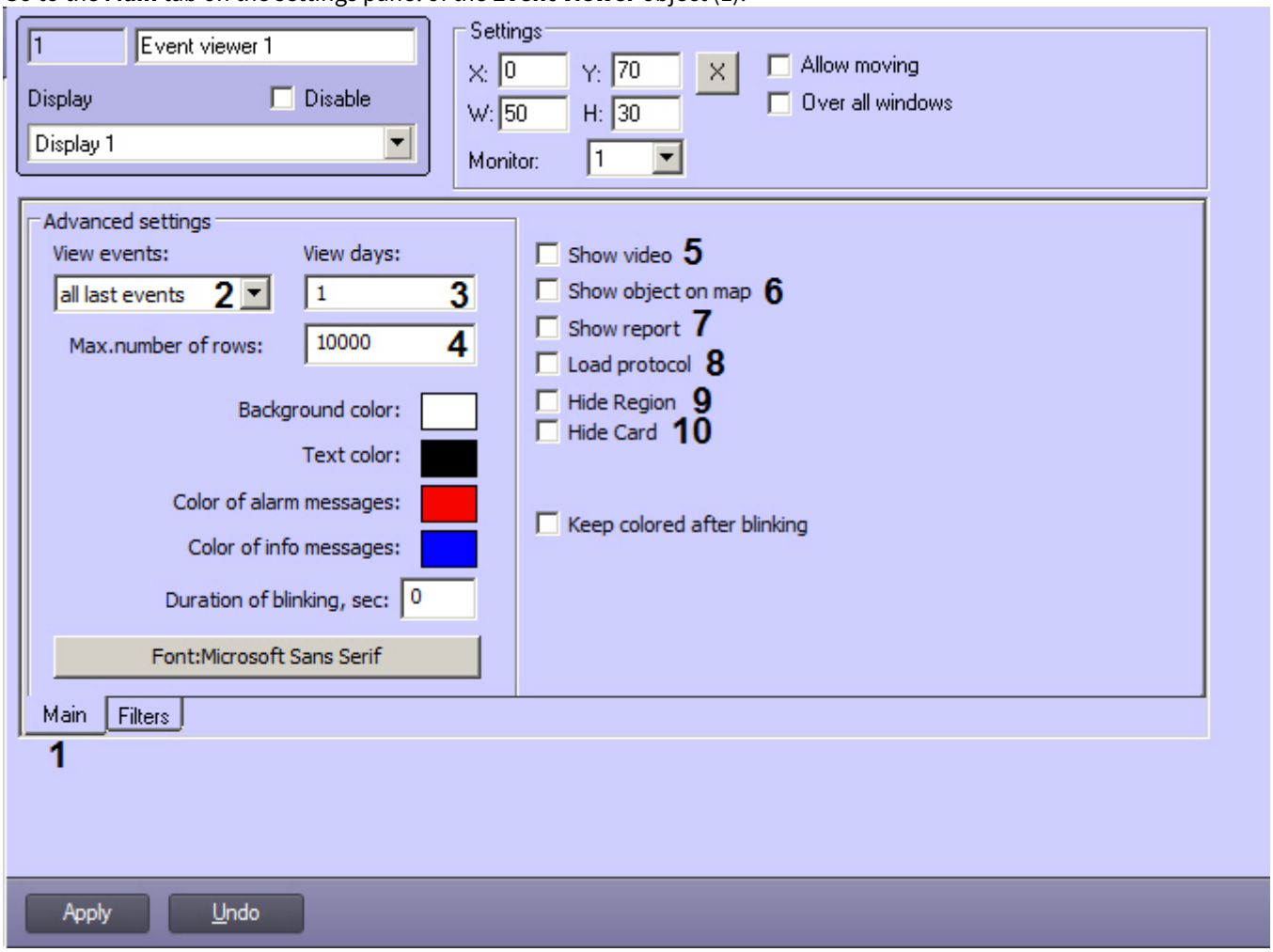
Events for logging to the **Events viewer** interface object are now selected.

Event control via Event viewer

23.4.8.3 Event viewer parameters

To set the event viewer parameters, do the following:

1. Go to the **Main** tab on the settings panel of the **Event viewer** object (1).



2. If it is necessary to display only one latest event or all latest events in **Event Viewer** interface box, select **One latest** or **All events** in the **View events:** list (2).

> **Note**
>
> If **All events** item is selected and the event is repeated for the object, there is time changing of present event recording and a new recording line is not created.

> **Note**
>
> By default all events are displayed in the **Event Viewer** interface box.

3. In the **View days** text field specify the time period (in days) over which the events are to be displayed in the Event Viewer interface window if there are more events than the number set in the **Max.number of rows** field (3). If there are less events than set in the **Max.number of rows** field, in the Event Viewer, events will be displayed for all days, regardless of this setting. And the events are excluded from being displayed until their number becomes equal to the **Max.number of rows** value. Verification of the fulfillment of this condition and exclusion of events from being displayed happens every 50 events.
4. In the **Max.number of rows** field, enter the maximum number of events to be displayed in the Event Viewer (4). The default value is 10,000, the maximum possible value is 50,000. The value in this field should be increased if you notice that events of objects that rarely generate events are deleted from the log when switching the filters.

5. Set the **Show video** checkbox to enable viewing the video recordings from the **Event viewer** interface box (5). Viewing the events of the **Record to disk** type of the **Camera** objects is only possible.
6. Set the **Show object on map** checkbox to enable viewing the logged events on the map (6).
7. Set the **Show report** checkbox to enable creating a printed report about events in the **Events viewer** interface box for a specified time period (7).
8. If the last 1000 logged events are to be displayed in the Event Viewer interface box, then set the **Load protocol** checkbox (8).

   Note

   When the **Load protocol** checkbox is set, the events of those objects that have been deleted without giving a source (the name of a deleted object is not displayed) can be displayed. Such operation of the Event Viewer allows the extra control over system objects.

   Note

   A thousand of last events for each object or each object type is loaded when the **Load protocol** checkbox is set if the filter of Event log is configured for displaying events from several objects or several object types.
   For example, if the Event log is receiving events from **Camera 1** object and from all **Macros** objects, a thousand of events from **Camera 1** object and a thousand of events from **Macros** objects will be loaded.
9. Set the **Hide Region** checkbox checked if there is no need to show the **Region** column in the **Event viewer** (9).
10. Set the **Hide Card** checkbox checked if there is no need to show the **Card** column in the **Event viewer** (10). This column is in use for displaying the access card number for events coming from ACS integration modules included in *ACFA Intellect* subsystem. See Card number displaying in the Event viewer window for access events section in Access Manager Module Settings and Operation Guide.

    Note

    The card code is saved in the PROTOCOL table in the param1 field of the event associated with access (for instance, ACCESS_IN).
11. Click the **Apply** button to save all the changes.

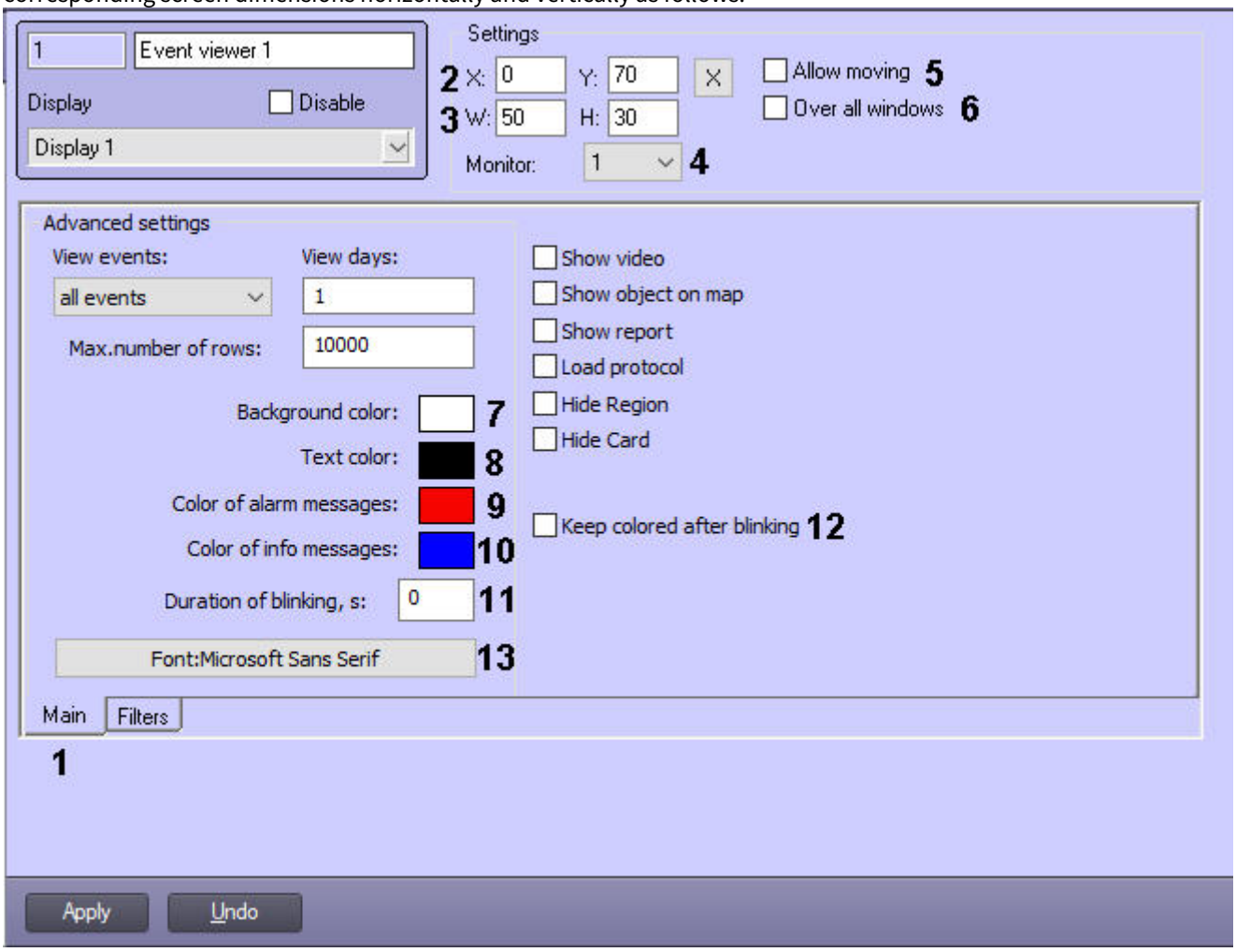
Event viewer parameters are now set.

23.4.8.4 Parameters of displaying the Event Viewer interface box

To configure displaying the **Event Viewer** interface box, do the following:

1. Go to the **Main** tab on the settings panel of the **Event Viewer** object (**1**).
2. Set the **X** (horizontally indented from screen's left border) and **Y** (vertically indented from screen's upper border) coordinates of the upper left corner of the Event Viewer interface box (**2**). Coordinates are set as a percentage of the

corresponding screen dimensions horizontally and vertically as follows.



3. Set the dimensions of the **Event Viewer** interface box: window's width «**W**» and window's height «**H**» (**3**). Dimensions are set as a percentage of the corresponding screen dimensions horizontally and vertically as follows.
4. From the **Monitor** drop-down list select the number of monitor for which coordinates are specifying (**4**).
5. By default the position of the **Event Viewer** interface box is fixed. To allow the **Operator** to move the **Event Viewer** by left-clicking on it, set the **Allow moving** checkbox (**5**).
6. If it is necessary for the Event viewer box to be displayed on top of all windows, set the **Over all windows** checkbox (**6**).
7. Set the background color of the Event viewer box (**7**).
8. Set the text color in the Event viewer box (**8**).
9. Set the color of alarm message rows in the **Event Viewer** interface box (**9**). For this, double-click upon the **Color of alarm messages** field. Standard Windows dialog box will open, select the required color and click **OK.**

> **Note**
>
> To apply the setting, the **Duration of blinking**, **sec** (**11**) parameter value must be different from 0.

10. Specify the color of information message rows in the **Event Viewer** interface box (**10**). For this double-click upon the **Color of info messages** field. Standard **Color** Windows dialog box will open, select the required color and click **OK.**

> **Note**
>
> To apply the setting, the **Duration of blinking**, **sec** (**11**) parameter value must be different from 0.

11. Enter the duration of blinking for alarm messages in seconds in the **Duration of blinking**, **sec** field of the **Event Viewer** interface box (**11**). The blink rate is 2 seconds, the blink duration is 1 second. To ensure the blinking, it is recommended to set the parameter value to at least 2.

12. By default, when the alarm message has finished blinking, it is no longer highlighted by the alarm message color in the Event viewer box; it becomes highlighted by the color specified in the filter (see Configuring event filters for displaying in the Event viewer). To continue highlighting the message by the alarm message color after the blinking stops, set the **Keep colored after blinking** checkbox (**12**).
13. Set the font of messages displayed in the **Event Viewer** interface box. For this click the **Font:**<current font> button (**13**). Standard **Font** Windows dialog box will open, set the font and click **OK.**
14. Click the **Apply** button to save all the changes.

Parameters of displaying the **Event Viewer** interface box are now set.

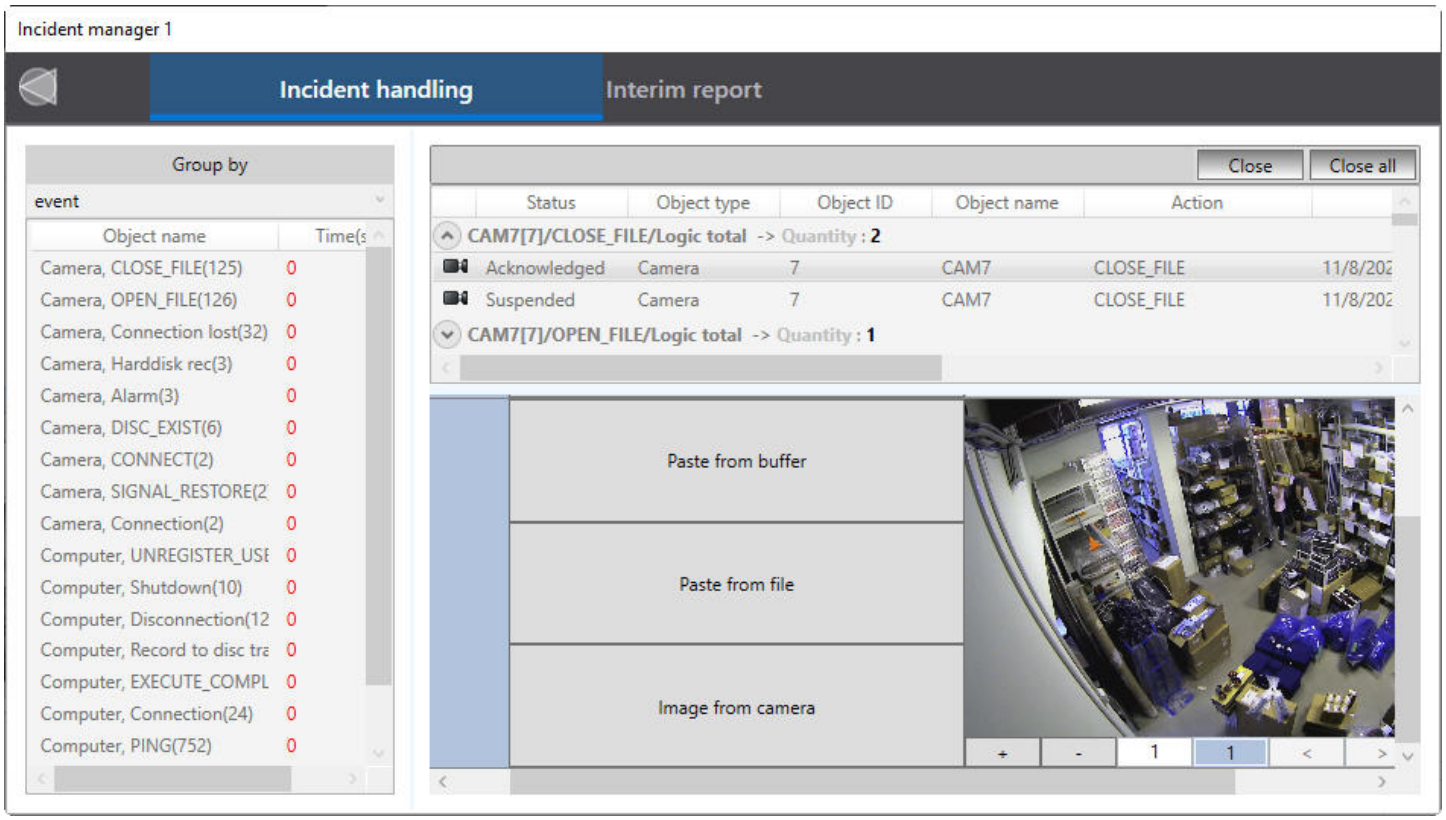
> **Note**
>
> The display of the **Event Viewer** icon on the Windows taskbar is set by the **ShowInTaskbar** registry key (see Intellect Enterprise base version).

23.4.9 Configuring the Incident manager interface object

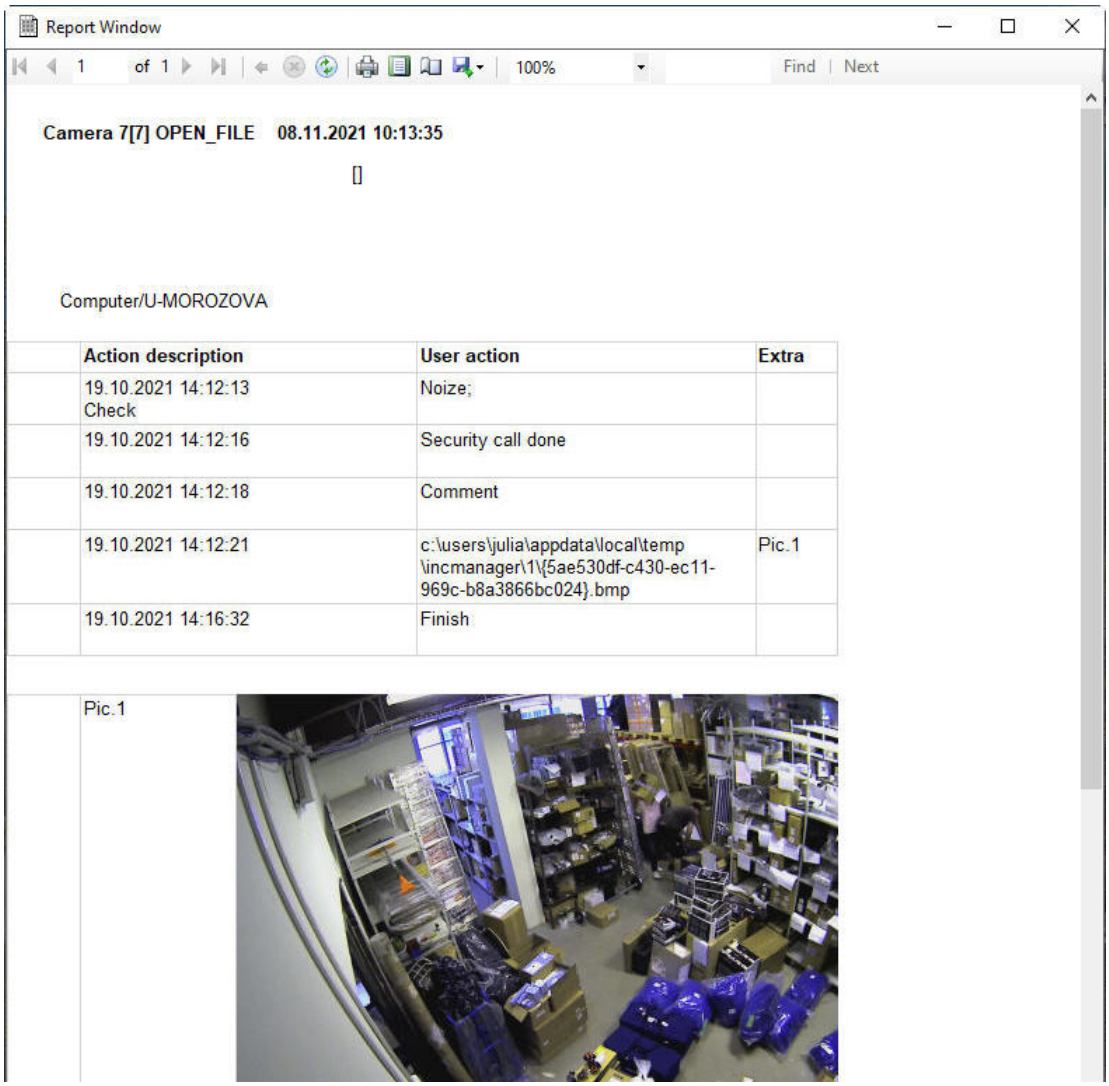
The **Incident manager** interface module is intended for:

- event handling by the operator according to a pre-configured script;
- automatic execution of macros that are triggered by certain operator actions;
- generating a report on the event and operator's actions.

Example of displaying the Incident manager interface:



Example of displaying the report:



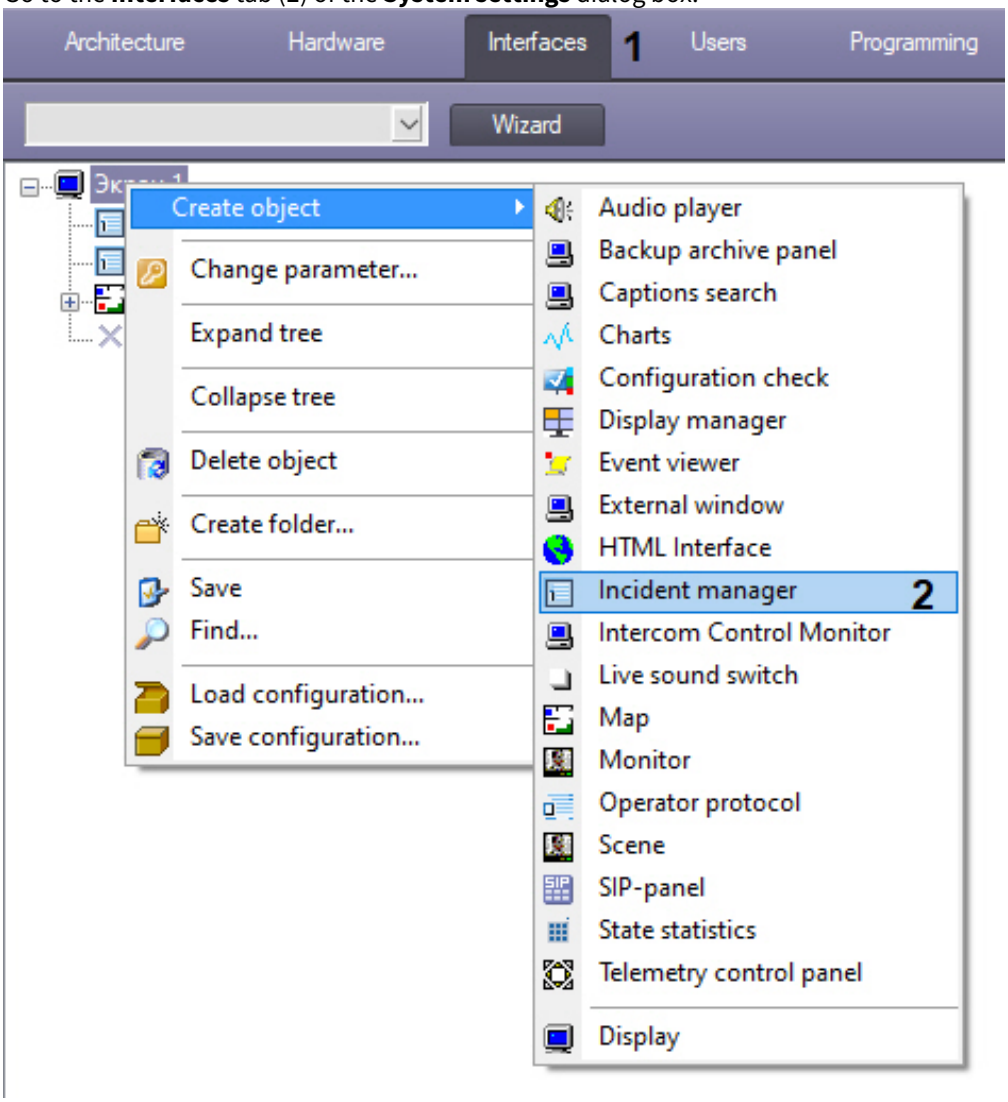
The **Incident manager** interface module is configured in the following order:

1. Creating the Incident manager object.
2. Configuring the Incident manager position on the screen.
3. Configuring the main parameters of the Incident manager.
4. Configuring the events filtering and grouping in Incident manager.
5. Configuring user rights in Incident manager.

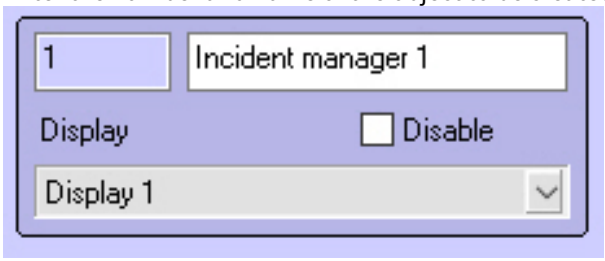
23.4.9.1 Creating the Incident manager object

To create the **Incident manager** object, do the following:

1. Go to the **Interfaces** tab (**1**) of the **System settings** dialog box.



2. Open the context menu of the **Display** object, on the basis of which the object should be created, in the **Create object** submenu select the **Incident manager** item (**2**).
3. Enter the number and name of the object to be created.



4. Click the **Apply** button.

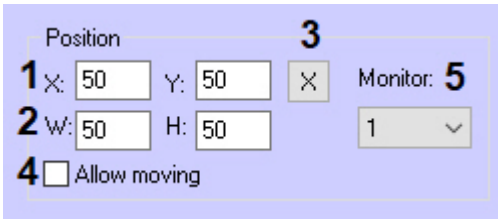
As a result, the settings panel for the **Incident manager** object will be displayed.

23.4.9.2 Configuring the Incident manager position on the screen

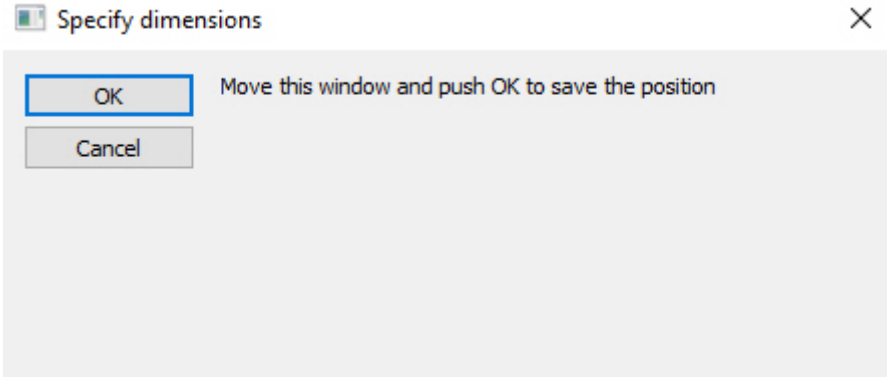
To configure the **Incident manager** position on the screen, do the following:

1. Go to the settings panel of the **Incident manager** object.

2. Set the window coordinates in one of the following ways:



   a. Manually:
      i. Enter the coordinates of the upper left corner: **X** field (horizontal offset from the left border of the screen) and **Y** field (vertical offset from the upper border of the screen). Coordinates are expressed as a percentage of the horizontal and vertical screen sizes, respectively (**1**).
      ii. Specify the window dimensions: **W** field (window width) and **H** field (window height). Dimensions are expressed as a percentage of the horizontal and vertical screen sizes, respectively (**2**).
   b. Using a test window:
      i. Click the **X** button (**3**).
      ii. Place the opened **Specify dimensions** test window where the **Incident manager** window should be displayed.



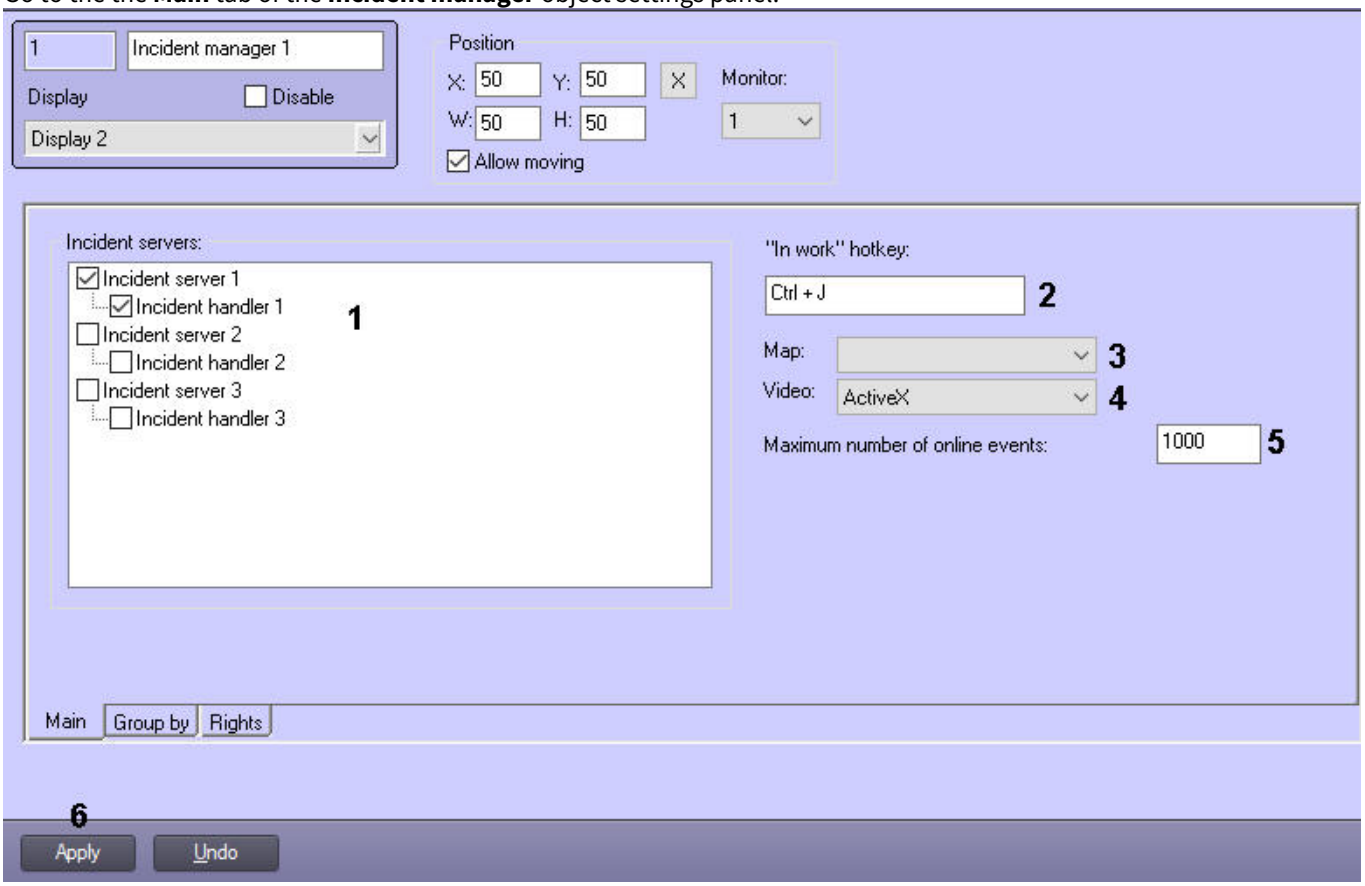
      iii. Click the **OK** button. As a result, the coordinates in the **X**, **Y**, **W**, **H** fields will be set in accordance with the size and position of the test window.
3. Set the **Allow moving** checkbox to manually change the position and size of the **Incident manager** (**4**).
4. From the **Monitor** drop-down list, select the number of the monitor in the system for which these coordinates are set and on which the **Incident manager** should be displayed (**5**).
5. Click the **Apply** button.

Configuring the **Incident manager** position on the screen is now complete.

23.4.9.3 Configuring the main parameters of the Incident manager

Configure the main parameters of the Incident manager as follows:

1. Go to the the **Main** tab of the **Incident manager** object settings panel.



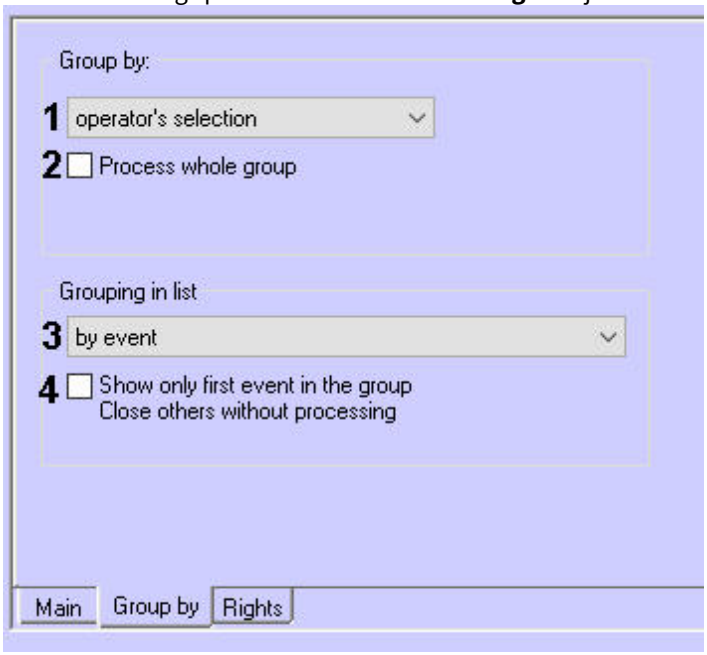
2. In the **Incident servers** window, set the checkboxes next to those **Incident server** and **Incident handler** objects, the events and processing logic from which will be displayed in the interface (**1**) (see Configuring Incident server and Incident handler).
3. If necessary, set a hotkey, using which the operator can start processing the event. To do this, place the mouse cursor in the **"In work" hotkey** field (**2**) and press the required key or key combination on the keyboard.
4. From the **Map** drop-down list (**3**), select the previously created Map object, which will be linked with the Incident manager. The operator can make the object with the event be highlighted on the map.
5. From the **Video** drop-down list (**4**), select a video display mode:
   a. **ActiveX** - archive and live video will open in a separate window.
   b. **Monitor** - archive and live video will open on the selected Surveillance Monitor. In this case, the Surveillance Monitor will operate in the **Active camera** mode, regardless of the corresponding setting - see Configuring the display mode of camera windows.
6. In the **Maximum number of online events** field (**5**), set the maximum number of events that can be simultaneously displayed in the interface. The default is 10 (minimum value), the maximum value is 5000.
7. Click the **Apply** button (**6**).

The the main parameters of the **Incident manager** are configured.

23.4.9.4 Configuring the events grouping in Incident manager

To configure grouping of events in the Incident manager, do the following:

1. Go to the settings panel of the **Incident manager** object and select the **Group by** tab.



2. In the **Group by** drop-down list (**1**), select the event grouping option for the **Incident manager** interface:
   a. **Operator** — the operator can choose the grouping method in the **Incident manager** interface.
   b. **Disabled** — the event grouping is disabled.
   c. **Region** — the events are grouped by region.
   d. **Event** — the events are grouped by event type.
   e. **Object** — the events are grouped by object.
3. Set the **Process whole group** checkbox (**2**), which sets two options:
   a. in case one operator takes an event from a selected group for processing, all events of this group will be blocked for processing by other operators. When the checkbox is set, all events of the selected group, including new incoming events, will be available for processing by only one operator until he finishes processing all the events of the group. Other operators will not be able to take events from this group for processing — when they try to do that, the warning message "Group is blocked" will be displayed.

      Note

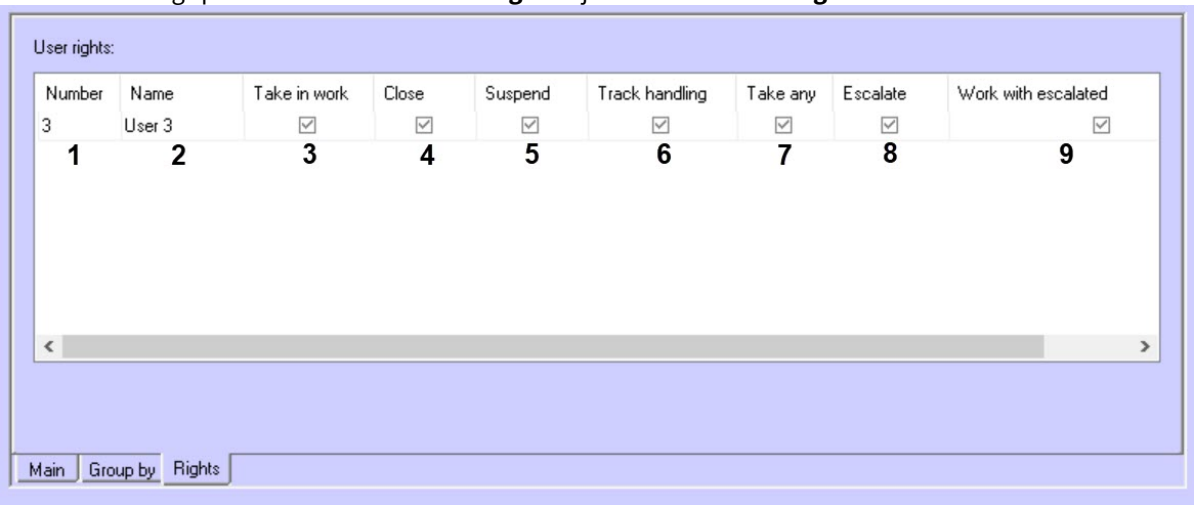
      If the operator took one event from the group for processing and released it without processing, then the events blocked by the group become released for other operators.

   b. when one event of the selected group is escalated, all events of this group will be escalated too.
4. From the **Grouping in list** drop-down list (**3**), select the event grouping option:
   a. **no grouping** — all events will be displayed in the event display window without grouping. If filtering is set, then all events of the selected filter will be displayed.
   b. **by event** — the events will be grouped by object type / object ID / event type / logic ID.
5. Set the **Show only first event in the group. Close others without processing** checkbox (**4**), it is necessary to show only the first event from the group and close the rest of the events without processing after the first event is processed.
6. Click the **Apply** button.

23.4.9.5 Configuring user rights in Incident manager

To configure user rights in Incident manager, do the following:

1. Go to the settings panel of the **Incident manager** object and select the **Rights** tab.



2. In the **Users** table:
   a. From the list in the **Number** column, select the user identification number (**1**). After selecting a number, the **Name** field (**2**) will be automatically filled in with the user's name (usually first or last name).
   b. Set the checkboxes in the required columns next to the user:
      i. **Take in work**, if it is necessary that the user can process the event (**3**);
      ii. **Close**, if it is necessary that the user can close the event without processing (**4**);
      iii. **Suspend**, if it is necessary that the user can suspend the processing of the event (**5**);
      iv. **Track handling**, if it is necessary that the user can see the processing steps of the event taken by other users (**6**);
      v. **Take any**, if it is necessary that the user can process the events with any status (**7**);
      vi. **Escalate**, if it is necessary that the user can escalate the event (i.e., pass it to another user for processing) (**8**);
      vii. **Work with escalated**, if it is necessary that the user can process the event escalated (passed) from another user (**9**).
3. Repeat step 2 for all required users.

> **Note**
>
> To add a row to the table, select the last row and press the ↓ button on the keyboard. To delete rows from the table, use the Ctrl + Del key combination.

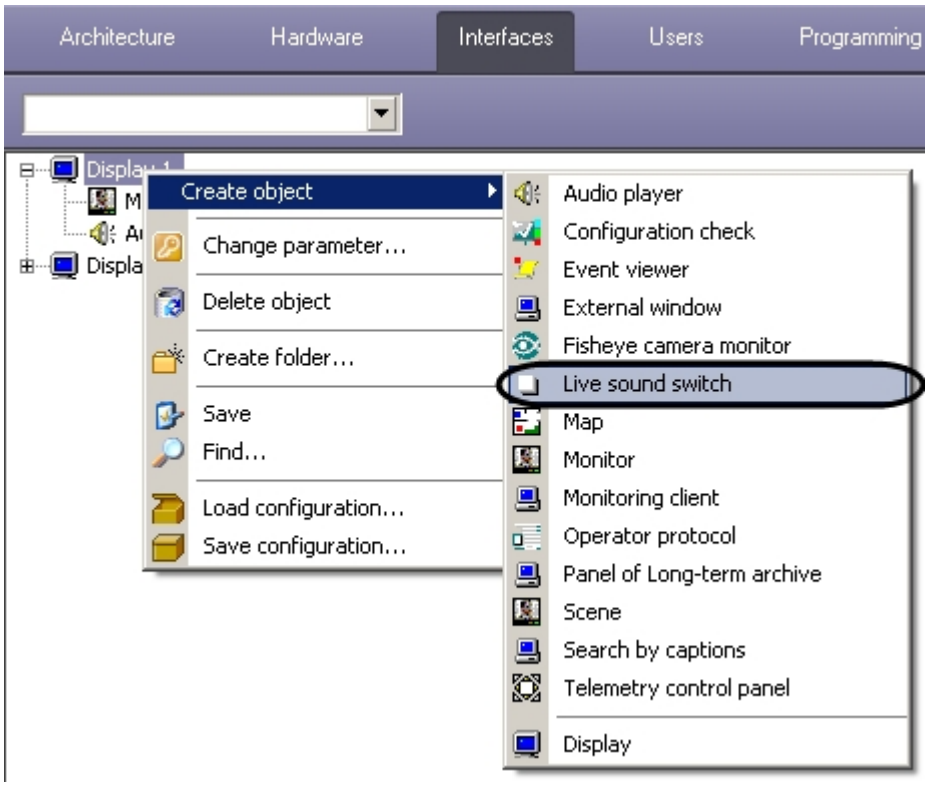
4. Click the **Apply** button.

23.4.10 Setting up the sound switch

You can direct audio signal that arrives from any sound source (microphone) to any sound detector (speaker) in order to play it back in INTELLECT™ software. The **Live sound switch** object is used for that.

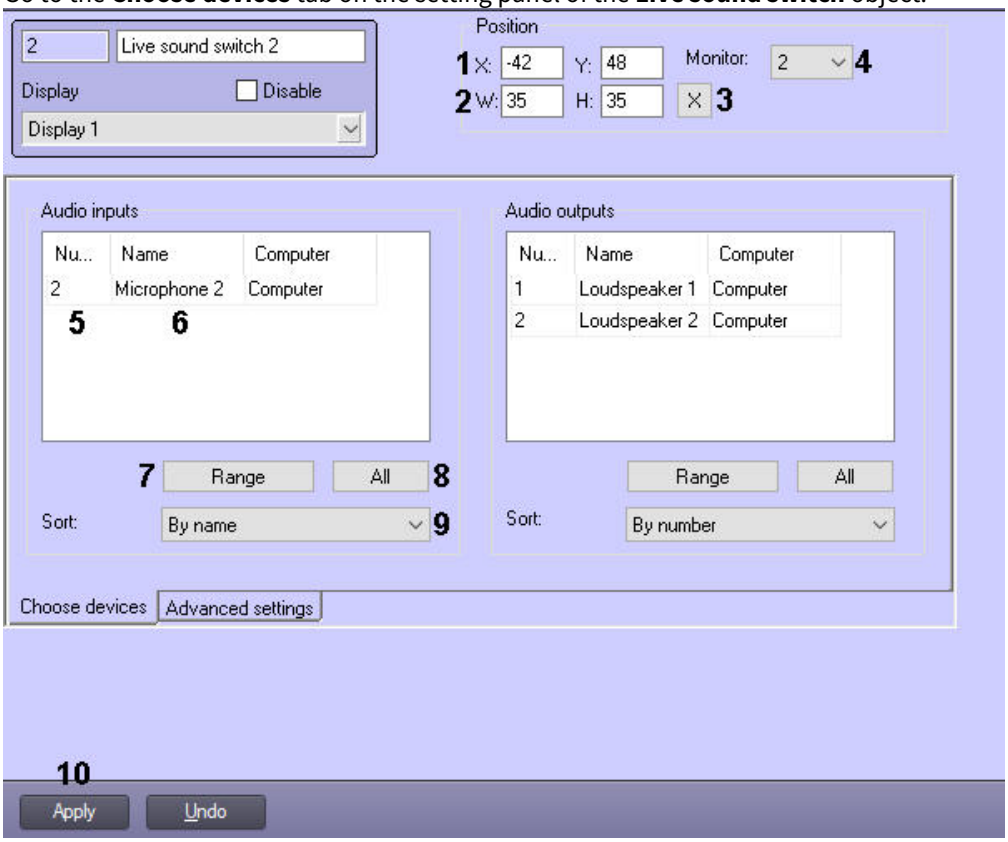
23.4.10.1 Creating and configuring the Live sound switch object

The **Live sound switch** object is created on the basis of **Display** object in **Interfaces** tab of **System setting** dialog box.



To set up the **Live sound switch** object, do the following:

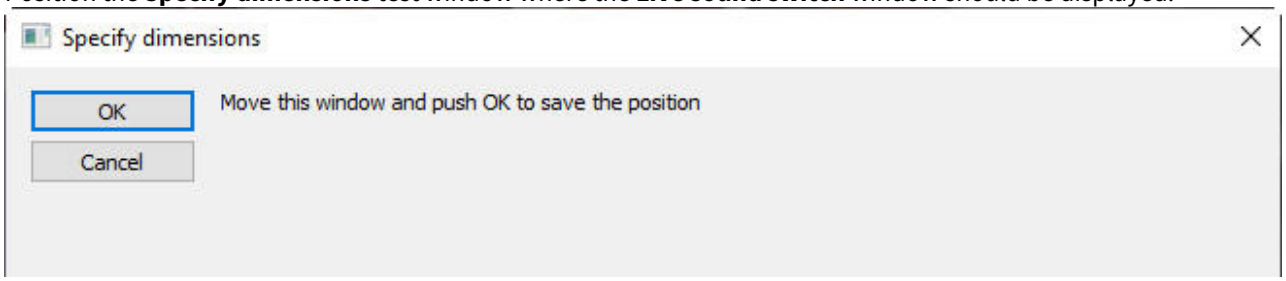
1. Go to the **Choose devices** tab on the setting panel of the **Live sound switch** object.



2. Adjust the position of the **Live sound switch** object dialog box in one of the following ways:
    a. Manually:

i. Enter the coordinates of the upper left corner: the **X** (horizontal indent from the left screen border) and **Y** (vertical indent from the top screen border) fields (**1**). The coordinates are expressed as a percentage relative to the screen size horizontally and vertically, respectively.
ii. Enter the dialog box dimensions: the **W** (window width) and **H** (window height) fields (**2**). The dimensions are expressed as a percentage relative to the screen size horizontally and vertically, respectively.

b. With a test window:
c. Click the **X** button (**3**).
d. Position the **Specify dimensions** test window where the **Live sound switch** window should be displayed.

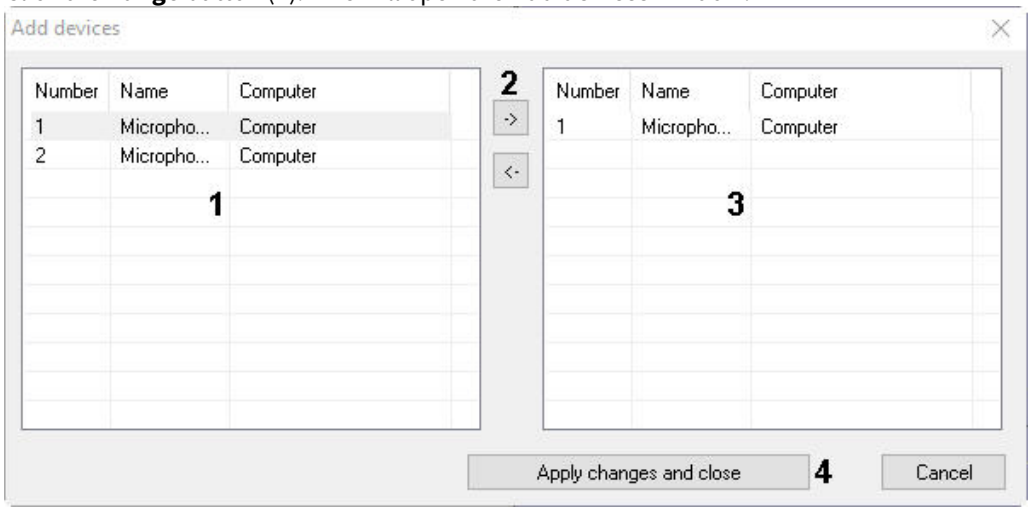


e. Click **OK**. As a result, the coordinates in the fields **X**, **Y**, **W**, **H** will be set in accordance with the size and position of the test window.

3. From the **Monitor** drop-down list (**4**), select the number of the monitor in the system for which the coordinates are set and on which the **Live sound switch** should be displayed.
4. In the **Audio inputs** field, add the audio sources in one of the following ways:
   a. One by one:
      i. From the drop-down list in the **Number** column (**5**), select the number of the **Microphone** object, or in the **Name** column (**6**), select the name of the **Microphone** object. The rest of the columns will be filled in automatically.
      ii. Repeat step i for all required **Microphone** objects.

> **Note**
>
> To add a new row to the table, press the "down" button on the keyboard. To delete a row, select it and press Ctrl+Del.

   b. Several microphones at once:
      i. Click the **Range** button (**7**). This will open the **Add devices** window.



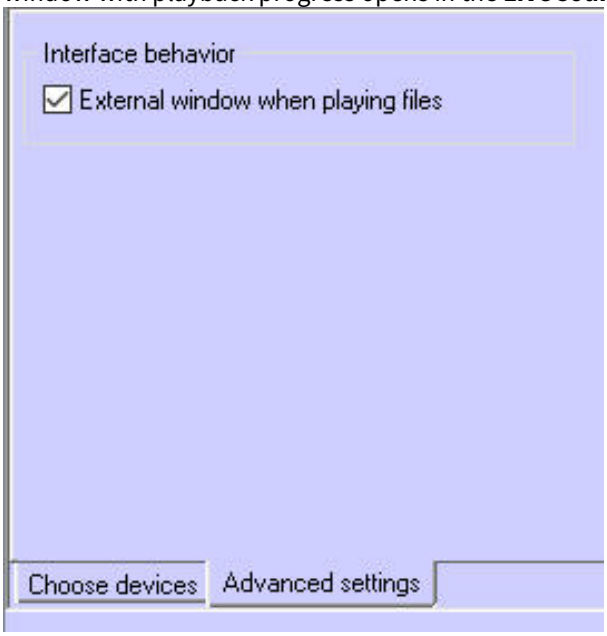
      ii. In the list on the left (**1**), select the necessary microphones to add. To select multiple lines, left-click on them while holding down the Ctrl key on the keyboard.
      iii. Move the microphones to the list on the right (**3**) using the **->** button (**2**).

> **Note.**
>
> To remove the audio sources from the list on the right, select them and click **<-**.

iv. Click the **Apply changes and close** button (**4**).
v. As a result, the selected microphones will be added to the list on the settings panel of the **Live sound switch** object.

c. All microphones created in the hardware tree: click the **All** button (**8**).

5. From the **Sort** drop-down list (**9**), select the sorting method for the Audio inputs list: by number or by name.
6. In the **Audio output**s field, add audio receivers and set up sorting similarly to audio sources in steps 4 and 5.
7. Go to the **Advanced settings** tab and set the **External window when playing files** check box, if it is necessary that a window with playback progress opens in the **Live sound switch** interface when playing files:



If the checkbox is not set, then the progress will be displayed as a percentage in the speaker name during the playback.

8. Click the **Apply** button to save the changes (**10**).

Setting up the **Live sound switch** object is now completed.

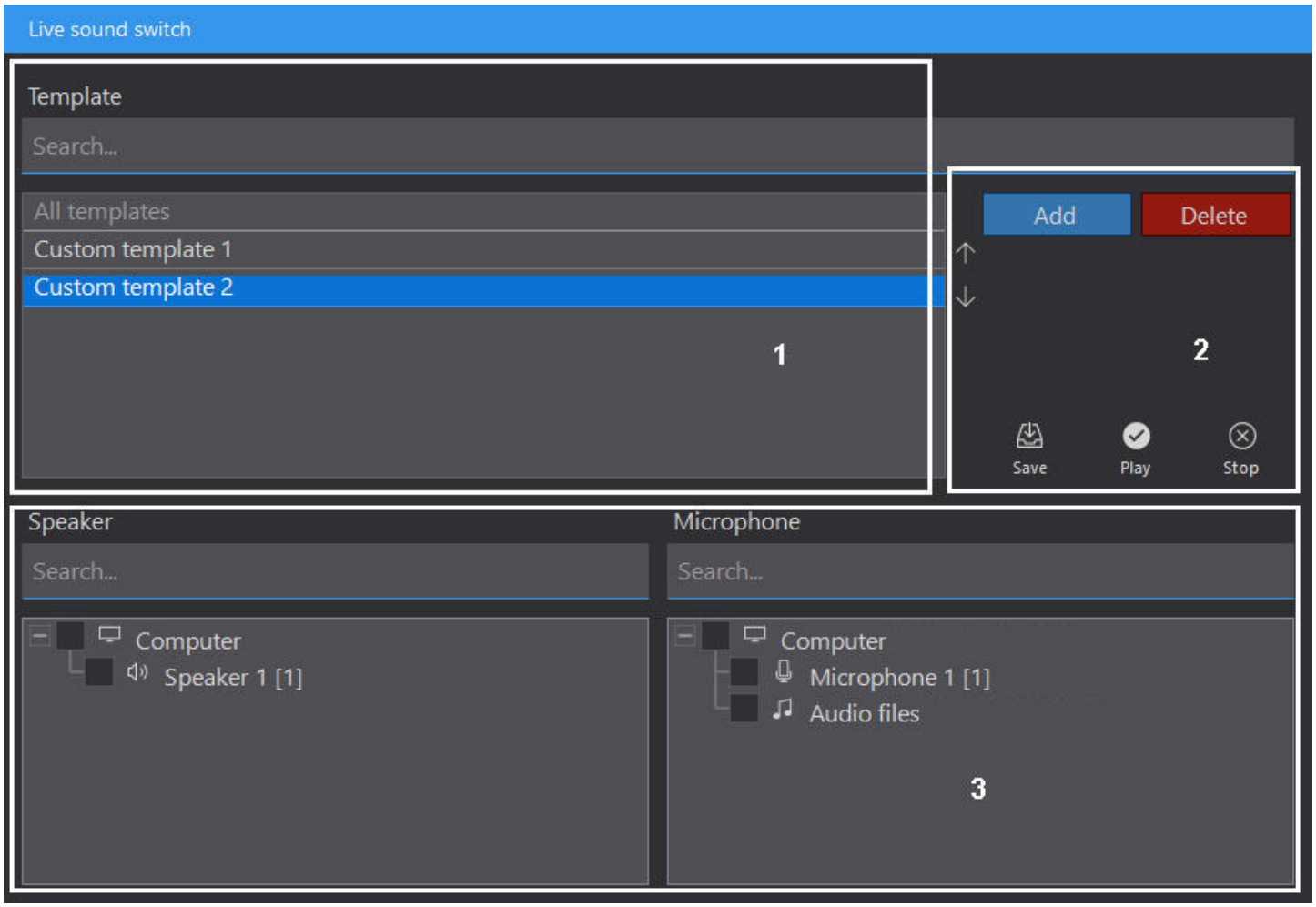
23.4.10.2 Using the Live sound switch object

On this page:

- Template configuration
- Managing templates
- Playing audio by template
- Adding audio files as sound sources

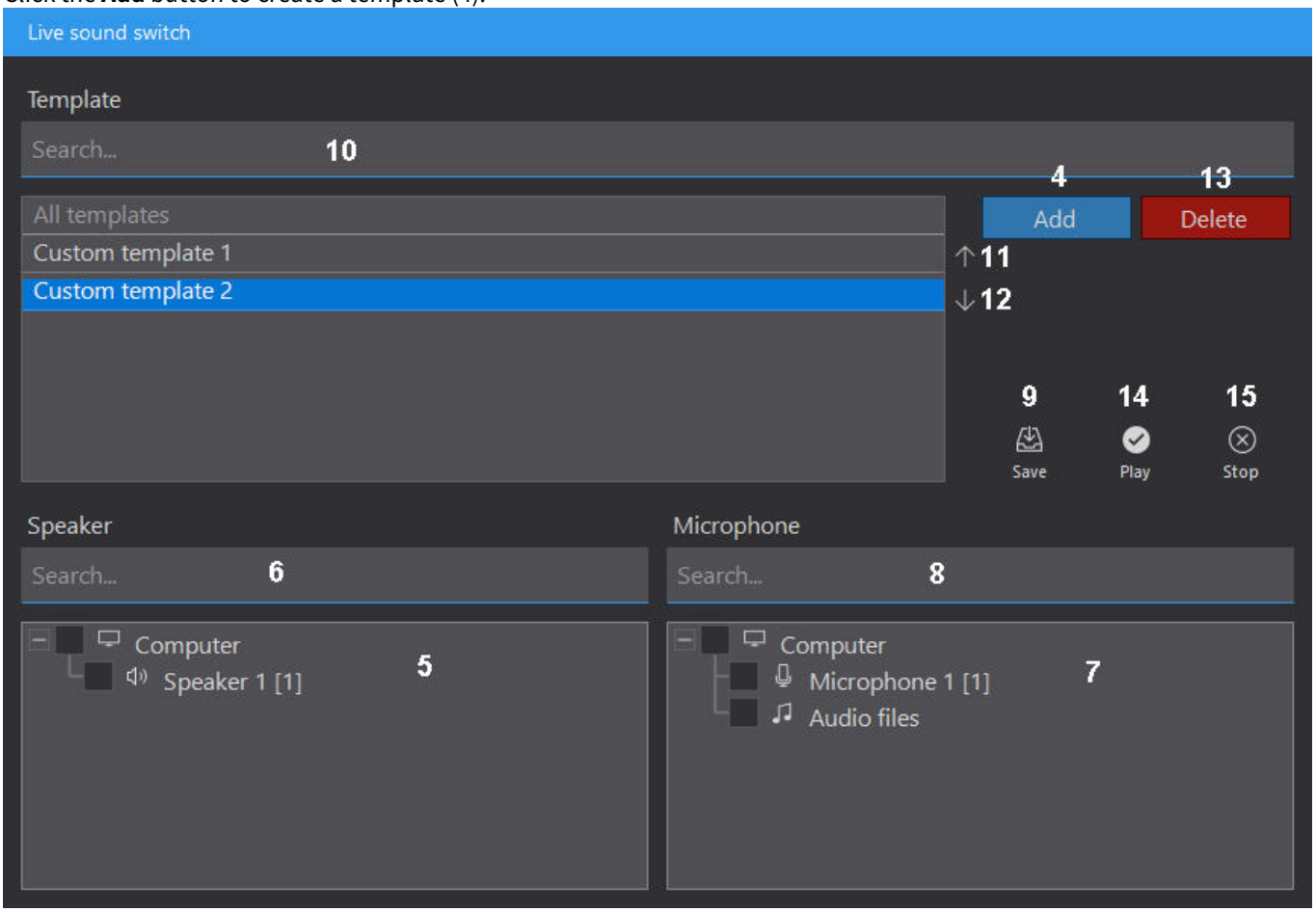
The **Live sound switch** operation is based on templates, each of which specifies the necessary interconnections between microphones and speakers. You can set an unlimited number of templates.

The display window of the **Live sound switch** object contains a list of templates (1), template control buttons (2) and template settings (3):


Live sound switch
Template
Search...
All templates
Custom template 1
Custom template 2
1
Add
Delete
2
Save
Play
Stop
Speaker
Search...
Computer
Speaker 1 [1]
Microphone
Search...
Computer
Microphone 1 [1]
Audio files
3

23.4.10.2.1 Template configuration

1. Click the **Add** button to create a template (4):



2. In the **Speaker** list (5), set the checkboxes for the speakers which should play sound. You can use the search box (6) to find the required speaker by writing its name or part of it.
3. In the **Microphone** list (7), set the checkboxes for the microphones or audio files, the sound from which should be sent to the speaker (the procedure of adding them to the list is described below). Similarly, you can find the required microphone or audio file by name in the search box (8).

> **Note**
>
> The sound on the speaker is mixed if multiple sound sources are selected. You cannot select both a microphone and an audio file as the audio source at the same time, but you can select multiple microphones.

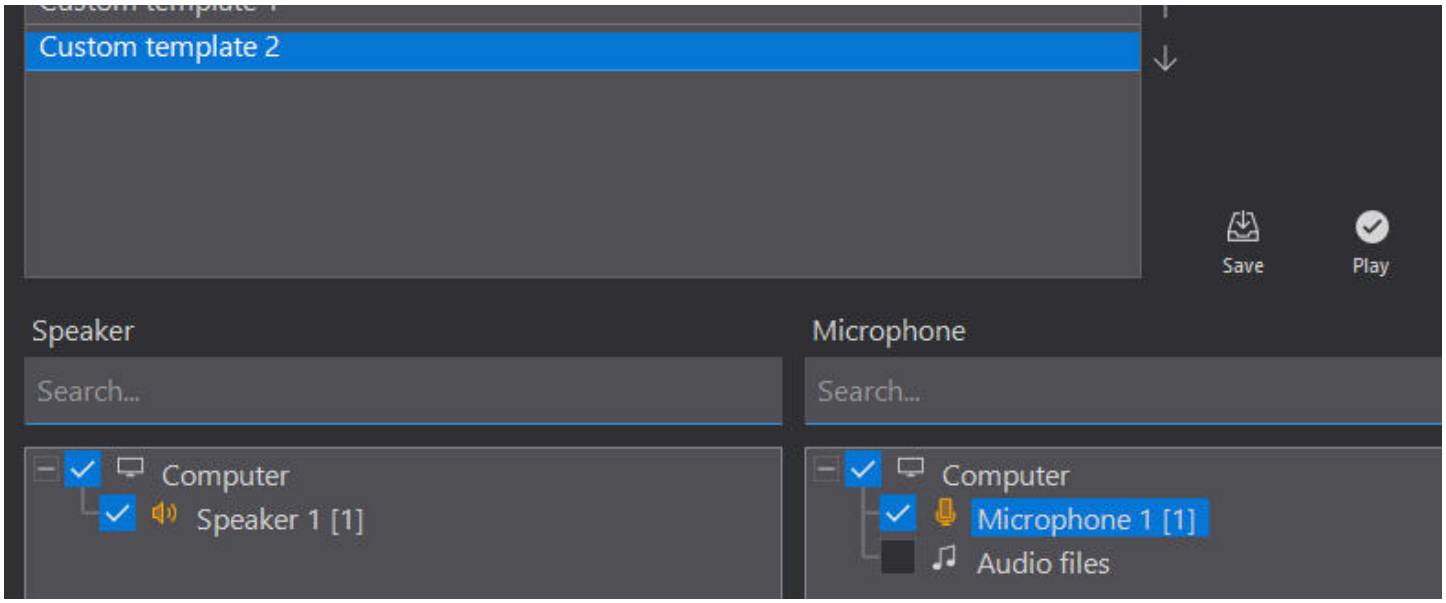
4. Click the **Save** button (9) to save the template settings.
5. Repeat steps 1-4 to configure the required number of templates.

23.4.10.2.2 Managing templates

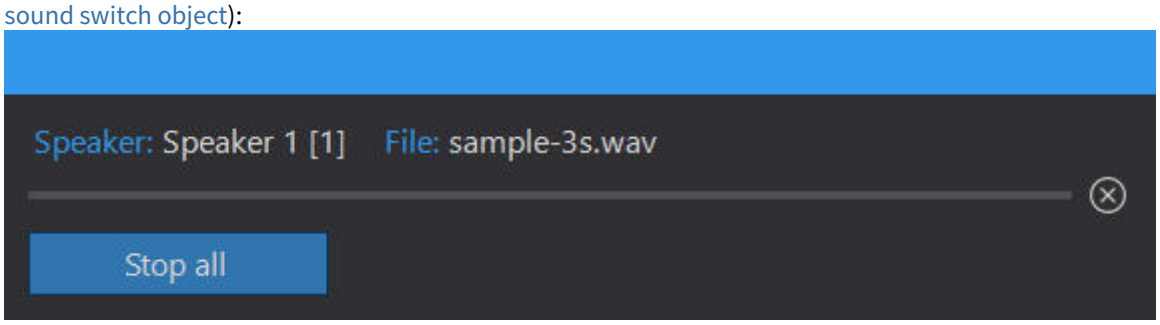
1. To search for a required template, enter the template name or part of it in the **Search** field (10).
2. To change the playback order of templates, select a template in the list and click the **Up** or **Down** button (11, 12). The first template in the list will be played first.
3. To rename a template, select it in the list and left-click on it once. You can also right-click on the template and select **Edit** from the context menu.
4. To delete a template, select the required template and click the **Delete** button (13). You can also right-click on the template and select **Delete** from the context menu.

23.4.10.2.3 Playing audio by template

To play sound on speakers, select a template in the list and click the **Play** button (14). As a result, the sound from the selected microphones will be sent to the selected speakers, and the icons of active devices will be highlighted with yellow:



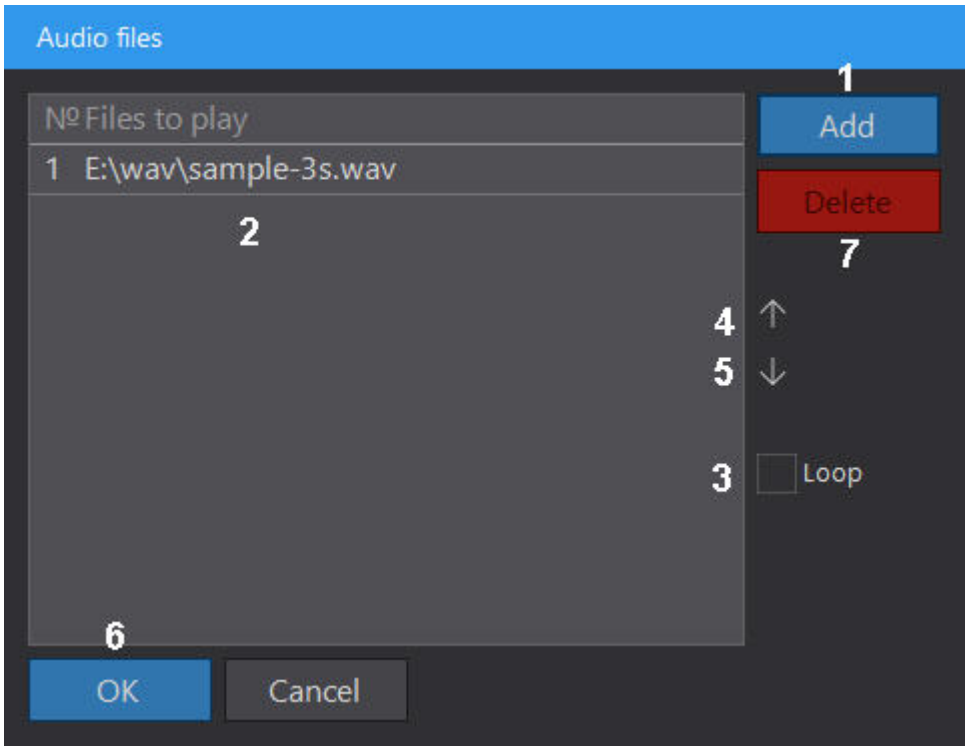
When playing sound from audio files, the sound transmission progress will be shown as a percentage next to the file name or in the form of a separate window illustrating the playback progress (depends on the settings, see Creating and configuring the Live sound switch object):



To stop sound transmission, click the **Stop** button (15).

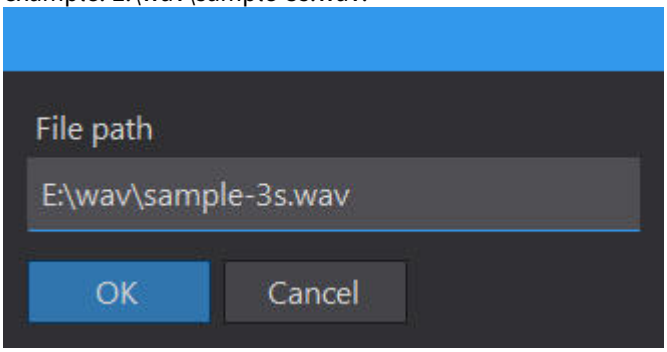
23.4.10.2.4 Adding audio files as sound sources

To send custom sounds to the speakers, set the check box for **Audio files** when selecting sound sources. The window for adding files will open:



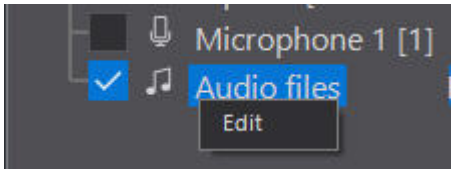
Add audio files as follows:

1. Click the **Add** button (1).
2. In the window that opens, specify the path to the audio file with its name. Files in wav format are supported. Path example: E:\wav\sample-3s.wav.



3. Click **OK**. As a result, the selected file (2) will appear in the list of files for playback.
4. If it is necessary to loop the file during playback, select it in the list and set the **Loop** check box (3).
5. Repeat steps 1-4 for the required number of audio files.
6. If necessary, adjust the playback order of files by selecting the required file in the list and moving it using the **Up** and **Down** buttons (4, 5). The first file in the list will be played first.
7. To edit the added file, right-click on it and select **Edit** from the context menu. To delete the file, select it in the list and click the **Delete** button (7) or right-click on it and select **Delete** from the context menu.
8. Click the **OK** button (6).

Adding audio files is now complete. To edit the list of audio files, right-click on **Audio files** object and select **Edit** from the context menu:

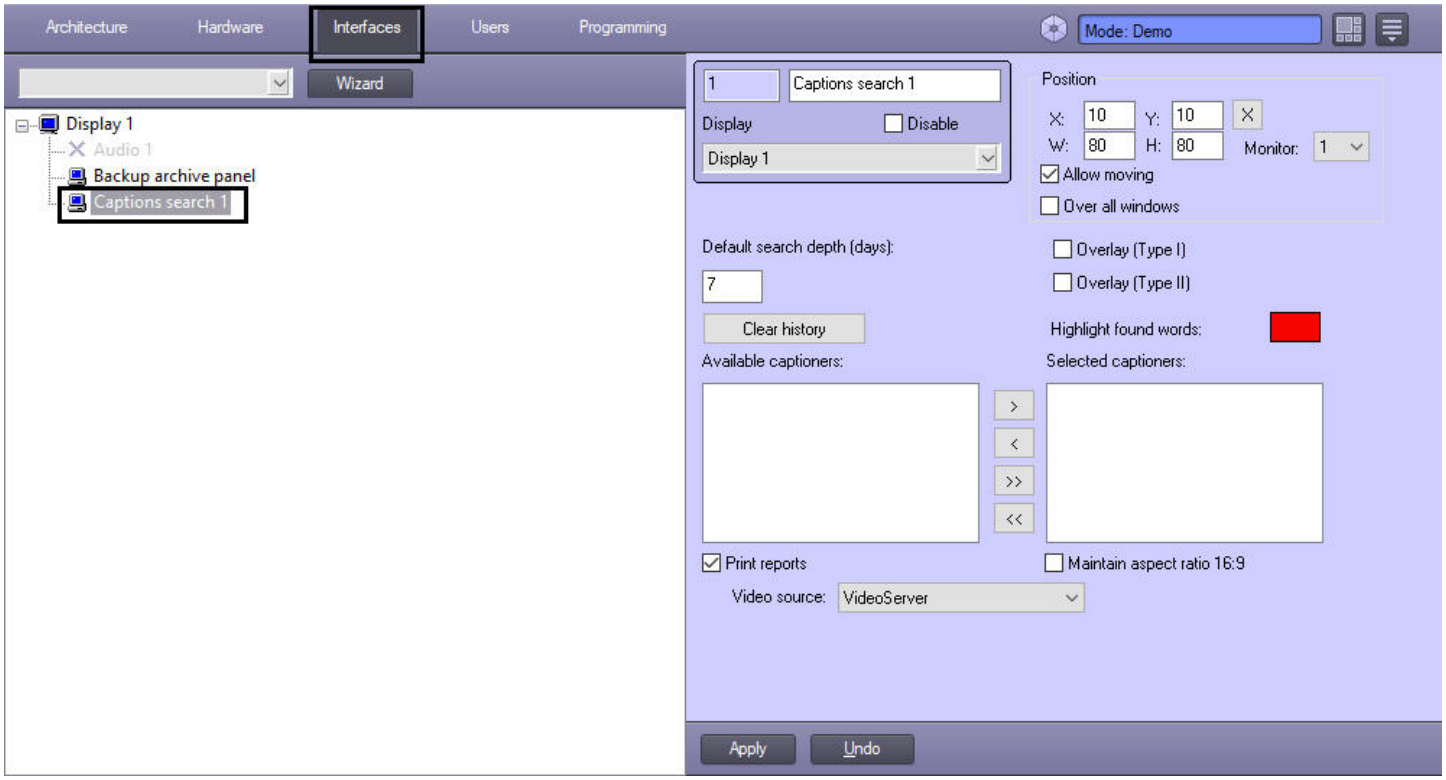


23.4.11 Setting up the Captions search window

23.4.11.1 The Captions search interface object setup procedure

The **Captions search** object is a child object of the **Display** system object. It is used to search for user queries in the captions database.

To create and set up the **Captions search** object, use the **Interfaces** tab in the **System Settings** window.



The **Captions search** interface object setup includes the following steps:

1. Select the captioners.
2. Specify the search criteria.
3. Set up the **Captions search** interface window.

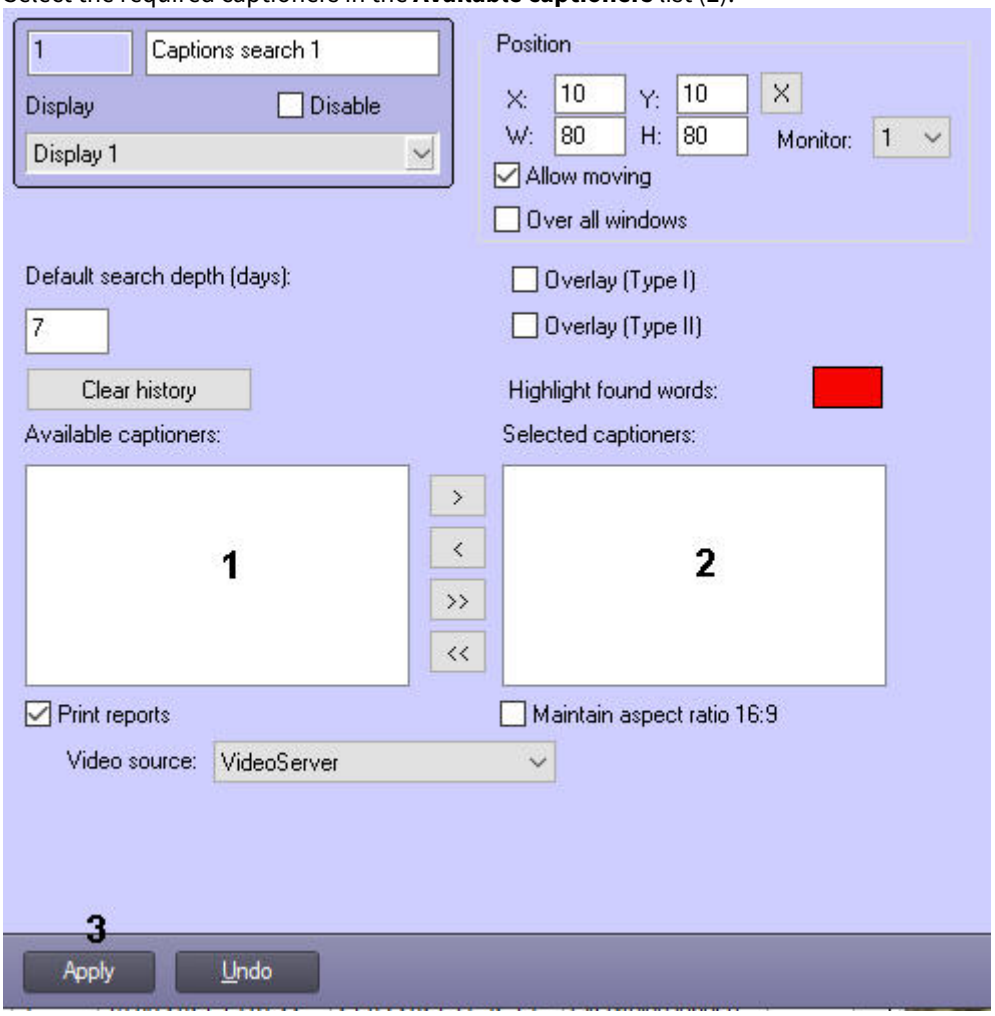
> **Attention!**
>
> The **Captions search** object also uses the **ElasticSearch** service (see Features of ElasticSearch service operation). If search by captions does not operate correctly, we recommend you to disable the **ElasticSearch** service using the SearchIndex parameter in the **cam_title.run.config** file (see XML-file parameters reference guide).

> Working with the Captions search interface object

23.4.11.2 Selecting the captioners

Selecting the captioners allows you to select the captioners archive where the search should be performed. To select the captioners, do the following:

1. Select the required captioners in the **Available captioners** list (**1**).



2. Click the > button to move the selected captioners, or the >> button to move all captioners from the list of the **Available captioners** to the **Selected captioners** list (**2**).

> **Note**
>
> Alternatively, the < and << buttons are used to move the selected or all captioners from the **Selected captioners** list to the **Available captioners** list.

3. Click the **Apply** button (**3**).

The captioners are now selected.

23.4.11.3 Specifying the captions search parameters

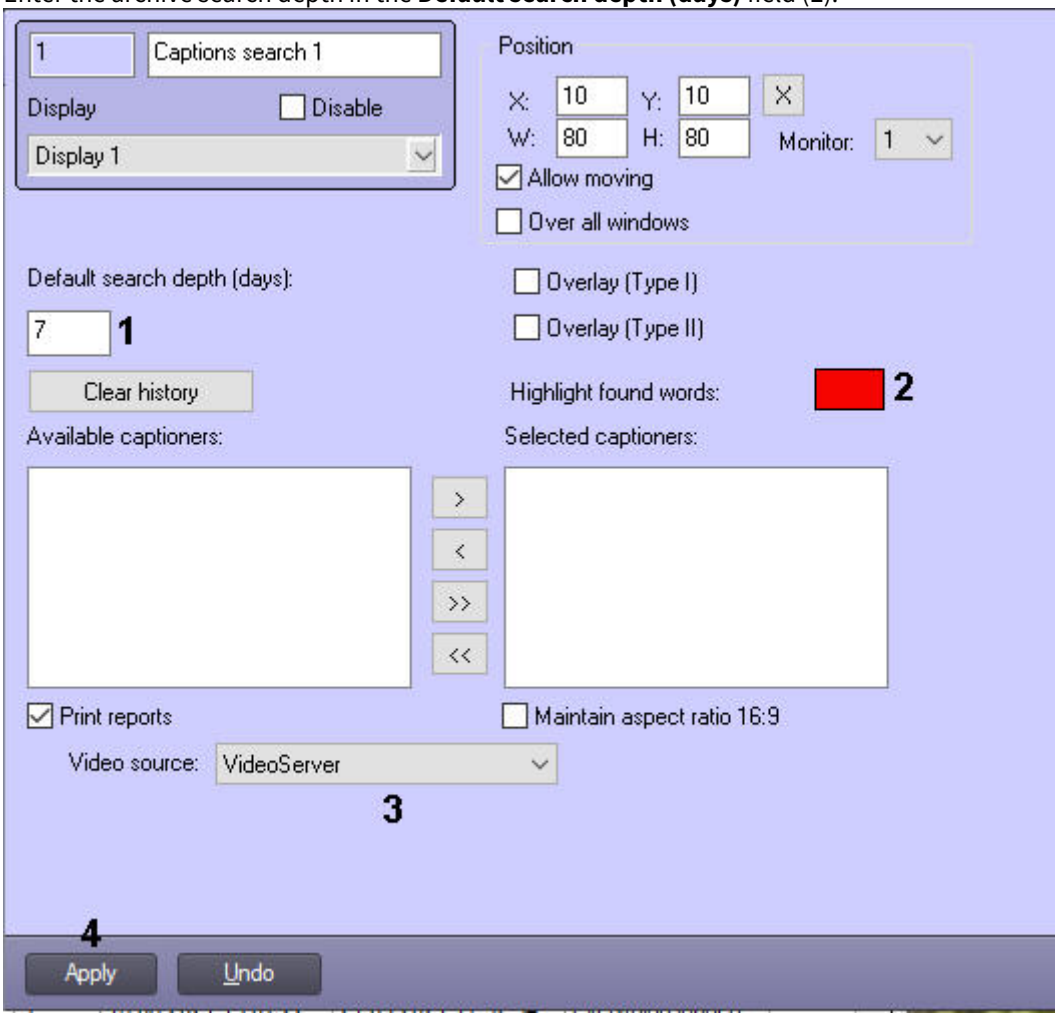
To configure the captions search, specify the following parameters:

1. **Search depth** – the captions search depth.
2. **Highlight found words** – the option for highlighting the found words in the search results.
3. **Video source** – select an archive from which video data is received: main or backup archive.

> **Note**
>
> Storing captions can be disabled by **NoSaveTitles** registry key – see Registry keys reference guide.

To specify the captions search parameters, do the following:

1. Enter the archive search depth in the **Default search depth (days)** field (**1**).



2. To enable highlighting of found words, double-click the **Highlight found words** color box and select the color in the standard Windows color selection box that opens (**2**).
3. From the **Video source** drop-down list select an archive from which video data is displayed as search results: video server main archive or backup archive (**3**).

> **Note**
>
> If the backup archive is selected as the Video source, and not all cameras have records in it, then only the search results for cameras that have records in the backup archive will be displayed.
> If there is no backup archive for all cameras, but it is selected as the Video source, the archive from the video server for all cameras is used by default.

4. Click the **Apply** button (**4**).

The captions search parameters are now configured.

23.4.11.4 Setting up the Captions search interface window displaying

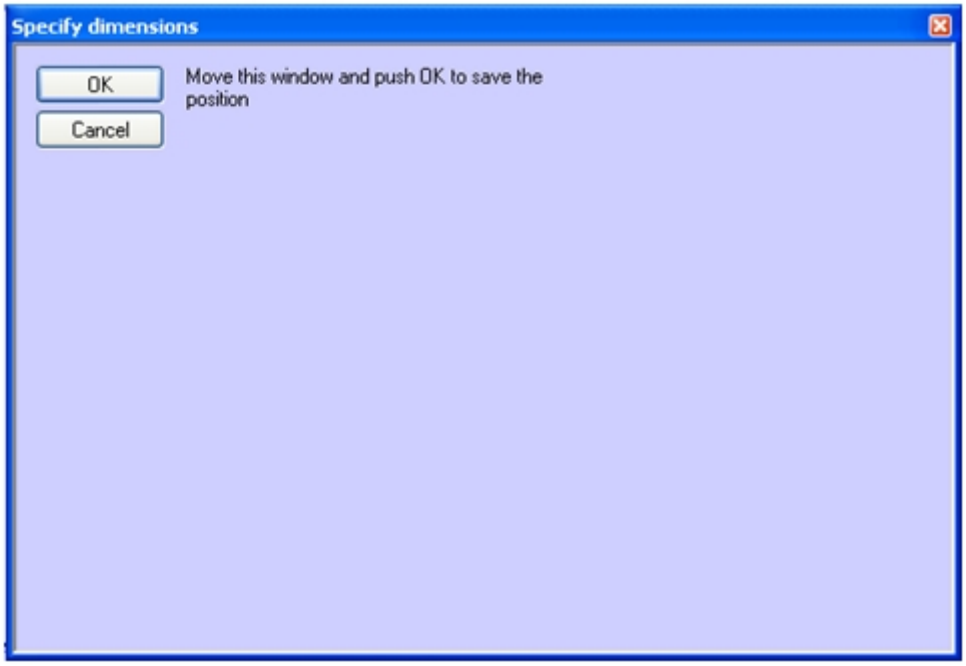
To set up the **Captions search** interface window displaying, the following parameters should be specified:

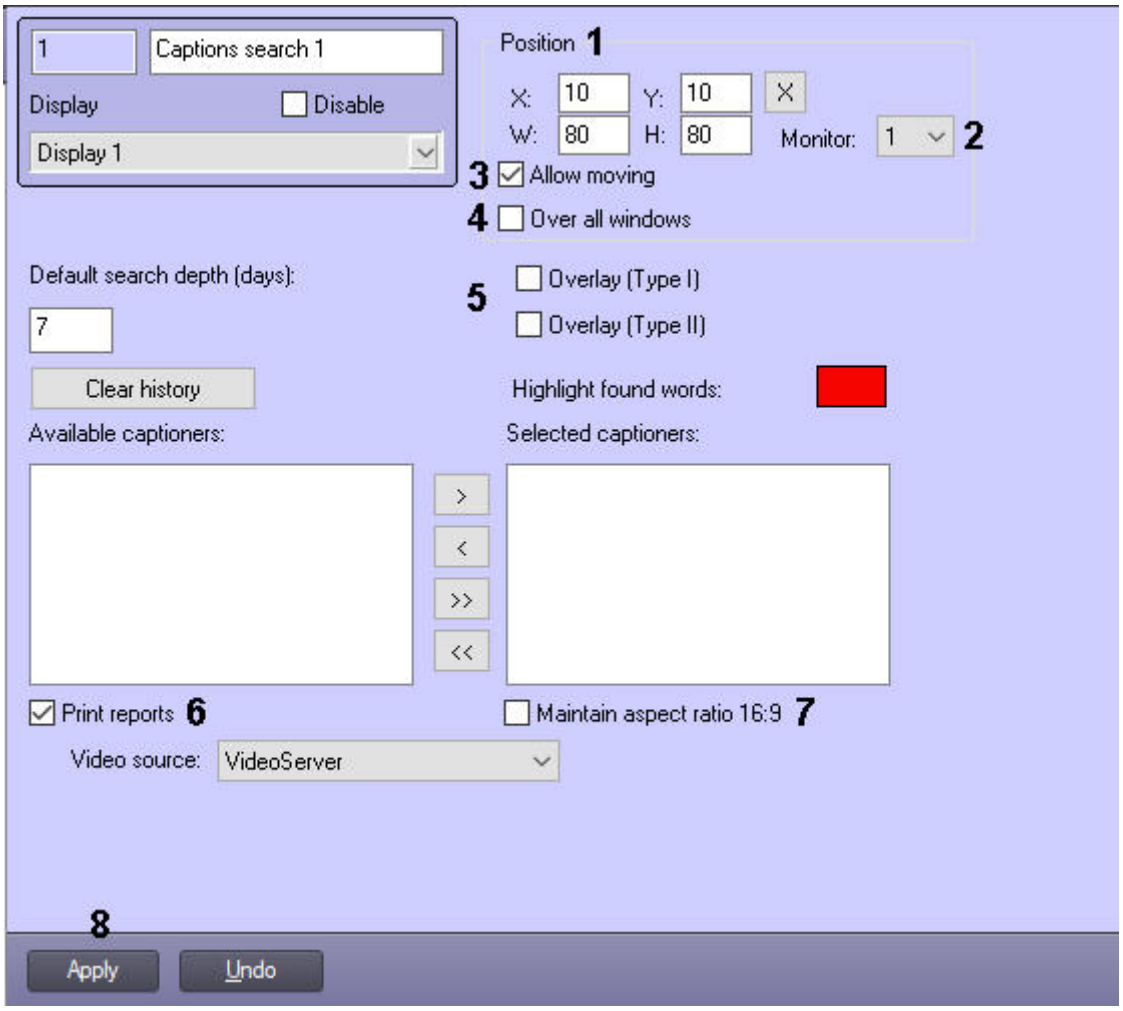
1. **Position** – the position and the size of the **Caption search** interface window.
2. **Overlay type** – the type of the overlay of the synchronous display of video image and search results.
3. **Print reports** – allows the operator to print the search results.

To set up the **Captions search** interface window displaying, do the following:

1. Specify the position and the size of the **Captions search** interface window: the **X** field (the horizontal indent from the left border of the computer screen), the **Y** field (the vertical indent from the top border of the computer screen), the **W** field (the window width), the **H** field (the window height) (**1**).

   The coordinates can be set up using the visual method. Click the button and use the mouse to set the location and size of the test window, then click the **OK** button. The coordinates of the test window will be automatically calculated and copied into the **X**, **Y**, **W** and **H** fields.





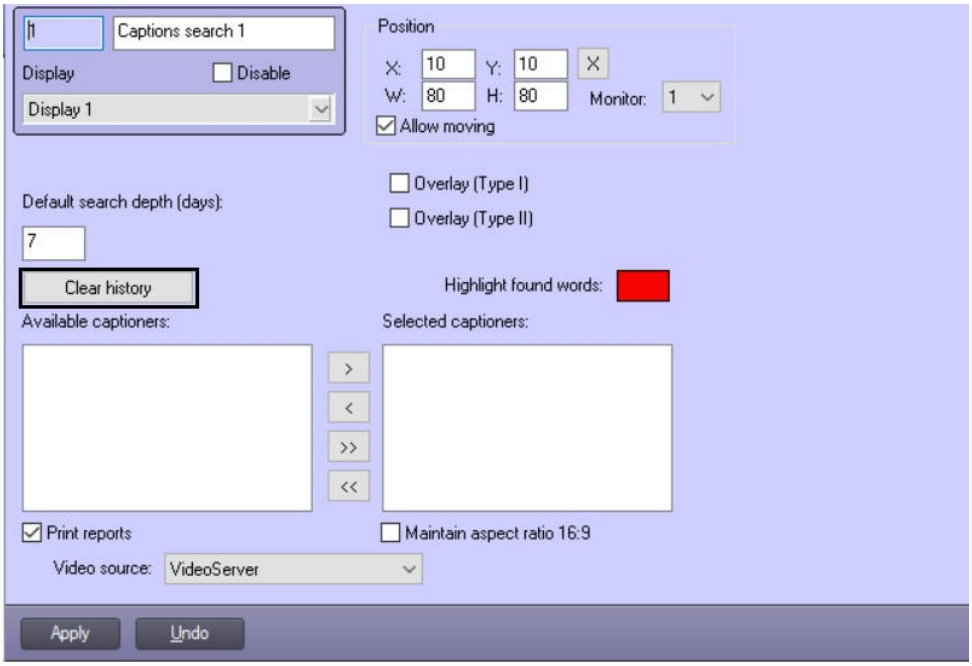
2. In the **Monitor** drop-down list, select the number of the computer monitor on which you want to display the **Captions search** interface window (**2**).
3. By default, it is possible to move the **Captions search** interface window using drag&drop. To disable it, clear the **Allow moving** checkbox (**3**).
4. To display the **Captions search** interface window over all windows, set the **Over all windows** checkbox (**4**).
5. Select the overlay type by setting the **Overlay (Type I)** or **Overlay (Type II)** checkbox (**5**).

> **Note**
>
> In most cases, the optimal mode of processing the video image is DirectDraw — **Overlay (Type II)**. If it is necessary to display the video signal from the Fisheye cameras or the signal decoded using the Intel QuickSync technology, select the **Overlay (Type I)** — Direct3D. The overlay can also be disabled completely.

6. To allow the operator to print the search results, set the **Print reports** checkbox (**6**).
7. If it is necessary to display the archive video in the **Captions search** interface window in the 16:9 format, then set the **Maintain aspect ratio 16:9** (**7**) checkbox. If the checkbox is clear, then the 4:3 aspect ratio is set even for the widescreen video.
8. Click the **Apply** button (**8**).

The **Captions search** interface window is now set.

> **Note**
>
> To clear the history of user queries in the **Captions search** interface window, click the **Clear history** button.



23.4.12 Configuring HTML interface

23.4.12.1 General description of HTML interface in Intellect software

The HTML interface object is designed for displaying web-pages, text files, images and more data, displaying of which is supported by Internet Explorer browser, in the *Intellect* interface window.The Chromium browser can also be used – see the **process** key description in the Registry keys reference guide.

It is possible to create one or several html-pages performing the following functions on the basis of the **HTML interface** object:

1. Loading web-pages and other files by URL or from the file.
2. Saving web-pages and other files and images to the file.

Note.

Web-page creating and editing is performed using the specialized editor programs.

If there is video displaying or sound playing back on the web-page, it will be also available in the **HTML interface** window.

HTML interface

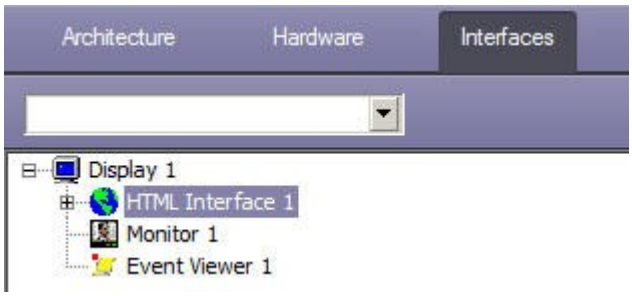
23.4.12.2 Procedure of HTML interface configuring

To configure HTML interface in the *Intellect* software, do the following:

1. Create the **HTML Interface** object and set its position.
2. Create and configure one or several **HTML page** objects.
3. Select start page for displaying in HTML interface.
4. Select objects to track their states in HTML interface window.

23.4.12.3 Creating HTML interface object and setting its position

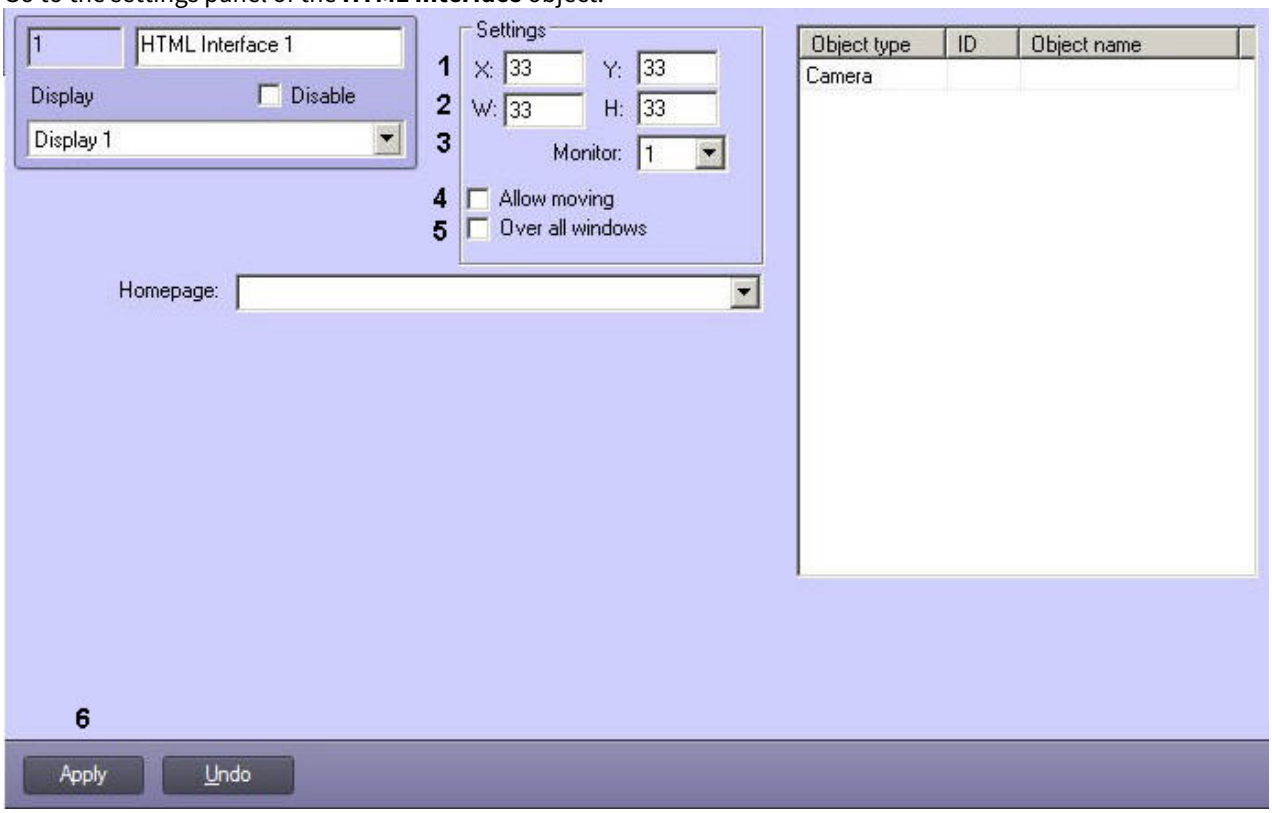
The **HTML interface** object is created on the basis of the **Display** object on the **Interfaces** tab of the **System settings** dialog window.



Object's settings panel will display on the right part of the **System settings** dialog window after the object creation.

To set position of the **HTML Interface** object on the screen, do the following:

1. Go to the settings panel of the **HTML Interface** object.



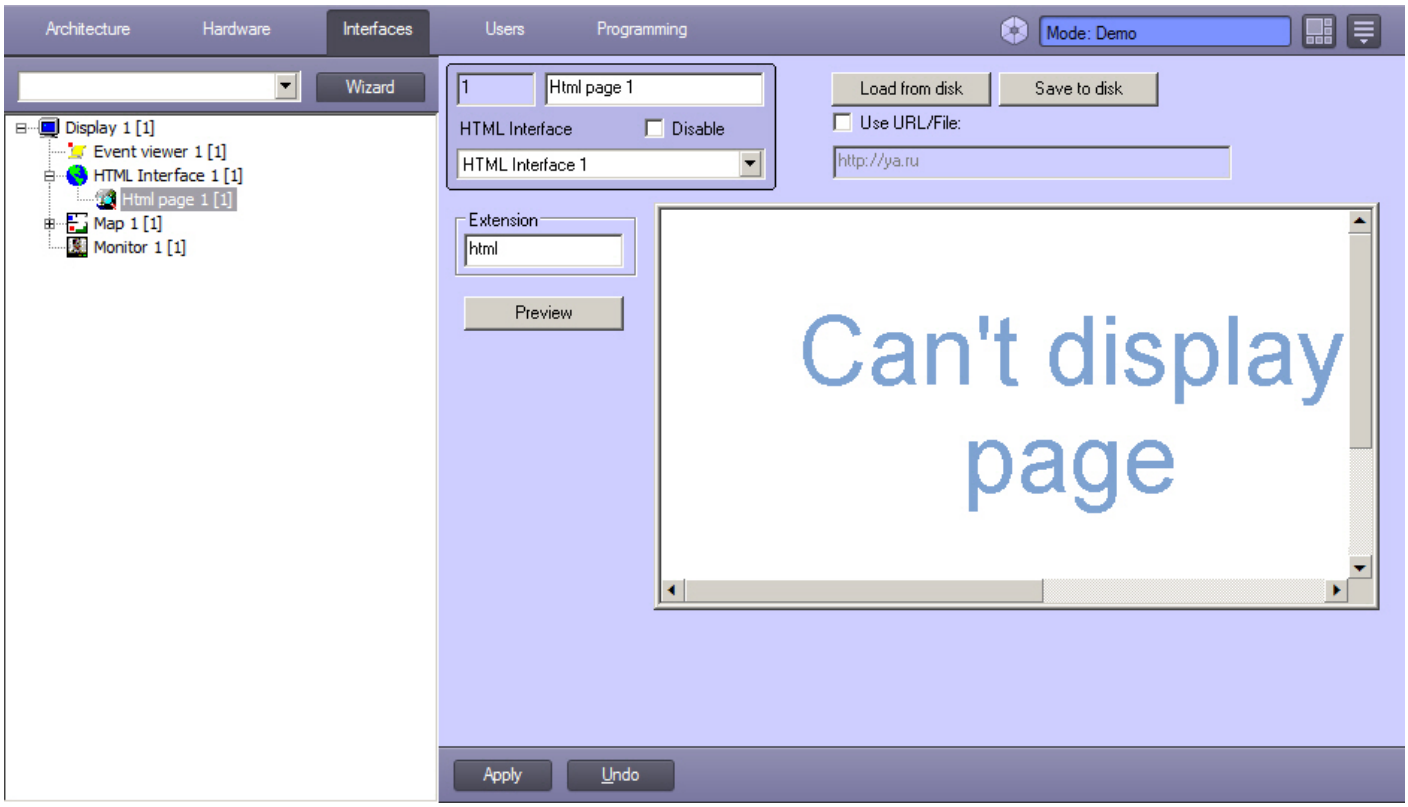
2. In the **X:** and **Y:** fields specify coordinates of the interface window's upper left corner (**1**). Coordinates are counting from the display's upper left corner and expressing as a percentage of the screen width and height respectively.
3. In the **W:** and **H:** fields specify width and height of the HTML interface window as a percentage of the screen width and height respectively (**2**).
4. From the **Monitor** drop-down list select number of the monitor on which the **HTML Interface** object is to be displayed via a mouse click (**3**).
5. Set the **Allow moving** checkbox to allow operator changing position of the **HTML Interface** window via a mouse click (**4**).
6. If it is necessary for the **HTML Interface** window to be displayed on top of all windows, set the **Over all windows** checkbox (**5**).
7. Click **Apply** button (**6**).

Setting position of the **HTML Interface** object on the screen is completed.

23.4.12.4 Creating and configuring the HTML page object

23.4.12.4.1 Creating the HTML page object

The **HTML page** object is created on the basis of the **HTML Interface** object on the **Interfaces** tab of the **System settings** dialog window.



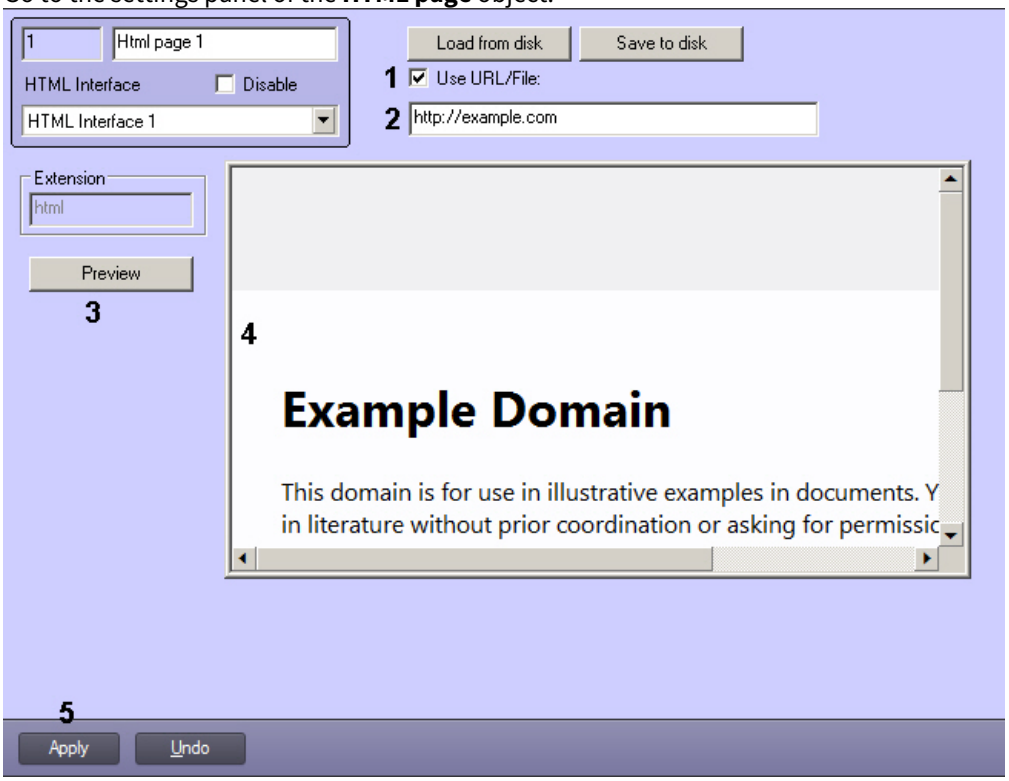
Object's settings panel will display on the right part of the **System settings** dialog window after the object creation.

Default HTML page contains example of code allows to arm and disarm cameras. To check out this example it's required to save the page (see Loading file from disk and saving to disk) and open it in text editor.

23.4.12.4.2 Open web-page by URL

To go to the specified URL while opening web-page in the **HTML Interface** window, do the following:

1. Go to the settings panel of the **HTML page** object.



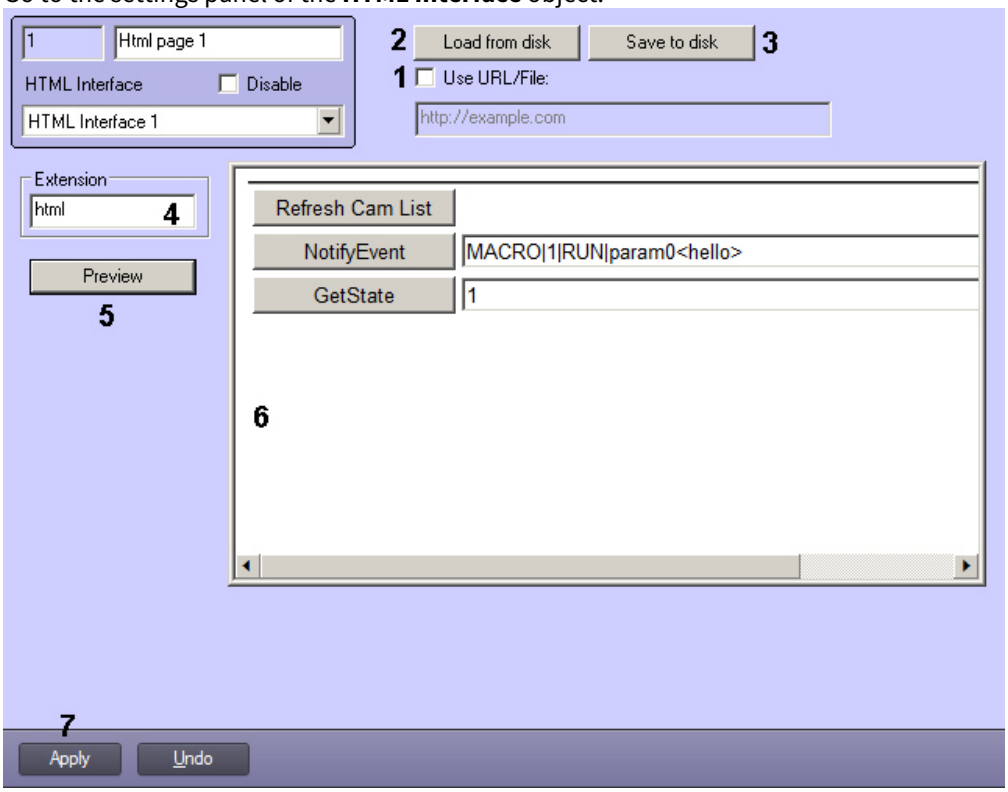
2. Set the **Use URL/File** checkbox (1).
3. In the text field enter the URL-address of required page (2).
4. Click the **Preview** button to display the selected HTML page (3). As a result the page content will display in the preview box (4).
5. Click **Apply** (5).

Configuring of opening web-page by specified URL is completed.

23.4.12.4.3 Loading file from disk and saving to disk

To load the specified file of the web-page, text file or image while opening web-page in the **HTML Interface** window, do the following:

1. Go to the settings panel of the **HTML Interface** object.



2. Deselect the **Use URL/File** checkbox if it was set (1).
3. Click the **Load from disk** button (2).
4. In standard dialog window select the required file (3).

> **Note.**
>
> Extension of the selected file will display in the **Extension** field (4).

5. Click the **Preview** button to display the selected HTML page (5). As a result the page content will display in the preview box (6).
6. Click **Apply** button (7).

> **Note.**
>
> To save opened file click the **Save to disk** button.

Configuring of loading file from disk is completed.

23.4.12.4.4 Link to the HTML page object

When apply settings, i.e. while clicking the **Apply** button or going to the settings panel of other object, the web-page is saving in the OPCIEPAGE<id of HTML page object>_<id of HTML Interface object>.html, for example OPCIEPAGE2_1.html file in the <Directory of the *Intellect* software installation>\OPCIEFolder\ folder.

It is possible to refer to such page in the normal way using the <a> tag, for example:

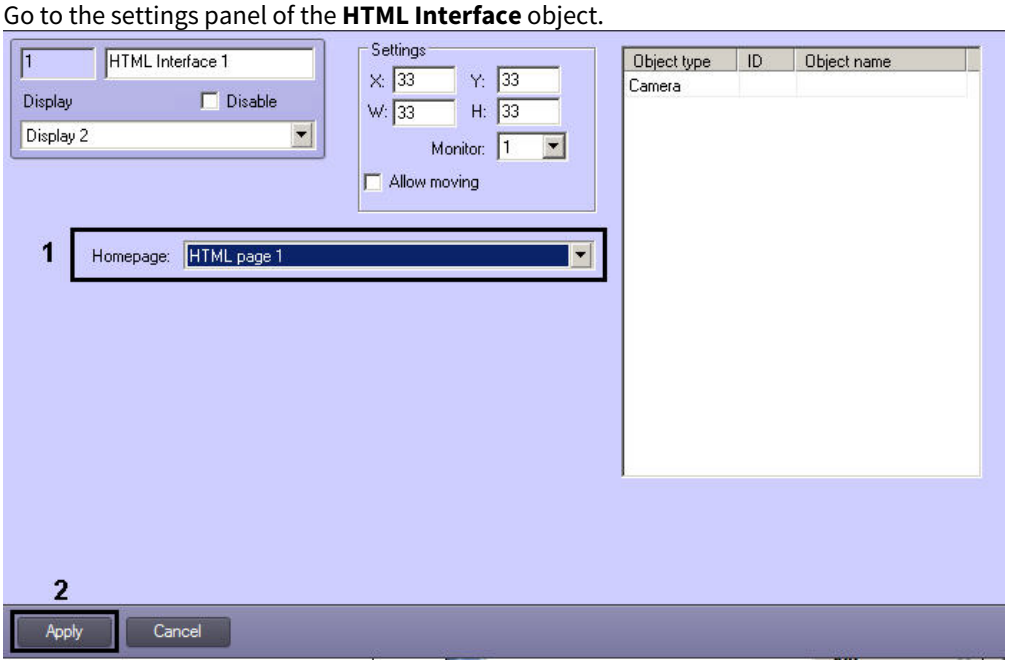
HTML page 2

> **Note.**
>
> If web-page is not opened by URL, the empty file will be saved.

23.4.12.5 Selecting start page for displaying in HTML interface

To select the start page for displaying in the HTML interface, do the following:

1. Go to the settings panel of the **HTML Interface** object.



2. From the **Homepage** drop-down list select the created HTML page object (1).
3. Click **Apply** button (2).

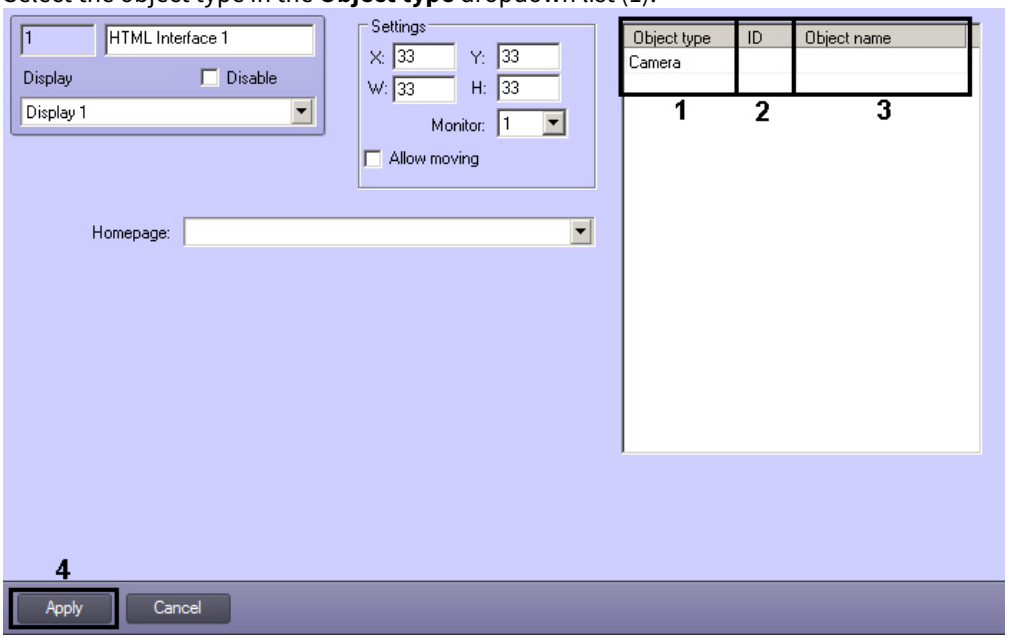
Configuring the start page is completed.

23.4.12.6 Selecting objects to track their states

An HTML page created by default has OnObjectState and GetState functions aimed to get object states. GetState function requires object state and OnObjectState function aims to get info on states.

Select objects states of which are to be tracked using these functions as follows:

1. Go to the settings panel of the **HTML Interface** object.
2. Select the object type in the **Object type** dropdown list (1).



3. If states from the specific object are to be received, then select its ID in the **ID** dropdown list (2).

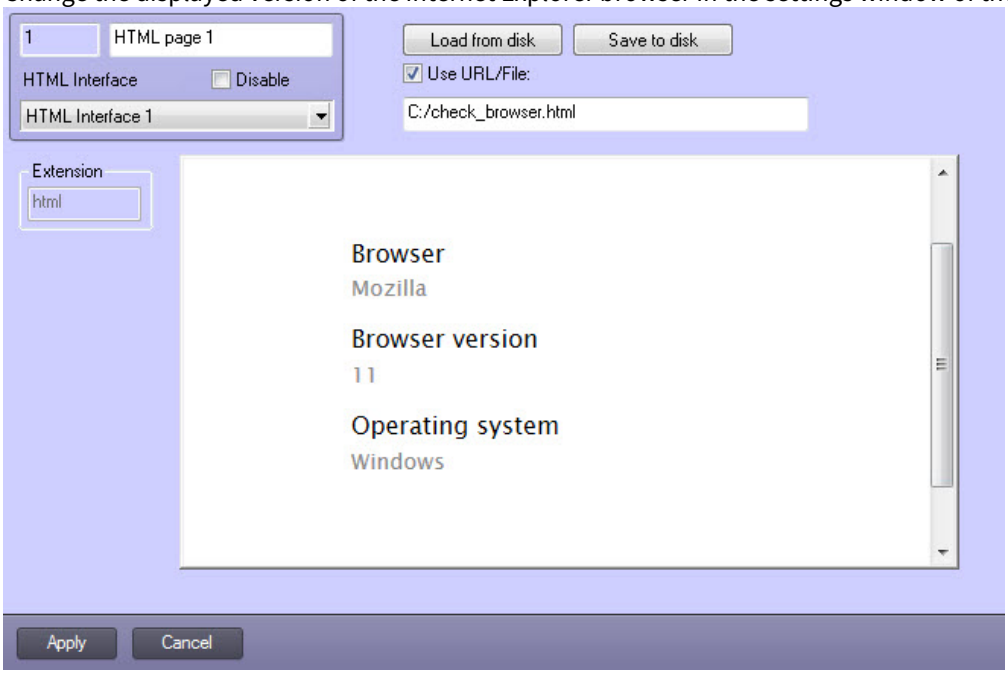
4. When left clicking in the **Object name** field it is automatically filled with the name of the object with this ID (3).
5. Repeat steps 2-4 for all required objects.
6. To save the settings click the **Apply** button (4).

Objects states of which are to be tracked are now selected.

23.4.12.7 Changing the displayed version of Internet Explorer

If there are messages saying that you need to update the Internet Explorer browser, you can change the displayed version without updating the browser itself. As a result, there will be no more messages about the update. To change the displayed version of Internet Explorer, do the following:

1. Change the displayed version of the Internet Explorer browser in the settings window of the **HTML page** object.



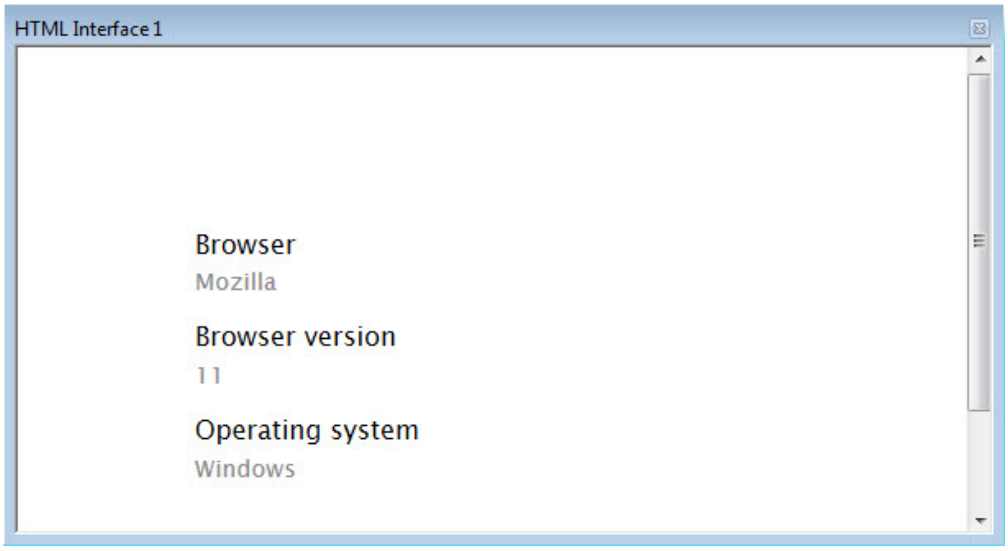
To do this, change the values of the **OpcIe.run** and **Intellect.exe** parameters to the required ones from the table below:

Internet Explorer version	Decimal value
11	11001
9	9000
8	8888
7	7000

The **OpcIe.run** and **Intellect.exe** parameters are located in the following registry key branch:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION
```

2. Change the displayed version of the Internet Explorer browser in the **HTML Interface** window.



To do this, change the value of the **OpcIe.run** parameter to the required one from the table below:

Internet Explorer version	Decimal value
11	11001
9	9000
8	8888
7	7000

The **OpcIe.run** parameter is located in the following registry key branch:

```
Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Main\FeatureControl\FEATURE_BROWSER_EMULATION
```

Attention!

It is necessary to specify the same value corresponding to the required Internet Explorer version in all the parameters described above.

Note

For more information about working with the registry, see Working with Windows OS registry.

Changing the displayed version of Internet Explorer is complete.

23.4.13 Setting up the voice notification

It is possible to transmit voice notification with the registration of alarms by main motion detectors of cameras.

When motion detector works, audio file which is situated in Wav subdirectory in INTELLECT™ software root directory, is played. The files have .wav extension and are called cam_md_start_N, where N is a number of a video camera.

Note.

By default INTELLECT™ software provides 16 audio files for 16 cameras, respectively. You can add your own audio file if the number of cameras is greater one specified by default. It is enough to move a new audio file (wav format required) to a Wav subdirectory and change its name to: cam_md_start_N, where N is a number of a video camera (> 16). If there is no file with name corresponding to camera, then there is a standard sound of Windows OS - **Ding**.

Before setting up the voice notification it's necessary to make sure that the following conditions are carried out:

1. Standard sound card is installed on the required computer (also integrated into the motherboard);
2. The devices of audio signals playback (dynamics and headphones) are connected to audio outputs of the sound card.

Setting up the voice notification is carried out in two ways:

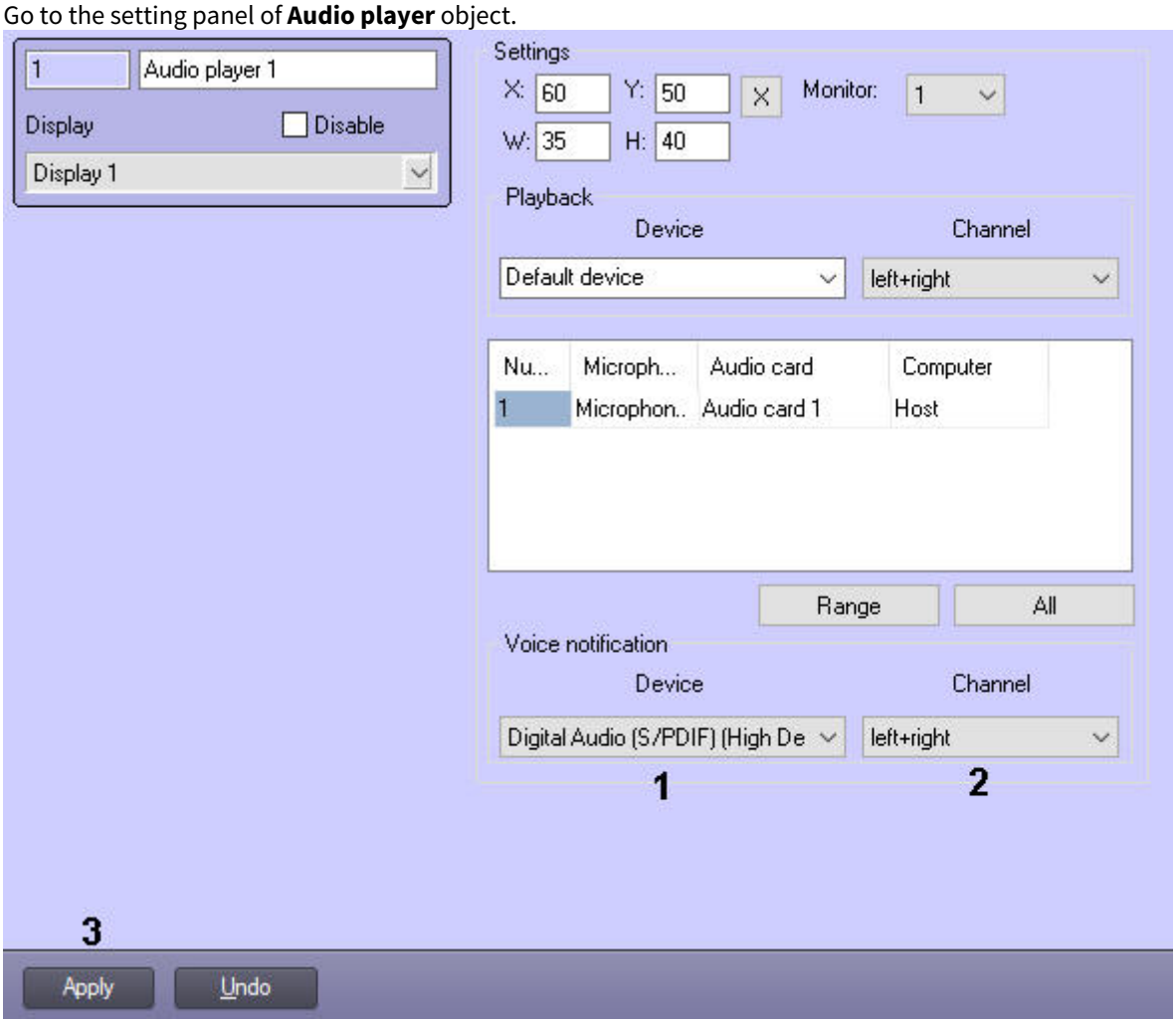
1. Using **Audio player** object;
2. Using **Sound notification** object;
3. Using **Voice Notification Service** object – this way allows selecting any audio file for voice notification, including a custom one.

It's recommended to use only one variant.

23.4.13.1 Setting up the voice notification using Audio player object

To set up the voice notification using **Audio player** object do the following:

1. Go to the setting panel of **Audio player** object.



2. Select required voice notification device in **Device** dropdown list of **Voice notification** group (1).

> **Note.**
>
> Standard sound card corresponds to **Default device**.
> To switch the voice notification off select **Switch off**.

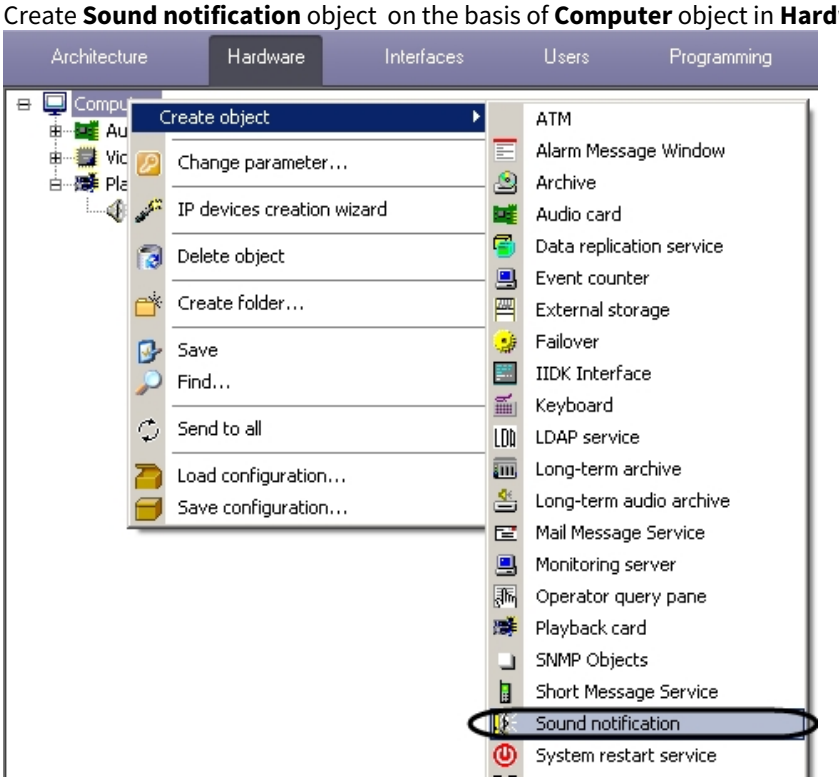
3. Select required voice notification channel in **Channel** dropdown list of **Voice notification** group (2).
4. Click **Apply** button to save all the changes (3).

Setting up the voice notification using **Audio player** object is completed.

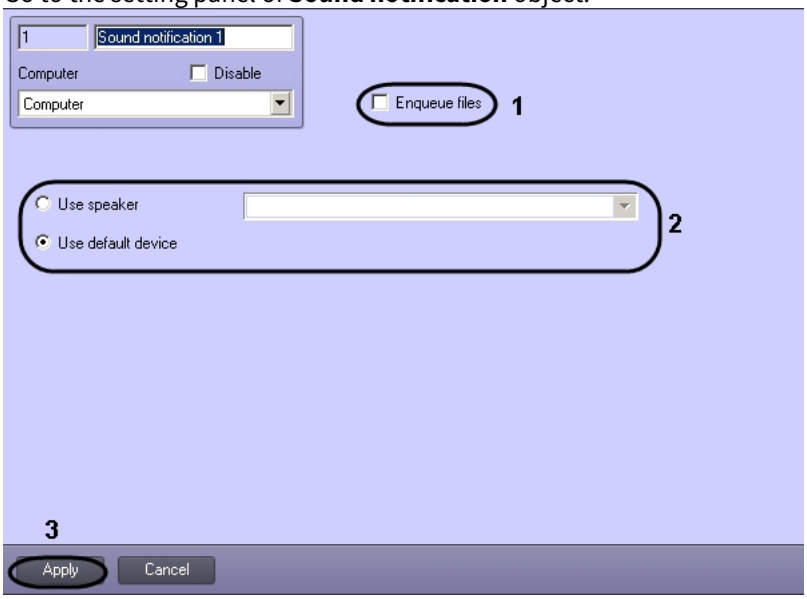
23.4.13.2 Setting up the voice notification using Sound notification object

To set up the voice notification using **Sound notification** object do the following:

1. Create **Sound notification** object on the basis of **Computer** object in **Hardware** tab of **System setting** dialog box.



2. Go to the setting panel of **Sound notification** object.



3. If it's necessary, set **Enqueue files** check box in order to play alarm sound notification files that appear simultaneously one after another (1).
4. If the voice notification device is a standard sound card, set the switch into **Use default device** mode. Otherwise set the switch into **Use speaker** mode and select the voice notification device in the dropdown list (2).
5. Click **Apply** button to save all the changes (3).

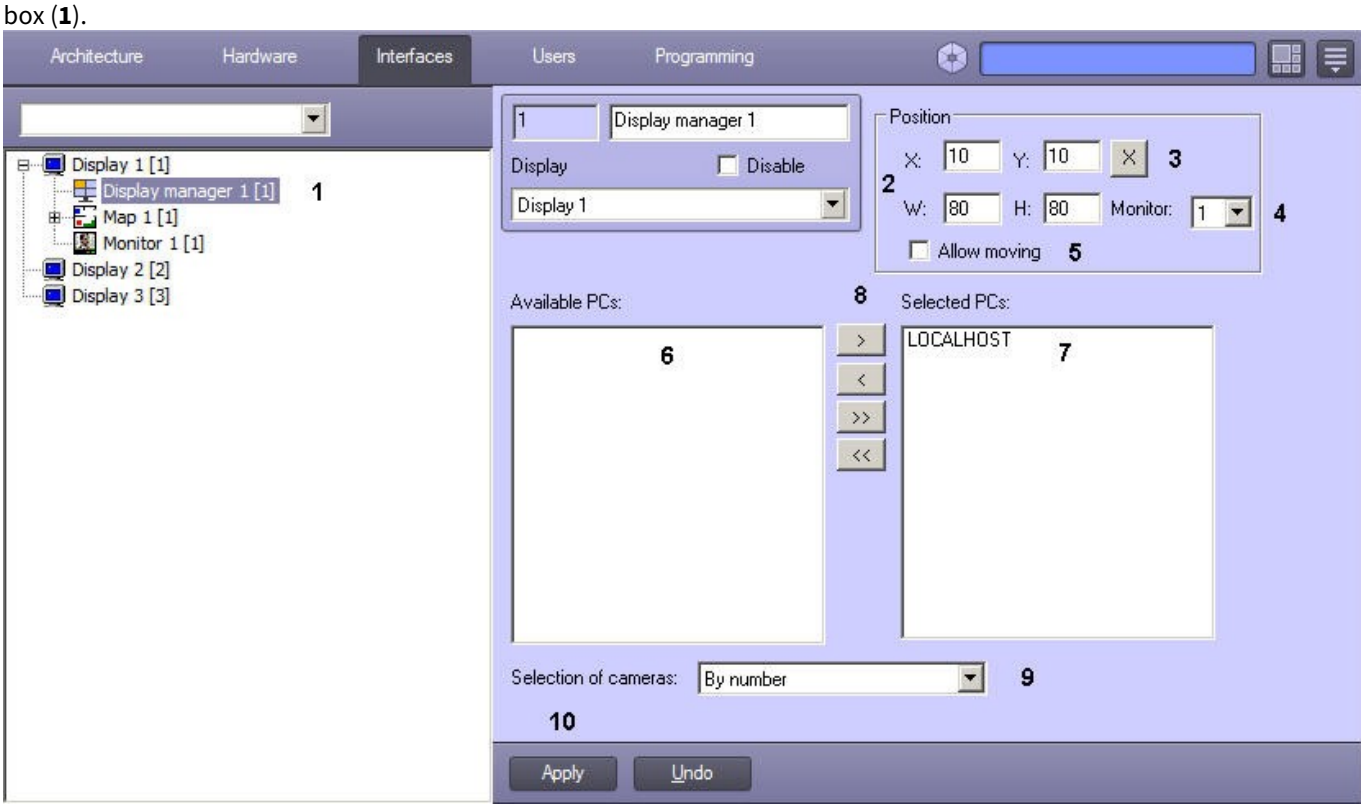
Setting up the voice notification using **Sound notification** object is completed.

23.4.14 Configuring the Display manager

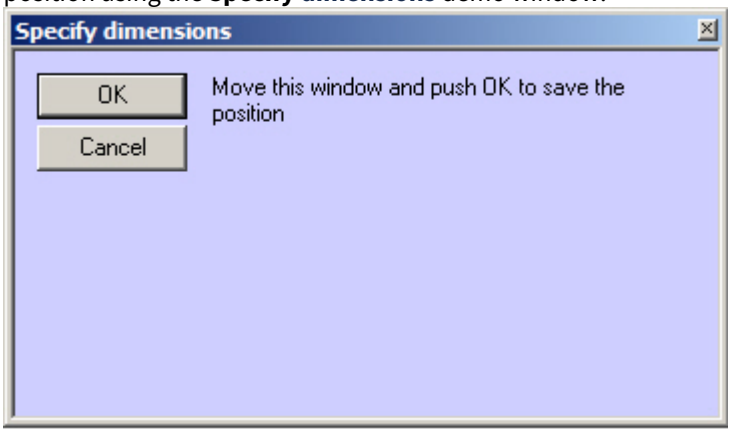
The **Display manager** interface object is designed to manage the video walls. It allows the Operator to conveniently configure the Video surveillance monitor layouts on the specified computers.

The **Display manager** object is configured as follows:

1. Create a **Display manager** object on the basis of the **Display** object on the **Interfaces** tab of the **System Settings** dialog box (**1**).



2. The settings panel of this object will appear in the right part of the **System Settings** dialog box.
3. Set the **Display manager** window size and position manually (**2**), or click the **X** button (**3**) and specify the window size and position using the **Specify dimensions** demo window:



After the window size and position are set, click **OK**.

4. From the **Monitor** drop-down list (**4**), select the number of the computer monitor on which the **Display manager** window should be displayed.
5. If it is necessary to allow the Operator to move the **Display manager** interface window, set the **Allow moving** checkbox (**5**).
6. Select the computers which screens should be managed from the **Display manager**. To do this, select the required computers in the **Available PCs** list (**6**) and click the **>** (**8**) button to move them to the **Selected PCs** list (**7**). All available computers can be moved to the list of selected ones at once by clicking the **>>** button.
   To move the computers from the **Selected PCs** list back to the **Available PCs** list, use the **<** and **<<** buttons respectively.

   > **Note.**
   >
   > Add to this list computers on which the video signal is displayed on the Video Surveillance monitor. For example, if there is a **Server** computer in a distributed system with corresponding **Camera** objects created under it, and there is also a **Client** computer to which a **Display** with a **Monitor** is assigned while cameras from the **Server** are selected in that **Monitor**, then you should add the **Client** computer to the **Selected PCs** list.

7. Select the sorting method for the cameras list: **By number** or **By name** (**9**).
8. Click the **Apply** button (**10**).

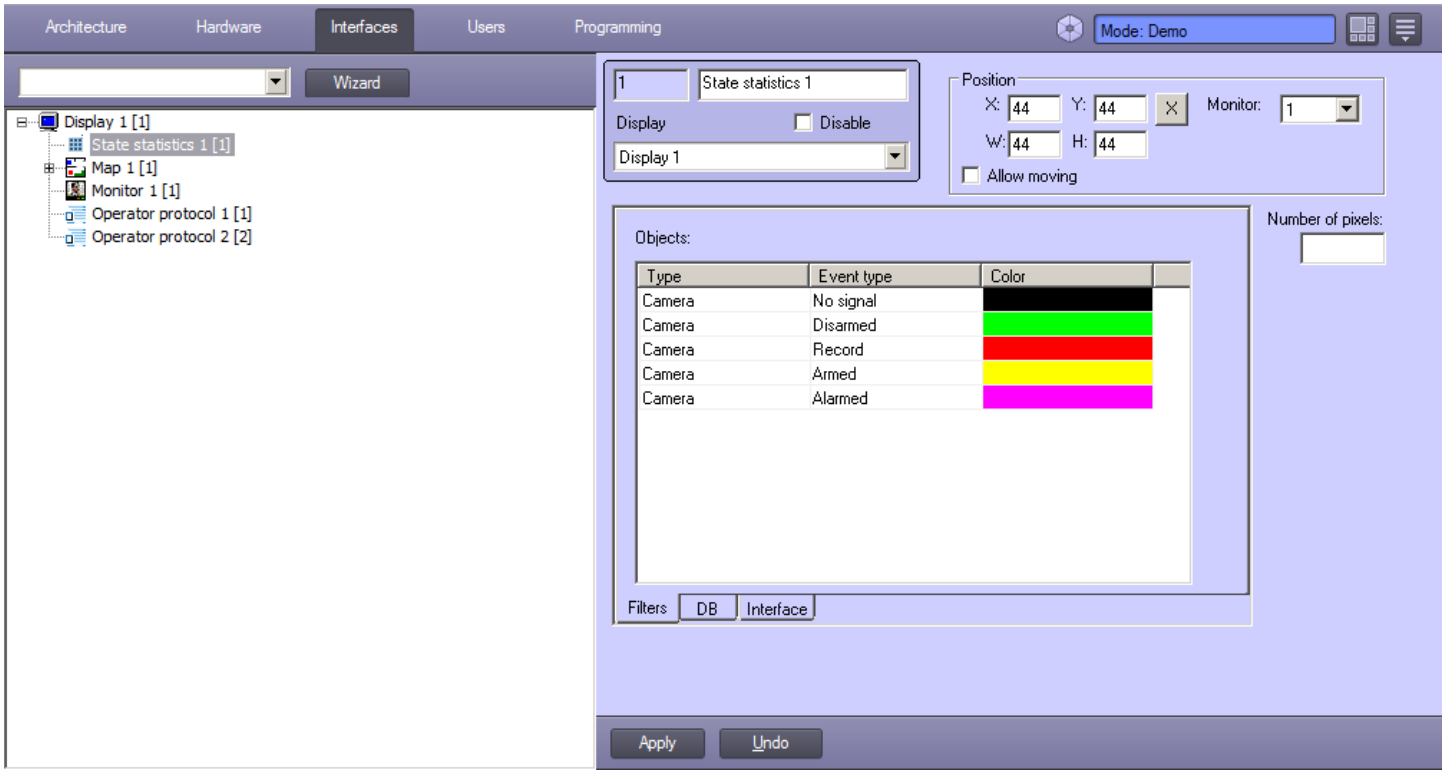
Configuring the **Display manager** interface object is complete.

Managing the displays using the Display manager

23.4.15 Configuring the State statistics display

The **State statistics** interface object is designed to monitor the states of selected system objects.

This object is created on the basis of the **Display** object on the **Interfaces** tab of the **System Settings** dialog box.



The **State statistics** display is configured in the following order:

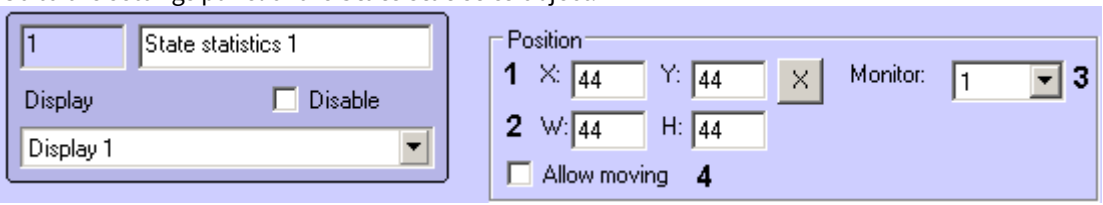
1. Configuring the State statistics window position on the screen
2. Selecting the objects to be included in State statistics and configuring the points number
3. Configuring the database connection

4. Configuring the interface parameters of the State statistics window

23.4.15.1 Configuring the State statistics window position on the screen

The **Status statistics** interface window position on the screen in configured as folows:

1. Go to the settings panel of the **State statistics** object.



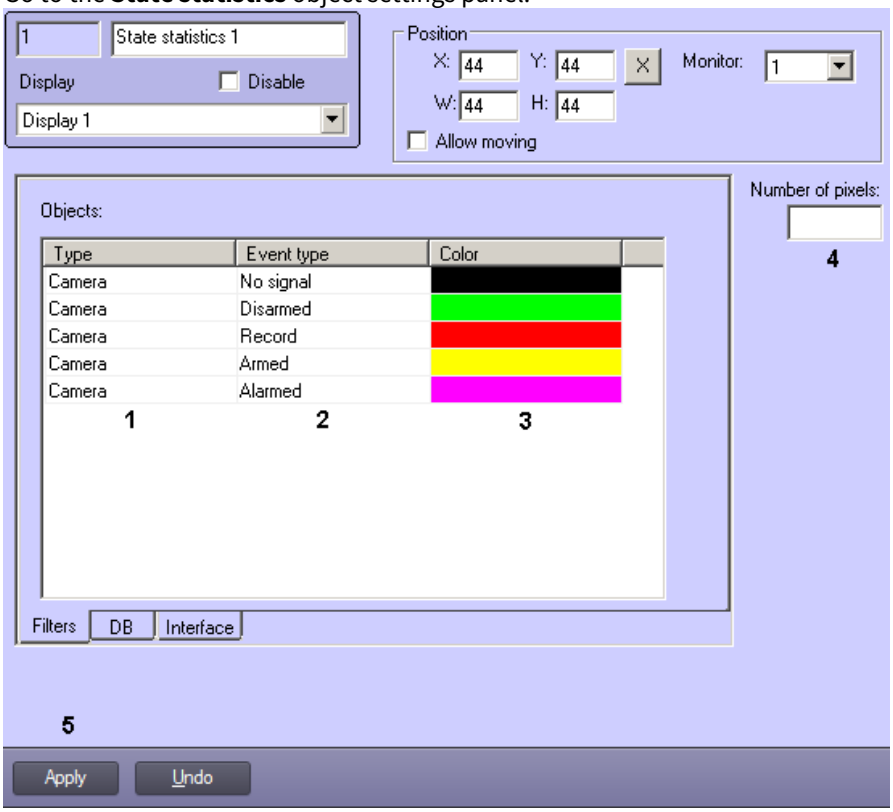
2. In the **X** and **Y** fields (**1**), specify the coordinates of the upper left corner of the interface window.
3. In the **W** and **H** fields (**2**), specify the width and height of the interface window.
4. From the **Monitor** drop-down list (**3**), select the physical monitor where the interface window should be displayed. The monitors are numbered in the order of physical placement from left to right and from top to bottom, regardless of the operating system numbering.
5. Set the **Allow moving** check box (**4**) to allow the Operator to change the **State statistics** window position.
6. Click **Apply** to save the settings.

Configuring the **State statistics** interface window position on the screen is complete.

23.4.15.2 Selecting the objects to be included in State statistics and configuring the pixels number

Selecting the objects to be included in **State statistics** and configuring the pixels number is performed as follows:

1. Go to the **State statistics** object settings panel.



2. From the **Type** drop-down list (**1**), select the object type.
3. From the **Event type** drop-down list (**2**), select the state of objects of the selected type which should be included in the statistics. If the state is not selected, then the statistics on all states will be displayed.
4. From the **Color** drop-down list (**3**), select the color to highlight the selected state in the table and the graph in the **State statistics** window .
5. In the **Number of pixels** field (**4**), enter the number of pixels to be displayed on the graph.

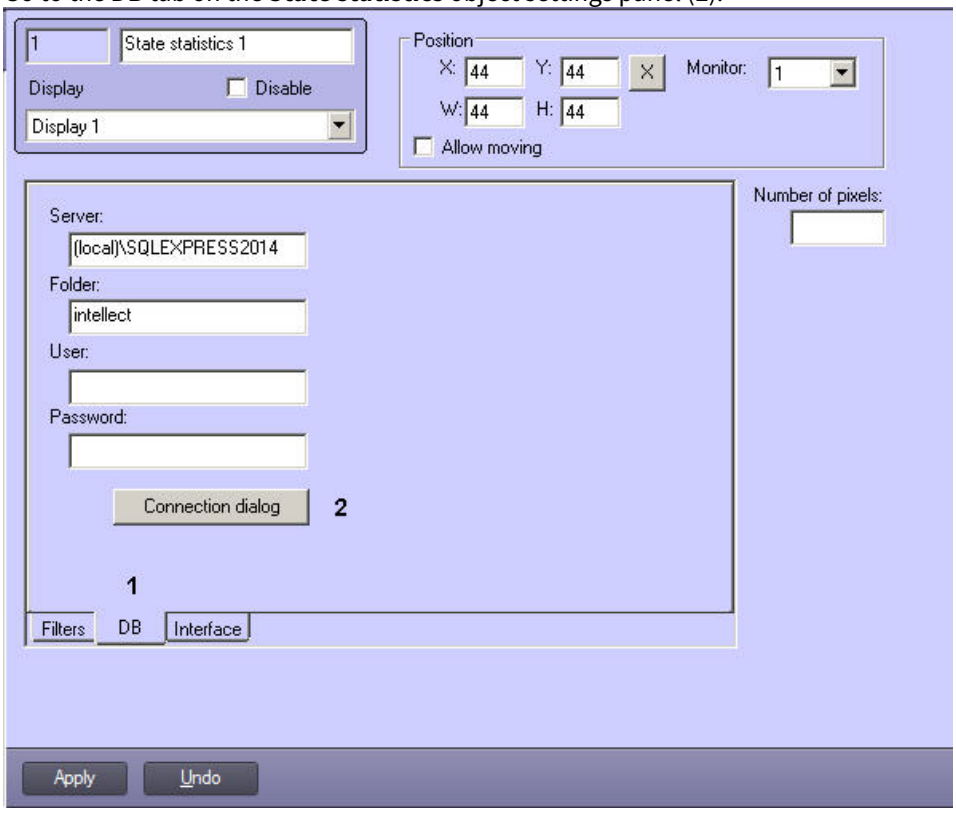
6. Click **Apply** (**5**).

Selecting the objects to be included in **State statistics** and configuring the pixels number is complete.

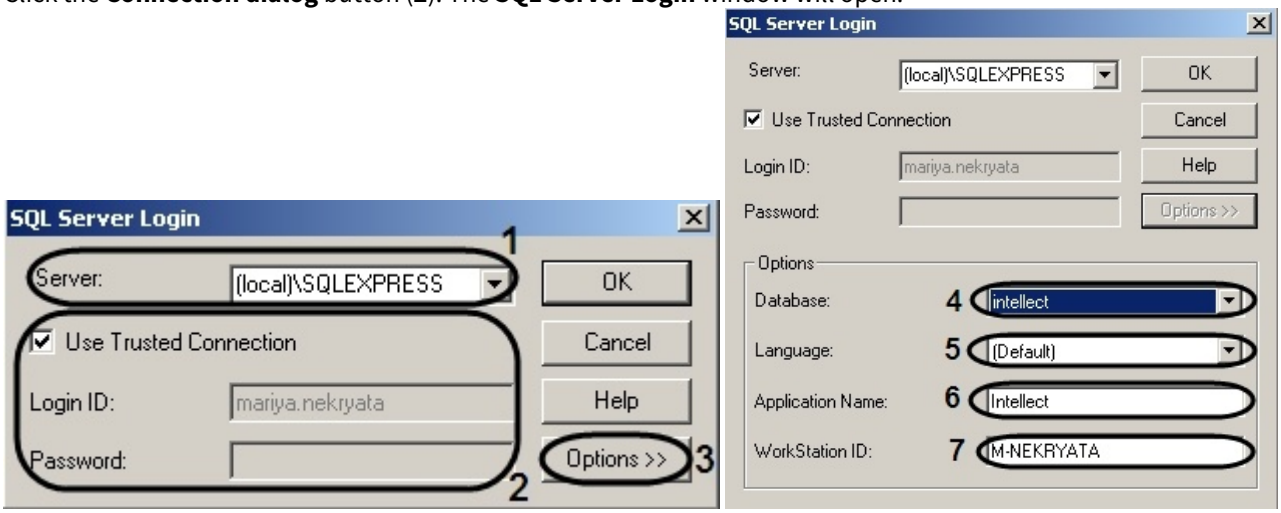
23.4.15.3 Configuring the database connection

By default, the *Intellect* local database is used as a data source for the State statistics displaying. In order to use a remote database, configure the connection to it as follows:

1. Go to the **DB** tab on the **State statistics** object settings panel (**1**).



2. Click the **Connection dialog** button (**2**). The **SQL Server Login** window will open.



3. In the **Server** list, specify the SQL server to connect to (**1**).

> **Note**
>
> If the **Server** list contains the required SQL server, then no further connection configuration is needed.

> **Note**
>
> When working in a distributed configuration, it is necessary to specify the computer name where the database is located, without using the value (local). For example, "WS1\SQLEXPRESS", where WS1 is the name of the computer where the database is located.

4. If it is necessary to enter the login and password for the SQL server authorization, unset the **Use trusted connection** checkbox (**2**). As a result, the **Login ID** and **Password** fields will become editable.

> **Note**
>
> If the **Use trusted connection** check box is set, then the SQL server authorization will be performed using the Windows credentials.

5. To specify the additional connection parameters, click the **Options >>** button (**3**).
   a. In the opened field, from the **Database** list (**4**), select the database where the events should be stored.
   b. From the **Language** list (**5**), select the language of the SQL server system messages.
   c. In the **Application Name** field (**6**), enter the application name (the default one is *Intellect*).
   d. In the **Workstation ID** field (**7**), enter the computer name (the default one is the computer identifier in Windows OS).
6. Click **OK** to save the settings.

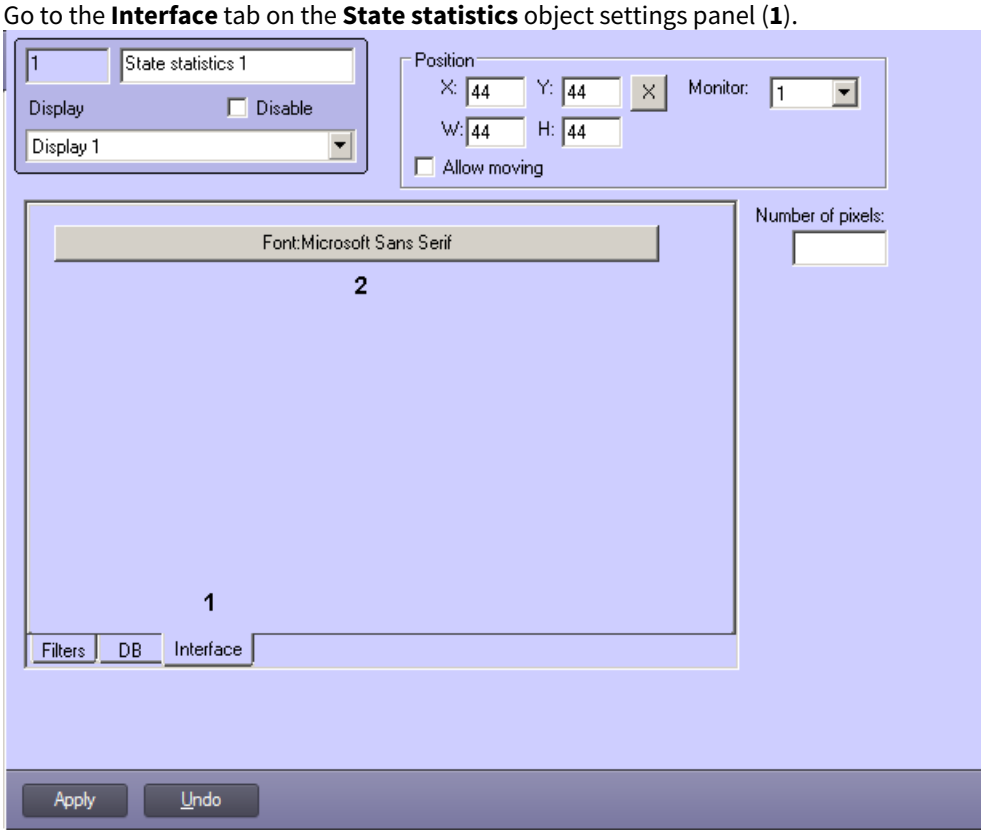
> **Note**
>
> For the help information about the **Login to SQL Server** dialog box, click the **Help** button.

Setting up database connection is complete.

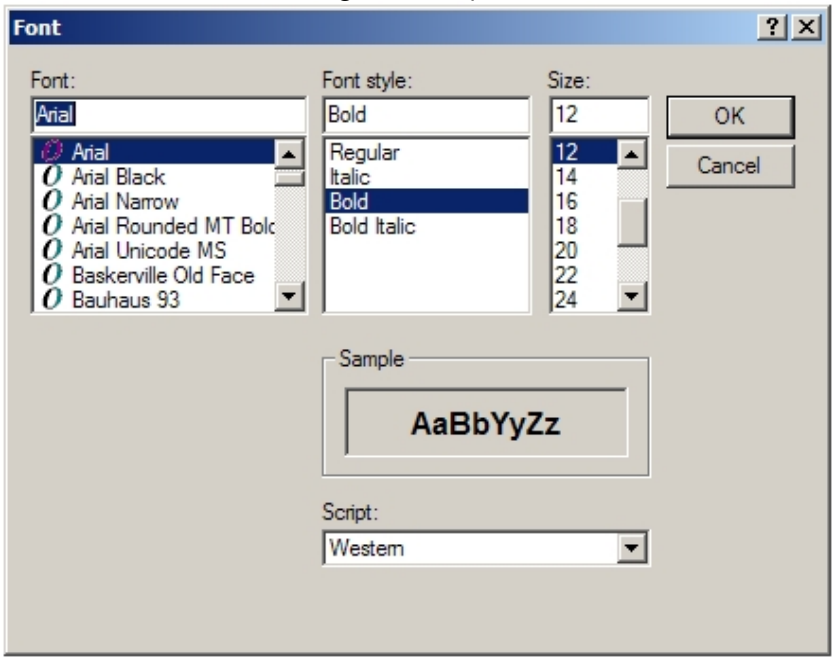
23.4.15.4 Configuring the interface parameters of the State statistics window

Configuring the interface parameters of the **State statistics** window means selecting the text font for the table and the graph (except for the legend). To select a font, do the following:

1. Go to the **Interface** tab on the **State statistics** object settings panel (**1**).



2. Click the **Font** button (**2**).
3. In the standard Windows dialog box that opens, select the font name, size, and style.



4. Click **OK**.
5. Click **Apply** to save the settings (**3**).

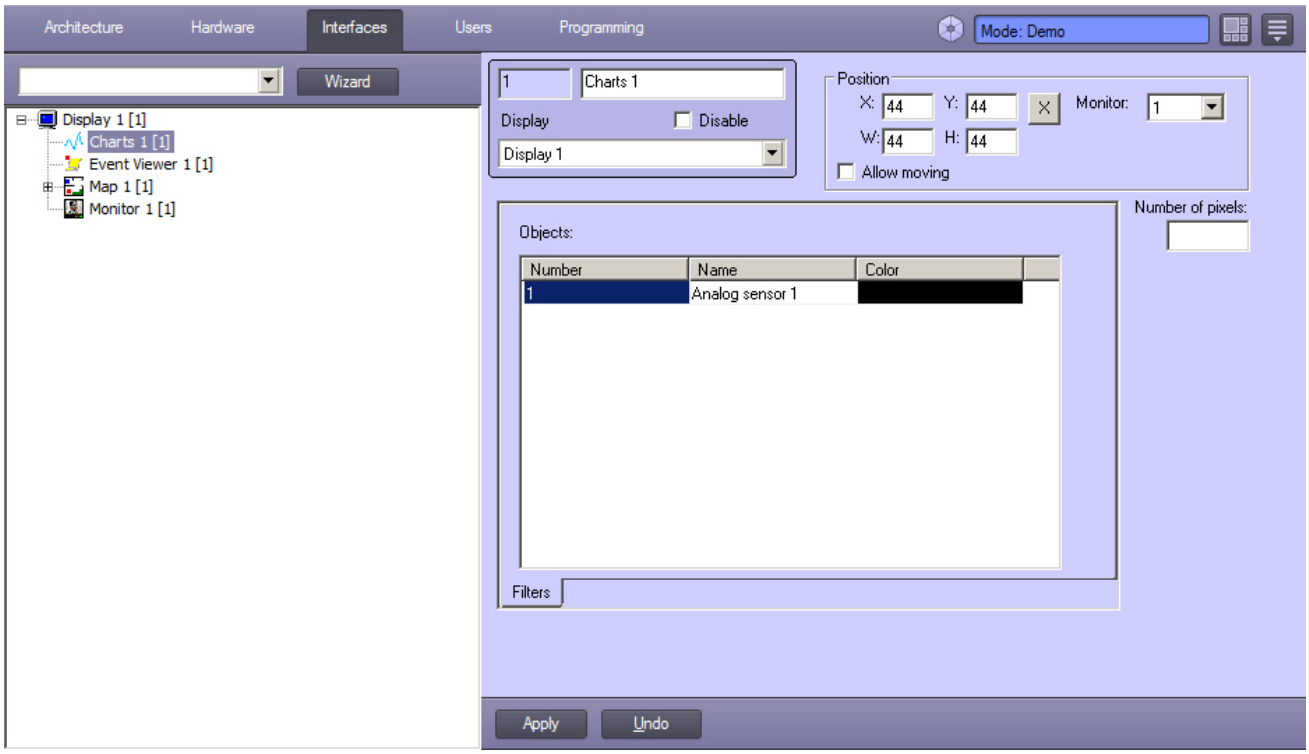
Configuring the interface parameters of the **State statistics** window is complete.

23.4.16 Configuring the Charts to display analog sensor readings

The *Intellect* software allows displaying data from the analog sensors (such as temperature humidity, etc. sensors) on a chart. For example, this function is available for the Tibbo sensor/relay cards integrated via Drivers Pack. Please check the Drivers Pack Documentation to find out if the analog sensors can be used for a particular device.

Create and configure all required analog sensors before configuring Charts – see Creating and configuring connection with the Analog sensor (input).

The analog sensor readings chart is configured on the **Charts** object settings panel. This object is created under the **Display** object on the **Interfaces** tab of the **System Settings** dialog box.



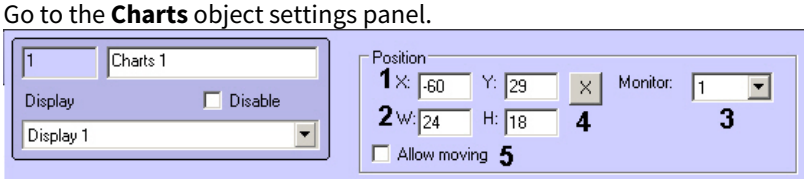
The analog sensor readings chart is configured in the following order:

1. Setting the Charts window position on the screen.
2. Selecting objects to display on chart and setting the number of points.

23.4.16.1 Setting the Charts window position on the screen

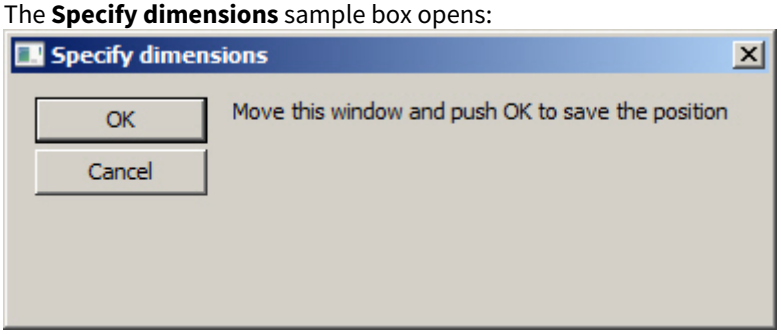
Set the **Charts** window position on the screen as follows:

1. Go to the **Charts** object settings panel.



2. There are two options to sen the window coordinates:
   a. Manually:
      i. Set the interface window top left corner coordinates as a percentage of the screen size in the **X** and **Y** fields (1).
      ii. Set the interface window width and height as a percentage of the screen size in the **W** and **H** fields (2).
      iii. Select physical monitor of the computer to display interface window from the **Monitor** drop-down list (3). The monitors are numbered as they are positioned physically from the left to the right and from the top to the bottom regardless the numbering in the operating system.
   b. With a sample box:
      i. Click the **X** button (4).

ii. The **Specify dimensions** sample box opens:



iii. Drag the **Specify dimensions** box to the position where the **Charts** interface window should be and stretch to desired size.
iv. Click **OK** to confirm.
v. The **X**, **Y**, **W, H** and **Monitor** fields are filled automatically according to the position set.

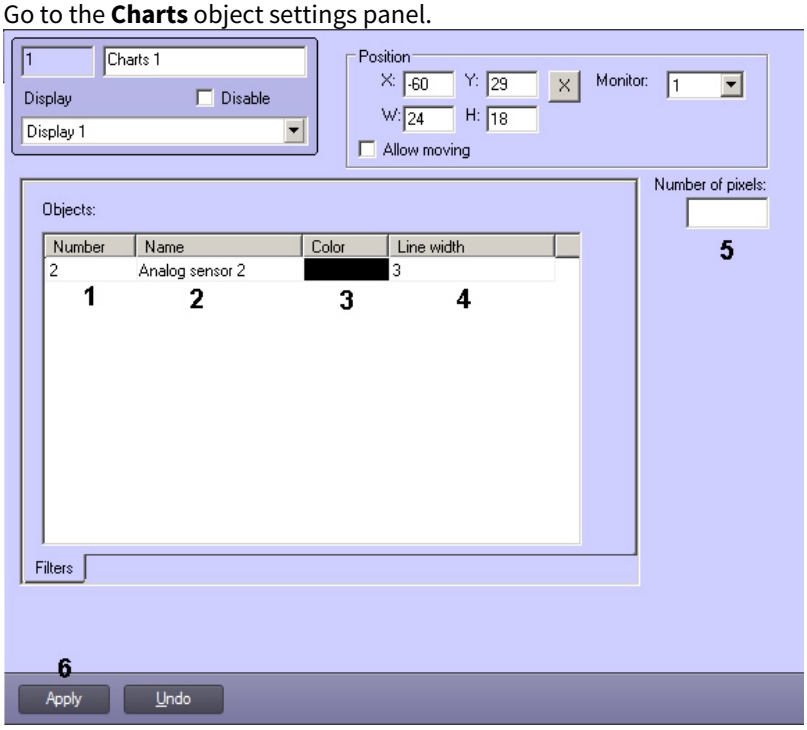
3. If an Operator should be able to move the **Charts** window on the screen, set the **Allow moving** checkbox (5).
4. Click **Apply** to save settings.

Setting the **Charts** window position on the screen is now complete.

23.4.16.2 Configuring the chart display

Select objects to display on the chart and set the number of points as follows:

1. Go to the **Charts** object settings panel.



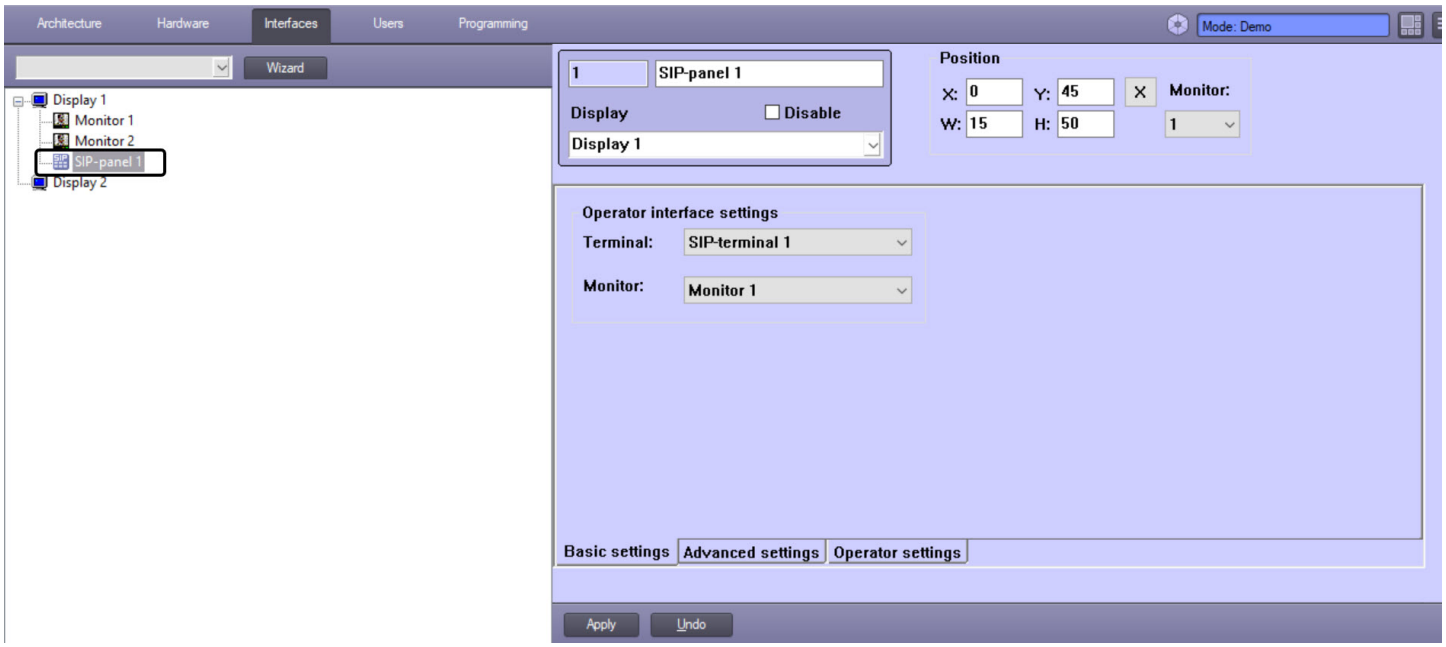
2. From the **Number** drop-down list, select the **Analog sensor** object ID according to the preset analog sensor (1). See also Creating and configuring connection with the Analog sensor (input).
3. The **Name** is filled automatically after ID selection (2).
4. From the **Color** drop-down list, select the color to mark the sensor readings on the chart in the **Charts** window (3).
5. In the **Line width** field, enter the line width in pixels (4). The value must be integer: if you enter an incorrect value, the default line width (5 pixels) is applied.
6. In the **Number of pixels** field, set the number of points to display on the chart (5).
7. Click **Apply** (6).

Selecting objects to display on the chart and setting the number of points is now complete.

23.4.17 Configuring the SIP-panel interface object

The **SIP-panel** interface object is used to work with SIP-devices in *Intellect* (see SIP-panel). For details about configuring these devices, see Configuring SIP-terminal.

Operator microphone, speaker and camera should also be selected on the **Computer** object settings panel for the SIP-panel operation – see Selecting speaker, microphone and camera for SIP-operator.



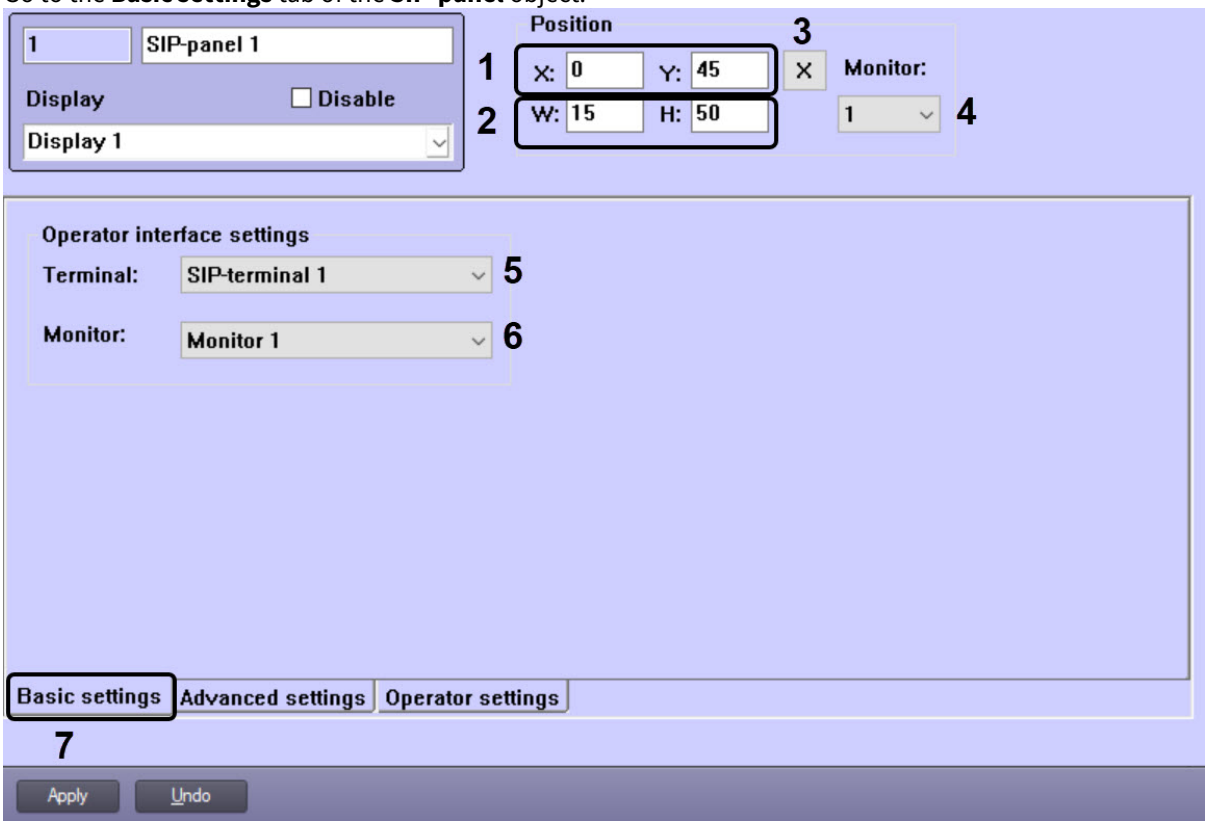
Note.

By default, the SIP-device will be disconnected if during a call you hide or change the screen with the SIP-panel. To prevent this, set the **1** value for the **NotEndCallWhenDeactivate** registry key (for details, see Registry keys reference guide).

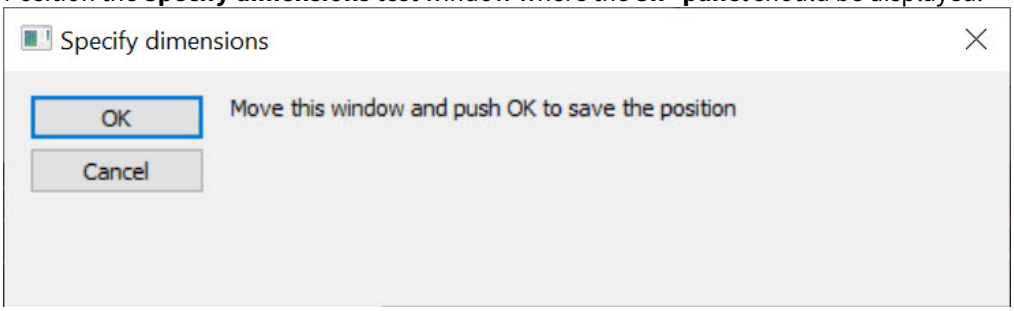
23.4.17.1 Basic settings of the SIP-panel interface object

The **SIP-panel** is configured as follows:

1. Go to the **Basic settings** tab of the **SIP-panel** object.



2. Set the coordinates of the **SIP-panel** interface window in one of the following ways:
   a. Manually:
      i. Set the coordinates of the upper left corner of the interface window: the **X** (horizontal indent from the left edge of the screen) and **Y** (vertical indent from the upper edge of the screen) fields. The coordinates are expressed as a percentage of the horizontal and vertical screen dimensions, respectively (**1**).
      ii. Set the dimensions of the interface window: the **W** (window width) and **H** (window height) fields. The dimensions are expressed as a percentage of the horizontal and vertical screen dimensions, respectively (**2**).
   b. Using the test window:
      i. Click the **X** button (**3**).
      ii. Position the **Specify dimensions** test window where the **SIP-panel** should be displayed.



      iii. Click the **OK** button. As a result, the coordinates in the **X, Y, W, H** fields will be set according to the dimensions and position of the test window.
3. From the **Monitor** drop-down list (**4**), select the computer monitor on which the interface window will be displayed.
4. From the **Terminal** drop-down list (**5**), select the SIP-terminal object which SIP-devices use the SIP-panel.

> **Note**
>
> Each Server/Remote Client should have its own display with its own SIP-panel (see Assigning the displays to the operator workstations). If the display with this SIP-panel is already selected for any computer, the **Terminal** drop-down list will be inactive. It is necessary to fix the incorrect configuration of the Server/Remote Client.

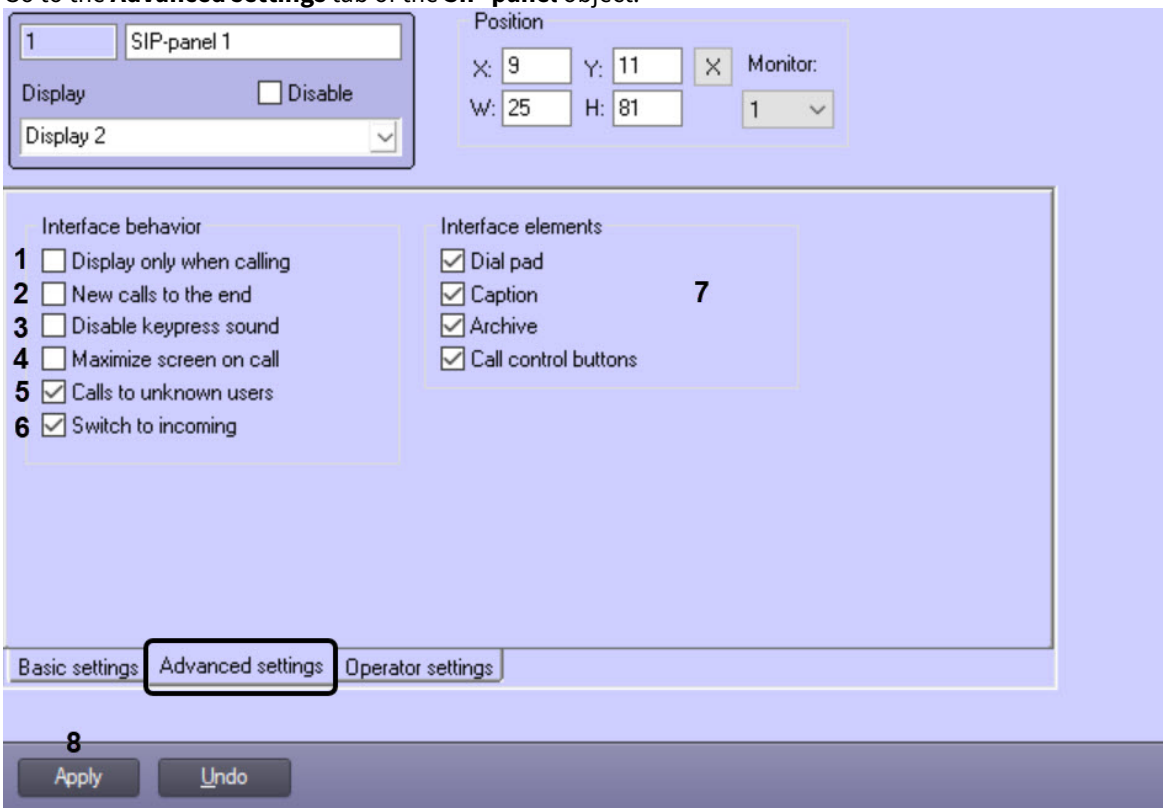
5. From the **Monitor** drop-down list (**6**), select the **Monitor** object corresponding to the Video Surveillance Monitor to which the video cameras associated with the corresponding SIP-devices are added. For details, see Selecting and configuring video cameras.
6. Click the **Apply** button (**7**).

The basic settings of the **SIP-panel** interface object are now configured.

23.4.17.2 Advanced settings of the SIP-panel interface object

The advanced settings of the SIP-panel are configured as follows:

1. Go to the **Advanced settings** tab of the **SIP-panel** object.



2. If it is necessary to display the SIP-panel only during a call, set the **Display only when calling** checkbox (**1**).
3. If new calls should be added to the end of the list on the SIP-panel, set the **New calls to the end** checkbox (**2**). By default, new calls are added to the top of the list.
4. To turn off sound when pressing the keys on the SIP-panel, set the **Disable keypress sound** checkbox (**3**).
5. To display the screen to which the SIP-panel is added when making a call, set the **Maximize screen on call** checkbox (**4**). If this checkbox is not set, there is a chance to miss a call to the SIP-panel when the corresponding screen is hidden.
6. If it is necessary to enable the option to call unknown subscribers, set the **Calls to unknown users** checkbox (**5**).

> **Note**
>
> Unknown subscriber is a number that is present in the SIP-terminal, but not present in the address book of the current SIP-operator.

7. If it is necessary to automatically switch to the SIP-panel tab with the incoming calls, set the **Switch to incoming** checkbox (**6**). By default, the checkbox is set. Automatic switching happens at incoming calls or calls on hold.
8. Set the checkboxes for the elements that should be displayed in the SIP-panel interface (**7**).
9. Click the **Apply** button (**8**).

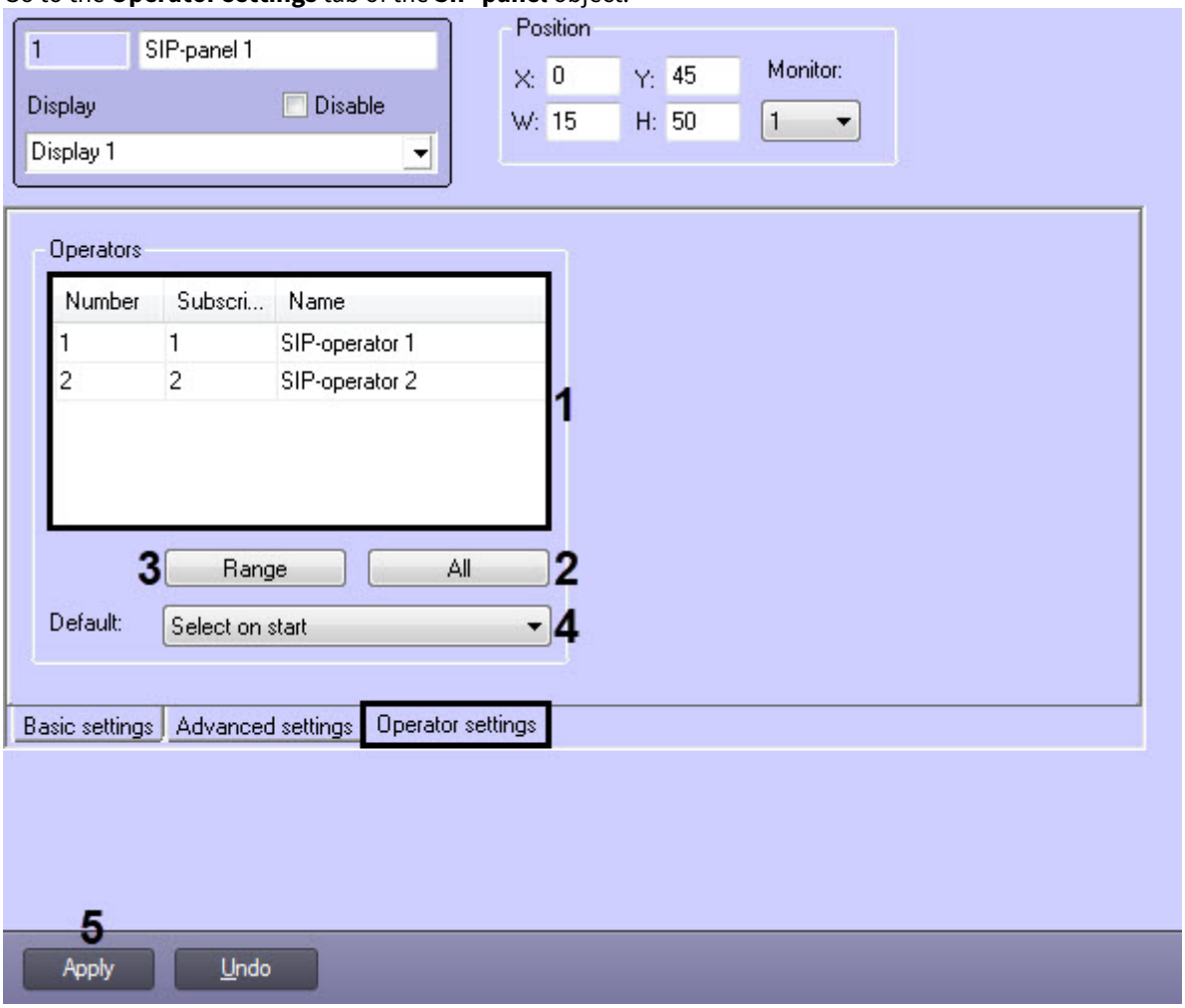
The advanced settings of the SIP-panel are now configured.

23.4.17.3 Operator settings of the SIP-panel interface object

On the **Operator settings** tab, you can specify a default operator and a list of operators who can work with this SIP-panel.

Operator settings of the SIP-panel are configured as follows:

1. Go to the **Operator settings** tab of the **SIP-panel** object.

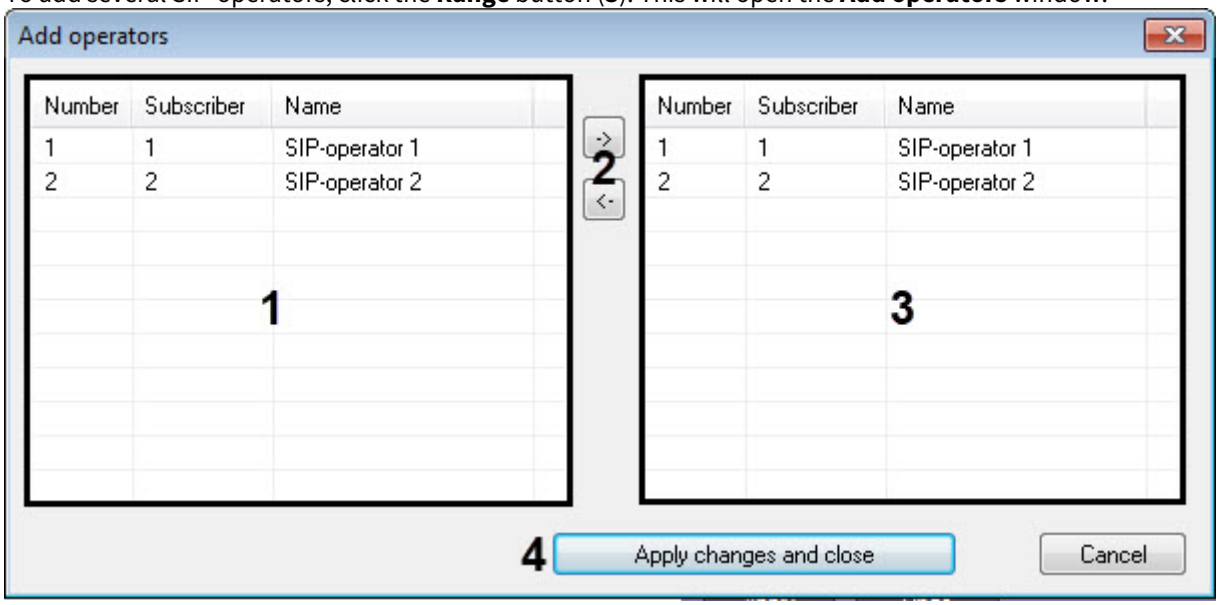


2. In the **Operators** table (**1**), select the required SIP-operators who can work with this SIP-panel:

> **Note**
>
> To add new lines to the table, use the Down key on your keyboard. To delete a line, use the Ctrl+Del key combination.

   a. To add all SIP-operators, click the **All** button (**2**).

b. To add several SIP-operators, click the **Range** button (**3**). This will open the **Add operators** window.



i. Select the required SIP-operators from the left list (**1**) and use the buttons (**2**) to move them to the right list (**3**).
ii. Click the **Apply changes and close** button (**4**).

3. From the **Default** drop-down list (**4**) select the default SIP-operator:
   a. **Select on start** – when you first start the SIP-panel, it is necessary to select the appropriate SIP-operator in the authorization window. Next time, you will be logged in under the previously selected SIP-operator.
   b. **User rights** – the SIP-panel will be logged in under the SIP-operator that is linked to the *Intellect* user rights. There should be the registration in *Intellect* with the rights of the corresponding user.
   c. **SIP-operator from the list** – the SIP-panel will be logged in under the selected SIP-operator.

> **Note**
>
> Selecting a SIP-operator from the list is available if the display is enabled for only one computer of the video surveillance system (see Assigning the displays to the operator workstations).

4. Click the **Apply** button (**5**).

Operator settings of the SIP-panel are now configured.

23.5 Configuration of users and permissions

23.5.1 Rights administration

23.5.1.1 The users' rights

The following user categories are available in the surveillance system based on the Intellect software:

1. Administrator.
2. Operator who may optionally be granted some rights for administration, control and viewing.

> **Important!**
>
> Make sure to register Administrator for the full and secure use of the users' rights and permissions. If the Administrator password is not registered in the system, in some cases, users with limited permissions can access all the functions of the system.
> See Administrator password registration for details on registering Administrator password.

The administrator has full control over the set up and usage of all components of the system.

Any other registered user of the system is an operator who may optionally be granted the rights for administration, controlling and viewing of particular components of the system.

To register an operator, a user account is created which holds this user's rights for administration, control and viewing. A password is assigned to each user at the time of registration, used for authorization at system start-up and exit. An operator may be optionally forbidden to shut the system down.

23.5.1.2 User registration and removal

23.5.1.2.1 General information about user registration in Intellect software

The registration procedure depends on the user category.

To register an administrator, an administrator password should be specified. An administrator password gives access to administrative functions of all system components. Only one administrator password may be registered in the system.

No account is created for the administrator, so the administrator password cannot be used for authorization on system start-up. The administrator password is used to access the **System Settings** window and the settings panels of system objects, to change the current user and to shut the system down.

To register operators, the corresponding accounts should be created. A **Person** system object is created for each operator account. Each operator has his (her) own user account which holds all the data about the rights and authorization password.

The account also indicates to which department the operator belongs. A **Department** system object is created for each department of the company.

The **Department** and **Person** objects form a hierarchy of two levels.

23.5.1.2.2 User registration procedure

The following user registration procedure is recommended for setting up the system:

1. Administrator password registration.

   Note.

   You must register the administrator password prior to registering the operators and granting the rights to them. This is a mandatory system requirement.

2. Registering departments by creating the **Department** objects.
3. Registering operators by creating the **User** objects.

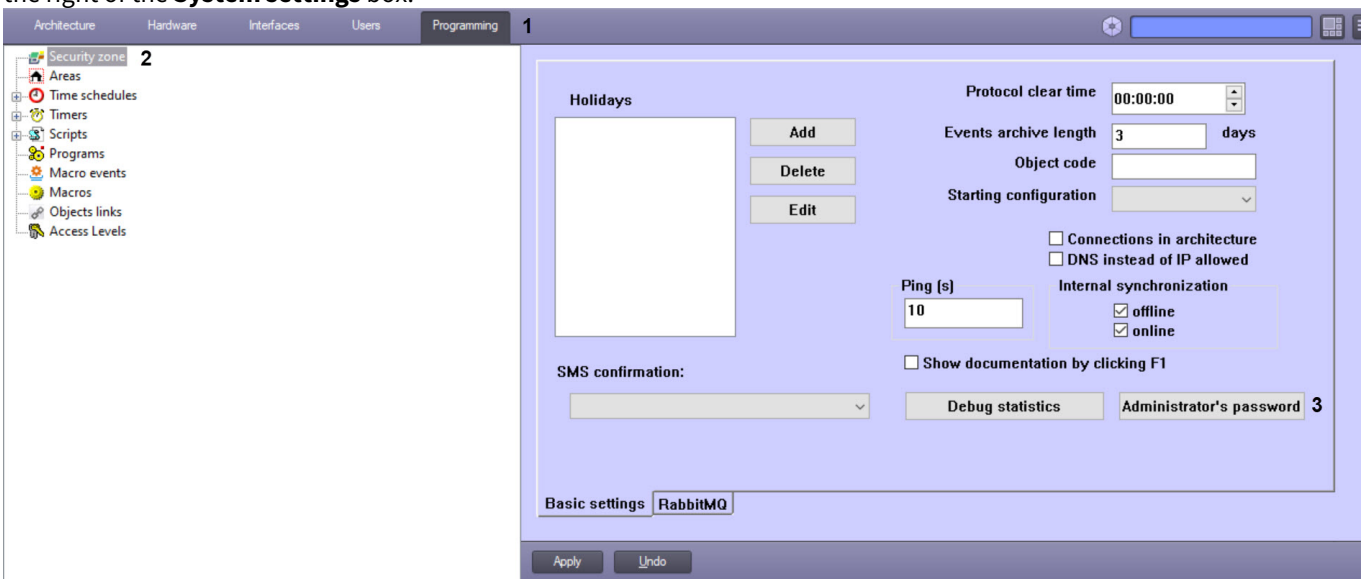
23.5.1.2.3 Administrator password registration

The administrator password gives access to administrative functions of all system components. Only one administrator password can be registered in the system. The administrator password is to be registered on the administration server when the system is configured.

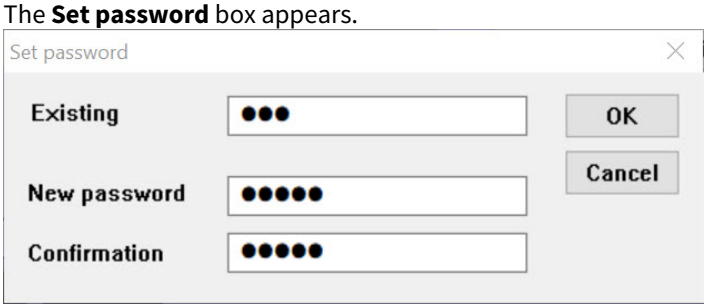
To register the administrator password, do the following:

1. Go to the **Programming** tab in the **System setting**s dialog box (**1**).

2. Select the **Security zone** object in the objects tree of the **Programming** tab (**2**). The settings panel for this object opens on the right of the **System settings** box.



3. Click the **Administrator's password** button (**3**).
4. The **Set password** box appears.

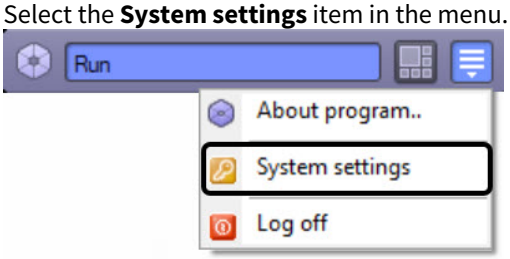


5. Specify the existing administrator's password in the **Existing password** field. If there is no administrator's password, this field is left empty
6. Type in the sequence of letters and figures that will be used as administrator's password in the **New password** field.
7. Retype in the new administrator's password in the **Confirmation** field.
8. Click the **OK** button. The **Set password** box is closed.
9. Click the **Apply** button in the **System settings** box.

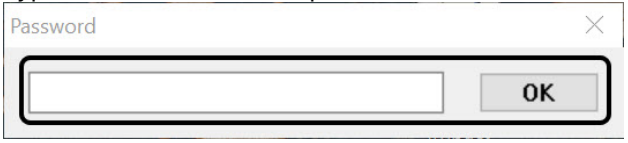
The administrator's password is now registered.

When the administrator's password is registered one with restricted access rights can access the **System settings** dialog box:

1. Call the **Main** control panel.
2. Press the Ctrl key on the keyboard.
3. Select the **System settings** item in the menu.



4. Type in the administrator's password and click the **OK** button.



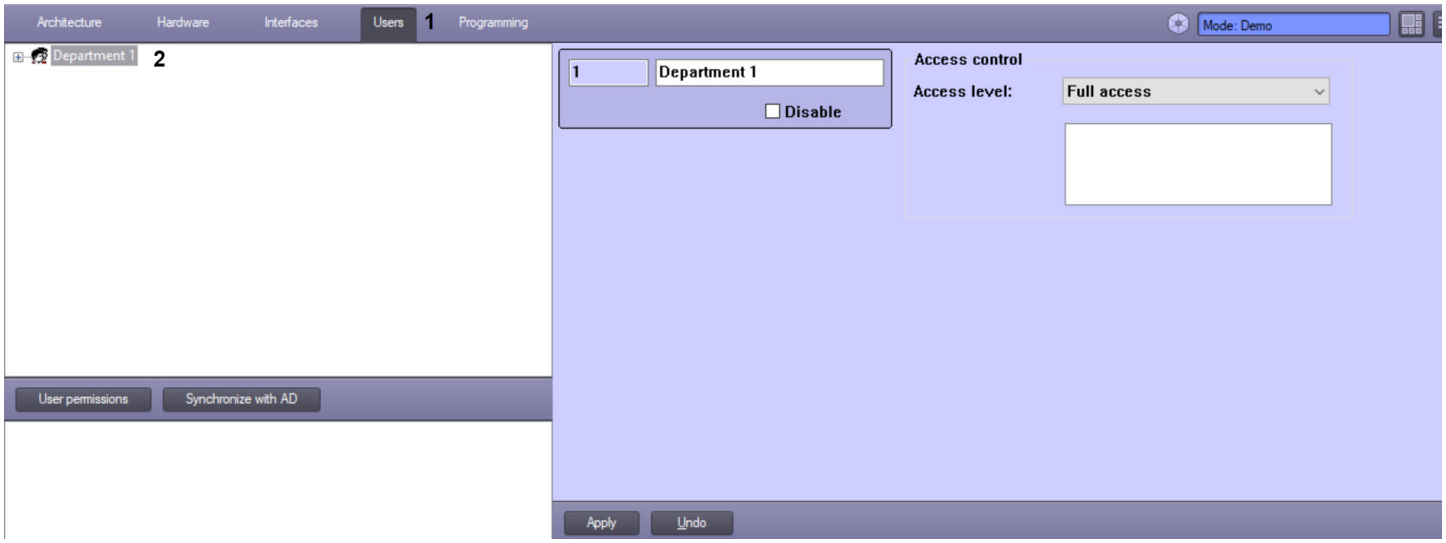
23.5.1.2.4 Department registration

To register departments, the **Department** objects should be created. The **Department** account consists of the department name and the list of its employees.

A separate account is created for each department. To register a department account, do the following:

1. Open the **Users** tab in the **System Settings** window (**1**).
2. Create a **Department** object in the objects tree of the **Users** tab (**2**).

The settings panel for this object opens on the right of the **System settings** box.



This completes registration of the department account.

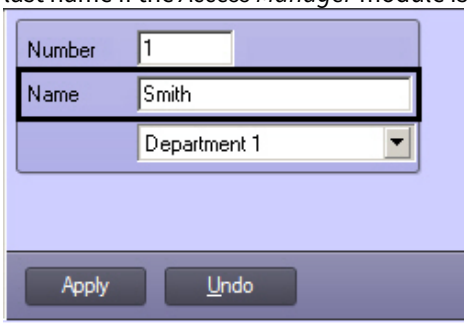
> **Note**
>
> Settings on the settings panel of the **Department** object are used to configure the access control system (see Visitor Management System Module Settings and Operation Guide).

23.5.1.2.5 Registration of Operator accounts

To register Operator accounts, the **User** objects are to be created.

An individual account is to be created for each Operator. To register an Operator account, do the following:

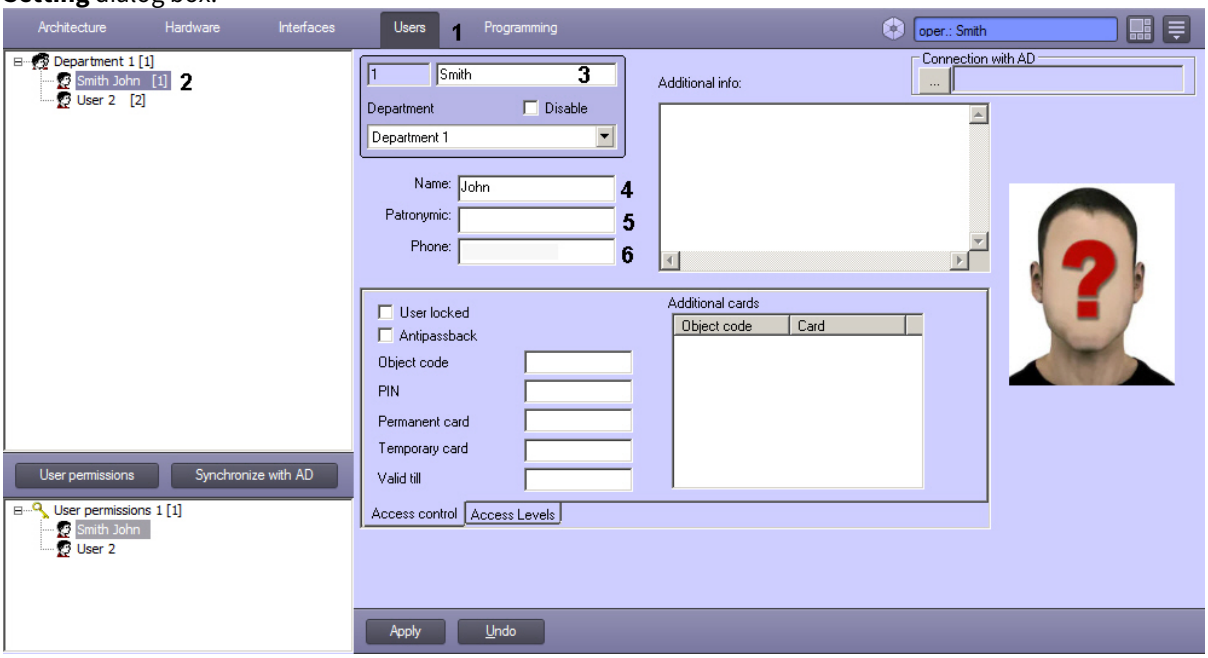
1. Open the **Users** tab in the **System Settings** dialog box (1).
2. Create a **User** object under the **Department** object in the objects tree (2). In the **Name** field enter the username (the user's last name if the *Access Manager* module is in use).



> **Note.**

Do not use **rs** as username when registering Operator accounts as this name is used by default in *Intellect Web Report System*. If the user with such name is careted in *Intellect*, then the error can occur when *Intellect Web Report System* is started.

3. The created object appears in the objects tree, and the settings panel for this object opens on the right side of the **System Setting** dialog box.



4. You can change username if necessary (3).
5. Set user's **Name** (4) and/or **Patronymic** (5) if needed.
6. If two-factor authentication is to be configured in the system, enter user phone number in the **Phone** field (6). See also Configuring two-factor authentication.
7. Click **Apply** or go to the settings panel of another object.

Note.

If user's name or patronymic is specified, it is displayed in the tree along with the last name (2).

The operator account is now registered.

Note.

The settings of the **User** object are intended to configure the access control system. They are usually set using the *Access Manager* module in the *ACFA Intellect* subsystem (see Access Manager Module Settings and Operation Guide). In the *Access Manager* you can also add the photo displayed on the **User** object settings panel.
Face recognition and search interface being part of *Face-Intellect* software also allows adding and editing user's photo (see *Face-Intellect* documentation in AxxonSoft documentation repository for details on its setting up and configuration).

23.5.1.2.6 Removing user accounts

The removal procedure depends on the user category.

To remove operator accounts, delete the corresponding **User** objects from the objects tree of the **Users** tab.

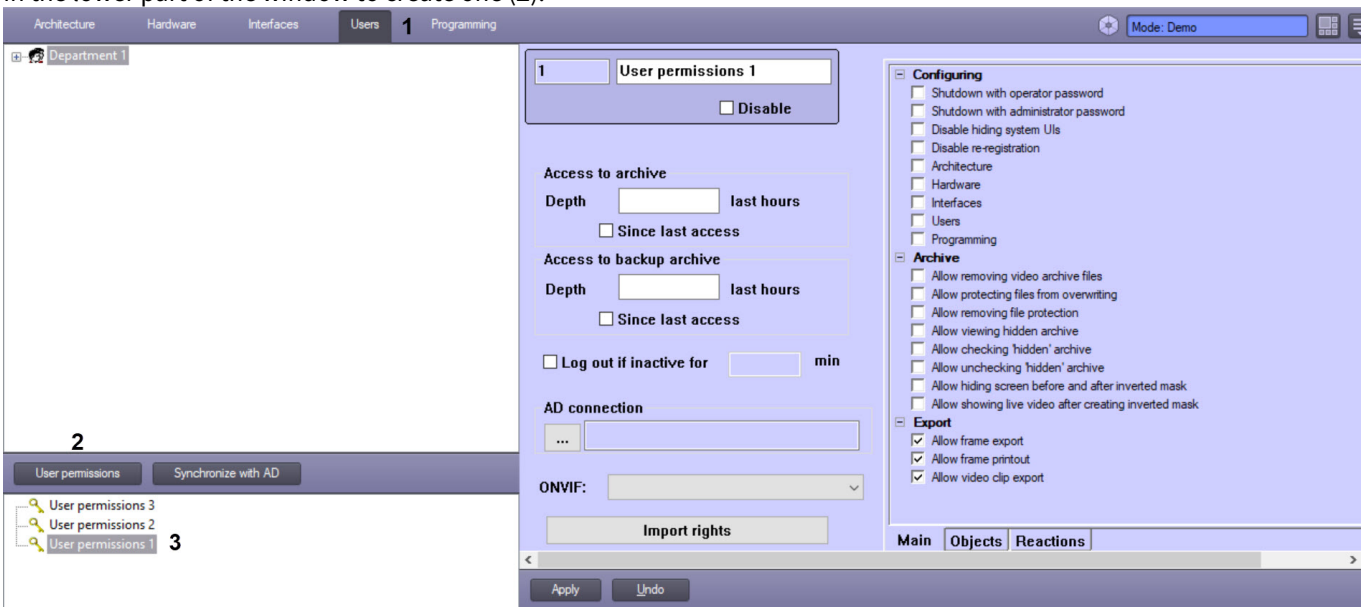
To remove the administrator account, remove the administrator password. The administrator password is removed in the same way as it is created (see Administrator password registration). To remove the administrator password, specify the current Administrator password in the **Existing Password** field and then clear the **New Password** and **Confirmation** fields in the **Set Password** box.

23.5.1.3 Registration of users' rights

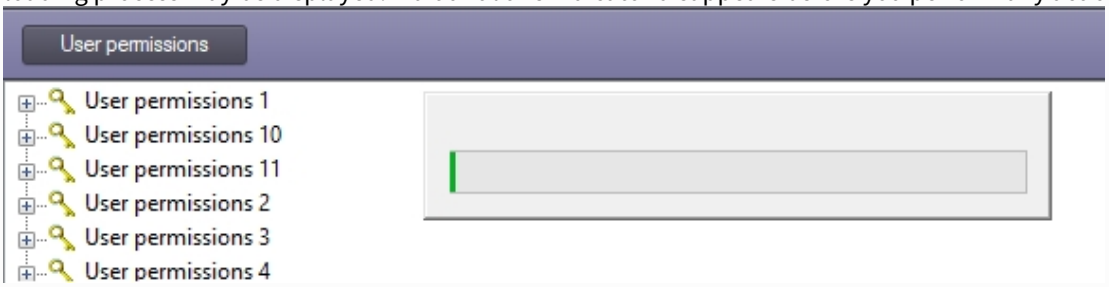
23.5.1.3.1 Registration of operator rights

To register the rights for an operator account, do the following:

1. Open the **Users** tab in the **System Settings** window (**1**).
2. Create a **User permissions** object. If no **User permissions** objects have been created, click the **User permissions** button in the lower part of the window to create one (**2**).



   If at least one registered rights object exists, which is shown in the objects tree below the **User permissions** button, the new rights object can be created from the context menu of the existing object.
3. The object appears in the objects tree under the **User permissions** button, and the settings panel for this object opens on the right side of the **System Setting** window (**3**).

> **Note**
>
> If the **User permissions** are created in the system, then when you open the **Users** tab, an indicator of the permissions loading process may be displayed. Wait until this indicator disappears before you perform any actions on this tab.
>
> 
>

This completes registration of the operator rights.

23.5.1.3.2 General information on the limits to the administrative functions

The administrative functions include:

1. Creation or removal of system objects;
2. Editing the settings of the system objects;
3. Moving the system objects across the objects tree.

By default, the operator has access to all administrative, control and viewing functions of all system objects. Administration of specific objects and groups of objects can be forbidden for an operator.

The objects are grouped according to the tabs of the **System Settings** window.

When an operator receives administration rights for an object, he (she) also receives the control and viewing rights for that object. The forbidden tabs are blacked out in the System Settings window.

Figure below shows a tabs panel of the **System Settings** window where the **Architecture**, **Hardware**, **Interfaces** and **Users** tabs are allowed for editing by the current operator, while the objects in the **Programming** tab cannot be edited by the current operator.

If an operator is forbidden to access any of the tabs, he (she) cannot open the **System Settings** window altogether, and cannot use any of the administrative functions.

> **Note.**
>
> Lack of administrative rights for the **System Settings** tabs does not imply any limitation on control or viewing of the corresponding objects.

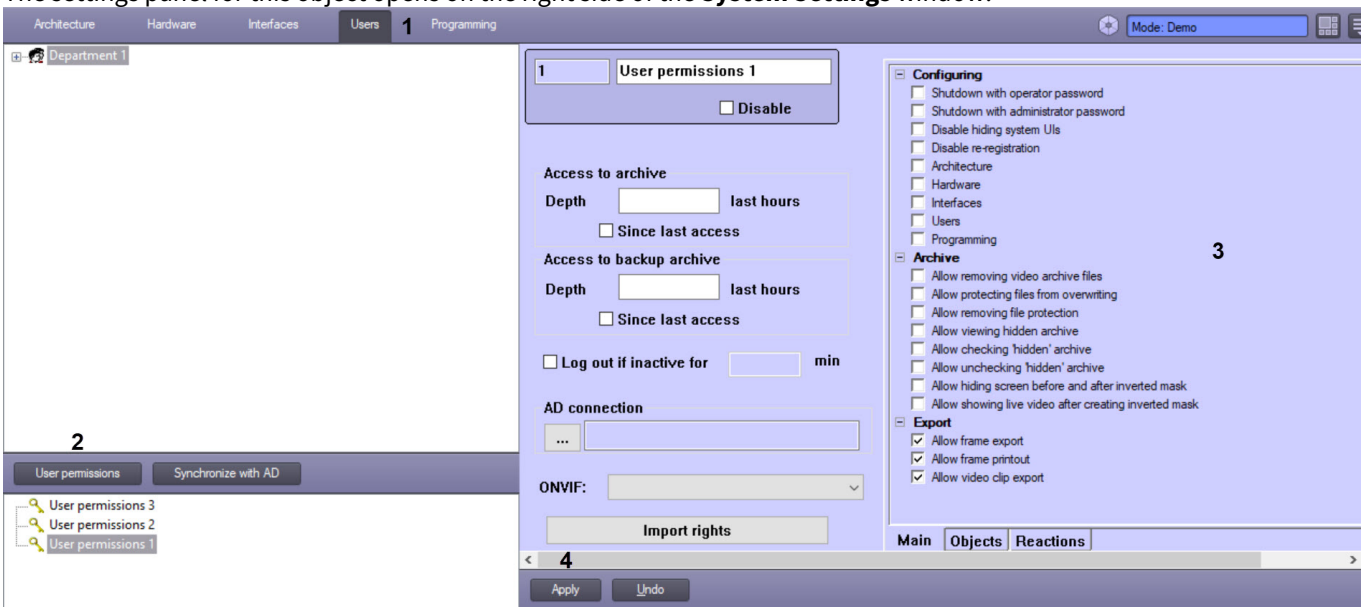
23.5.1.3.3 Limiting access to the tabs of the System Settings window

By default, the operator has no access to the administrative functions of the system objects in the **System Settings** tabs.

An operator can be granted administrative rights to the system objects of one or more tabs. In this case the operator will be able to open the **System Settings** window.

To allow an operator to administer objects in one or more tabs, do the following:

1. Open the **Users** tab in the **System Settings** window (**1**).
2. Open the required **User permissions** object in the objects tree under the **User permissions** button (**2**).
3. The settings panel for this object opens on the right side of the **System Settings** window.



   The last 5 checkboxes of the **Configuring** group correspond to the tabs of the **System Settings** window (**3**). Check the checkboxes for the tabs that the operator will be allowed to access.
4. Press the **Apply** button (**4**).

This completes the setup of the operator access to the **System Settings** tabs.

23.5.1.3.4 Limiting access to the system objects administration, control and viewing functions

By default, an operator is forbidden to administer any objects. If an operator is granted access to one or more tabs of the **System Settings** window, they automatically receive the rights to administer, control and view all system objects on these tabs.

When the operator has the rights for control functions, they can use the buttons, menu items and other interface elements allowing to control the corresponding objects (cameras, microphones, telemetry, event viewer, etc). In addition to overall restriction of object control functions, the separate commands can be prohibited (see Limiting access to sending commands (reactions)).

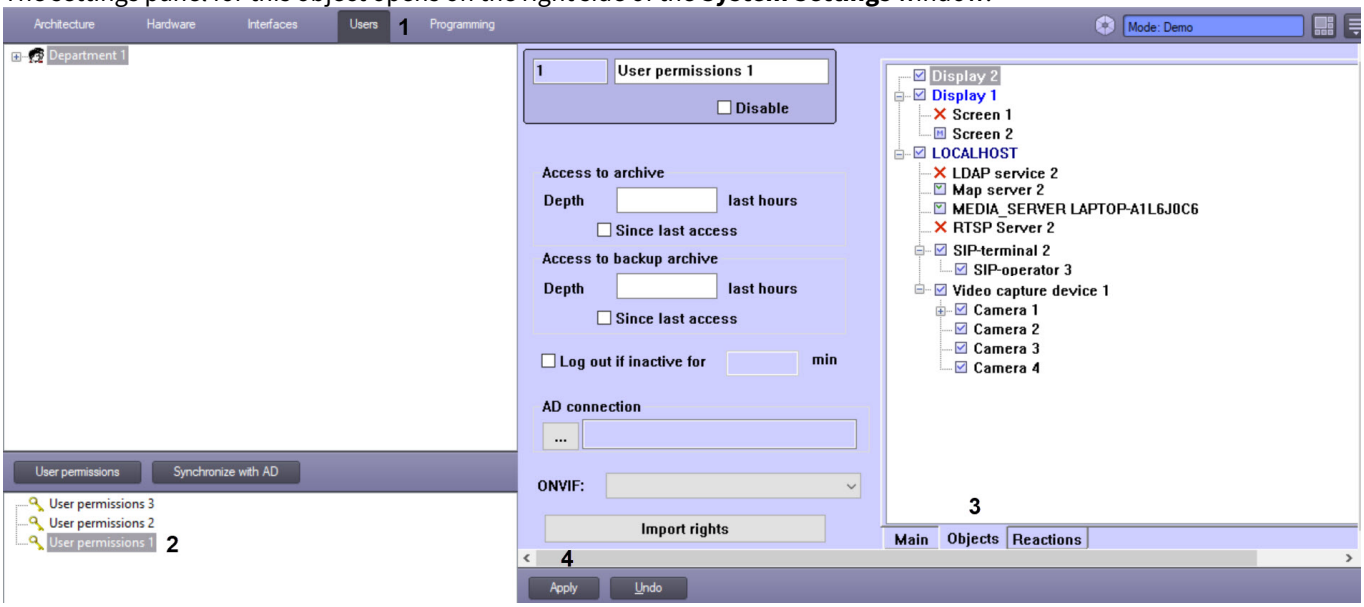
Viewing functions allow the operator to view the interface components (user screens, surveillance monitors, Backup archive window, microphone indicators, etc.).

By default, operator can have a full access to administrator, operator and control functions of the objects with the given functions. It is possible to prohibit the operator to administer one or several objects, limit the list of available functions of object control and also limit monitor opportunities.

> **Note**
>
> If the administrator password is not set (see Administrator password registration) and the access to the required tabs of the **System settings** dialog window is limited (see Limiting access to the tabs of the System Settings window), then the limitation of the object configuration rights will not be available.

To limit operator access to the administration of certain objects of *Intellect*, do the following:

1. Open the **Users** tab in the **System Settings** window (**1**).
2. Open the required **User permissions** object in the objects tree under the **User permissions** button (**2**).
   The settings panel for this object opens on the right side of the **System Settings** window.



3. Go to the **Objects** tab (**3**). The object tree corresponds to the rights of the current *Intellect* operator. In the object tree, to the left of each object there is a field that can be edited—it indicates the Operator's rights to administer, control, and view system objects. The names of the icons correspond to the names of objects, the administration, control and viewing of which can be available to the Operator with the appropriate rights. The correspondence of the icon type to the Operator's rights is given in the table:

Icon	Right to administer	Right to control the object	Right to view the object
A gray mark	Yes	Yes	Yes
A green mark	No	Yes	Yes
An **M** mark	No	No	Yes
A cross mark **x**	No	No	No

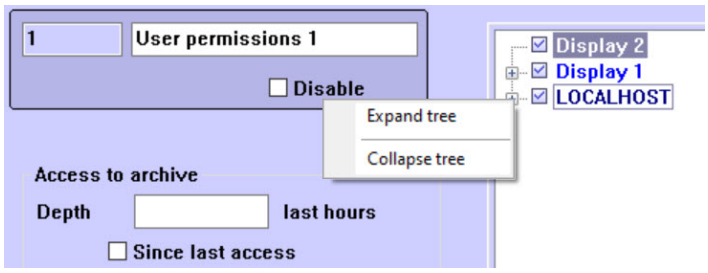
> **Note**
>
> The administrative, control or viewing rights to interface objects depend on the rights to the **Computer** objects. The rights to the **Computer** object have a higher priority. For example, if the user rights allow the administration of the **Display** object, but prohibit the administration of the **Computer** object to which this **Display** is assigned, then a user logged on to the computer prohibited for administration will not be able to administer the **Display** object (see also Assigning the displays to the operator workstations).

4. After finishing the setting, click the **Apply** button (**4**).

The following keyboard hotkeys can be used for objects tree control:

Key	Function
+	Grants all rights to the selected objects (sets the gray mark)
-	Forbids the selected object (sets the red cross)
Space	Sequential change of the rights to the selected object in the direction of increasing (forbidden-monitoring-control-administration and then cyclically)
Left and right arrows	Expand / collapse the selected tree branch
/	Fully collapse the selected branch of the objects tree
*****	Fully expand the selected branch of the objects tree
Shift + **/**	Fully collapse all branches of the objects tree. This view will be saved for the current user even after *Intellect* restart
Shift + *****	Fully expand all branches of the objects tree. This view will be saved for the current user even after *Intellect* restart

Expanding and collapsing the tree functions are also available when you right-click on an object in the object tree (see The Expand tree function and The Collapse tree function).



23.5.1.3.5 Limiting access to shutting the system down

To eliminate unauthorized shutdown of the surveillance system, the shutdown function can be protected by a password. The following options for system shutdown are available:

1. Shutdown by the password of any registered operator.
2. Shutdown by the password of the current authorized user only.
3. Shutdown by the administrator password.
4. The operator cannot shut the system down.

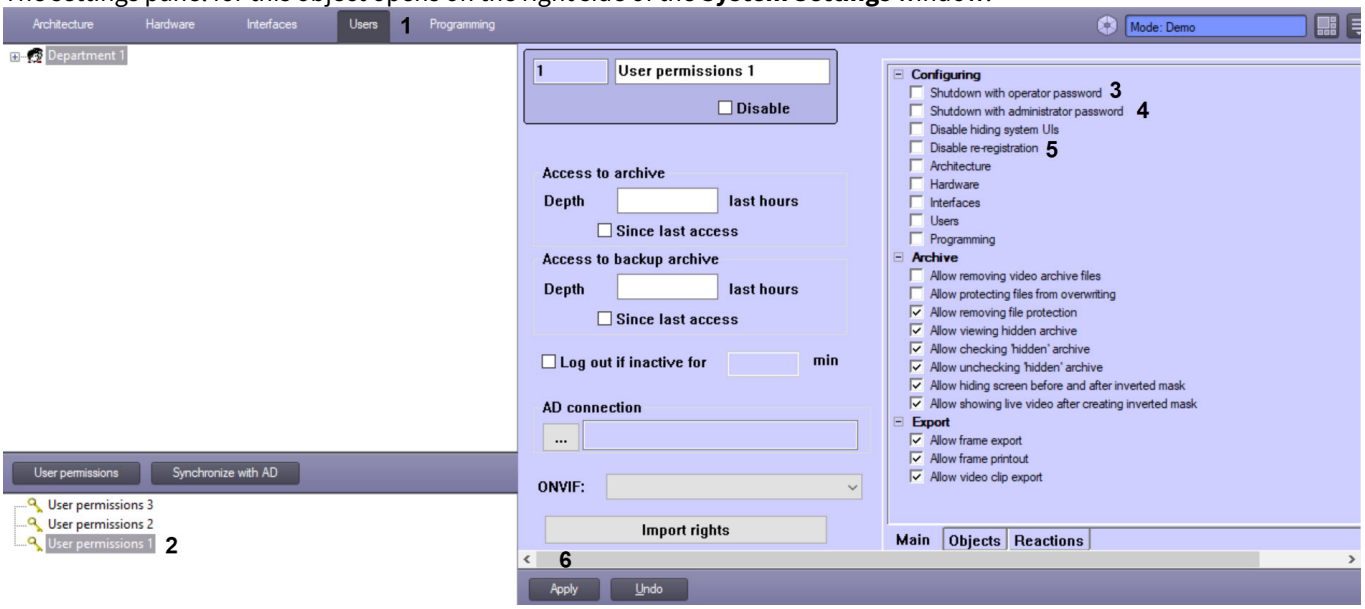
If the operator is forbidden from shutting the system down, the **Run** menu of the **Main Control Panel** does not contain the **Shut Down** option. This menu item appears only after opening the administrator password window and entering the valid

administrator password. To shut the system down, the password should be entered once more. Thus, it is recommended to use the option for shutdown by the administrator password, as well.

By default, the system is set for shutdown by any registered operator's password, regardless of the current authorized user.

To change the shutdown option, do the following:

1. Open the **Users** tab in the **System Settings** window (**1**).
2. Open the required **User permissions** object in the objects tree under the **User permissions** button (**2**).
   The settings panel for this object opens on the right side of the **System Settings** window.



3. To enable system shutdown by the current operator's password only, set the **Shutdown with operator password** checkbox (**3**).
4. To enable system shutdown by the administrator password only, set the **Shutdown with administrator password** checkbox (**4**).
5. To forbid the current operator from shutting the system down, set the **Shutdown with administrator password** and the **Disable re-registration** checkboxes (**4**,**5**).
6. To revert to the default shutdown option, clear all the related checkboxes: **Shutdown with operator password**, **Shutdown with administrator password**, **Disable re-registration** (**3**,**4**,**5**).
7. Click the **Apply** button (**6**).

This completes the setup of the system shutdown options.

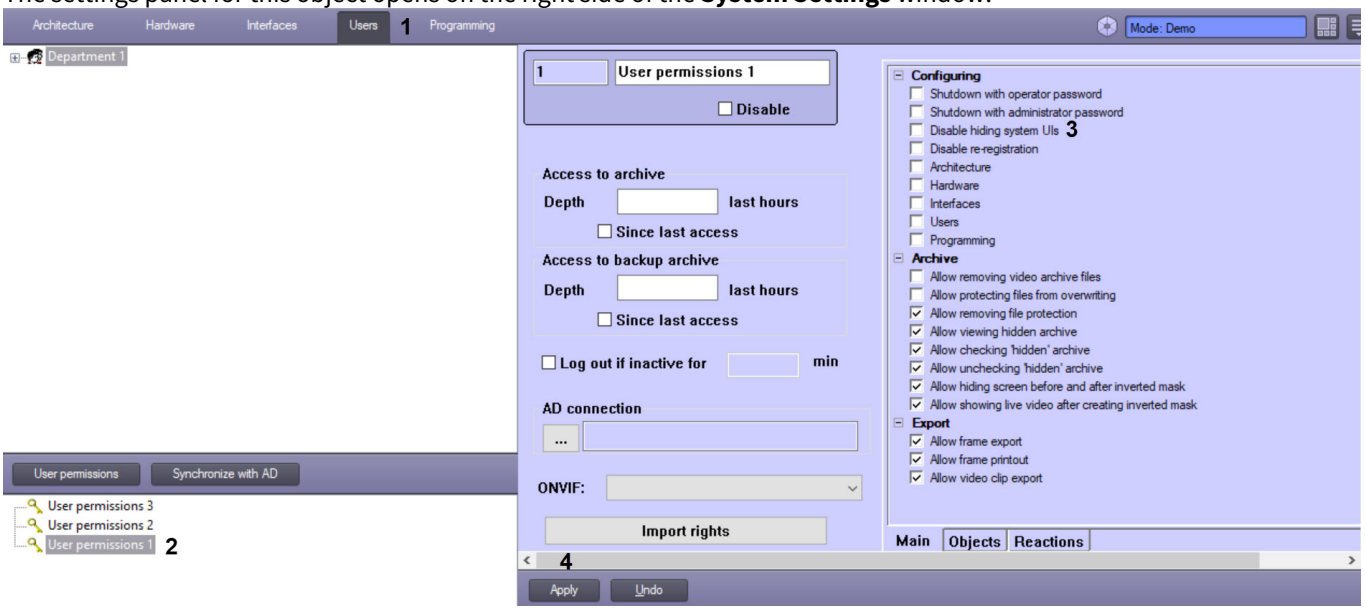
23.5.1.3.6 Limiting the rights to hide the interface components

Hiding all interface components can be forbidden. In this case, the **Hide All** button in the **Main Control Panel** becomes disabled, and at least one **Display** object allowed for the current user will stay open.

By default, the operator is allowed to hide all interface components. To forbid the operator to hide all interface components, do the following:

1. Open the **Users** tab in the **System Settings** window (**1**).

2. Open the required **User permissions** object in the objects tree under the **User permissions** button (**2**).
   The settings panel for this object opens on the right side of the **System Settings** window.



3. Set the **Disable hiding system UIs** checkbox (**3**).
4. Click the **Apply** button (**4**).

This completes the process of forbidding the hiding of all interface components.

23.5.1.3.7 Permissions for working with archives

In *Intellect*, it is possible to prohibit the Operator from accessing playback of video archives from the videoserver or Backup archive using the **Video surveillance monitor**.

If the Operator is denied access to video archives, the button for entering the archive will not be displayed in the **Video surveillance monitor** window, and the functions described in this section will also be unavailable.

By default, Operators are allowed access to archive playback.

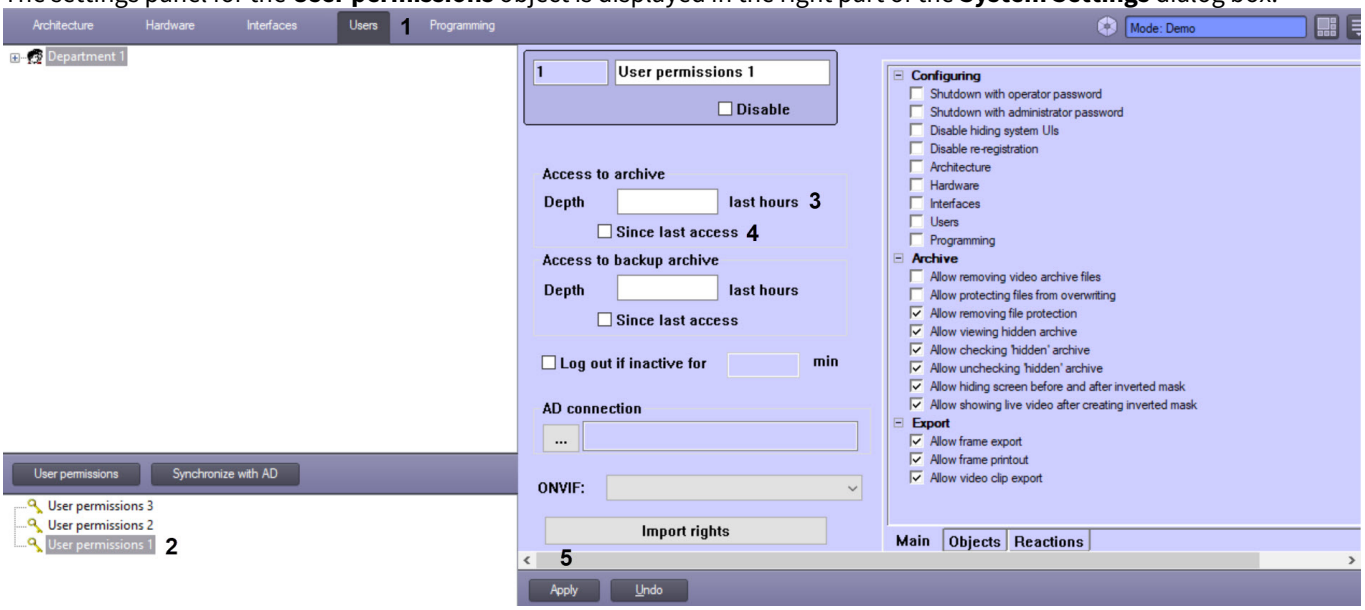
Working with the archives

23.5.1.3.7.1 Limiting access to archive playback

To limit access for Operator to playback the archive, do the following:

1. Go to the **Users** tab in the **System Settings** dialog box (**1**).
2. In the objects tree that is below the **User permissions** button in the **Users** tab, select an object with the same name as the permissions to be changed (**2**).

The settings panel for the **User permissions** object is displayed in the right part of the **System Settings** dialog box.



3. Specify the number of hours for viewing in the **Depth ___ last hours** field (**3**).

> **Note**
>
> The number of last video archive hours for viewing should be whole.

> **Note**
>
> Input the 0 value in the **Depth ___ last hours** field to disable access to the archive.

4. If the hours since the last entrance to the system are counted, set the **Since last access** checkbox (**4**). If the hours are to be counted since the current moment, then leave the **Since last access** box clear.

> **Note**
>
> If the **Since last access** checkbox is set and the number of hours for viewing is specified, then last hours are counted till the registration moment.

> **Note**
>
> If the **Since last access** checkbox is set, but the **Depth ___ last hours** field is left blank, the access to the main archive playback is not limited.

5. Click the **Apply** button (**5**).

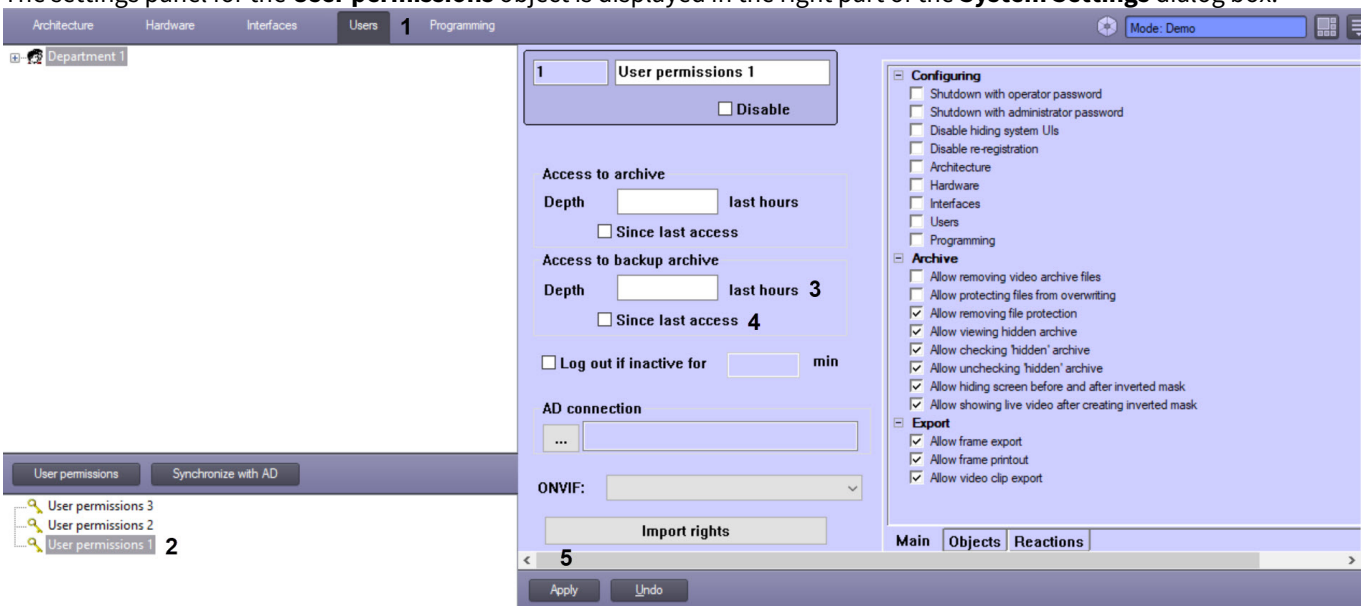
The access to archive playback is now limited.

23.5.1.3.7.2 Limiting access to Backup archive playback

To limit access for Operator to playback the Backup archive, do the following:

1. Go to the **Users** tab in the **System Settings** dialog box (**1**).
2. In the objects tree that is below the **User permissions** button in the **Users** tab, select an object with the same name as the permissions to be changed (**2**).

The settings panel for the **User permissions** object is displayed in the right part of the **System Settings** dialog box.



3. Specify the number of hours for viewing in the **Depth ___ last hours** field (**3**).

> **Note**
>
> The number of last video archive hours for viewing should be whole.

> **Note**
>
> Input the 0 value in the **Depth ___ last hours** field to disable access to the Backup archive.

4. If the hours since the last entrance to the system are counted, set the **Since last access** checkbox (**4**). If the hours are to be counted since the current moment, then leave the **Since last access** checkbox clear.

> **Note**
>
> If the **Since last access** checkbox is set and the number of hours for viewing is specified, then last hours are counted till the registration moment.

> **Note**
>
> If the **Since last access** checkbox is set, but the **Depth ___ last hours** field is left blank, the access to the Backup archive playback is not limited.

5. Click the **Apply** button (**5**).

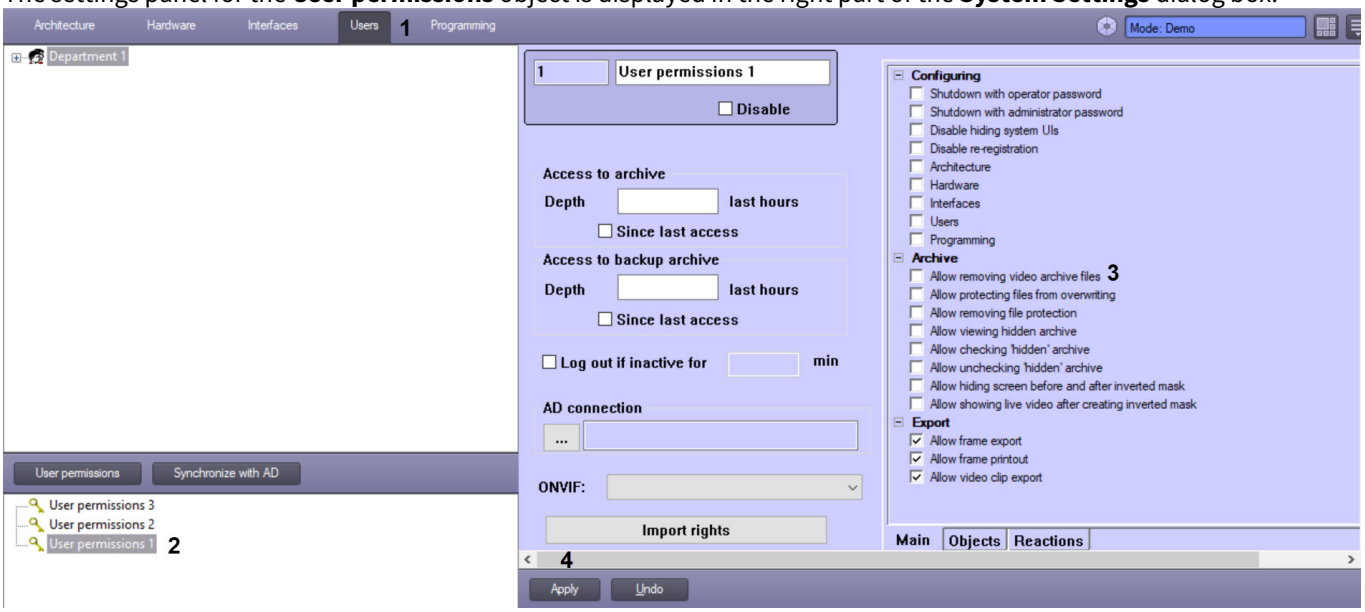
The access to Backup archive playback is now limited.

23.5.1.3.7.3 Permission to remove archive video files

To allow the Operator to remove archive (both main and active) video files, do the following:

1. Go to the **Users** tab in the **System Settings** dialog box (**1**).
2. In the objects tree that is below the **User permissions** button in the **Users** tab, select an object with the same name as the permissions to be changed (**2**).

The settings panel for the **User permissions** object is displayed in the right part of the **System Settings** dialog box.



3. To allow the Operator to remove video archive files, set the **Allow removing video archive files** checkbox (**3**). If the Operator is not allowed to remove video archive files, leave this checkbox clear.
4. To save the changes in *Intellect*, click the **Apply** button (**4**).

The Operator now can remove video archive files.

> **Note**
>
> Video recordings are deleted as follows:
>
> 1. From the Video surveillance monitor interface – see Deleting video recordings from the archive section of Operator's Guide.
> 2. Using ARCH_DEL_RECORD reaction of the CAM object that is executed using the script or program – see *CAM* section of *Programming Guide* (not available in English).

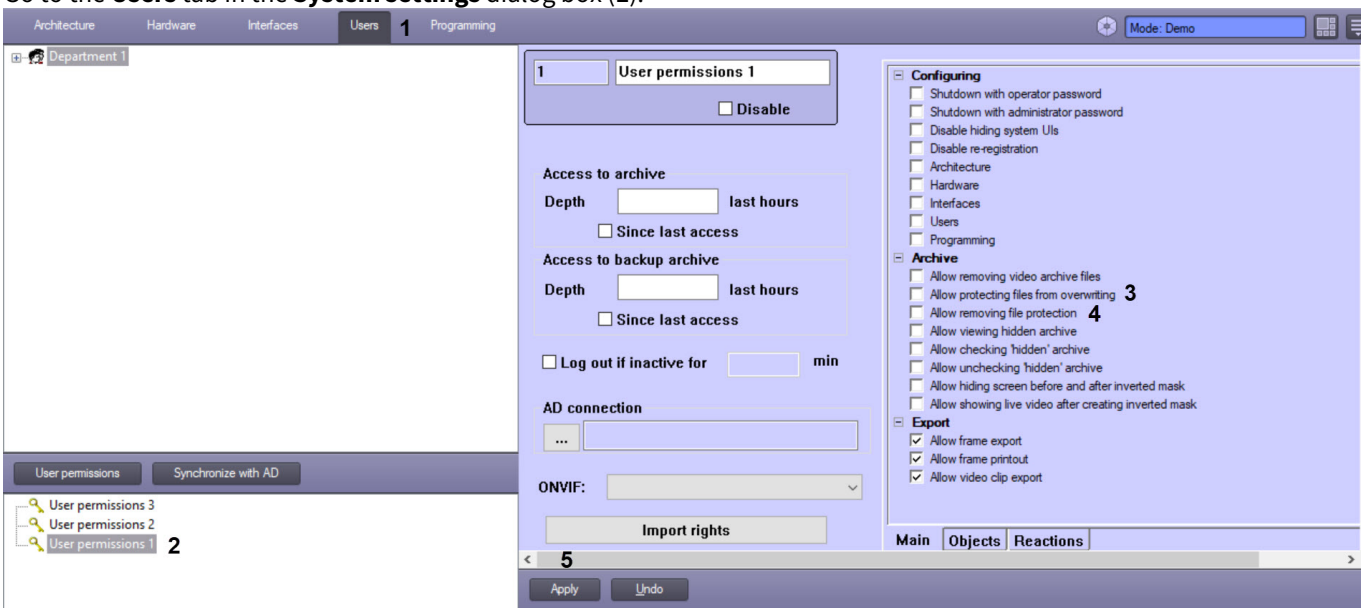
23.5.1.3.7.4 Permissions to protect archive files from rewriting

Recording to archive is performed on a loop in *Intellect* (see the General information on video archiving section). Therefore, old archive recordings can be replaced by new ones. But sometime it is required to protect important recordings from loop recording. In such case, permissions to protect files from rewriting are needed.

Protected files are moved to the PROTECTED folder in the VIDEO folder on the disk with archive. When the file is deprotected, it is moved back to the folder from which it was taken (if it exists). If this folder was removed because of all files in it were rewritten, then the file will stay in the PROTECTED folder but won't be displayed in the Monitor. Later, this file will be deleted by loop recording.

Give permissions to protect archive files from rewriting as follows:

1. Go to the **Users** tab in the **System settings** dialog box (**1**).



2. In the objects tree located under the **User permissions** button in the **Users** tab, select the same-name object corresponding to the Operator access permissions which should be changed (**2**).
3. The settings panel of the **User permissions** object will display on the right of the **System settings** dialog box.
4. To allow the operator to protect archive files from rewriting, set the **Allow protecting files from overwriting** checkbox (**3**). Don't set this checkbox if the operator should not have this permission.
5. To allow the operator to disable protection of files protected from rewriting, set the **Allow removing file protection** checkbox (**4**). Don't set this checkbox if the operator should not have this permission.
6. Click the **Apply** button (**5**).

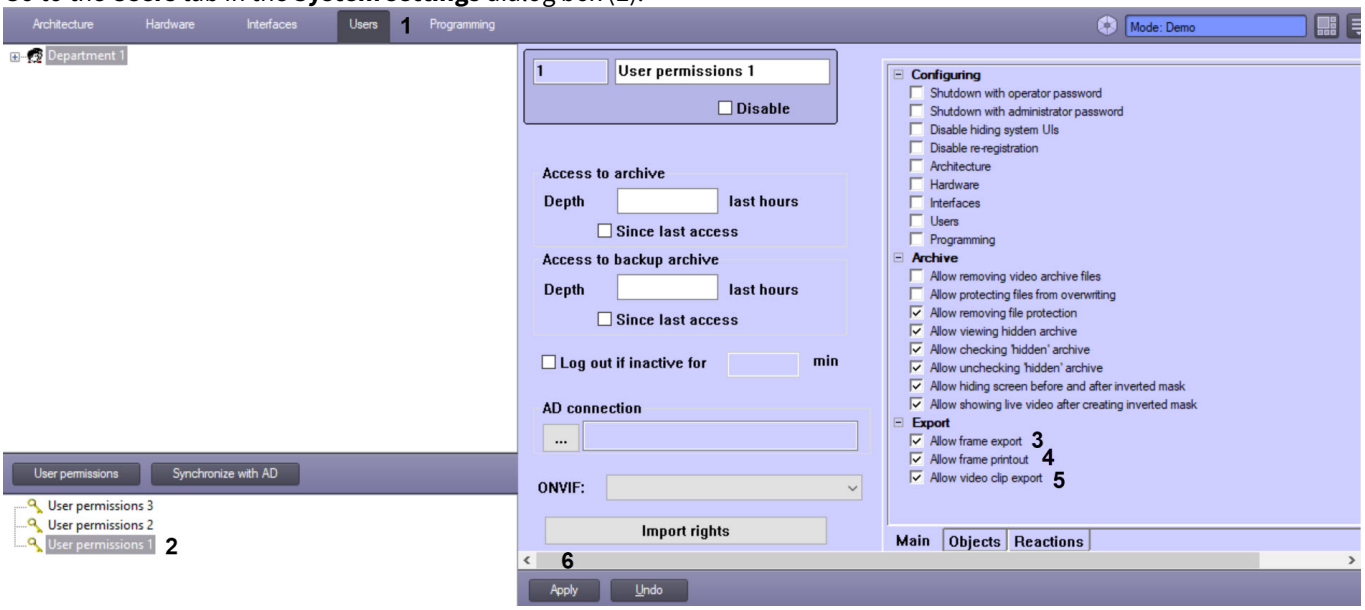
Permissions for the Operator to protect archive files from rewriting are now set.

23.5.1.3.7.5 Permissions for export and printout

By default, the Operator is allowed to export archive files and frames as well as to print frames.

Forbid export or printout as follows:

1. Go to the **Users** tab in the **System settings** dialog box (**1**).



2. In the object tree located under the **User permissions** button in the **Users** tab, select the same-name object corresponding to the Operator access permissions which should be changed (**2**).
3. The settings panel of the **User permissions** object will display on the right of the **System settings** dialog box.

4. In order to forbid the Operator to export archive frames, set the **Allow frame export** checkbox clear (**3**).
5. In order to forbid the Operator to print archive frames, set the **Allow frame printout** checkbox clear (**4**).
6. In order to forbid the Operator to export archive clips, set the **Allow video clip export** checkbox clear (**5**).
7. Click the **Apply** button (**6**).

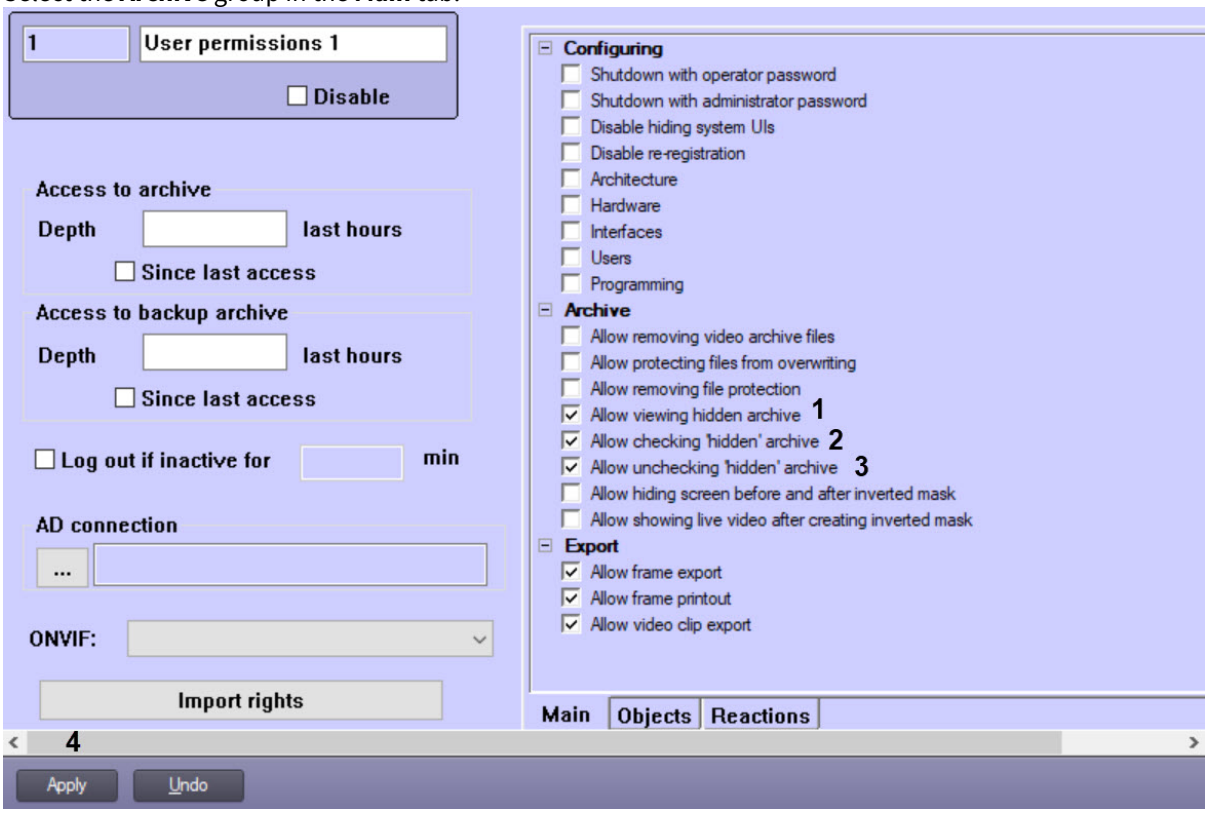
Export and printout permissions are now set.

23.5.1.3.7.6 Permissions to the hidden archive

The hidden archive is not displayed in the Video Surveillance Monitor depending on the Operator permissions but is stored on the hard drive in the same way as the main archive. The Operator has no default permissions to browse the hidden archive as well as to set or unset the "hidden" label to the archive records.

In order to allow the Operator to perform operation of the hidden archive, proceed as follows:

1. Go to the **User permissions** object settings panel.
2. Select the **Archive** group in the **Main** tab.



3. Set the **Allow viewing hidden archive** checkbox in order for the Operator with these rights to be able to view a hidden archive (**1**).
4. Set the **Allow checking "hidden" archive** checkbox in order for the Operator to be able to hide archive entries (**2**).
5. Set the **Allow unchecking "hidden" archive** checkbox in order for the Operator to be able to unhide archive entries (**3**).
6. Click the **Apply** button (**4**).

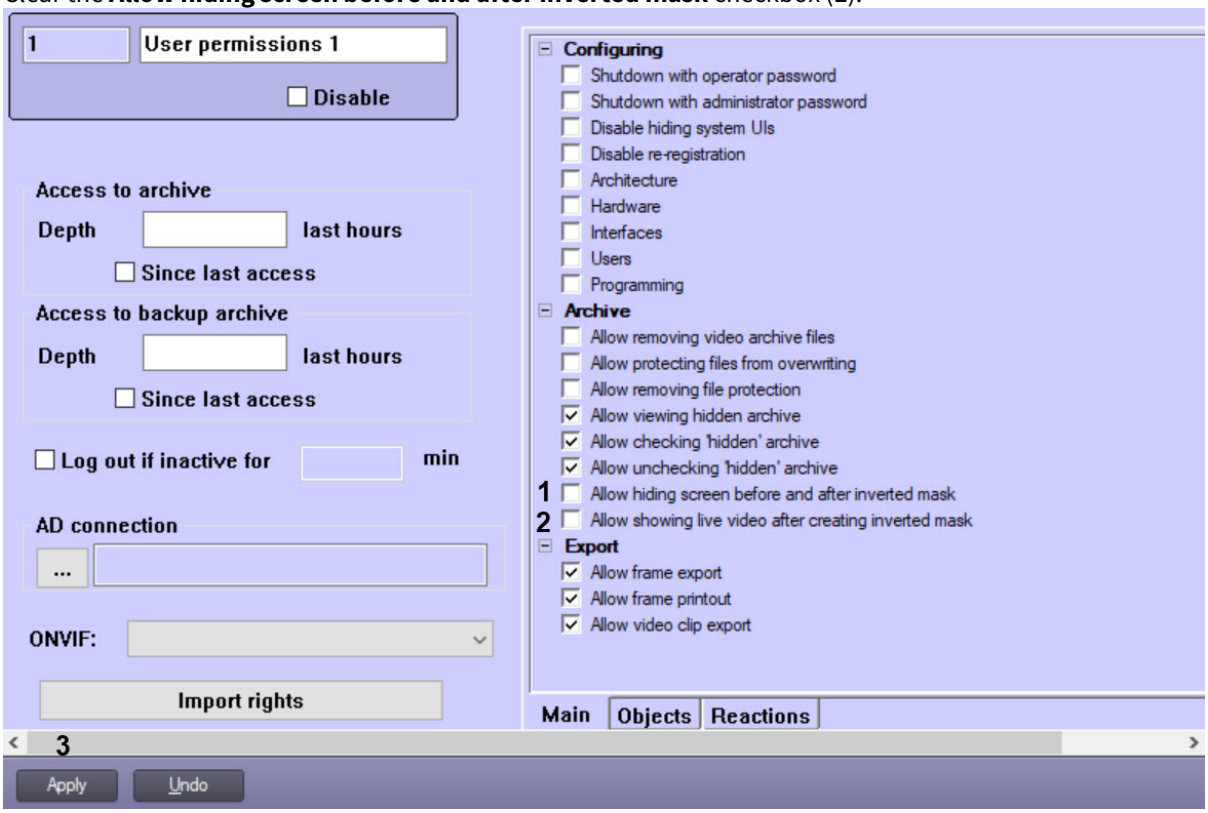
Restriction of rights to hide the archive is completed.

23.5.1.3.7.7 Permissions to view video before and after inverted mask

In the Video Surveillance monitor interface, when you create an inverted hiding mask, the **Hide screen completely before and after mask** checkbox is displayed, which allows the Operator to choose whether to hide the screen before and after the selected segment with inverted masking (see Masking areas on video at export). To hide this option for the Operator, do the following:

1. Go to the settings panel of the **User permissions** object.
2. On the **Main** tab, select the **Archive** group.

3. Clear the **Allow hiding screen before and after inverted mask** checkbox (**1**).



4. Click the **Apply** button (**3**).

At the same time, you can allow the Operator to view live video before and after the specified mask by setting the **Allow showing live video after creating inverted mask** checkbox (**2**) and clicking the **Apply** button (**3**).

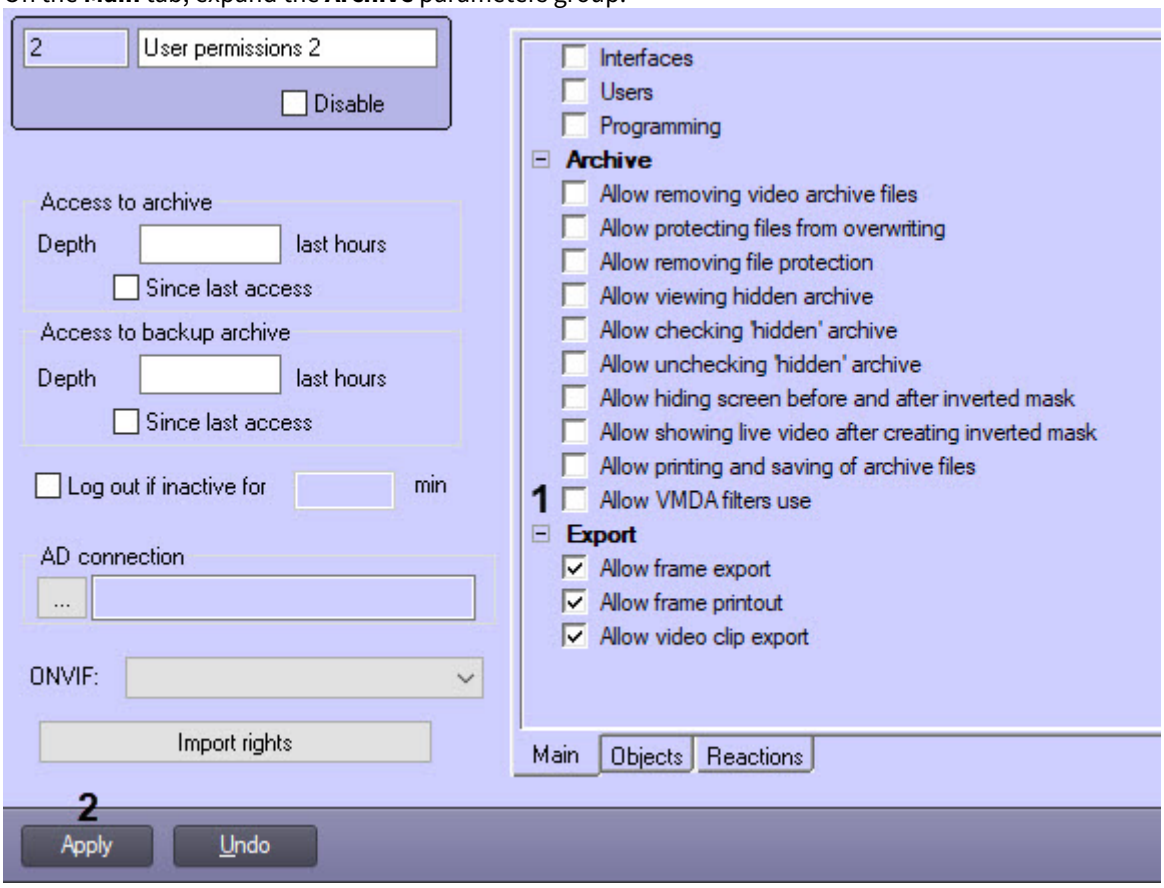
Configuring the permissions to view video before and after inverted mask is completed.

23.5.1.3.7.8 Permissions to use VMDA filters

By default, when working with the **Video surveillance monitor**, the Operator is not allowed to save and load archive search templates (see Smart search templates). To allow the Operator to use templates, do the following:

1. Go to the settings panel of the **User permissions** object.

2. On the **Main** tab, expand the **Archive** parameters group.



3. Set the **Allow VMDA filters use** checkbox (**1**).
4. Click the **Apply** button (**2**).

Now the **Save the template** and **Load the template** buttons in the **Video surveillance monitor** will be available for the Operator with the appropriate rights.

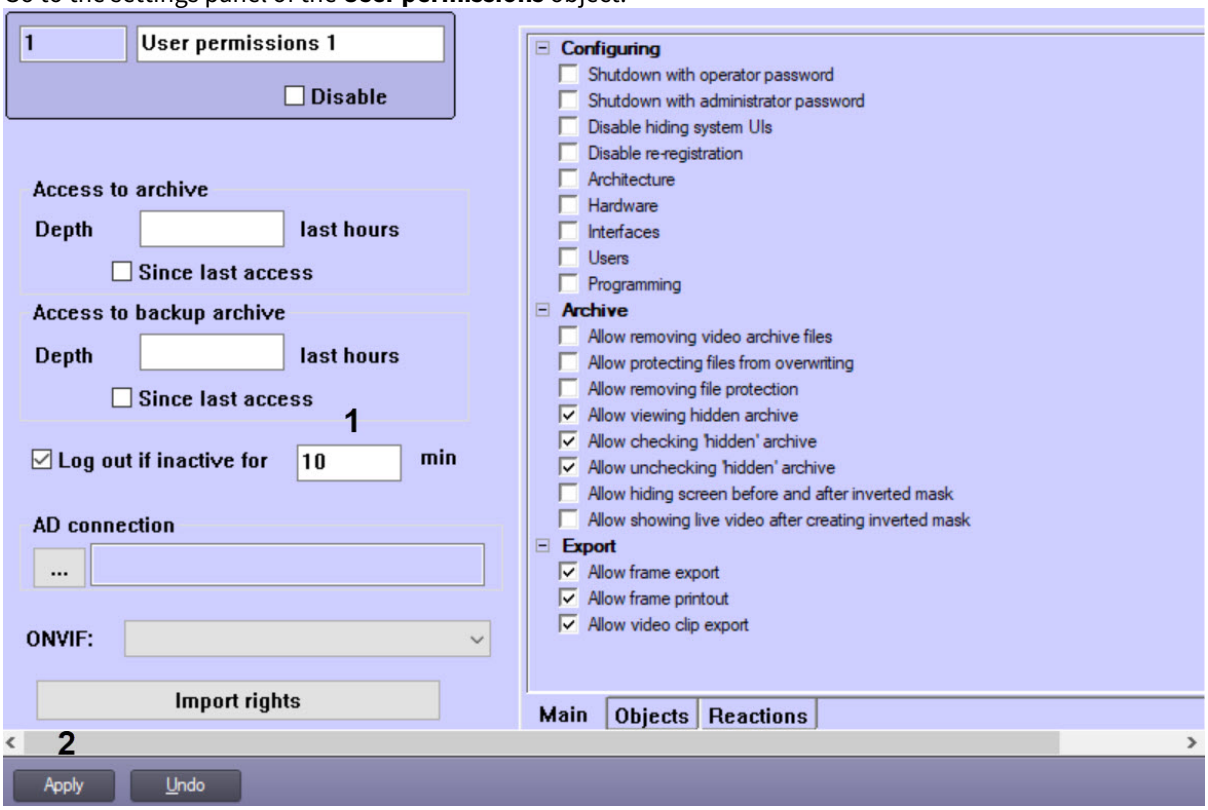
> **Note**
>
> The display of the **Save the template** and **Load the template** buttons is also configured by the CanUseVmdaFilters registry key (see Registry keys reference guide).

23.5.1.3.8 Configuring session auto termination when user is inactive

It is possible to configure the session auto termination when the operator is inactive for some period of time.

For this, do the following:

1. Go to the settings panel of the **User permissions** object.



2. Set the **Log out if inactive for __ min** (**1**) checkbox and in the corresponding field specify the time period (in minutes) at the end of which the session is to be terminated after the latest action of the user and the login window is to be displayed (see Intellect software start and shutdown section in Operator's Guide).
3. Click the **Apply** button (**2**).

The session auto termination when the user is inactive is now configured.

23.5.1.3.9 Configuring rights to use ONVIF Server

If ONVIF Server module is in use, the user rights can be configured to connect to it.

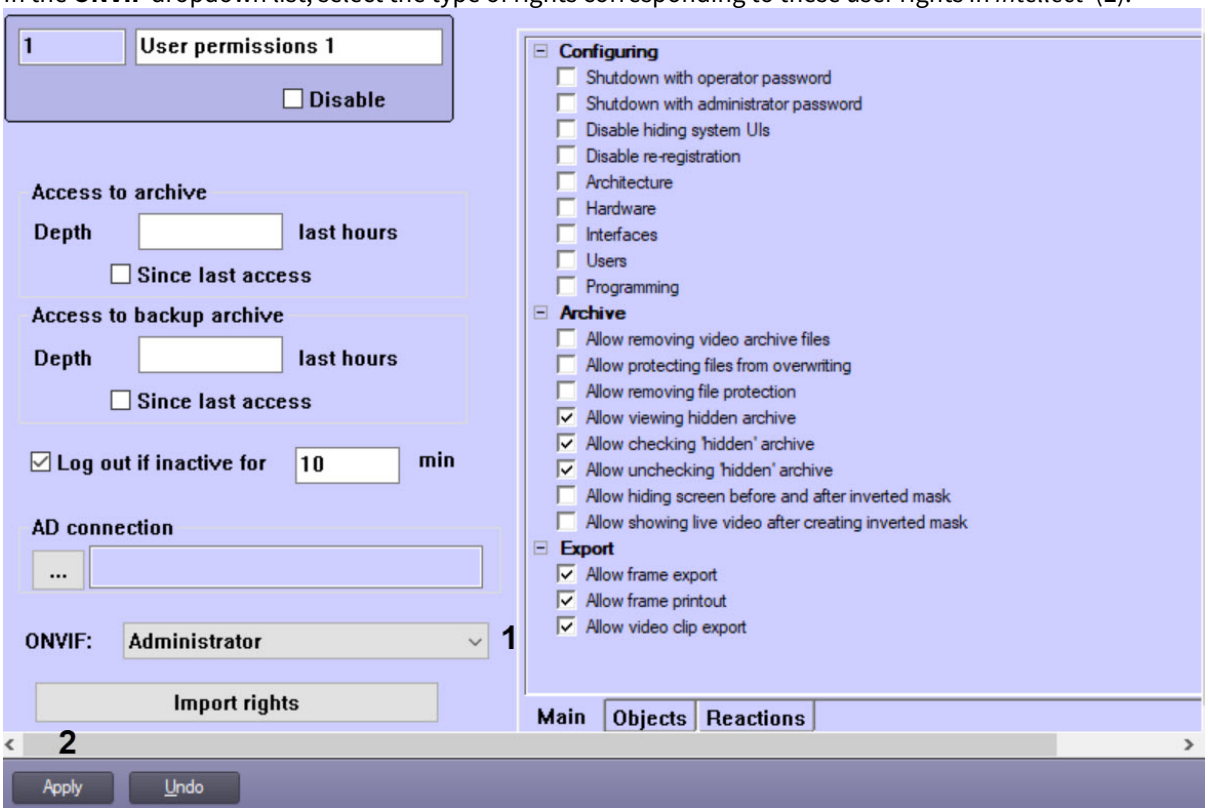
There are 4 types of rights in ONVIF specification: Administrator, Operator, User and Anonymous. Users with Anonymous rights can get data via ONVIF Server without authentication. For the rest three types, the correspondence between user rights in *Intellect* and user rights in ONVIF Core specification is to be configured.

> **Note**
>
> Find details about types of rights in ONVIF Core specification at https://www.onvif.org/profiles/specifications/

Intellect rights to use ONVIF Server are configured as follows:

1. Go to the settings panel of the **User permissions** object.

2. In the **ONVIF** dropdown list, select the type of rights corresponding to these user rights in *Intellect* (**1**).



3. Click the **Apply** button (**2**).
   Intellect rights to use ONVIF Server are now configured.

23.5.1.3.10 Combining (importing) permissions

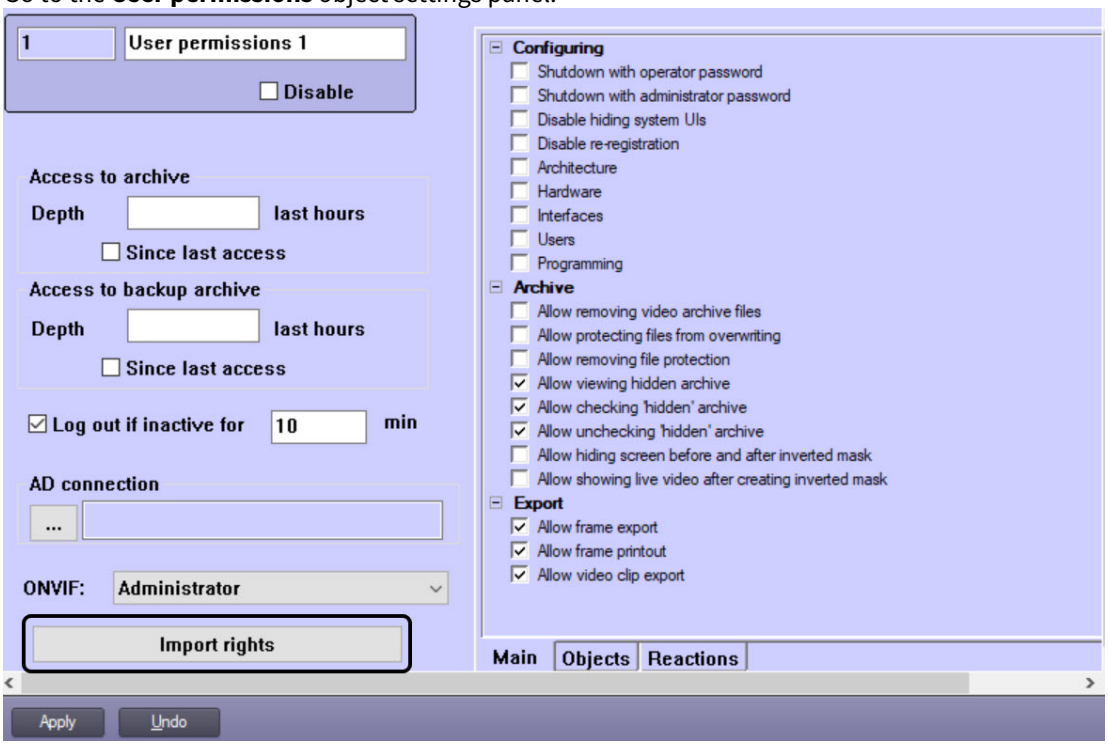
Intellect allows several users' rights to be combined into a newly created **User permissions** object. While the copy-paste function (Ctrl+C - Ctrl+V) just copies all users' rights parameters, the function of permissions combining unites several users' permissions into the configured object.

The following rules are applied for combining process:

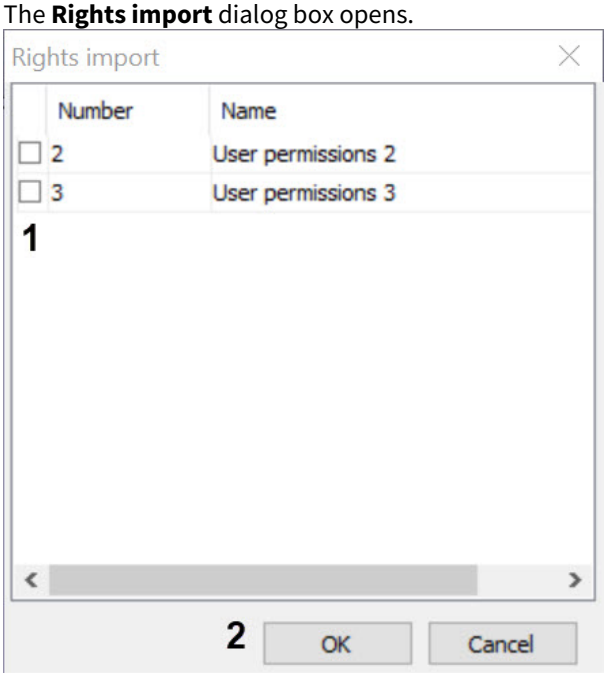
1. The permissions set by template rights are added, i.e. if an action is prohibited in one of the rights, but is permitted in the other, then the action is allowed in the new rights as a result of their combination.
2. The rights for the administration, control and viewing functions are set to the maximum among those permitted in the combined rights.
3. The maximum value in hours for the depth of the archive among the selected template rights is set.

In order to combine several user rights when creating new rights, do the following:

1. Go to the **User permissions** object settings panel.



2. Click the **Import rights** button**.**
3. The **Rights import** dialog box opens.



4. Set checkboxes next to **User permissions** objects to combine (**1**).
5. Click the **OK** button (**2**). The results of combination are displayed on the object settings panel.
6. Click the **Apply** button to save the changes.

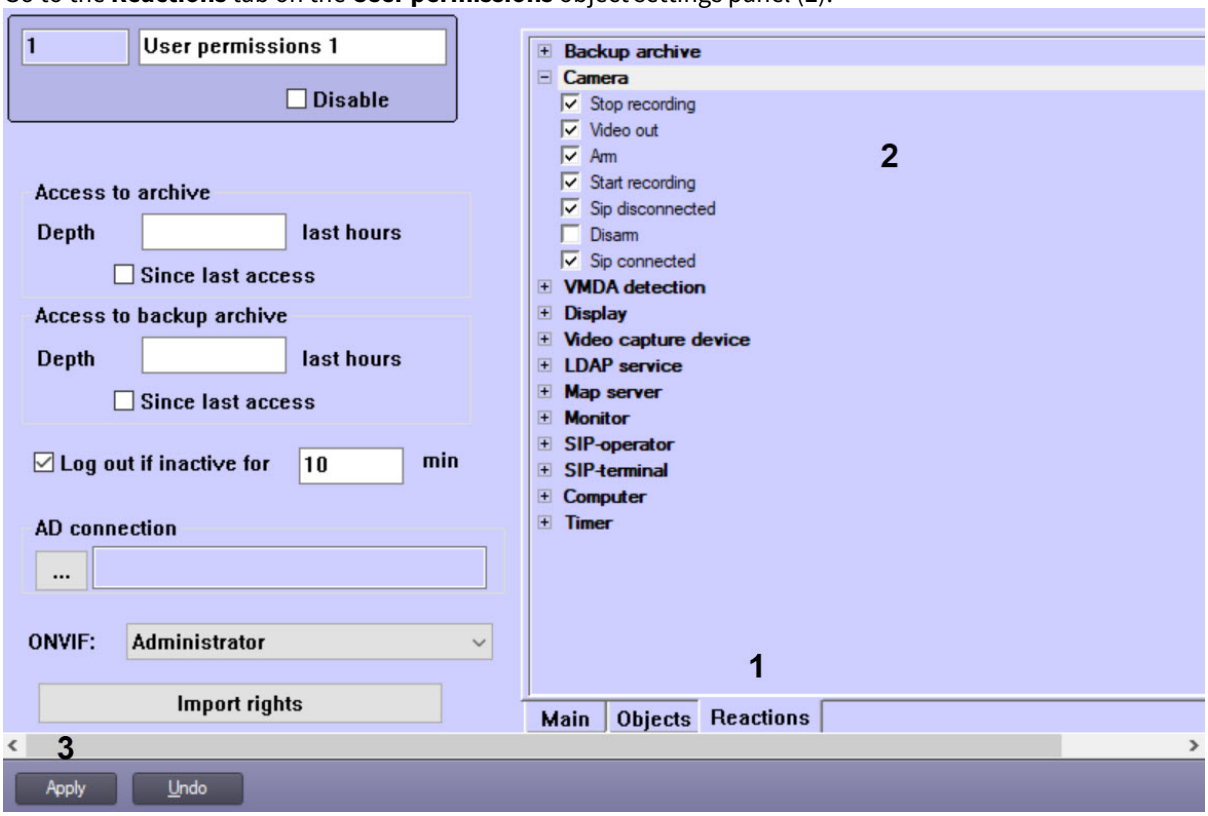
Combine several user rights is completed.

23.5.1.3.11 Limiting access to sending commands (reactions)

By default, *Intellect* Operators have rights to execute any commands for objects allowed for control (see Limiting access to the system objects administration, control and viewing functions). Execution of commands both from interface and macros or scripts can be limited.

Set limits to execution of selected commands as follows:

1. Go to the **Reactions** tab on the **User permissions** object settings panel (**1**).



2. Clear the checkboxes next to the reactions that are to be forbidden for the Operator (**2**).
3. Click the **Apply** button (**3**).

Setting limits to execution of selected commands is completed.

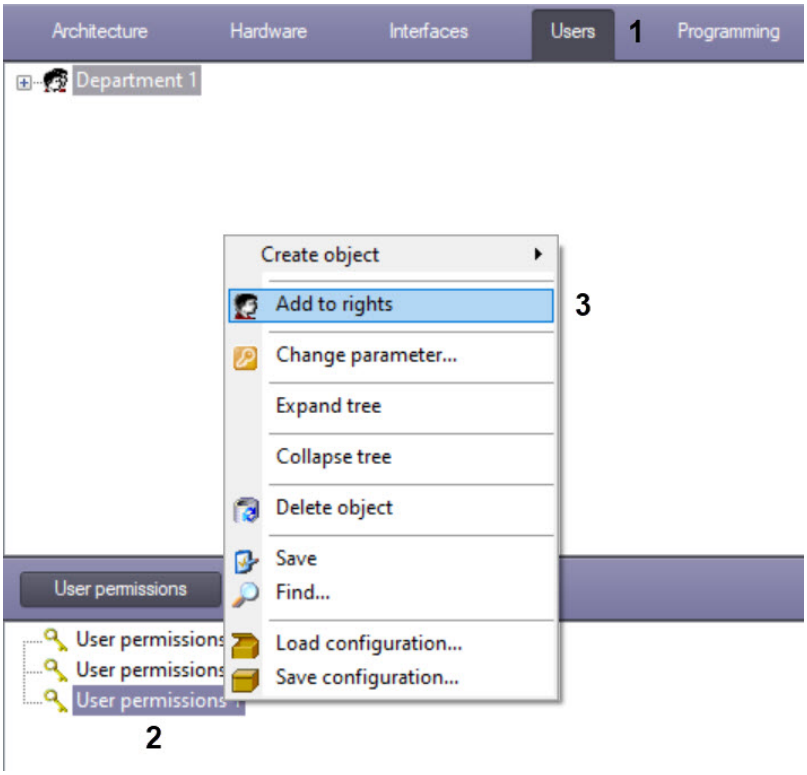
23.5.1.4 Assigning the rights and password to operators for authorization in the Intellect

User accounts are stored separately from operator accounts in *Intellect*. The same rights may be assigned to several operators. But the operator may be assigned only single rights.

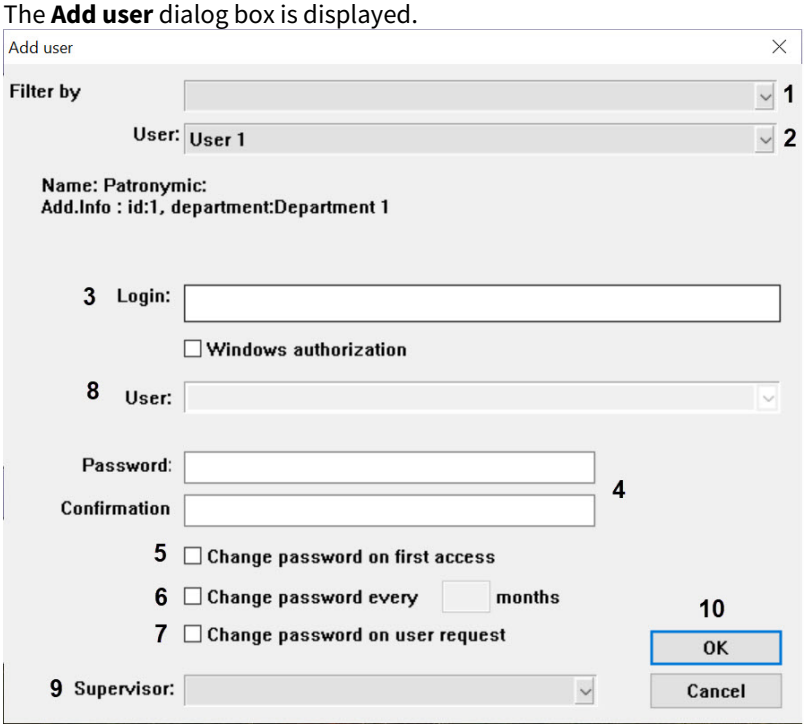
To assign the rights and password to the operator for authorization in *Intellect*, do the following:

1. Go to the **Users** tab in the **System settings** dialog box (**1**).
2. Select an object, corresponding to the rights account that has to be assigned to the operator, in the objects tree under the **User permissions** button (**2**).

3. Call the context menu by right clicking upon the selected **User permissions** object (**3**). Select the **Add to rights** command in the menu.



4. The **Add user** dialog box is displayed.



5. In the **Department** drop-down list select the department the user belongs to (**1**). If the department is selected, then accounts of users belonging to the department will be displayed in the **User** drop-down list. If the department is not selected, then accounts of all users registered in the system will be displayed in the **User** drop-down list.
6. Select the account name registered for operator in the **User** list (**2**).
7. In the **Login** field specify the login that will be assigned to the operator for authorization in *Intellect* (**3**).
8. In the **Password** field specify the password that will be assigned to the operator for authorization in *Intellect* (**4**).

Note

If the password has not been specified, then access rights will not be assigned to the operator.

9. Respecify the password in the **Confirmation** field (**4**).
10. Configure the rules of password change by the user:
    a. Set the **Change password on first access** checkbox to ask the user to change the password on the first login to the system (**5**).
    b. Set the **Change password every __ months** checkbox to ask the user to change the password periodically (**6**). After setting the checkbox, the text field becomes editable. Enter the period (in months) of request to change the password in this field.
    c. Set the **Change password on user request** checkbox to allow the user changing the password at any start system (**7**).
11. If the Windows account is to be used for user authorization in *Intellect*, then set the **Windows authorization** checkbox and select the name of account in the **User** list (**8**).

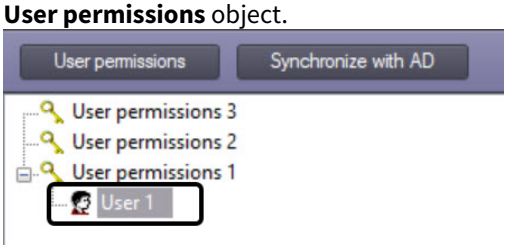
> **Note**
>
> When this way of authorization is selected, no other data is to be specified in the login and password fieldswhen *Intellect* is started and shut down. To start *Intellect* when password is requested, click the **Register** button. To shutdown *Intellect*, click the **Log off** button.

12. If user login to the system shall be confirmed by another user, select the user which has to do the confirmation from the **Supervisor** drop-down list (**9**).

> **Note**
>
> The user-supervisor has to be added to rights.

> **Attention!**
>
> All system users including supervisors have to log-in to the system by login and password instead of Windows user account in case of the authorization type by four-eyes rule (i.e. with the supervisor confirmation) is in use in the system (see 7-10 steps).

13. Click the **OK** button (**10**).
14. The object of the same name as the user account registered for the operator will be displayed in the child branch of the **User permissions** object.



This completes the process of assigning the rights and passwords to the operator for authorization in *Intellect*.

23.5.1.5 Setting up the default user

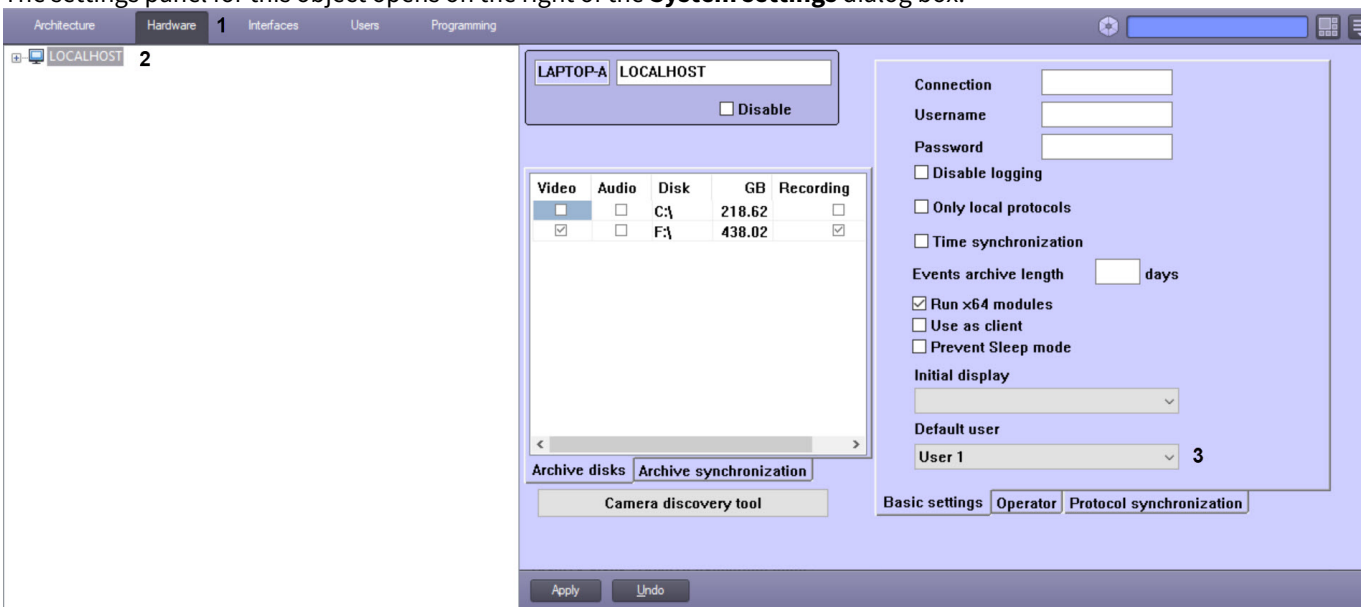
To allow starting the system without specifying the password, default user is to be set up. The administrative, controlling and viewing functions will be limited according to the rights of the default user.

The user is to be registered in the system before becoming the default user.

To set the default user, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box (**1**).

2. Select the **Computer** object, representing the workstation the default user will be assigned to (**2**).
   The settings panel for this object opens on the right of the **System settings** dialog box.



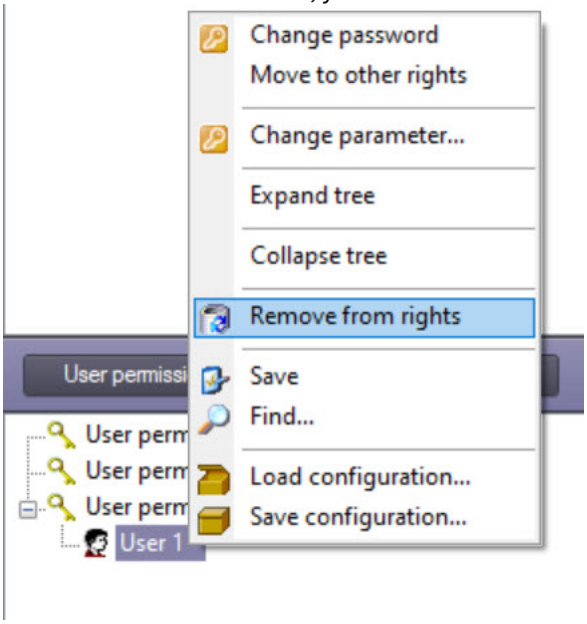
3. Select the user account in the **Default user** list (**3**).
4. Click the **Apply** button.

The administrative, controlling and viewing functions will then be limited according to the rights of the default user.

23.5.1.6 Changing permissions assigned to Operator

The rights and permissions assigned to the Operator can be changed in one of the following ways:

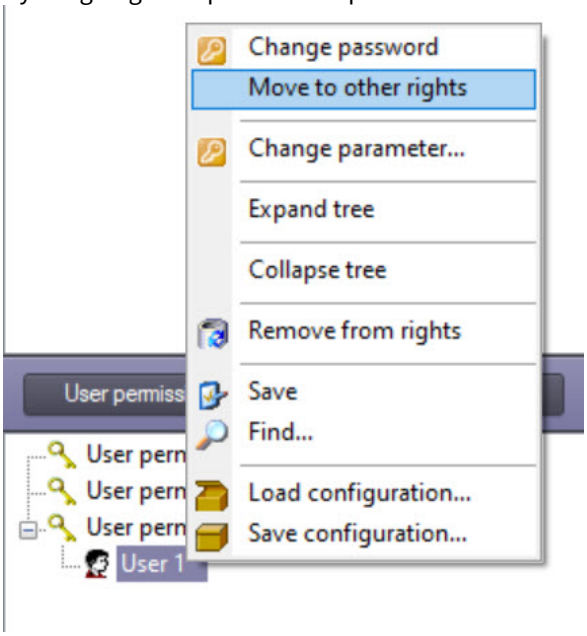
- By deleting the Operator from the old permissions using the **Remove from rights** item in the **User** object context menu and assigning new permissions as described in Assigning the rights and password to operators for authorization in the Intellect. To delete the User, you can also select the User in the list and press Ctrl+Del on the keyboard.



Note

When you click the **Remove from rights** item in the menu, the confirmation is not requested. The Operator permission is deleted immediately.

- By assigning the Operator new permissions with the **Move to other rights** item in the **User** object context menu.



As a result, the **Move to other rights** dialog box opens.

Select the **User permissions** object from the drop-down list, then click the **OK** button. The Operator will be assigned with the selected rights and permissions.

- Edit the **User permissions** object settings selected when registering user's permissions.

> **Attention!**
>
> The changes to user permissions do not apply "on the fly", i.e. the Operator logged into the system should re-login in order for the changes to be applied.

23.5.2 Configuration of the LDAP Service

23.5.2.1 General information about the LDAP Service module

The *LDAP Service* module offers the ability to perform the following actions:

1. Import data from an LDAP address book into the *Intellect* database.
2. Synchronize the *Intellect* database with an LDAP address book.

> **Important!**
>
> All entries stored in an LDAP directory have uid (unique user id) and ou (department) attributes. If these attributes are absent, then LDAP service fails to import and synchronize users between LDAP address book and *Intellect* DB.
> If other attributes are used as unique id and department name in the address book, then these attributes are to be specified while configuring **LDAP Service** – see Configuration of correspondence between address attributes and Intellect DB fields.

When importing or synchronizing, users which have been manually created in the *Intellect* Software System before or after the import operation are not affected.

Importing data and synchronizing the *Intellect* database with an LDAP address book are accomplished using macros (the **LDAP Service** object's **Get all employees** action – see Example macro for user import from LDAP address book; see Creating and using

macros for detailed information about macros). Use a **Timer** object for scheduled synchronization (see Creating and using the Timer object).

The following LDAP attributes are supported by *Intellect:*

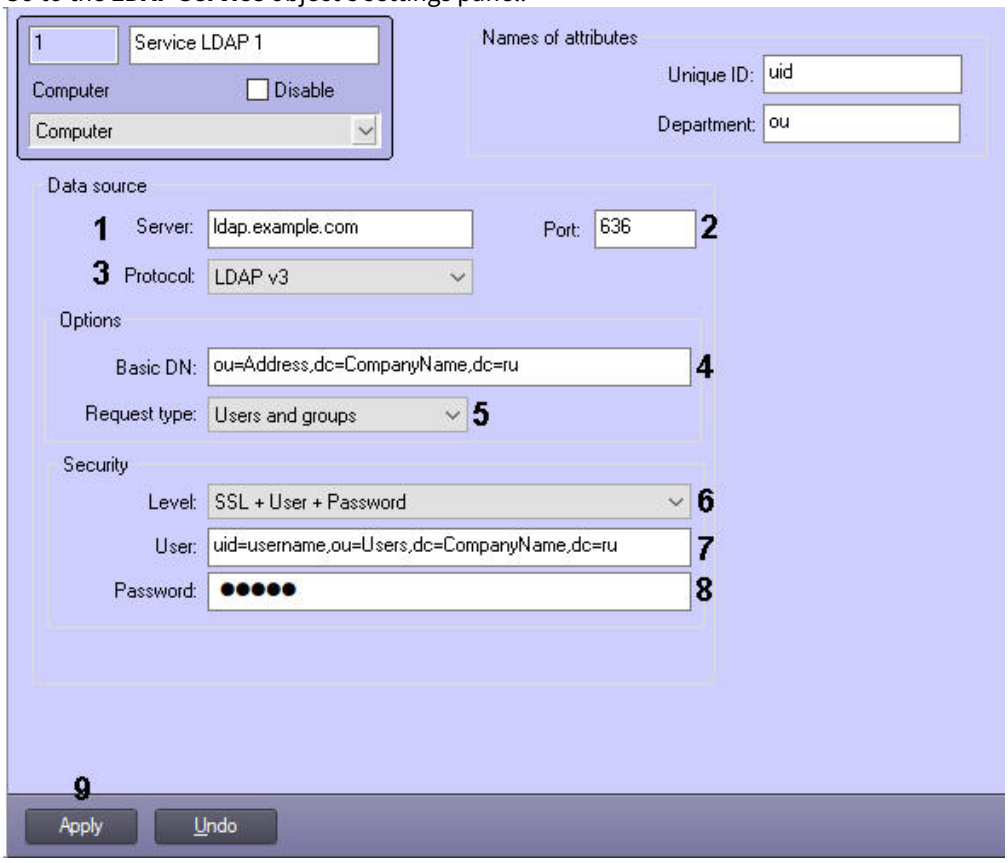
LDAP attribute	Field in Intellect	Commentary
User		
sn	Surname (the **User** object, the name parameter)	If there is no sn attribute in return data, then this entry is ignored. Please note that the last name of the user is stored in the "name" field in the *Intellect* database.
givenname	Name (the **User** object, the surname parameter)	Please note that the first name of the user is stored in the "surname" field in the *Intellect* database.
uid	ID in the external DB (the **User** object, the, external_id parameter)	If there is no uid attribute in return data, then a new employee is created i.e. there is duplication of employee. If another attribute is used as uid in the address book, then this attribute is to be specified while configuring **LDAP Service** – see Configuration of correspondence between address attributes and Intellect DB fields.
mail	E-mail address (the **User** object, the email parameter)	
telephoneNumber	(the **User** object, the phone parameter)	
title	(the **User** object, the post parameter)	
Department		
ou	Department name (the **Department** object, the name parameter)	If another attribute is used as ou in the address book, then this attribute is to be specified while configuring **LDAP Service** – see Configuration of correspondence between address attributes and Intellect DB fields.
Group		
group	User group in **Request type** (see Configuring the connection to the LDAP address book)	The attribute is used to import user groups when selecting the request type **Group** or **Users and groups**.

23.5.2.2 Configuring the connection to the LDAP address book

The connection to an LDAP address book is configured on the **LDAP Service** object's settings panel. This object is created based on a **Computer** object on the **Hardware** tab of the **System Settings** dialog.

The connection to an LDAP address book is configured as follows:

1. Go to the **LDAP Service** object's settings panel.



2. In the **Server** field specify then name of the server on which the LDAP is started (1).
3. In the **Port** field enter the number of the LDAP server port, specified in the previous step, designed to receive incoming connections (2).
4. Select the version of the LDAP protocol being used from the **Protocol** dropdown list (3).
5. In the **Basic DN** field specify the unique identifier of the LDAP base entry that will be the first when the search for users starts (4).

> **Example.**
>
> The example of how to fill in the **Basic DN** field: ou=Address,dc=MyCompany,dc=com

6. From the **Request type** drop-down list, select the type of user import (5):
   a. **Users**: only users are imported.
   b. **Groups**: only groups are imported.
   c. **Users and groups**: both groups and users are imported.
7. Select the connection security method being used by the LDAP server from the **Level** dropdown list (6).
8. In the **User** field specify the unique name of the user with rights to access the LDAP address book (7). *Intellect* will access the LDAP address book under this username. Up to 255 characters.

> **Example.**
>
> The example of how to fill in the **User** field: uid=user.name,ou=Users,dc=MyCompany,dc=com

9. Enter the user's LDAP address book password in the **Password** field (8).

> **Note.**
>
> The username and password should not be entered if the selected connection security method does not require them.

10. To save the settings, click the **Apply** button (9).

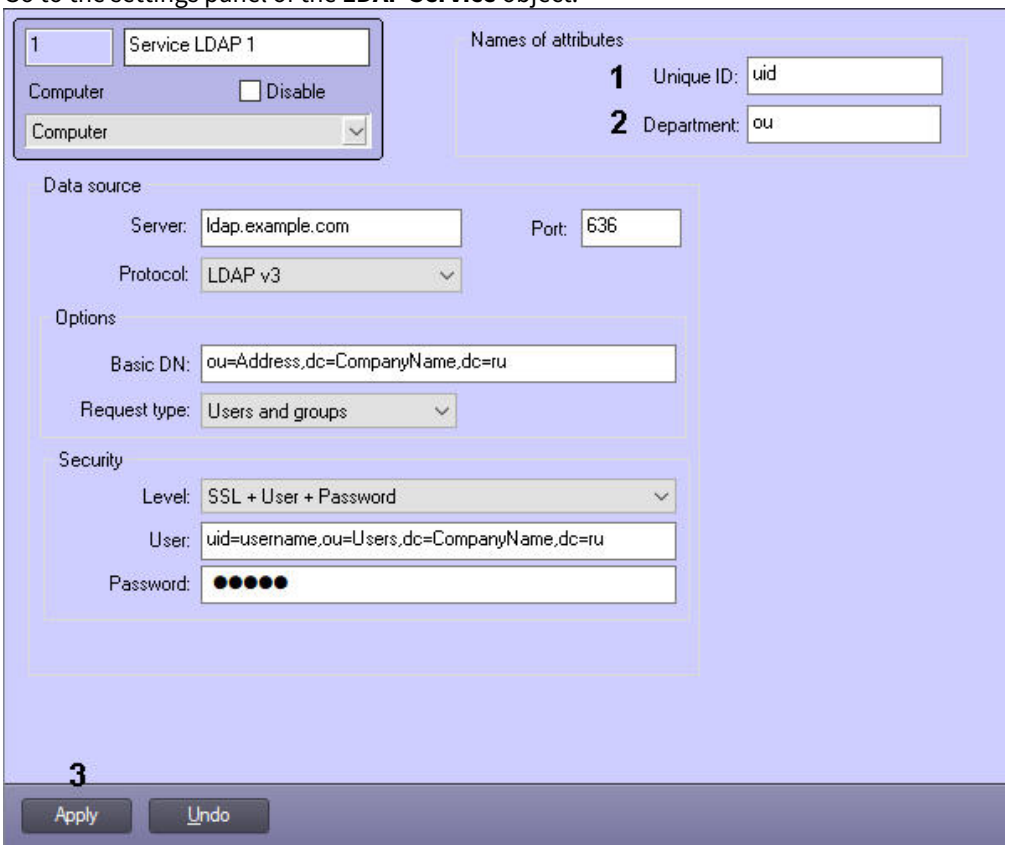
This completes the process of configuring the connection to an LDAP address book.

23.5.2.3 Configuration of correspondence between address attributes and Intellect DB fields

Default correspondence between address attributes and *Intellect* DB fields is given in General information about the LDAP Service module section. The correspondence between attributes and fields for unique ID and department name can be modified.

Configure correspondence between address attributes and *Intellect* DB fields as follows:

1. Go to the settings panel of the **LDAP Service** object.



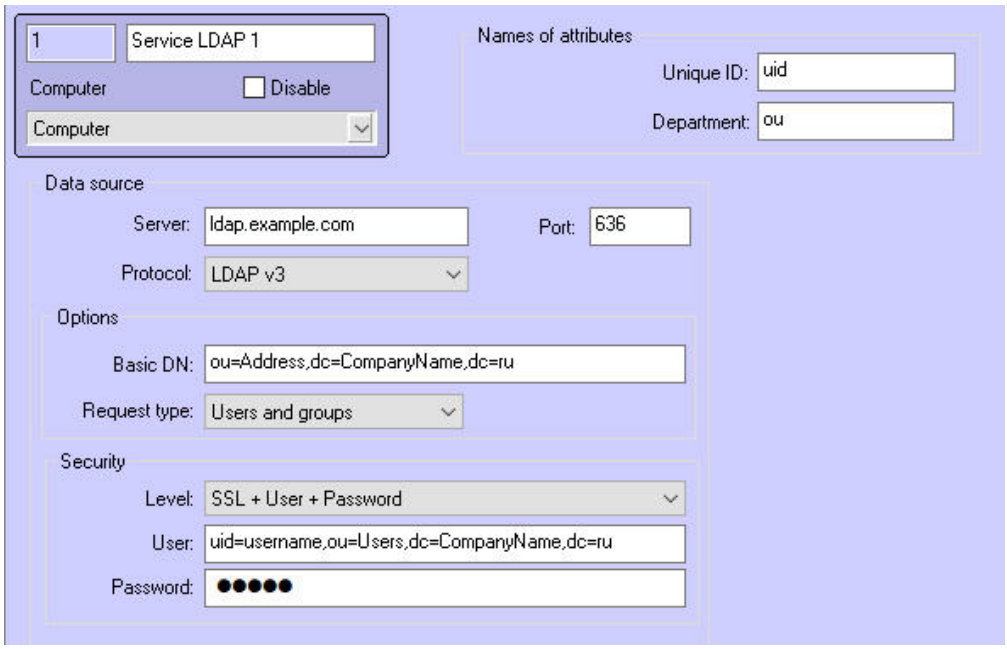
2. In the **Unique ID** field specify the attribute name that is a unique ID corresponding to external_id parameter of the **User** object in *Intellect* (1).
3. In the **Department** field specify the attribute name that is the name of the department and corresponding to the name field of the **Department** object in *Intellect* (2).
4. To save the changes click the **Apply** button (3).

Configuration of correspondence between address attributes and *Intellect* DB fields is now complete.

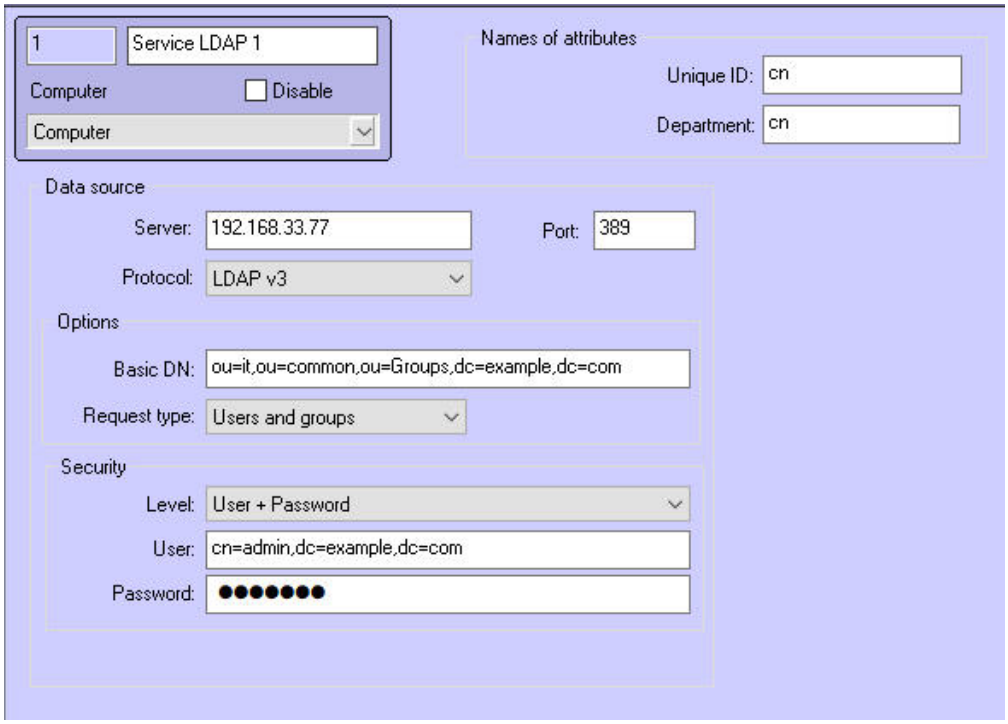
23.5.2.4 Examples of LDAP Service configuration

Find below some examples of the LDAP Service object configuration for use with different systems.

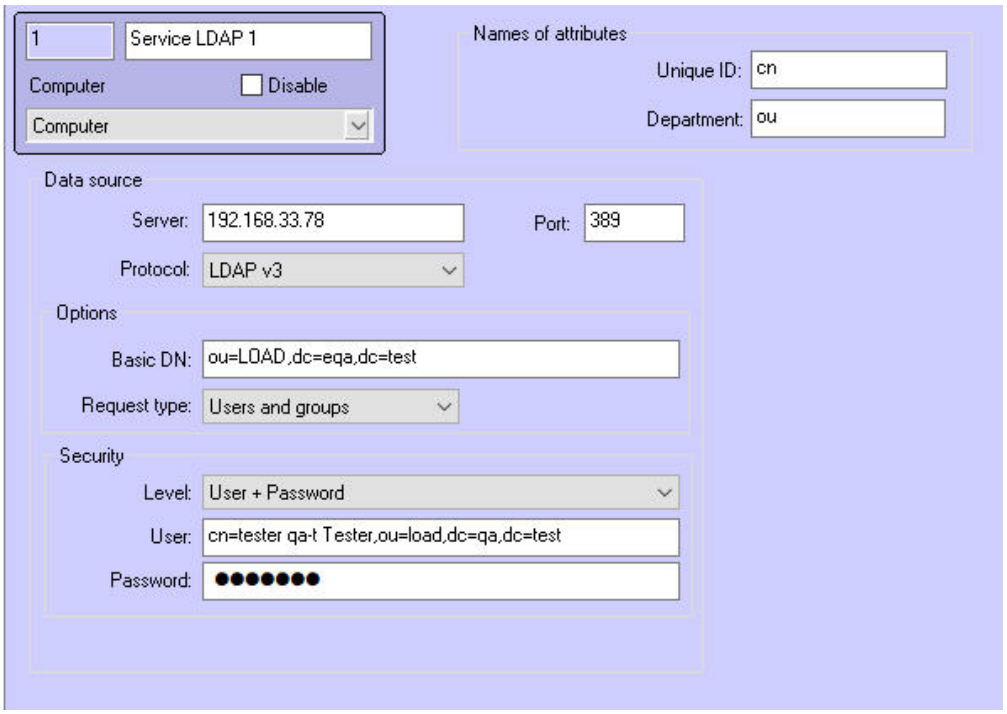
For LDAP address book:



For OpenLdap:

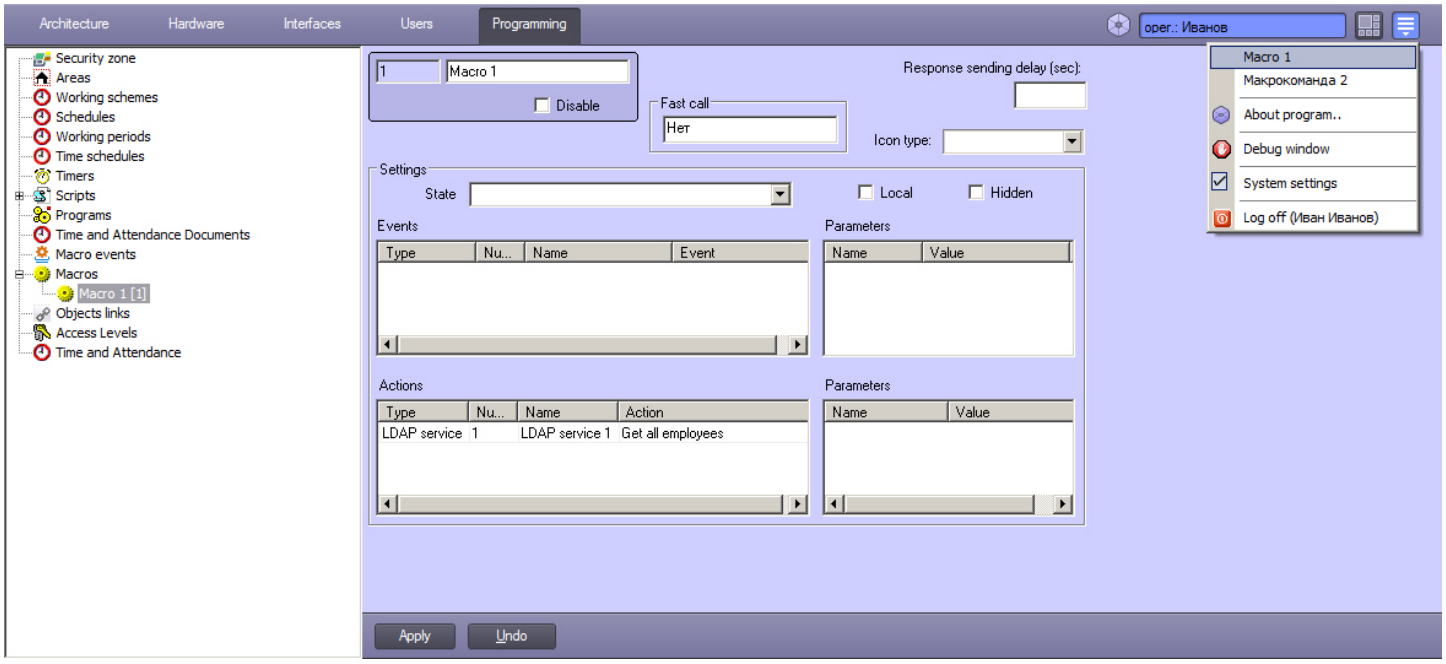


For Active Directory based on Windows Server 2012 R2:



23.5.2.5 Example macro for user import from LDAP address book

Create and run the below macro after the **LDAP service** object is configured to import user accounts from LDAP address book to *Intellect* database:



See Creating and using macros for detailed information about macros.

23.5.3 Active Directory configuration

23.5.3.1 General information about Active Directory and Intellect operation

The joint operation of *Intellect* and Active Directory means that the *Intellect* users and user permissions are connected with the Active Directory users and security groups. User accounts are pre-imported into *Intellect* from the LDAP address book—see Configuration of the LDAP Service.

Prior to configuring the *Intellect* and Active Directory joint operation, it is necessary to create the groups in Active Directory that correspond to the user permissions in *Intellect*. It is not recommended to use the Active Directory groups created earlier for other purposes. Each user should be included in only one of the created groups, otherwise the correct joint operation of *Intellect* and Active Directory is impossible.

The Active Directory operation is configured as follows:

1. Configuration of the LDAP Service.
2. Users import from LDAP address book to *Intellect* database—see Example macro for user import from LDAP address book.
3. Connecting the Intellect and Active Directory users.
4. Connecting the Intellect user permissions to Active Directory groups.
5. Starting the Active Directory synchronization.

> **Attention!**
>
> The connection between the *Intellect* user permissions and Active Directory security groups must be configured by an administrator who has full Active Directory rights in Windows.

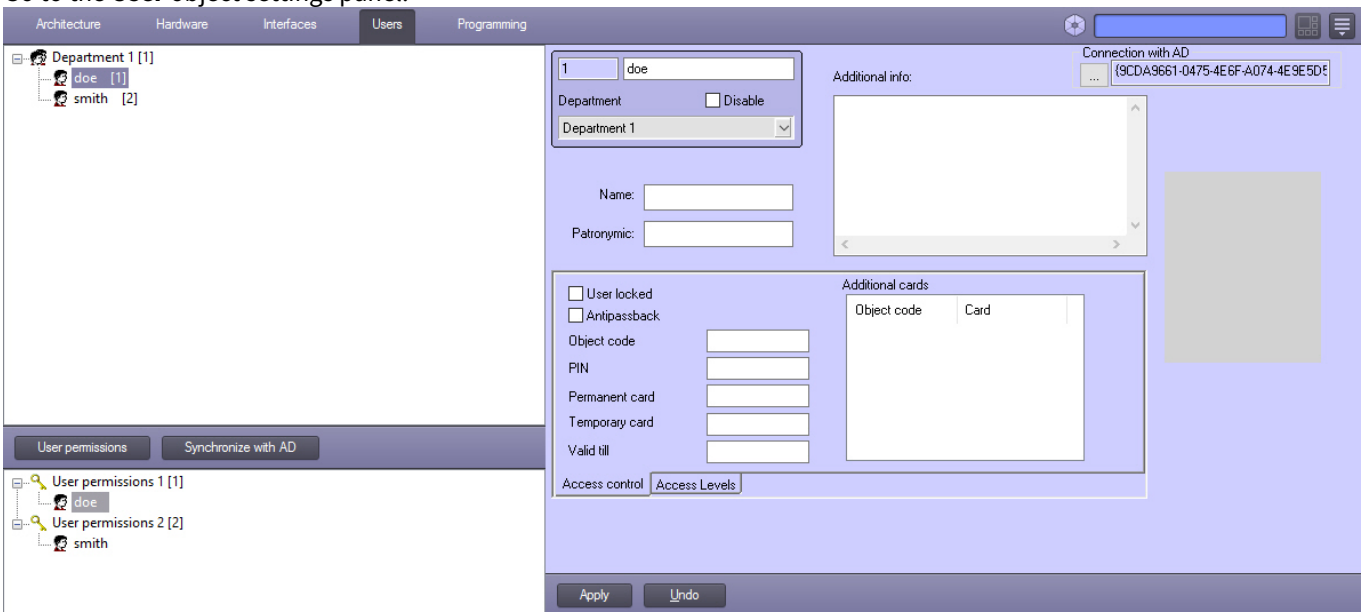
After the *Intellect* and Active Directory joint operation is configured, the Active Directory users are able to launch, use and configure *Intellect* using their Windows account in accordance with the *Intellect* user permissions. The Active Directory users which are connected with the *Intellect* users, but do not belong to any of the groups associated with the *Intellect* user permissions, will not be able to launch *Intellect*.

Important! The automatic changes synchronization is not supported, that is, if the Active Directory user is deleted, disabled, moved to another group, etc., it is necessary to perform the Active Directory synchronization in order to apply these changes in *Intellect*.

23.5.3.2 Connecting the Intellect and Active Directory users

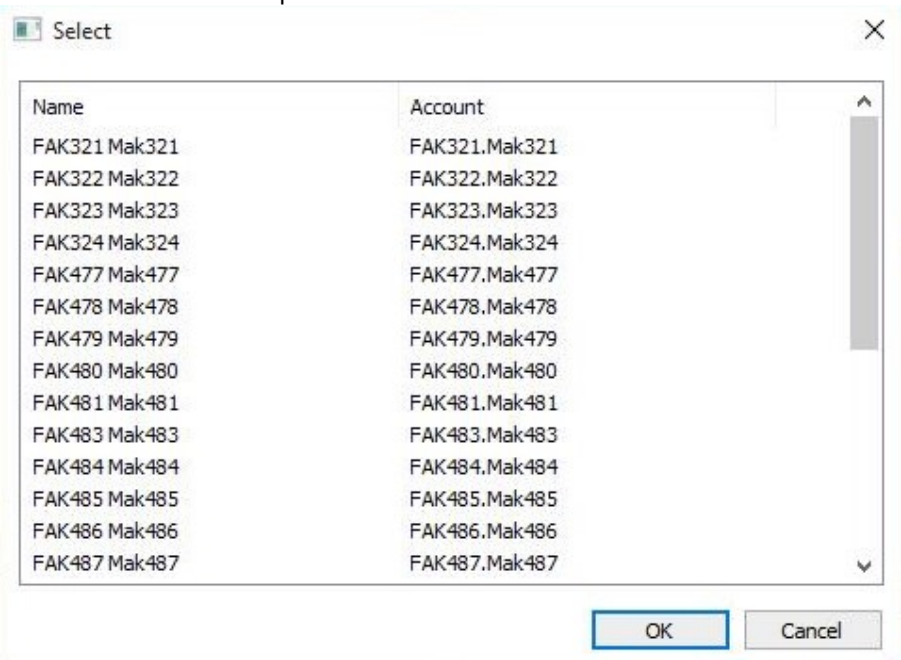
Configure the connection between the *Intellect* users and the Active Directory users as follows:

1. Go to the **User** object settings panel.

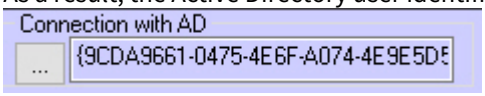


2. Click the **...** button in the **Connection with AD** group.

3. The **Select** window will open.



4. In this window, select the Active Directory user and click the **OK** button.
5. As a result, the Active Directory user identifier will be displayed in the **Connection with AD** field.



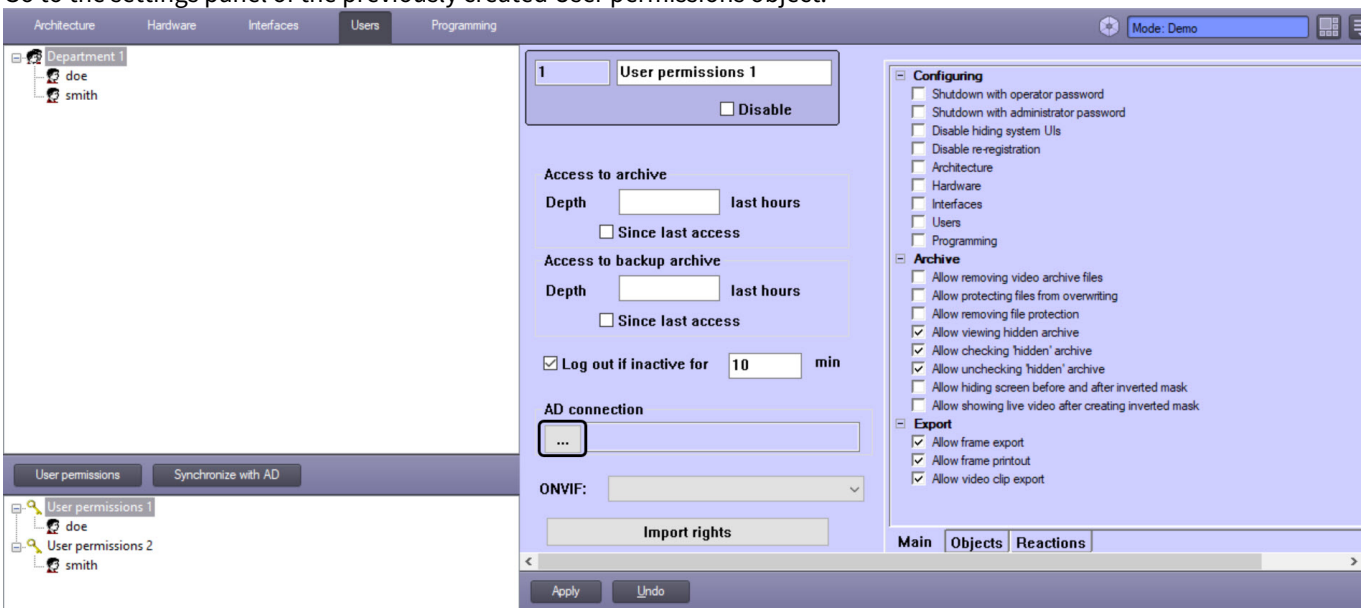
6. Click the **Apply** button.
7. Repeat steps 1-6 for all required users.

The connection between the *Intellect* users and the Active Directory users is configured.

23.5.3.3 Connecting the Intellect user permissions to Active Directory groups

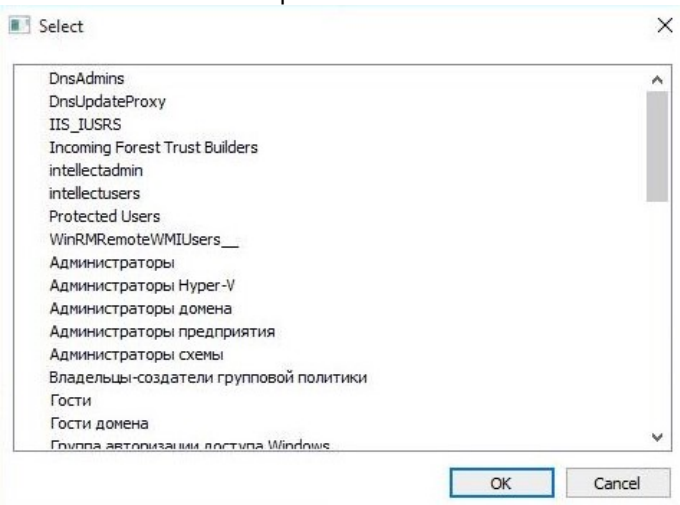
Configure the connection between the Intellect user permissions and Active Directory security groups as follows:

1. Go to the settings panel of the previously created User permissions object.

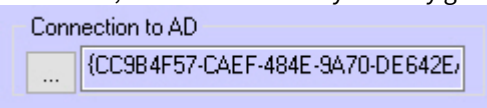


2. Click the **...** button in the **Connection to AD** group.

3. The **Select** window will open.



4. In this window, select the Active Directory security group and click **OK**.
5. As a result, the Active Directory security group identifier will be displayed in the **Connection to AD** field.



6. Click **Apply**.
7. Repeat steps 1-6 for all required user permissions.

The connection between the Intellect user permissions and Active Directory security groups is configured.

23.5.3.4 Starting the Active Directory synchronization

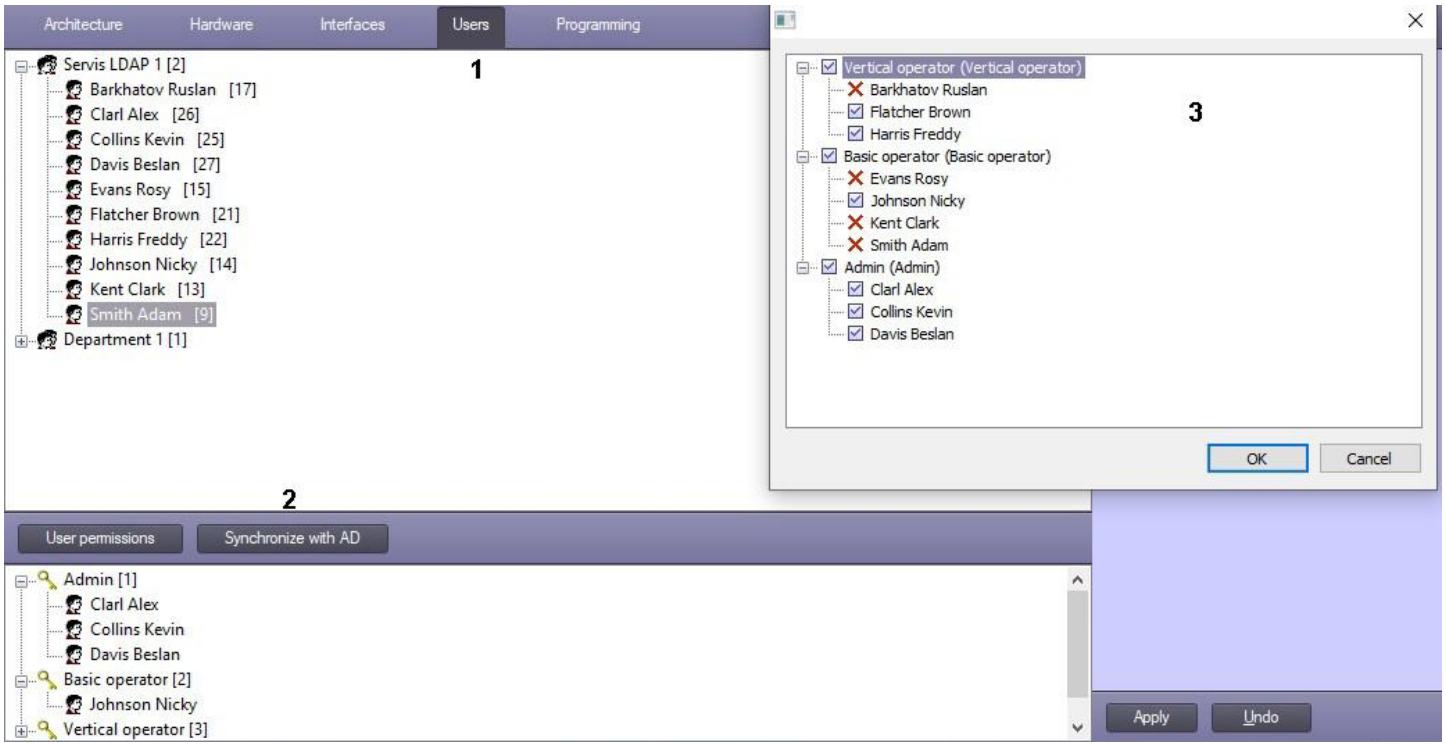
The Active Directory synchronization should be started both after connecting the *Intellect* users and user permissions with the corresponding Active Directory objects, and in case the Active Directory users and security groups are changed: deleted, disabled, moved to another group, etc.

The following methods of Active Directory synchronization are available:

1. Using the **Users** section in *Intellect*.
2. Using scripts and macros.
3. Using the ADSyncOnStart registry key (see Registry keys reference guide).

To start the Active Directory synchronization in *Intellect*, do the following:

1. In the **Users** section (**1**), click the **Synchronize with AD** button (**2**).
2. The updated structure of the *Intellect* users and user permissions will be displayed in the opened window (**3**). Set the checkboxes next to the objects that need to be synchronized.
3. Click the **OK** button.



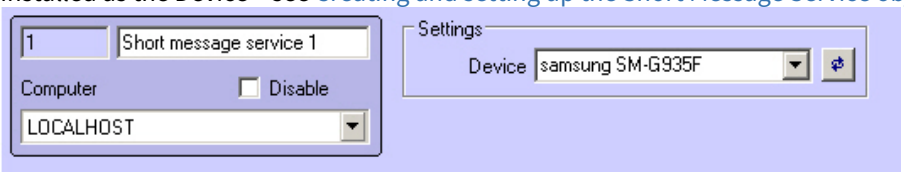
To start the Active Directory synchronization using a script or a macro, use the following values: objtype = SLAVE, action = AD_SYNC. Example: SLAVE|<Server Name>|AD_SYNC.

23.5.4 Configuring two-factor authentication

Intellect allows the use of two-factor authentication when a user logs in at startup. In this case, the user will have to enter login+password credentials and a code from a short message (SMS), which is sent to the user's phone number.

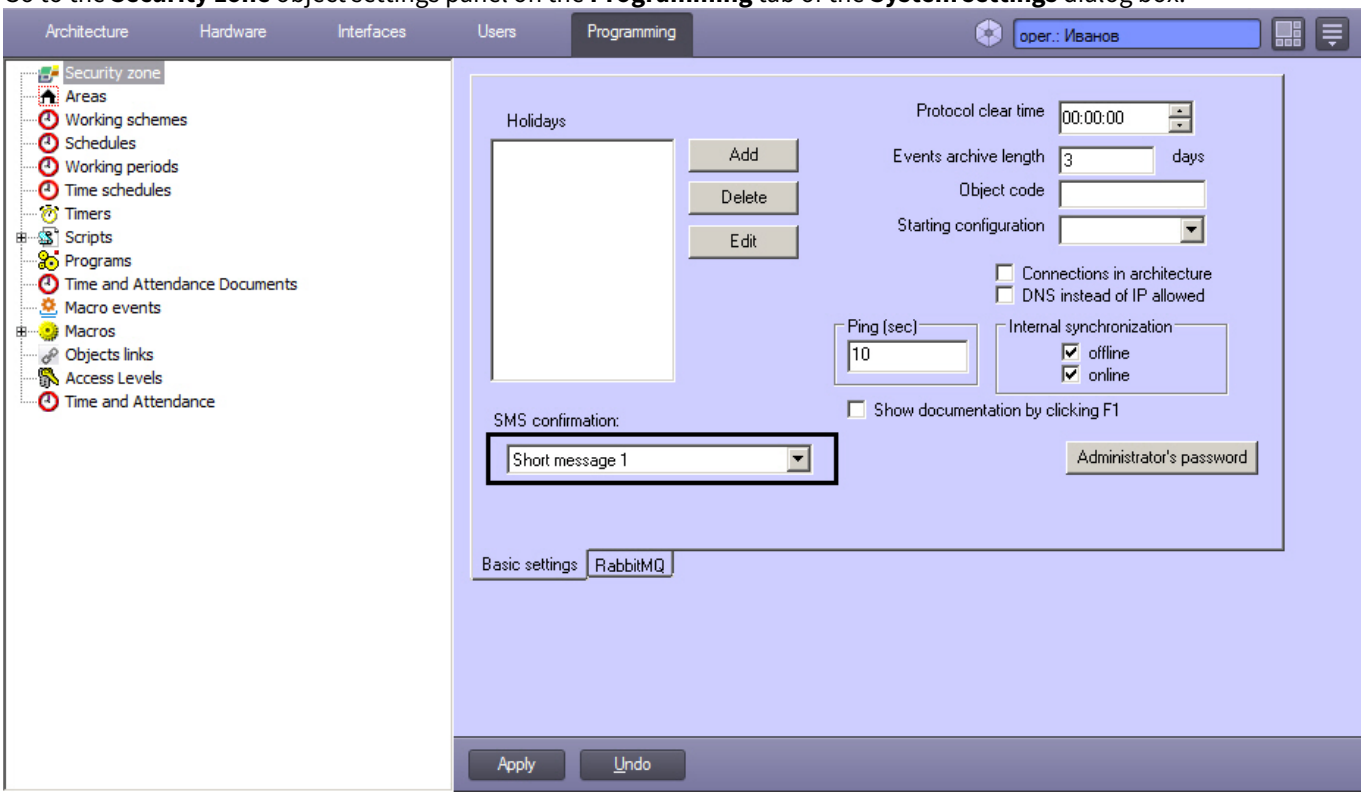
Configure two-factor authentication as follows:

1. Install and configure the **Intellect SMS Sender** app on the smartphone – see Android-based Intellect SMS Sender Mobile Application. User Guide. This smartphone will be further used as modem, i.e. the short messages will be sent from its SIM card. Please notice that the mobile operator may charge for the SMS service.
2. Create and configure the **Short message service** object; make sure to select the smartphone with **Intellect SMS Sender** installed as the Device – see Creating and setting up the Short Message Service object.



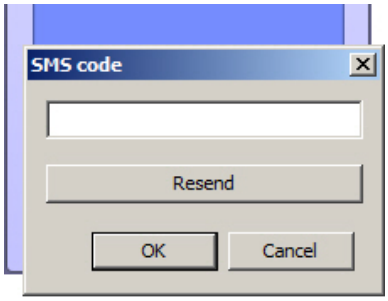
3. Create the **Short message** object; all settings may be left with default values – see Creating and setting up the short messages.
4. Create and configure users and permissions, make sure to enter the phone number for the users – see Rights administration.

5. Go to the **Security zone** object settings panel on the **Programming** tab of the **System settings** dialog box.



6. From the **SMS confirmation** drop-down list, select the **Short message** object created on step 3.
7. Click the **Apply** button.

As a result, a randomly generated code from SMS automatically sent to the user's phone number will be requested after entering the password when starting *Intellect*:



See also Intellect software start and shutdown.

The two-factor authentication is now configured.

23.6 System settings (the Programming tab)

23.6.1 Configuring internal synchronization

By default *Intellect* uses internal synchronization, i.e. there is data interchange between computers in the distributed configuration (see Configuring the interaction of distributed system components):

1. If a computer is in the distributed system, then all the events are sent just as they appear. This is online synchronization.
2. If a computer lost connection with the distributed system and cannot interchange the events with other computers, then events that are to be sent to this computer are stored in the database and sent on it after the computer is reconnected. This is offline synchronization.

If the computer has not been in the distributed system for too long, then the accumulated sequence of events can be quite long and processing of all these events can take much time. Thus offline synchronization can be disabled.

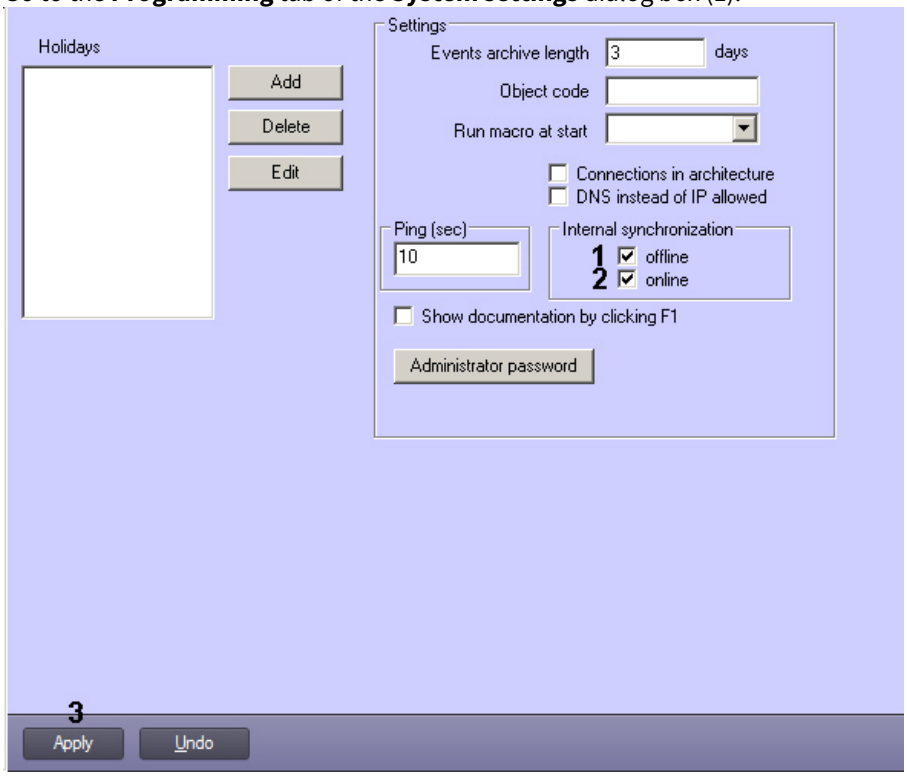
Online synchronization can also be disabled, i.e. events won't be sent.

> **Note.**
>
> Internal synchronization, both offline and online, can be enabled and disabled for all computers in the distributed system.

> **Important!**
>
> DB synchronization must be configured when any internal synchronization mechanism is disabled — see Database synchronization setup and Configuring the Event Viewer databases synchronization.

Configure internal synchronization as follows:

1. Go to the **Programming** tab of the **System settings** dialog box (1).



2. Select the **Security zone** object in the tree (2). The settings panel of this object is displayed on the right side of the **System settings** dialog box.
3. To disable offline synchronization, set the **offline** checkbox unchecked in the **Internal synchronization** group (3).
4. To disable online synchronization set the **online** checkbox unchecked in the **Internal synchronization** group (4).
5. Click the **Apply** button (5).

Internal synchronization is now configured.

23.6.2 Connection of objects with cameras

In the Intellect software package it is possible to link cameras to objects.

Objects assigning is performed on the settings panel of the **Objects connection** object on the **Programming** tab of the **System settings** dialog window.

It is possible to link several cameras to each object and several and several objects to each camera. Also it is possible to link groups of objects and cameras.

To configure connection of objects with cameras, do the following:

1. Go to the settings panel of the **Objects connection** object.

2. In the **Select object** table specify type, identification number and name (is entered automatically after select type and id of camera) of all required objects.
3. In the **Select camera** table specify identification number and names of all required cameras.
4. To save changes click the **Apply** button.

To get list of objects linked to camera and list of cameras linked to object, use the script (see The GetLinkedObjects method section).

Configuring of connection objects with cameras is completed.

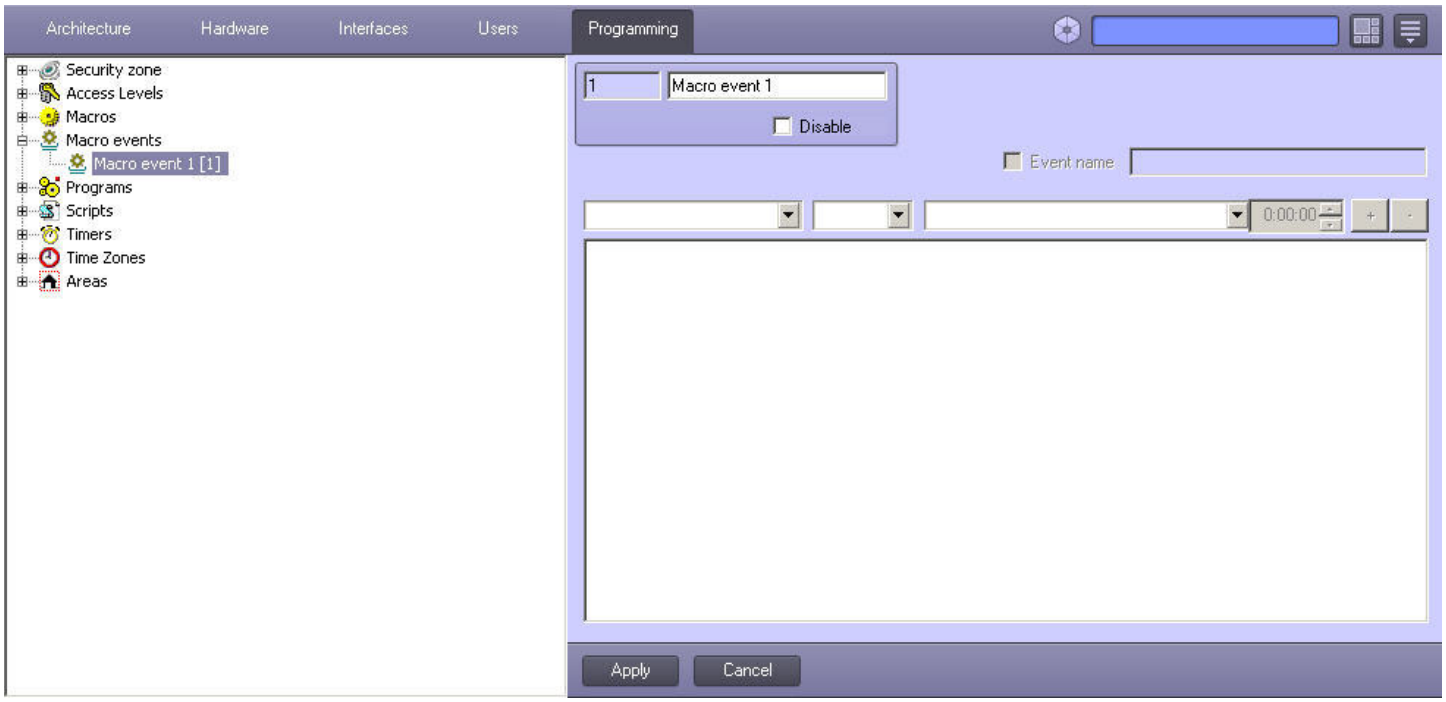
23.6.3 Creating and configuring Macro events

Macro events are designed for controlling required events in the defined time interval and for generating new events in the system in case of appearing or not some chain of events.

Macro events are presented by **Macro event** objects in the *Intellect* software.

Generated macro event can be used in macros or scripts to perform some actions.

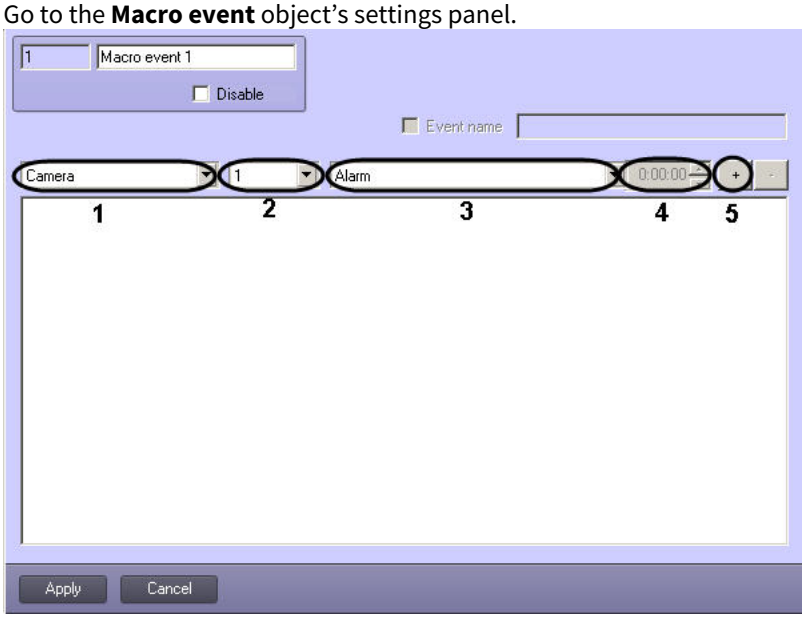
The **Macro event** object is created and configured on the basis of **Macro events** object on the **Programming** tab of the **System settings** dialog box.



23.6.3.1 Configuring the macro events

To configure macro events, do the following:

1. Go to the **Macro event** object's settings panel.

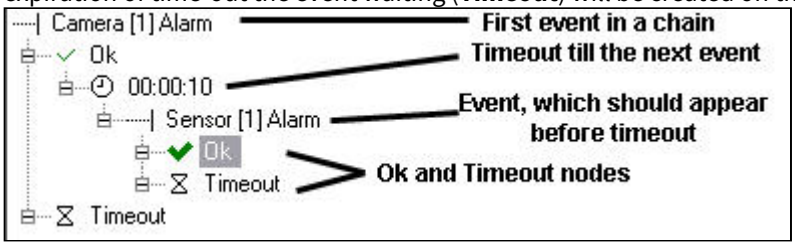


2. Select the object type from the drop-down list (1).
3. Select the object ID from the drop-down list (2) if it's required. If the object ID is not selected, then events from all objects of such type will be considered in.
4. Select the event type from the drop-down list (3). All events from the selected object or objects will be considered in if the event type is not selected.
5. In the field (4) enter the time period in HH:MM:SS format during which the selected event occurrence after occurrence the previous one is waiting for. The occurrence time for the first event in the chain is not specified. For other events the time of waiting is 15 seconds on default.

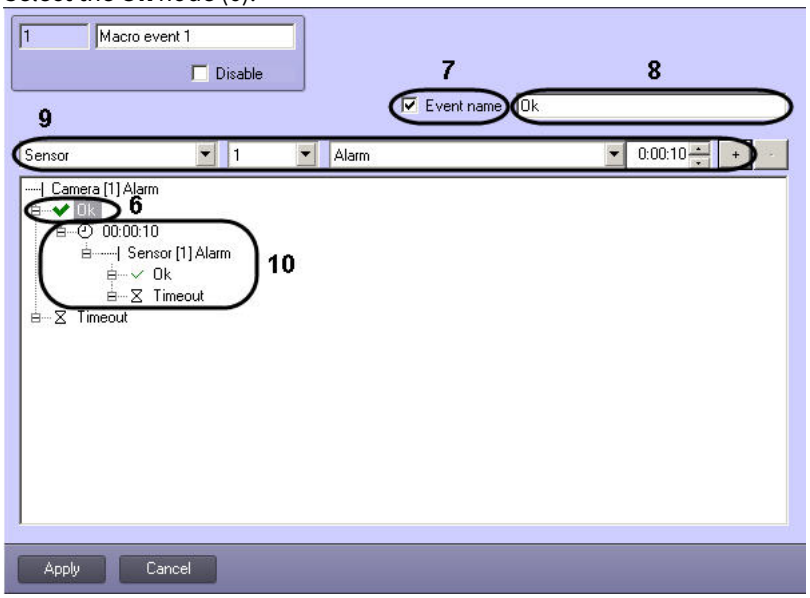
> **Note.**

To edit the time-out period select the occurrence time of event in the chain and enter the time again in the text field.

6. Click the **+** button (5). The event will be added to the chain with name in the “Object type [object number] Event type” format. Nodes corresponding to the event occurrence on the specified time interval (**Ok**) and nodes corresponding to the expiration of time-out the event waiting (**Timeout**) will be created on the basis of the event.



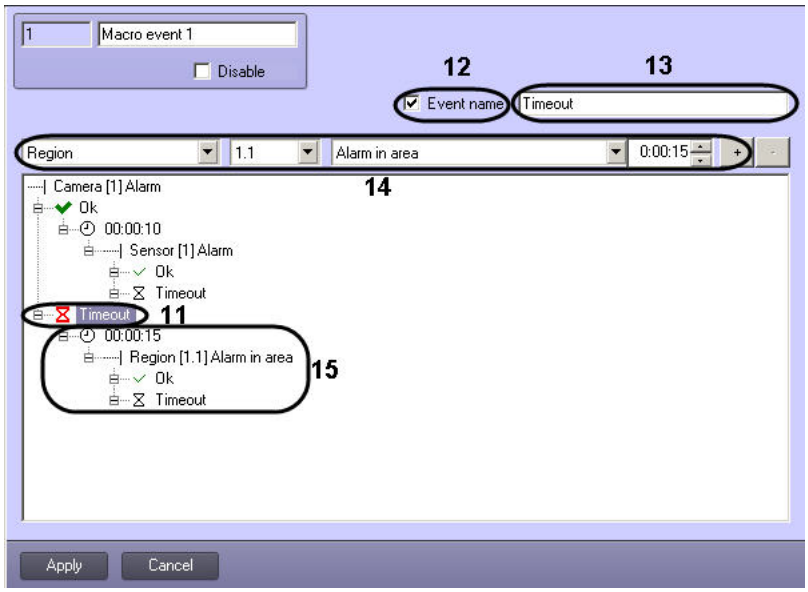
7. Set the next event in the chain in case of performing the previous chain of conditions:
   a. Select the **Ok** node (6).



   b. Set the **Event name** (7) checkbox and enter the name of generated event in the text field (8) in case of macro event is to be generated when all previous events in the chain have occurred. The node will be marked by ✔ sign.

> **Note.**
>
> The **Event name** is limited by 120 symbols.

   c. Set the Event type (9) as it was performed in 1-5 steps.
   The event will be added to the chain on the basis of the **Ok** node (10).
8. Set the next event in the chain in case of the time-out of waiting the performing previous chain of conditions was expired:
   a. Select the **Timeout** node (11).



b. Set the **Event name** (12) checkbox and enter the name of generated event in the text field (13) in case of macro event is to be generated when all previous events in the chain except the last one have occurred. The node will be marked by ⧖ sign.

> **Note.**
>
> The **Timeout** condition created on the basis of the first event in the chain is performed if only the first event of the chain has occurred for the specified time.

> **Note.**
>
> The Event name is limited by 120 symbols.

c. Set the **Event** type (14) as it was performed in 1-5 steps.
The event will be added to the chain on the basis of the **Timeout** node (15).

9. Repeat steps 7 and 8 with **Ok** and **Timeout** nodes created on the basis of new events if it's required.
10. Click the **Apply** buttons.

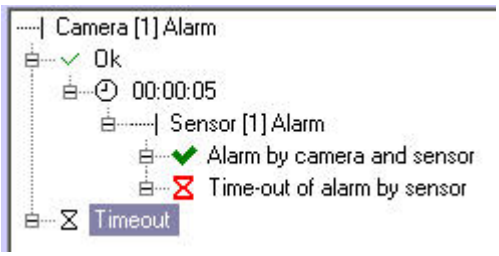
> **Note.**
>
> To delete the event from the chain select its name or occurrence time and click the **–** button. All underneath events in the chain will be also deleted.

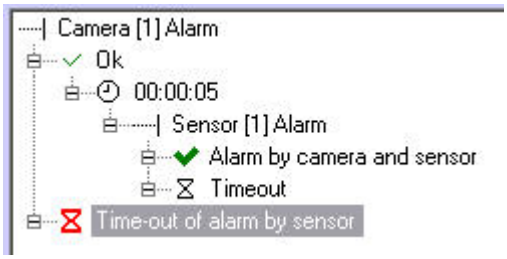
Configuring the macro events is completed.

23.6.3.2 Example of macro event

It is required to generate events with the "Alarm by camera and sensor" name, when alarm by Sensor 1 is initiated less than in 5 seconds after alarm by Camera 1. Generate the event with the "Time-out of alarm by sensor" name if alarm by sensor is not initiated or initiated more than in 5 seconds after alarm by camera.

To perform it, create the **Macro event** object and configure the chain of events by one of the following ways:





23.6.4 Creating and using macros

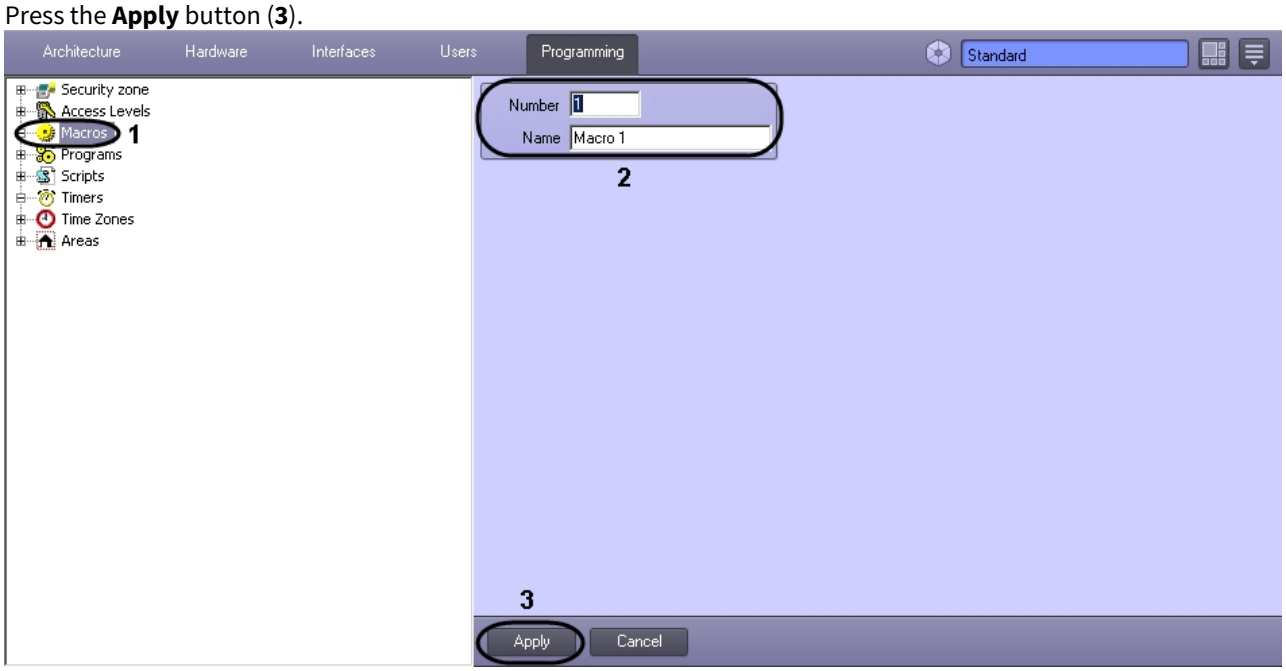
A macro in the *Intellect* system is a system object, designed to maintain logic interaction among other system objects. The **Macro** object settings define the conditions and the corresponding actions. The **Macro** objects are used for automatic controlling of the surveillance system.

An unlimited number of **Macro** objects can be created in the system.

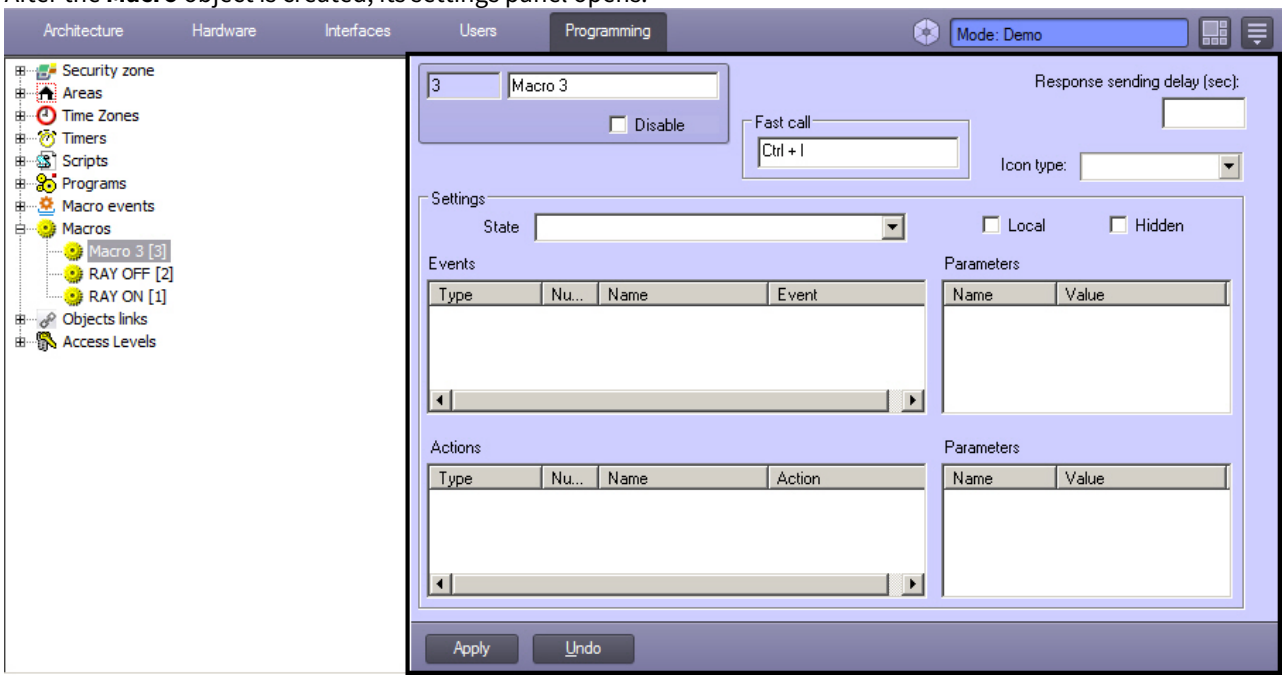
23.6.4.1 Creating macros

To create a macro, do the following:

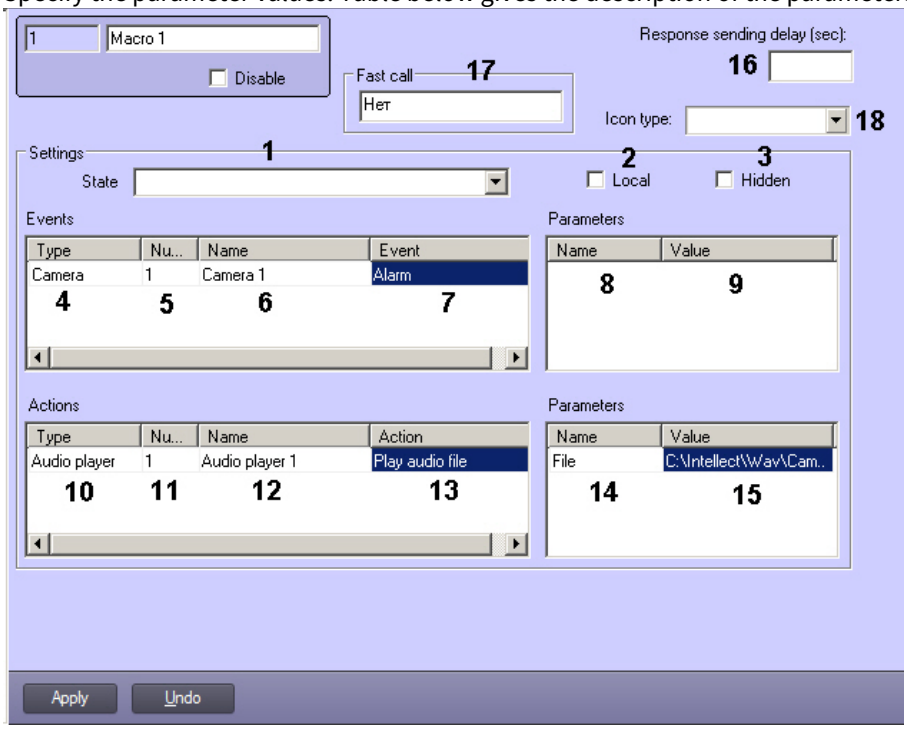
1. Create the **Macro** object.
    a. Choose the **Macros** object in the objects tree of the **Programming** tab (**1**).
    b. Specify the name of the **Macro** object (**2**).
    c. Press the **Apply** button (**3**).



After the **Macro** object is created, its settings panel opens.



2. Specify the parameter values. Table below gives the description of the parameters.



Note.

To add a row to the **Events** or **Actions** table, select a cell in the bottom row of the table and press the "down" arrow on your keyboard.
To delete a row, select a cell in the row and press the Ctrl+Del buttons on the keyboard.

№	Name	Field type	Description	Format	Default value	Value range
Settings group						

№	Name	Field type	Description	Format	Default value	Value range
1	State	Select from drop-down list, or type in	The message to display during macro execution. A Standard value is selected, no message is displayed.	-	Empty	A list of available messages plus Standard.
2	Local	Checkbox	If the checkbox is checked, the macro can be executed on the local computer only. *Note. This checkbox does not apply to Hide and Show reactions of any Display. Regardless of the checkbox, wen called from Server/RAW, they are executed on the Server and all connected Clients; when called on Client, they are executed only on the client.*	-	No	**Checked** - local only. **Unchecked** – any computer.
3	Hidden	Checkbox	If the checkbox is checked, the macro cannot be executed manually.	-	No	**Checked** – execute. **Unchecked** – don't execute.
Events table						
4	Type	Drop-down list	Defines the object to be the source of the event that will trigger this macro.	-	Empty	All active device and module objects
5	Number	Drop-down list	Defines the number of the object to be the source of the event that will trigger this macro.	-	Empty	The numbers of all active device and module objects. If the **Computer** object is selected in the **Type** column, enter its name here.
6	Name	Enters automatically on right-click	Information type	-	Empty	Enters automatically according to the **Type** and **Number** values
7	Event	Drop-down list	Event type	-	Empty	The list of registered event types
Parameters table (is set, when parameter should be set for events, selected in **Events** table)						
8	Name	Automatically	Displays name of event's parameter	Latin alphabet, digits and characters	Empty	Depends on the event, selected in **Events** table
9	Value	Entering of the text into the field	Set the value of event's parameter	Latin alphabet, digits and characters	Empty	A line of any characters. The number of characters is from 1 to 250.
Actions table						
10	Type	Drop-down list	Defines the object to be the source of the event that will trigger this macro.	-	Empty	All active devices and module objects

№	Name	Field type	Description	Format	Default value	Value range
11	Number	Drop-down list	Defines the number of the object to be the source of the event that will trigger this macro.	-	Empty	The numbers of all active devices and module objects. If the **Computer** object is selected in the **Type** column, enter its name here. If the field is left blank, the reaction will be performed for all objects of the selected type. If you enter the symbol # in the field, the identifier of the object from which the event was received will be substituted into the reaction. Object types in **Events** and **Actions** tables may differ. When the macro is run manually from the main control panel, the # symbol is treated as if the field was blank, i.e. the macro is executed for all objects of the selected type. Example of using the # symbol: disarm the camera if the “Detach” event is received from it.
12	Name	Automatically	Displays name of the selected object	Name of objects, registered in the system and of specified type	Empty	A line of any characters. The number of characters is from 1 to 60.
13	Action	Drop-down list	Reaction to be executed for the selected object when the event is registered	-	Empty	The list of registered reaction types for the selected object type
		Parameters table (is set, when parameter should be set to perform action, selected in **Actions** table)				
14	Name	Automatically	Displays name of action’s parameter	Latin alphabet, digits and characters	Empty	Depends on the action, selected in **Actions** table
15	Value	Entering of the text into the field	Set the value of action’s parameter	Latin alphabet, digits and characters	Empty	A line of any characters. The number of characters is from 1 to 255.
Outside the groups						
16	Response sending delay (sec)	Entering of the value into the field	Sets time period (in seconds) that must pass after events specified in the **Events** column occur and before executing reactions specified in the **Actions** column. ***Note.*** *If the events reoccur before the specified time period expires, the reaction execution wait period is prolonged, i.e. reactions will be executed only once when*	Integer number	-	>0

№	Name	Field type	Description	Format	Default value	Value range
			events do not reoccur over the specified period.			
17	The **Fast call** field	Left-click in the field and click the required key combination	Sets a shortcut for a macro. If the same combination of hot keys is set for several macros, when clicking a key combination, all of these macros run. *Note. You can disable keyboard shortcuts for macros using the UseHotKeys key — see Registry keys reference guide.*	Key combinations	No	Some keys of the main or numeric keyboard, as well as these keys in combination with Shift, Ctrl and Alt.
18	The **Icon type** dropdown list	Select in the dropdown list.	Sets a set of icons for displaying a macro on the map. By default, an empty value is set for all macros which corresponds to the Macro 1 icon. *Note. Changing the icon appearance will take effect after restarting the map interface. To restart the interface, restart Intellect or log in once again under the corresponding Operator account.*	Available icon appearances on the map	-	Macro 1 - Macro 7, empty value.

Note.

As action's parameter **Play sound file** may be used only files of WAV format. Otherwise action **Play sound file** is not carried out.

Note.

If required action, event or parameter is absent in the corresponding table, add it in the ddi-file with the ddi.exe utility (see Editing the external setting file (intellect.ddi) using the ddi.exe utility)

Note.

Compressed sound in WAV format may be played back incorrectly, that's why it is strongly recommended to play back only PCM WAV files. Maximum values of frequency and depth of files digitization for playing back are determined by technical characteristics of digital to analog converter of the installed video card.

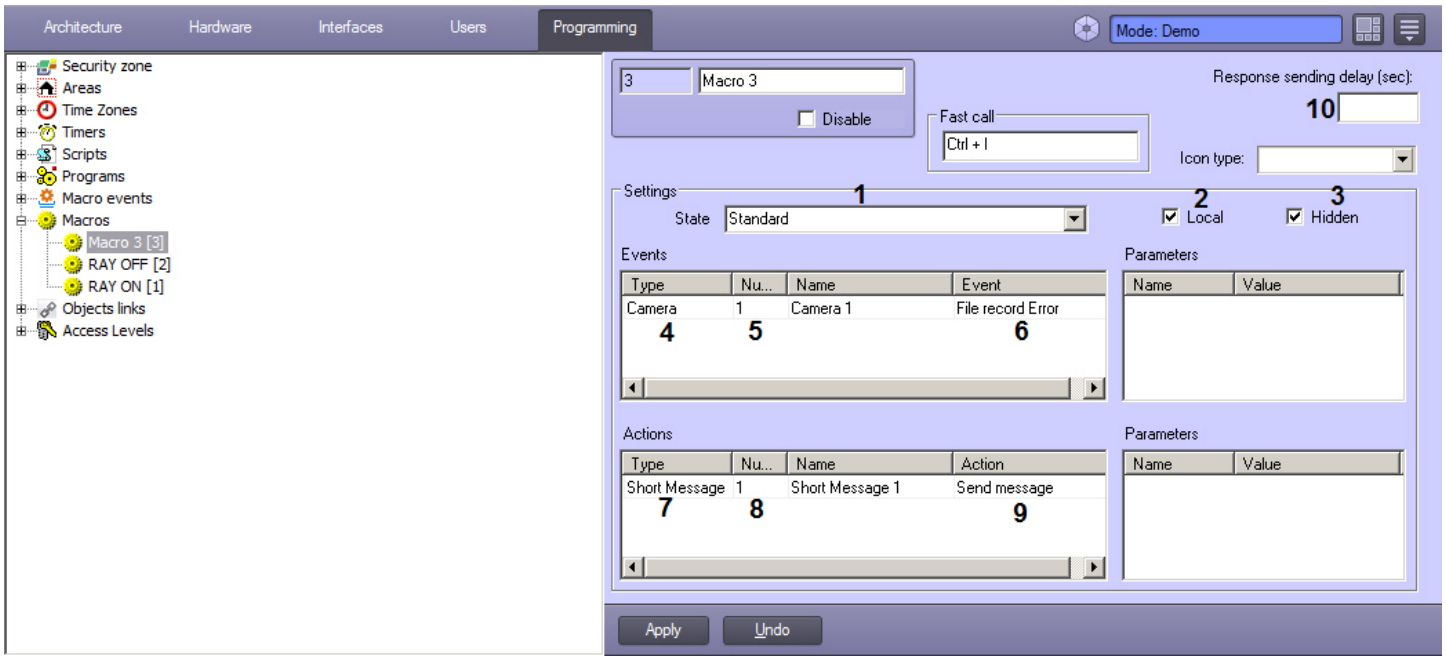
3. Click the **Apply** button to save the settings.

23.6.4.2 Examples of macros

Macros are used to automate the actions of the operator. They inform the operator or administrator about software failures, automate the backup process, etc.

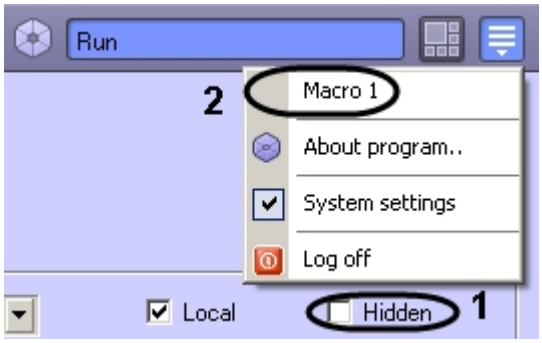
Let's consider the macro that generates the voice message and sends it to the specified telephone number. The message should be sent on a condition – the 'write to disk' error. To create the macro for sending the voice message, do the following:

Create a **Macro** object in the objects tree of the **Programming** tab.



1. Specify the **State** parameter (1).
2. Check the **Local** checkbox if the macro should be sent from the local computer only, if necessary (2).
3. Check the **Hidden** checkbox if the macro should be sent automatically, if necessary (3).
4. If the manual start of macros from the main control panel of Intellect software should be forbidden, set the **Hidden** checkbox (3).
5. Select the number of the object to be the source of the event generating the message (4, 5).
6. Select the name of the event to activate sending of the message (6).
7. Choose the **Voice Message** object in the **Type** column (7).
8. Choose the number of the **Voice Message** object to be sent by the macro (8).
9. Choose **Send Message** in the **Action** column (9).
10. If a voice message is to be sent some time later the event occurs, specify the **Response sending delay (sec.)** parameter value (10).
11. Press the **Apply** button.

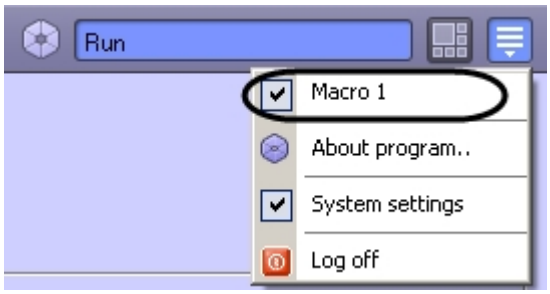
If the **Hidden** checkbox is not checked, the macro will need manual activation, which is done by clicking the **Run** button in the **Main control** menu and by selecting the macro in the list.



Note.

The **System settings** item is also available in the menu that appears on clicking the icon in the Windows notification area (system tray), or by short-time holding the “hot” button F8.

Manual activation of the macro is indicated by the tick next to the macro name in the **Run** menu.



Note.

The Macro can also be run from the Map or Video Surveillance Window (see Operations with macros and Running macros from the Surveillance window).

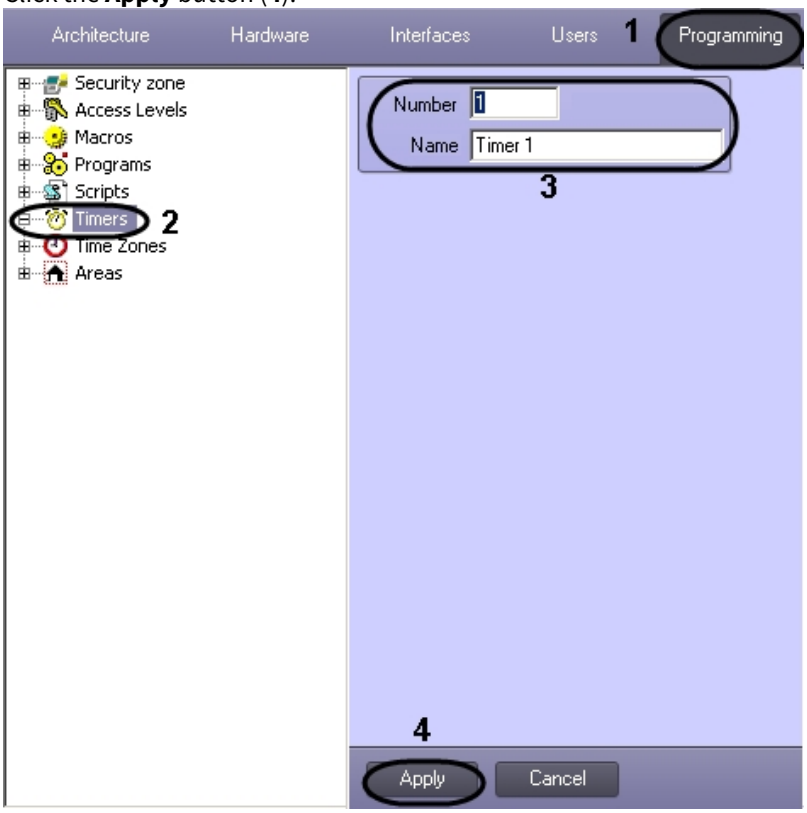
23.6.5 Creating and using the Timer object

The **Timer** object sets a time point upon reaching which an action (a macro) is executed. Thus, the **Timer** object is used together with the **Macro** object and for other objects setup.

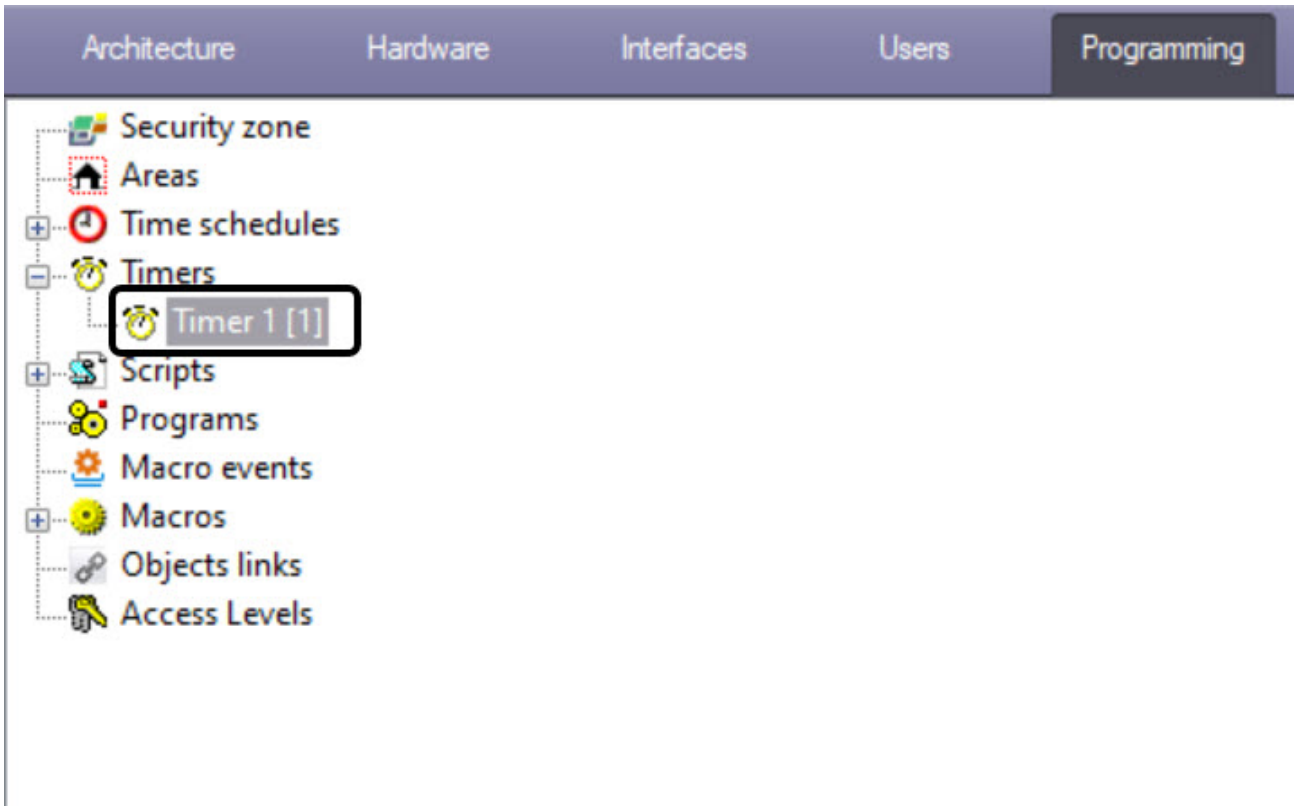
23.6.5.1 Creating and configuring the Timer object

To create the **Timer** object, do the following:

1. Open the **Programming** tab (**1**).
2. Create the **Timer** object on the basis of the **Timers** object in the objects tree (**2**).
3. Enter the number and the name of the **Timer** object in the corresponding fields of the identification panel (**3**).
4. Click the **Apply** button (**4**).



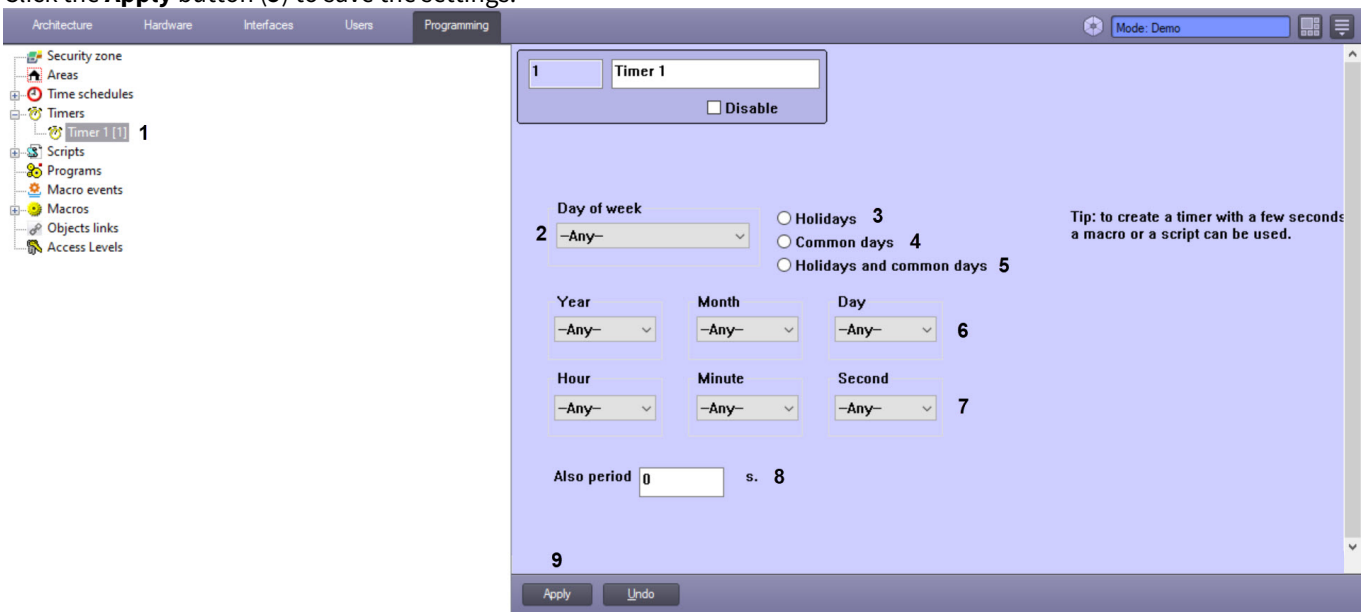
The **Timer** object will appear in the objects tree.



To configure the **Timer** object, do the following:

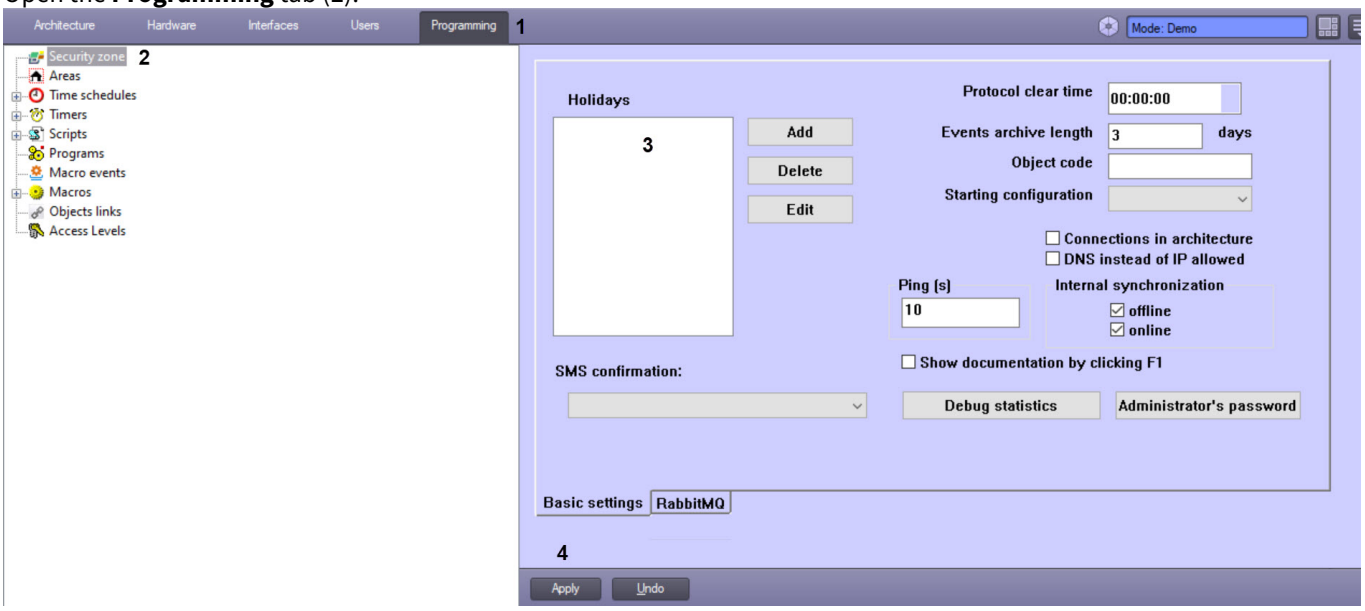
1. Select the **Timer** object (**1**) in the objects tree.
2. Set the time point using one of the following methods:
    a. Select the day of the week from the drop-down list (**2**) and the exact time (hour, minute, second) in the corresponding fields (**7**).
    b. Select the exact date (year, month, day) from the corresponding fields (**6**) and the exact time (hour, minute, second) in the corresponding fields (**7**).
3. To enable the timer triggering with the specified periodicity in seconds after the first triggering, enter the required interval in seconds in the **Also period** field (**8**).
4. Set the radio button to one of the following positions:
    a. **Holidays** (**3**), if you want to take into account the dates/days of the week that fall on holidays (set in the **Security zone** object settings).
    b. **Common days** (**4**), if you don't want to take into account the dates/days of the week that fall on holidays.
    c. **Holidays and common days** (**5**), if you want to take into account both the common days and the dates/days of the week that fall on holidays.

5. Click the **Apply** button (**9**) to save the settings.



To create the list of holidays, do the following:

1. Open the **Programming** tab (**1**).



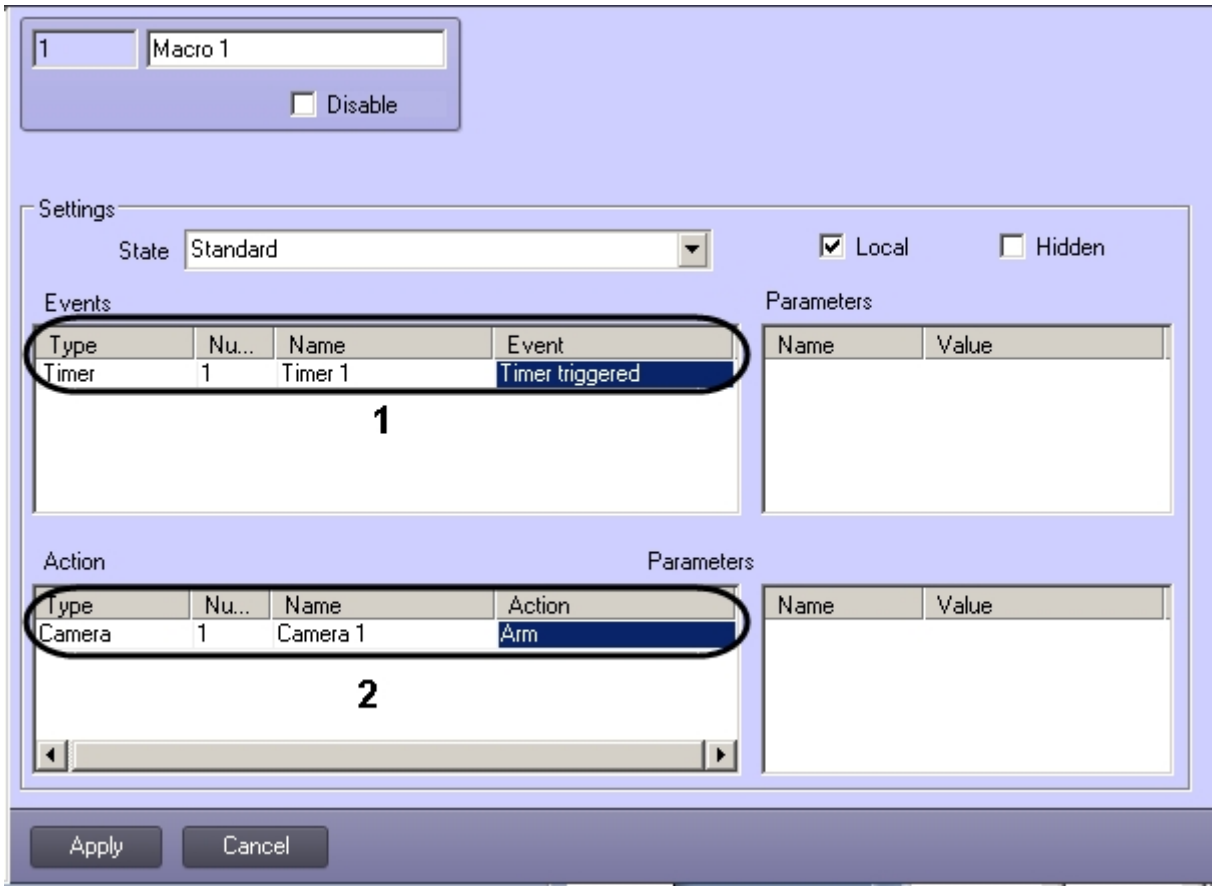
2. Select the **Security zone** object (**2**).
3. Enter a holiday date in the DD.MM.YYYY format (**3**).
4. Click the **Apply** button (**4**).

Creating and configuring the **Timer** object is complete.

23.6.5.2 Using the Timer object

Example 1. Consider a macro that activate an arming mode in selected camera when the timer triggers.

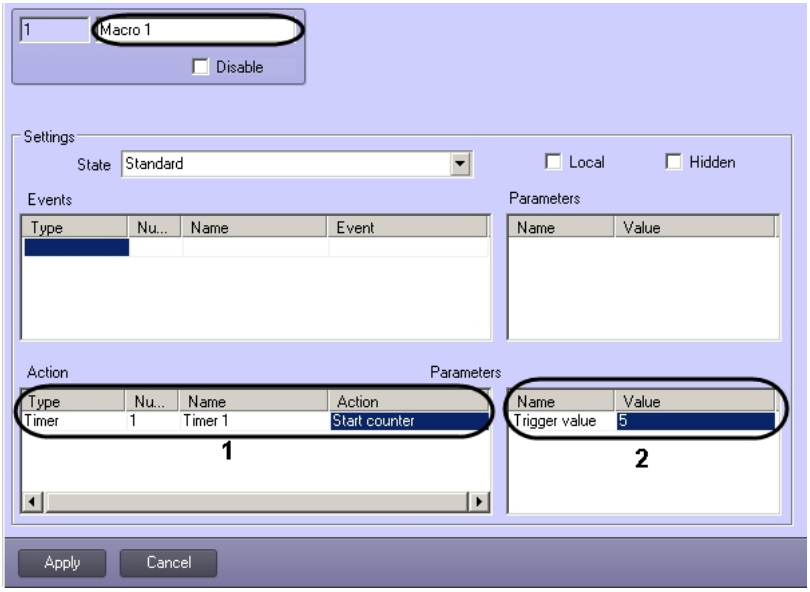
No	Event	Action
1	The timer triggered (1).	Activate an arming mode (2)



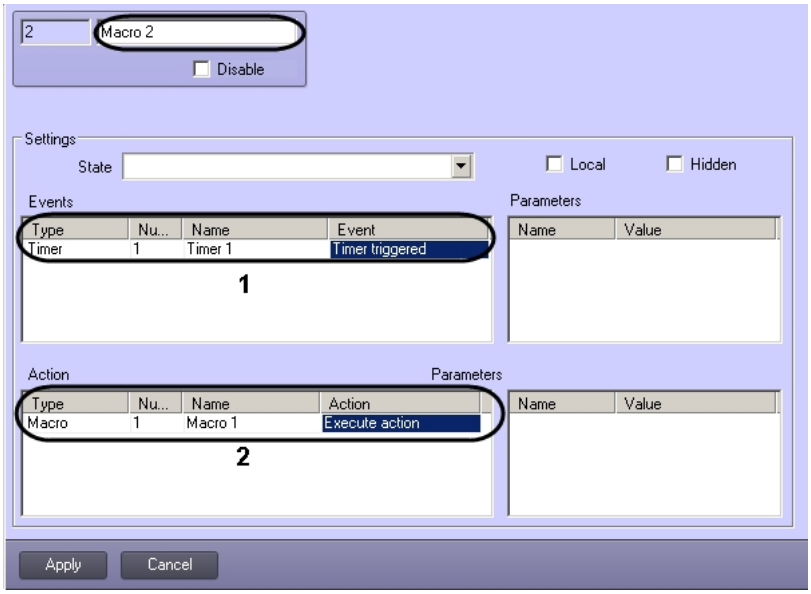
Example 2. Consider macros that allow to set the timer with trigger period of several seconds.

Macro	Event	Action	Parameters
1		Start counter of Timer 1 (1)	Trigger value is 5 seconds (2)
2	The timer 1 triggered (1)	Macro 1 execution (2)	

Macro 1 object setting window



Macro 2 object setting window



Note.

After starting the macro (**Macro 1**) in menu of Intellect software main control panel, the timer will trigger every 5 seconds and also in accordance with the **Timer 1** object settings which are specified on its seting panel. To avoid the timer triggering in the latter case, it is necessary to specify the date of triggering in the past.

Note.

To stop the timer set **Disable** check box in **Timer 1** object setting window.

23.6.6 Creating and using time schedules

A time schedule is comprised of a set of any number of time intervals during a day (24 hours) defined for several days (1 to 366), and the time intervals during specific dates.

The **Time schedule** object is used in conjunction with the **Macro** object and for setting up other system objects.

An unlimited number of **Time schedule** objects can be created in the system.

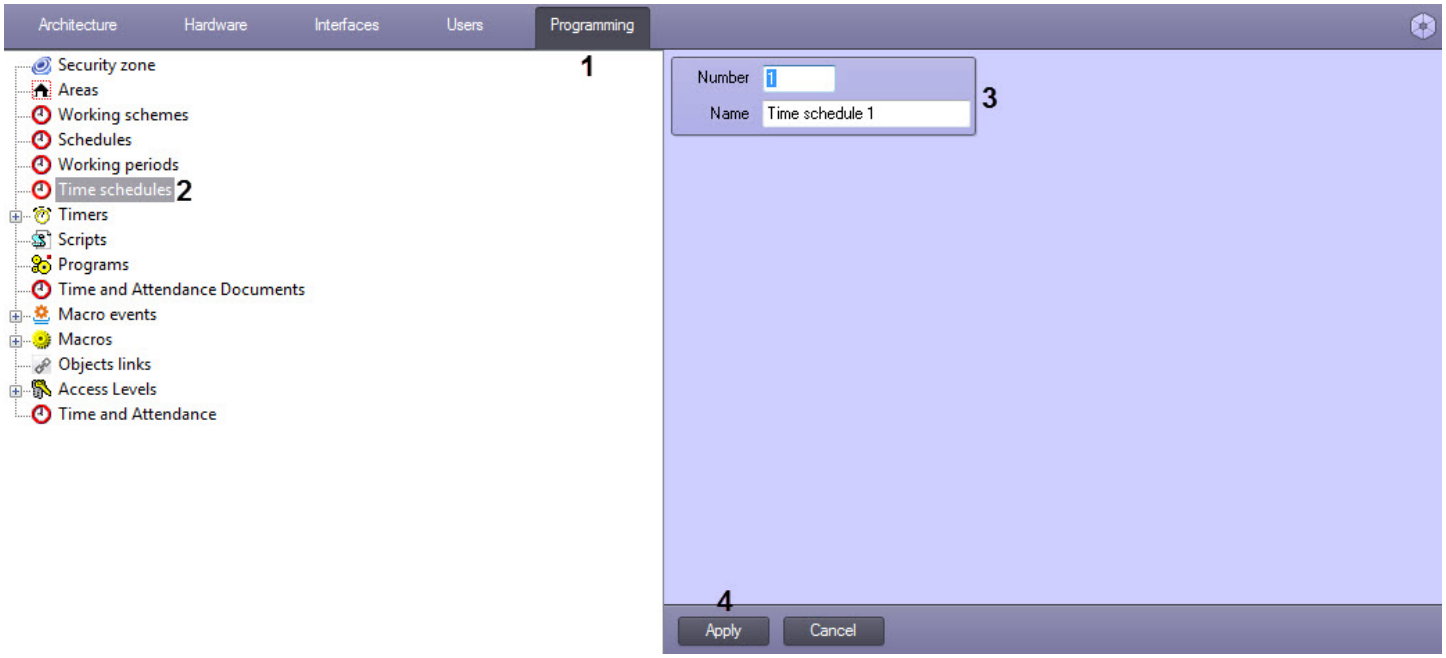
23.6.6.1 Creating and configuring Time schedules

To create the **Time schedule** object, do the following:

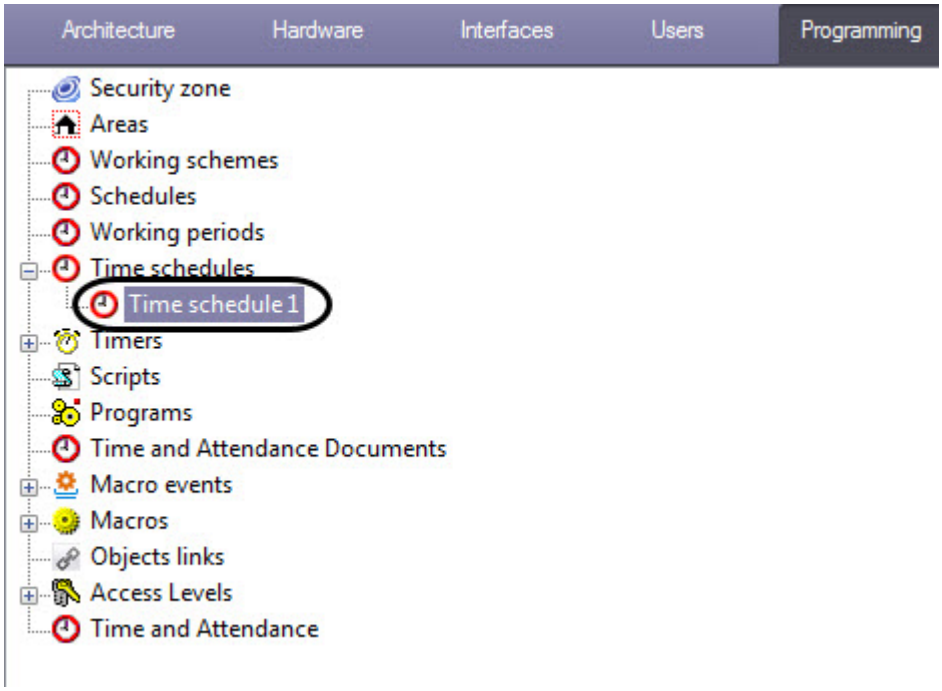
1. Open the **Programming** tab (**1**).
2. Create the **Time schedule** object on the basis of the **Time schedules** object in the objects tree (**2**).
3. Specify the number and the name of the time schedule in the corresponding fields of the **Time schedule** identification panel (**3**).

   Note

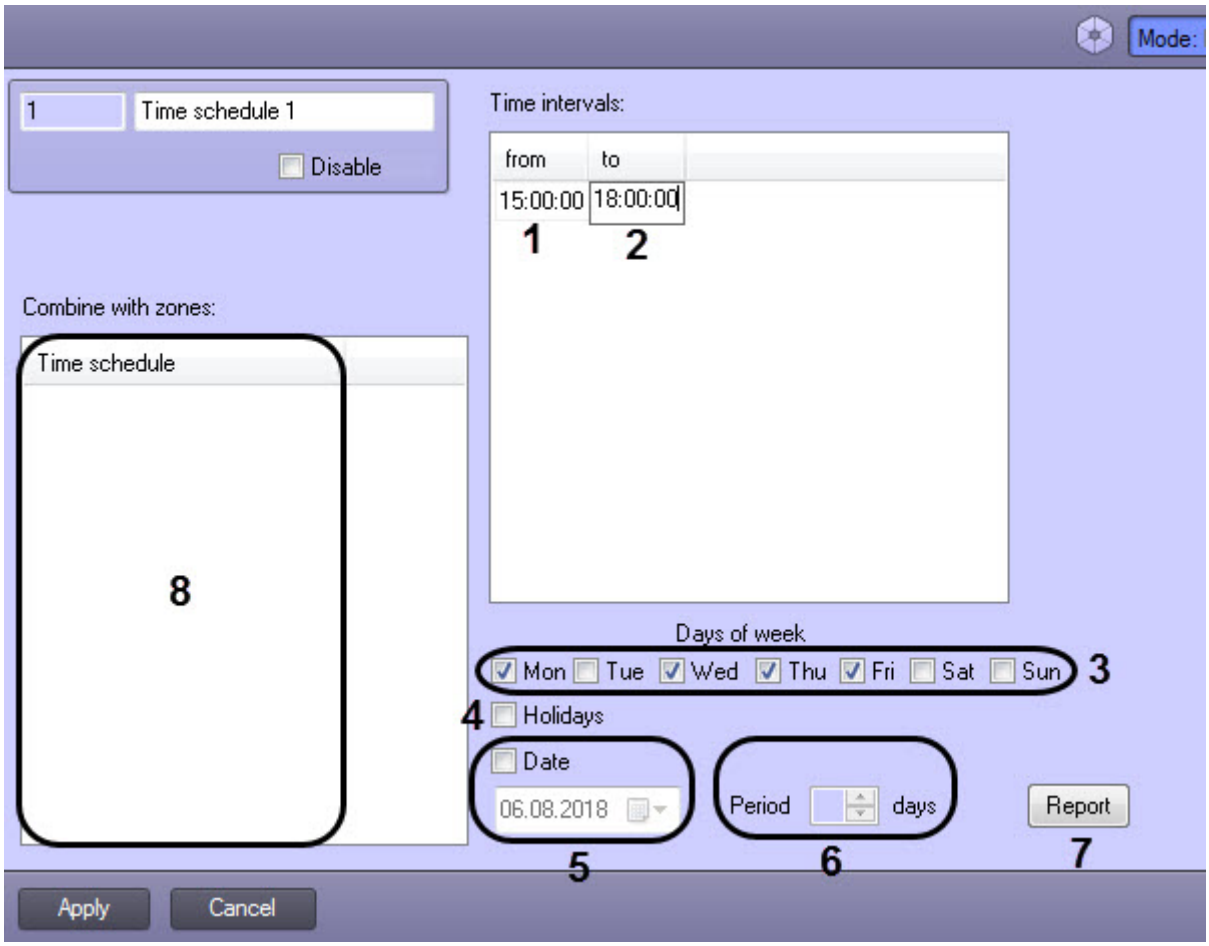
   The object number should be in the range from 1 to 65534.
4. Click the **Apply** button (**4**).



The **Time schedule** object will appear in the objects tree.



To configure the **Time schedule** object, specify the values of the following parameters:



No	Parameter name	Method for entering the parameter	Parameter description	Format	Default value	Value range
The **Time intervals** group						
1	The **from** column	Enter the value in the field	Exact time of starting the macro execution	Mask: HH:MM:SS	00:00:00	From 00:00:00 to 23:59:59
2	The **to** column	Enter the value in the field	Exact time of ending the macro execution	Mask: HH:MM:SS	00:00:00	From 00:00:00 to 23:59:59
The **Days of week** group						
3	The checkboxes group: **Mon** **Tue** **Wed** **Thu** **Fri** **Sat** **Sun**	Set the checkbox	Adds days to the timetable. The days of the week are added individually for each time interval	-	Clear	Set – the day of the week is included in the timetable Clear – the day of the week is not included in the timetable
The **Holidays** group*						

No	Parameter name		Method for entering the parameter	Parameter description	Format	Default value	Value range
4	The **Holidays** checkbox		Set the checkbox	Adds holidays to the timetable. The holidays are added individually for each time interval	-	Clear	Set – the list of holidays is included in the timetable Clear – the list of holidays is not included in the timetable
The **Date** group							
5	**Date**	Checkbox	Set the checkbox	Makes the **Period__days** field active. If set, the **Days of week** group is disabled. The days are added individually for each time interval	-	Clear	Set – makes the **Period__days** field active Clear – the **Period__days** field is inactive
		Field	Enter the value in the field	Specifies the exact date. The days are added individually for each time interval	Mask: DD.MM.YYYY	Current date	From 00.00.0000 to 31.12.9999
6	The **Period** field		Enter the value in the field	Sets the periodicity in N days of time schedule triggering, starting from the specified date (i.e. the time schedule triggers every N-th day)	Numeric value	Inactive	From 0 to 999999999999999. Periodicity is set individually for every time interval
7	The **Report** button		-	Displays the dialog box with the time schedule activity table	-	-	-
The **Combine with zones** table							
8	The **Time schedule** drop-down list		Selected from the list	Sets the time schedule with which the given time schedule should be combined	Names of the registered **Time schedule** objects	-	Depends on the number of the registered **Time schedule** objects

* The **Holidays** checkbox adds the list of days to the timetable specified in the **Security zone** object in the **Programming** tab.

If the moment of time interval beginning is set later than the moment of ending, then time schedule will cover the present day (from the time interval beginning) and part of the following day (to the time interval ending) on conditions that the Time schedule is set for the present and following day. If the Time schedule is set only for the present day, then the Time schedule will end at 0:00:00.

Note

Time schedule combination can be used for correction of the main time schedule on special days, for example, days before holidays. The date of a special day and the time interval, that should be added to the interval of the main schedule, should be set on the settings panel of the additional time schedule.

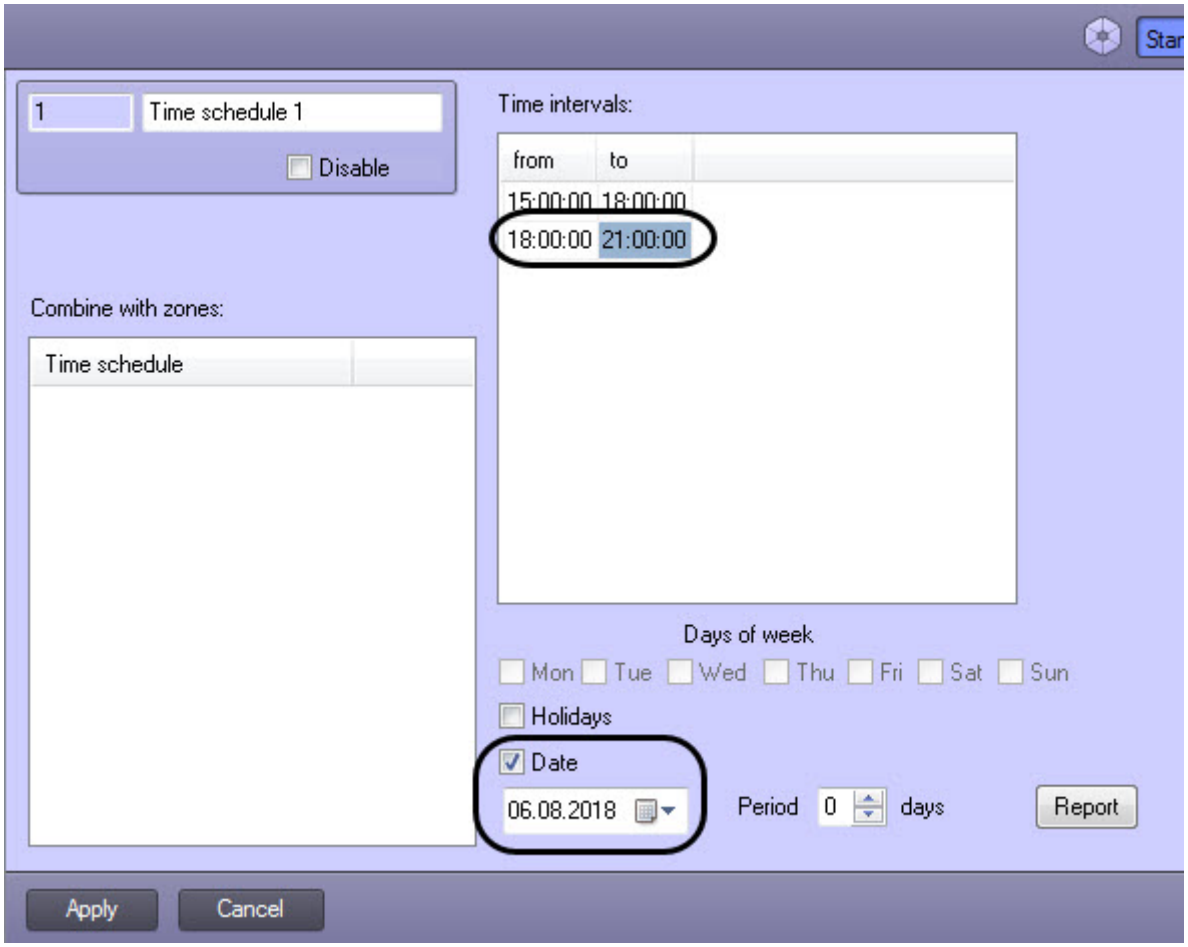
Attention!

If the time schedule parameters are changed to a disabled state, the changes will come into effect after you restart *Intellect*.
Example: Now it is 16:00. The time schedule end time (the **to** column) was set to 20:00. Then it was changed to 16:00. In this case in order for the changes to come into effect, you should restart *Intellect*. Otherwise, the time schedule will be until 20:00.

Attention!

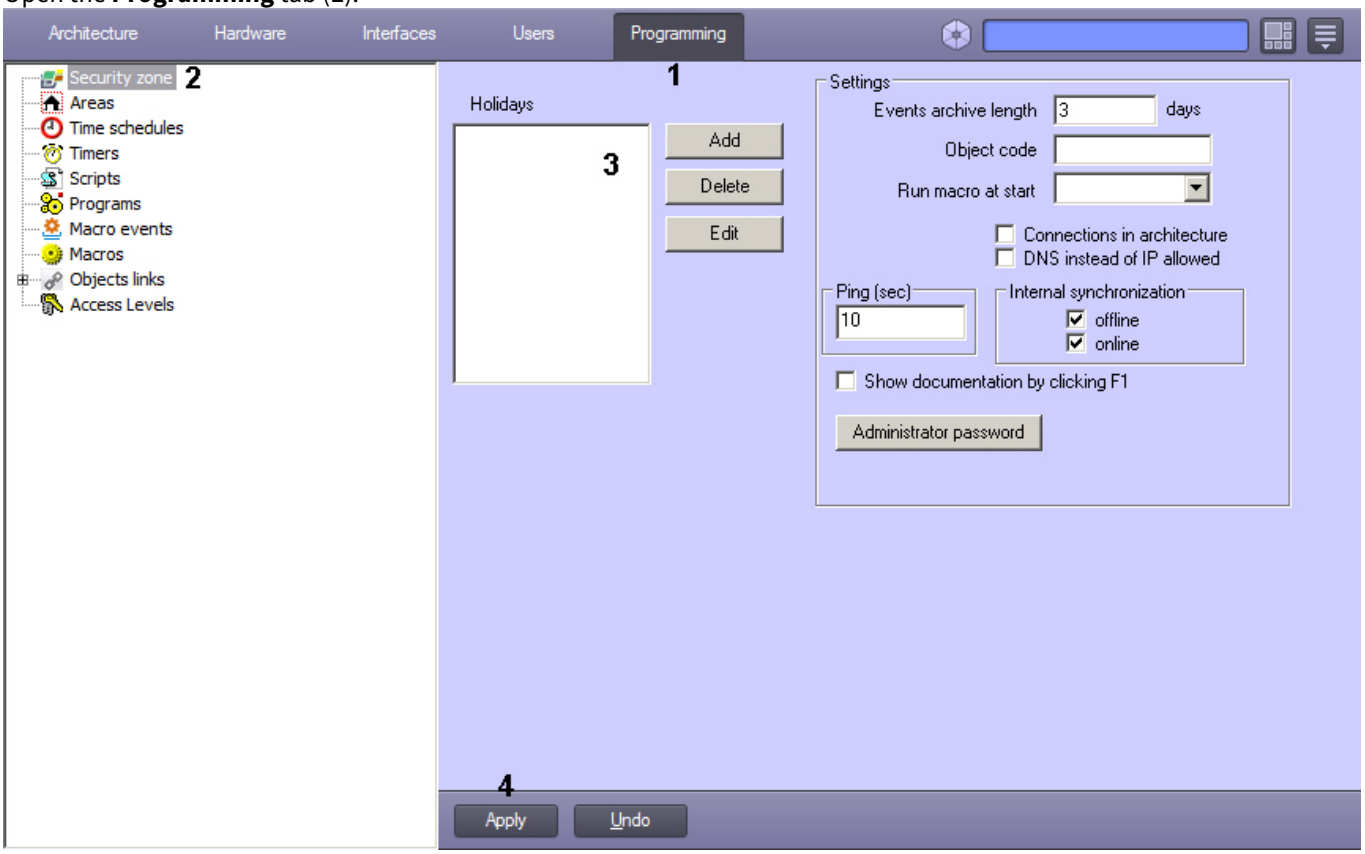
The duration of the time schedule usage in days is not set on the settings panel. So the time schedule combining should be disabled right after its application.

Configuration of the additional time interval:



To create the list of holidays, do the following:

1. Open the **Programming** tab (**1**).



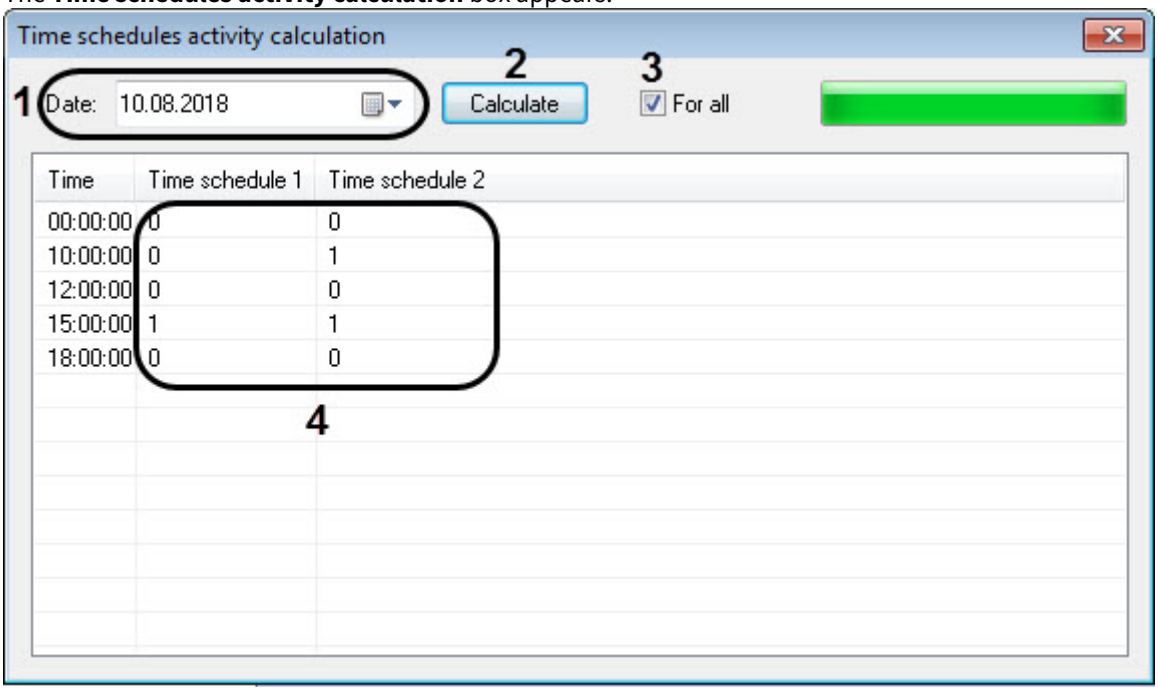
2. Select the **Security zone** object (**2**).
3. Specify the holiday date in the DD.MM.YYYY format (**3**).
4. Click the **Apply** button (**4**).

23.6.6.2 Viewing time schedules states

In INTELLECT™ one can view time schedules states by all specified time intervals.

To view time schedules states, do the following:

1. Click the **Report** button on the settings panel of the **Time schedule** object.
   The **Time schedules activity calculation** box appears.



2. Select the required date in the **Date** list (1).
3. If the data on all time schedules created in the system is to be displayed, then set the **For all** checkbox (3).
4. Click the **Calculate** button (2).

As a result the table with active time schedules (marked 1) and inactive time schedules (marked 0) is created (4).

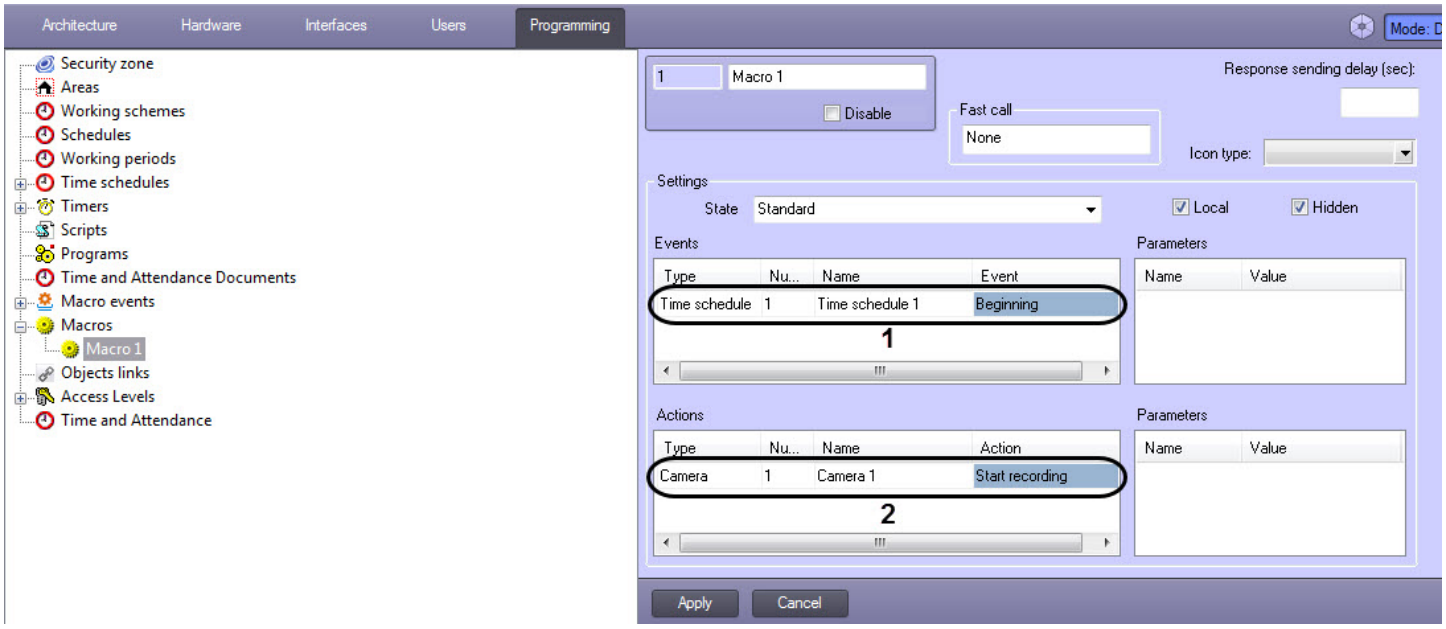
23.6.6.3 Examples of time schedules usage

Example 1. Consider two micros which work together and allow recording a video within the time schedule limits.

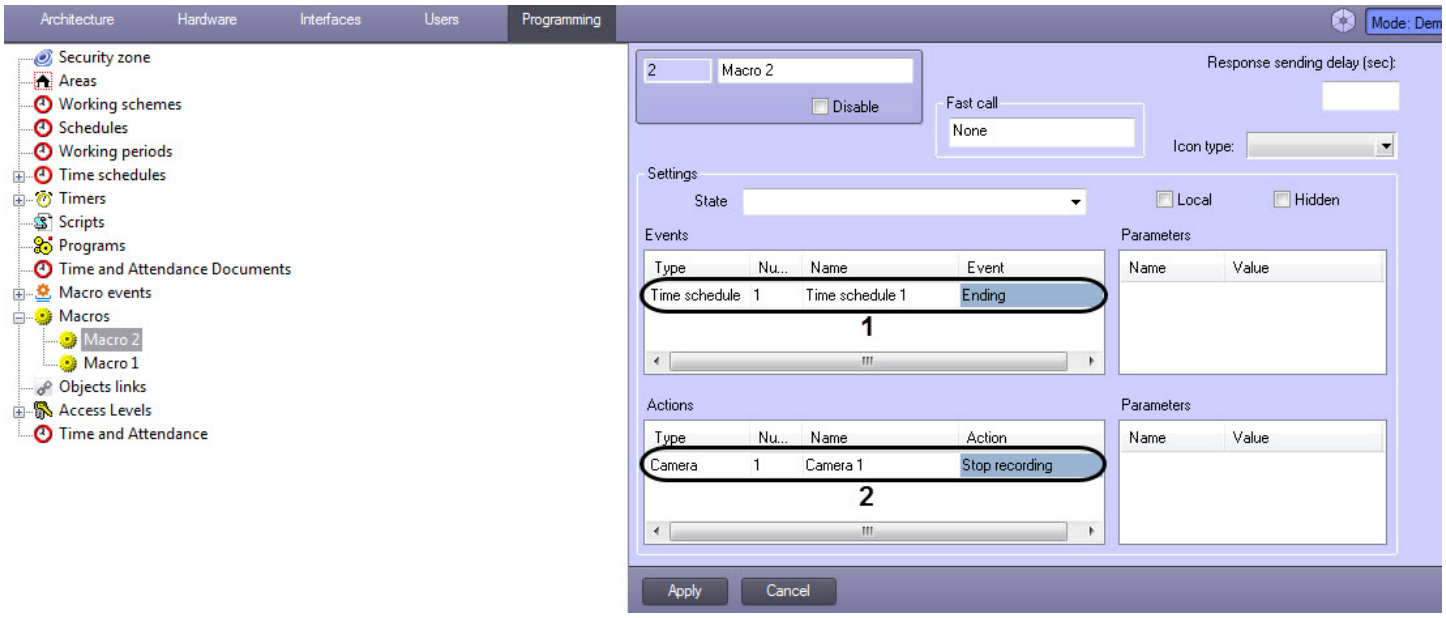
Set the events and actions values in **Macro** setting window that is given in the table.

№	Event	Action
1	Time schedule 1 begin (1)	Start recording from Camera 1 (2)
2	Time schedule 1 end (1)	Stop recording from Camera 1 (2)

Example of a macro with a time schedule . Time schedule begining.



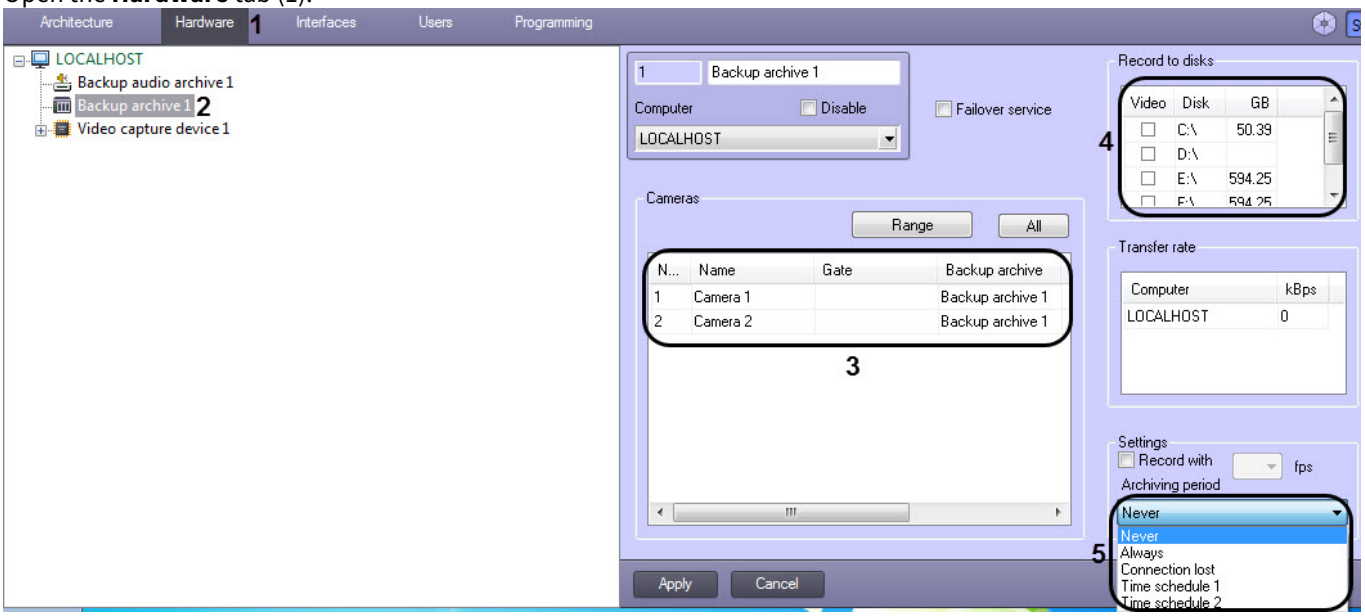
Example of a macro with a time schedule. Time schedule ending.



Example 2. Time schedules can be used for the Backup archive. Consider an example of scheduling the archiving of the video feed from a camera at a specific time.

To configure the Backup archive object, do the following:

1. Open the **Hardware** tab (1).



2. Select the **Backup archive** object (2).
3. Select the disk to record the video to (3).
4. Specify the camera to record from (4).
5. Select the **Time schedule 1** value in the **Archiving period** list (5).
6. Click the **Apply** button (6).

23.6.7 Subdivision of the protected facility into areas and regions

23.6.7.1 About areas and regions

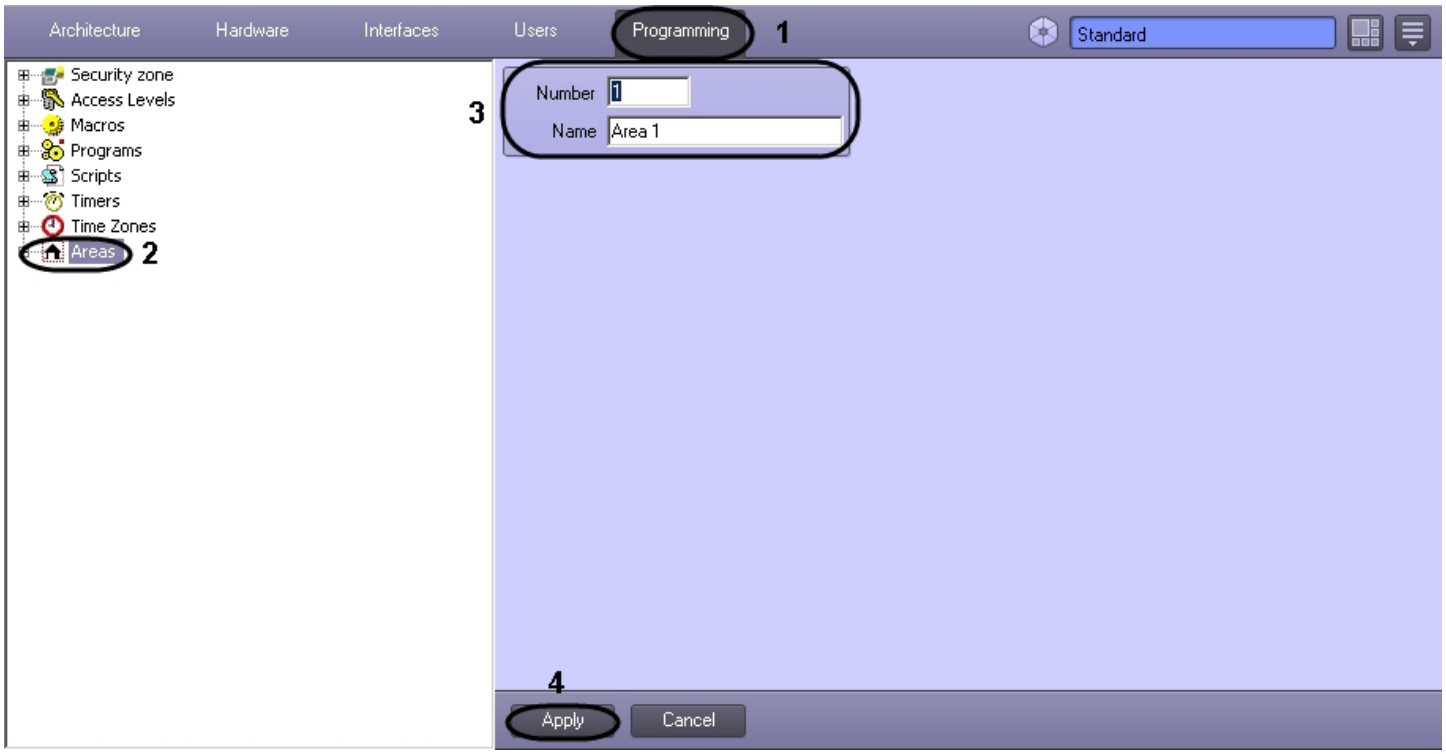
If the *Intellect* system is used to protect the large territory of complex topology (buildings, groups of buildings), we recommend dividing the whole territory into smaller zones. This allows to group relevant devices by location and makes it easier to view and control them, as well as to analyze the reports.

There are two levels of division: area and region. The region is the smallest element. The area is a set of regions grouped by location or by function. For example, if the protected territory is the building, it can be divided in this way: the floors make the areas, while the rooms become the regions.

We recommend dividing the protected territory into areas and regions at the time of designing the video surveillance system, before the actual system configuration.

23.6.7.2 Creating areas

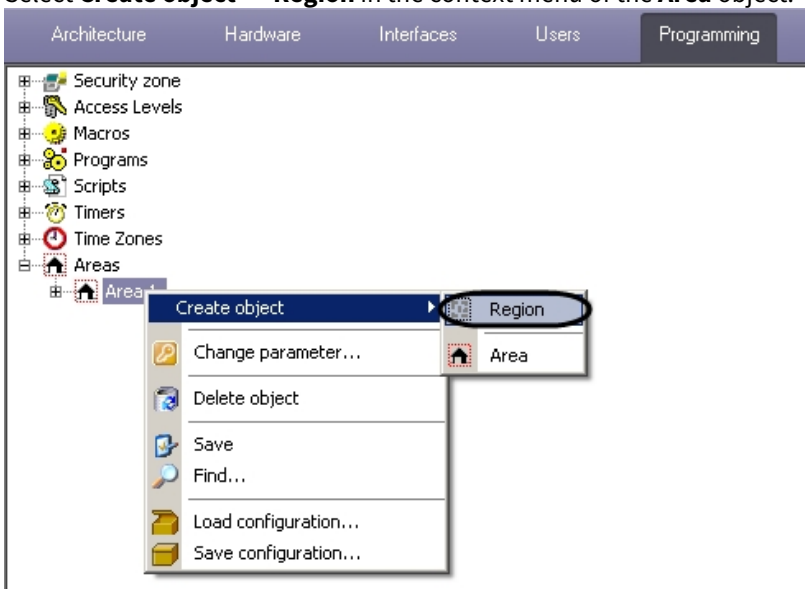
The areas are represented by **Areas** objects created in the **Programming** tab. The **Areas** object has no parameters of its own and is used to group the **Region** objects only. Figure below shows the process of creating an **Areas** object.



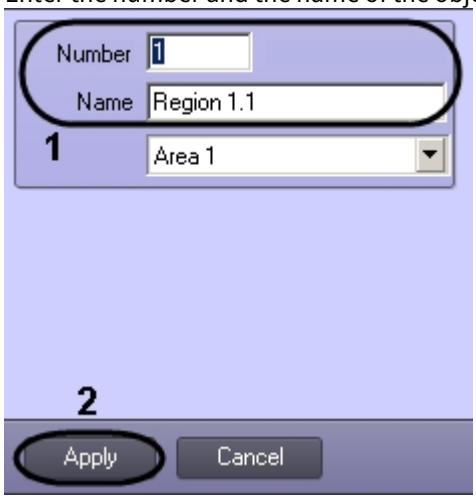
23.6.7.3 Creating Regions

To create a Region, do the following:

1. Create the **Region** object.
    a. Select **Create object** => **Region** in the context menu of the **Area** object.



b. Enter the number and the name of the object in the corresponding fields (**1**).

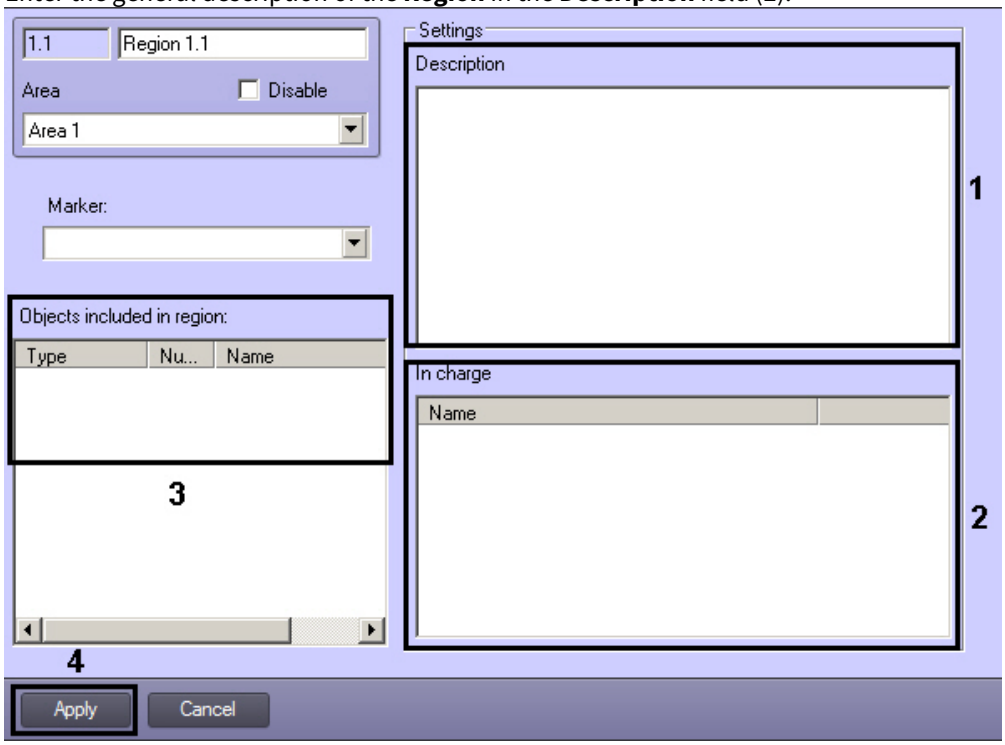


> **Note**
>
> The number of the object should be in the range from 1 to 65534.

c. Click the **Apply** button (**2**).

> **Note**
>
> As a result, the settings panel of the **Region** object will be displayed.

2. Configure the created **Region** object.
   a. Enter the general description of the **Region** in the **Description** field (**1**).



   b. From the **Name** list of the **In charge** table, select the user responsible for this region (**2**).

> **Note**

> The **Name** list consists of the names of the users registered in the system (see User registration and removal).

c. Click the **Apply** button (**4**) to save the changes.

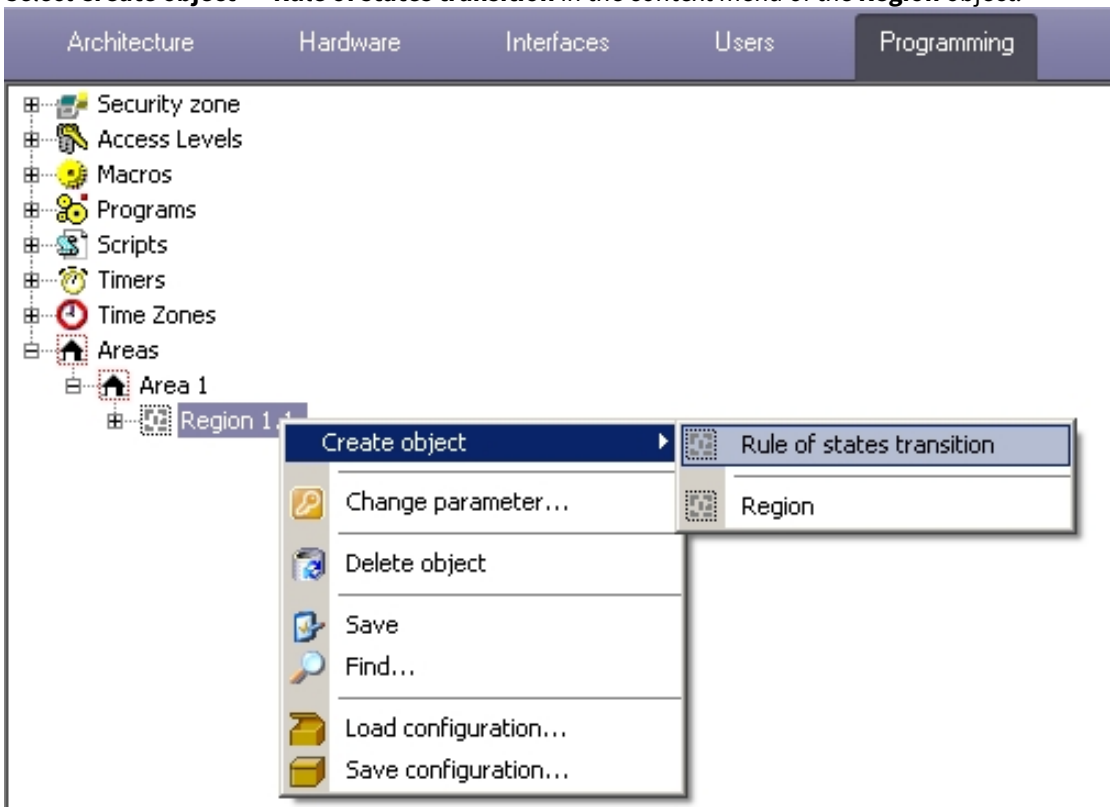
3. Create the links between the **Region** object and the objects in the **Hardware** tab that will be included into the **Region**. For this select the name of the created **Region** object on the settings panel of the object selected in the **Region** list (see Examples of using areas and regions).
4. After creating the links described above, the list of the objects added to the region is displayed in the **Objects included in region** table (**3**) on the **Region** object settings panel. This table cannot be edited.

The Region is now created.

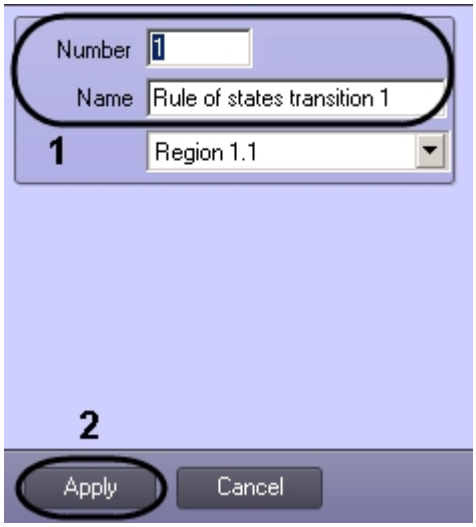
23.6.7.4 Creating the rule of states transition

To create the rule of states transition, do the following:

1. Create the **Rule of states transition** object.
   a. Select **Create object** => **Rule of states transition** in the context menu of the **Region** object.



b. Enter the number and the name of the created object (**1**).



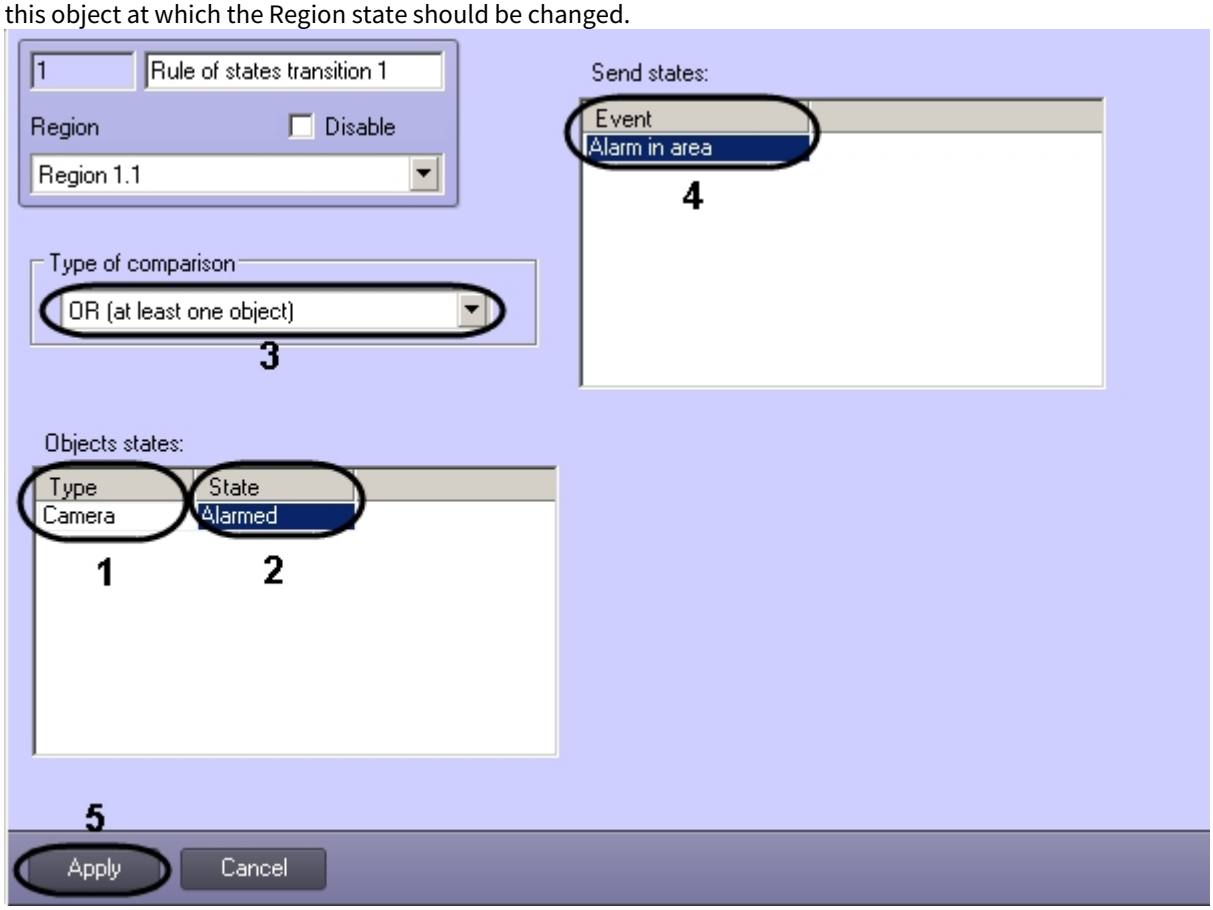
> **Note**
>
> The number of the object should be in the range from 1 to 65534.

c. Click the **Apply** button (**2**).

> **Note**
>
> As a result, the settings panel for the **Rule of states transition** object will be displayed.

2. Set the condition for triggering the rule on the settings panel of the **Rule of states transition** object.

a. Select the object type from the **Type** list (**1**) in the **Objects states** table and in the **State** list (**2**) specify the state of this object at which the Region state should be changed.



Note

Repeat step 2.a for all required object types.

i. If the state of the Region should be changed when all objects of the types added to the **Objects states** table are in these states, select the **AND** (all objects) value from the **Type of comparison** list (**3**).

ii. If the state of the Region should be changed when at least one object of the type added to the **Objects states** table is in at least one of the specified states, select the **OR** (at least one object) value from the **Type of comparison** list (**3**).

b. In the **Event** list of the **Send states** table, select the event generated by the **Region** object when the rule condition is met (**4**).

c. Click the **Apply** button (**5**) to save the changes.

The Rule of states transition is now created.

23.6.7.5 Examples of using areas and regions

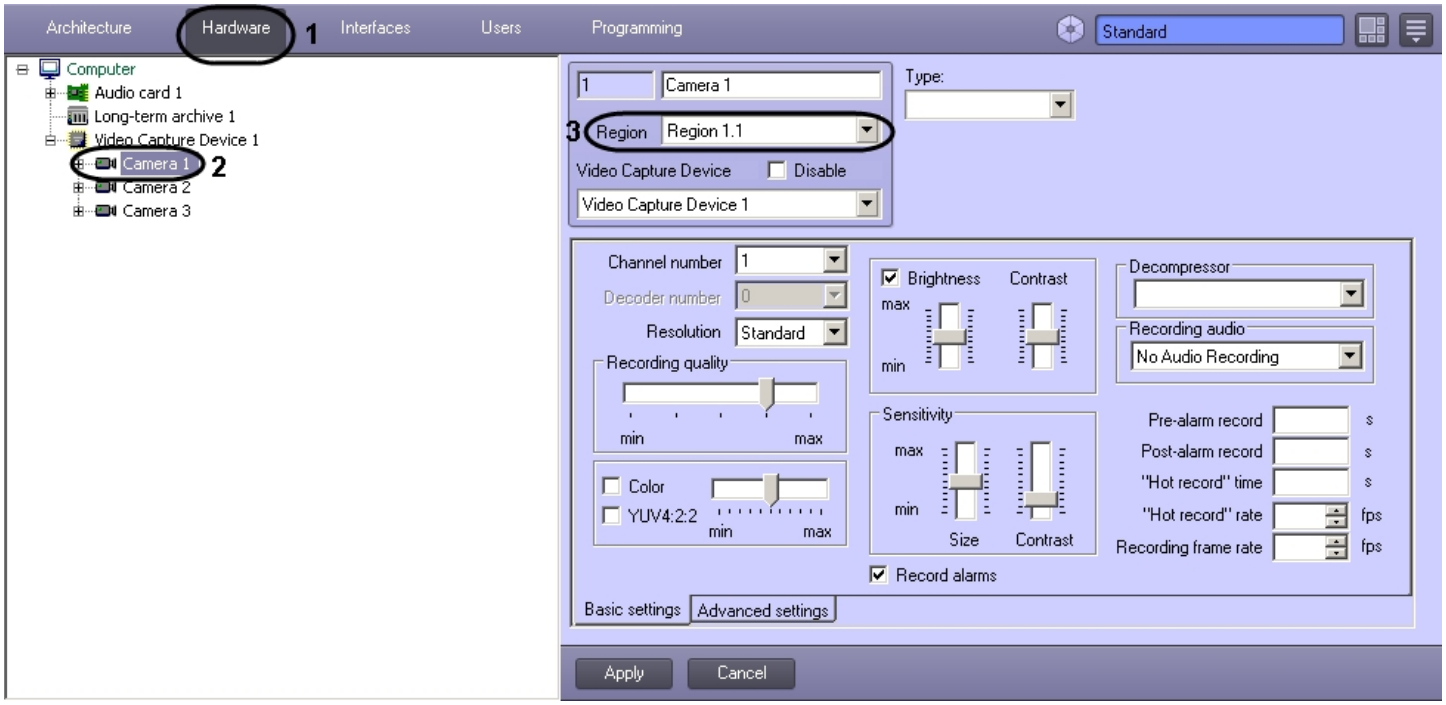
On the page:

- Example 1.
- Example 2.
- Example 3.

23.6.7.5.1 **Example 1.**

The Regions created in the system are used to group *Intellect* system objects, representing the security devices by their location on the protected territory.

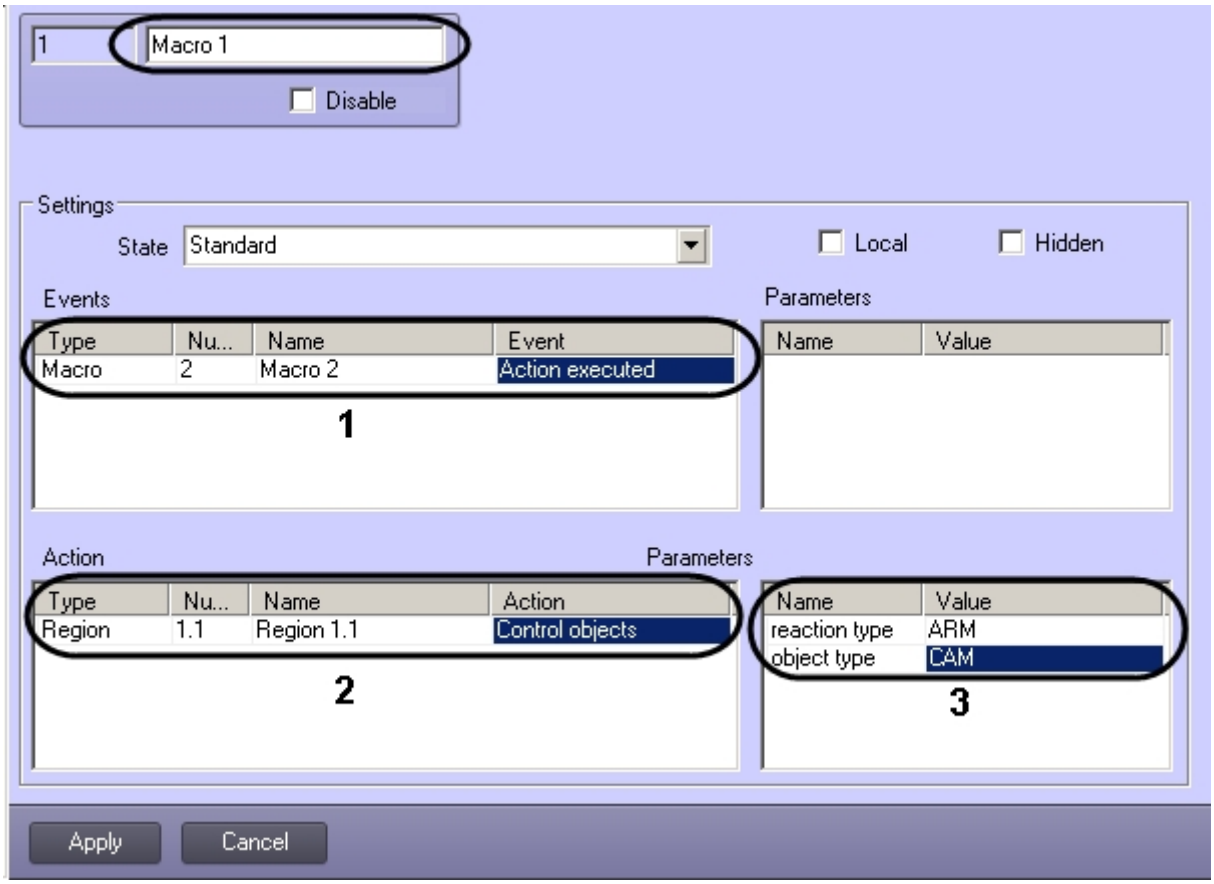
To include a device into the Region, select an appropriate **Region** in the **Region** field (**3**) on the identification panel of the corresponding object (**2**) on the **Hardware** tab (**1**).



23.6.7.5.2 **Example 2.**

Arming all cameras included into the **Region 1** when the **Macro 2** is run. The parameters of the macro (**Macro 1**) essential for this operation are given in the table.

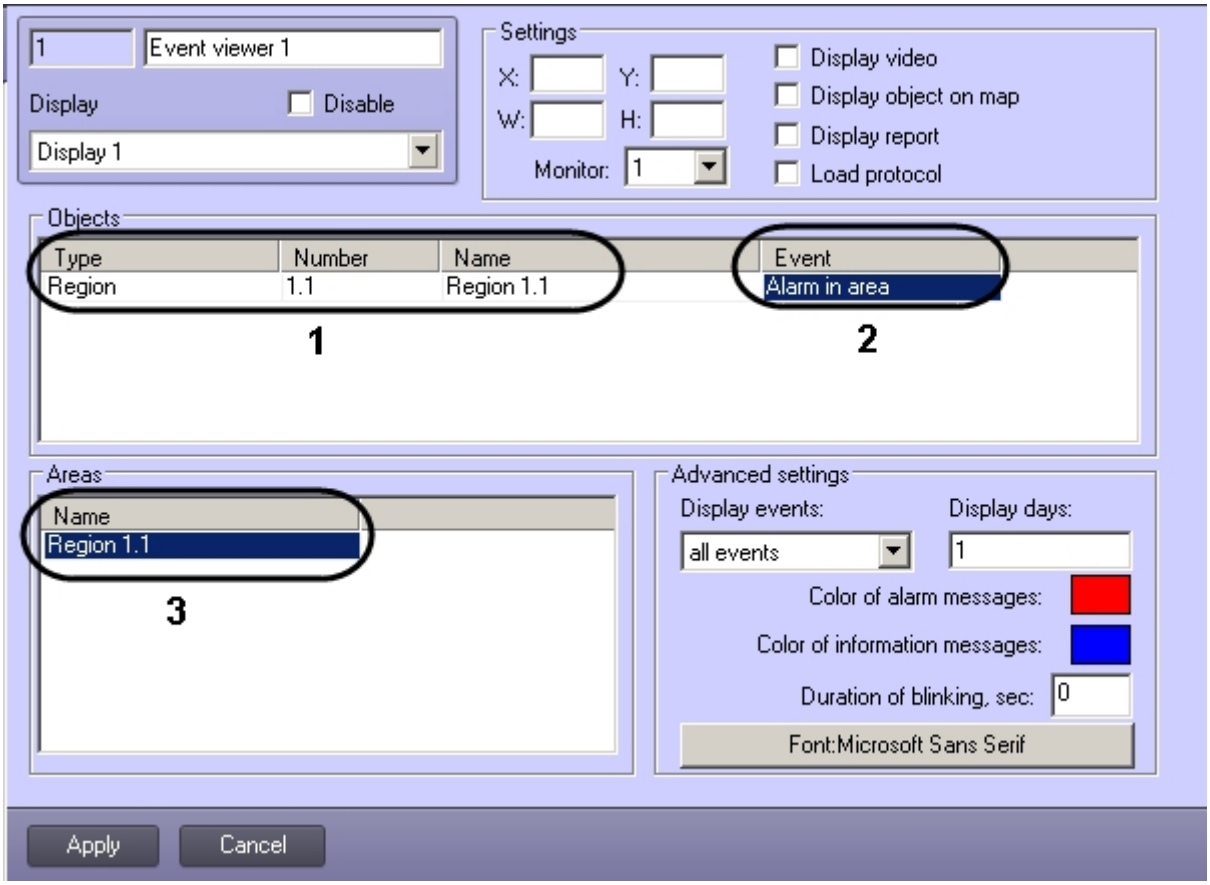
Event	**Action**	**Parameters**
Macro 2 is executed (**1**)	The **Control objects** action of the **Region 1** is executed (**2**)	Reaction type = ARM Object type = CAM (**3**)



23.6.7.5.3 **Example 3.**

Intellect allows displaying the reports about the devices grouped in the Regions.

The figure below shows the **Event viewer** object configuration to display a report on the **Alarm in area** event on any device in the **Region 1**.

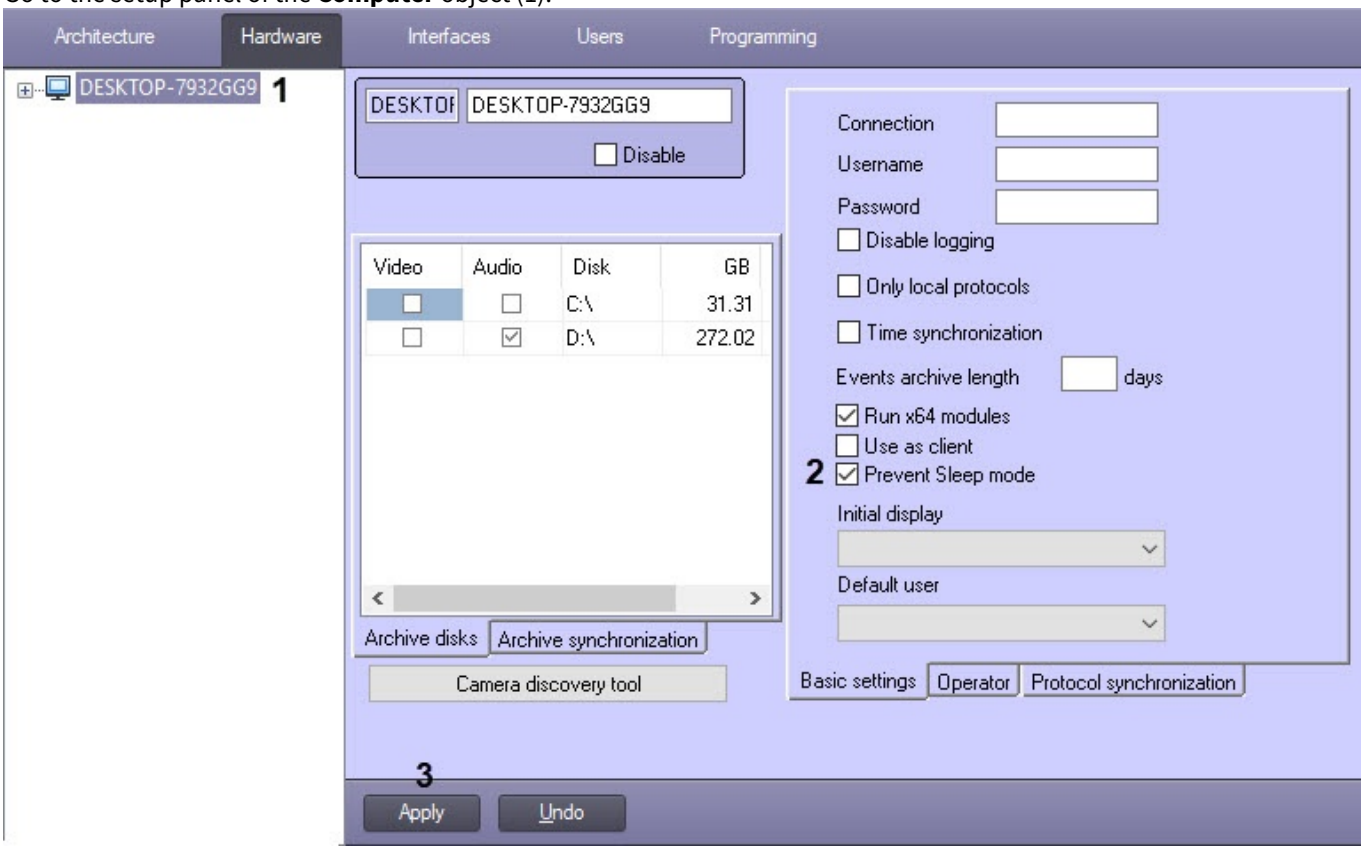


23.7 Disabling Windows OS sleep mode when Intellect is running

If sleep mode is enabled in Windows OS you can disable it when *Intellect* is running without disabling the sleep mode directly in the OS. The setting can be useful if you need to watch a video in *Intellect* without any actions from an Operator.

In order to prevent computer from going into sleep mode when *Intellect* is running, do the following:

1. Go to the setup panel of the **Computer** object (1).



2. Select the checkbox **Prevent Sleep mode** (2) on the **Basic settings** tab.
3. Click **Apply** (3).

As a result, when *Intellect* is running, sleep mode will be blocked.

24 The Report System

24.1 General information on the Report System

The Report system of the Intellect software package is designed for the following purposes:

1. Creating and printing the reports on the events registered in the surveillance system and on the actions taken in response to these events.
2. Viewing the video archive starting from the time of the event registered in the report.

The Report system supports the following functionality:

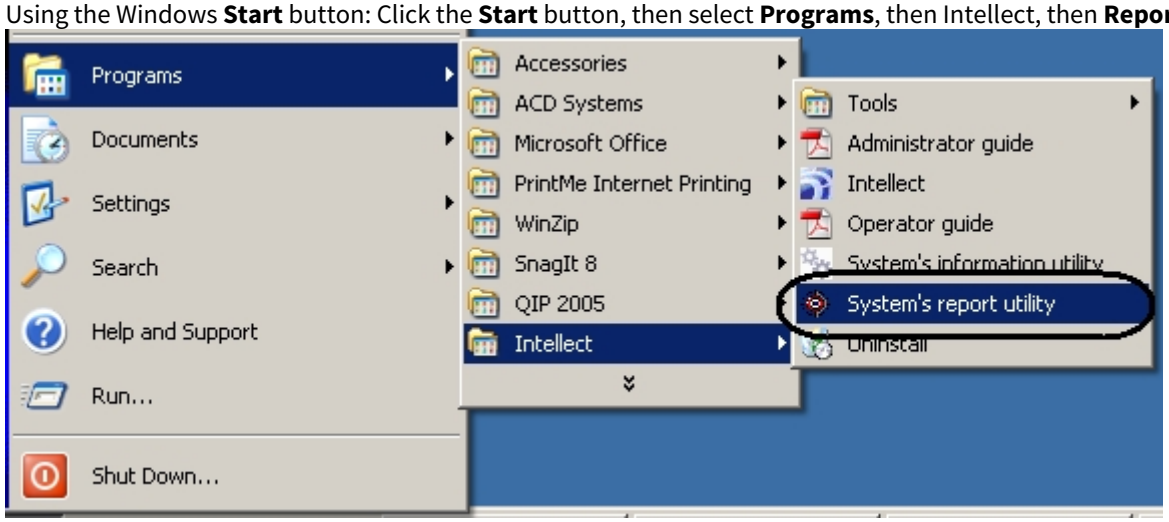
1. Selecting the objects (or groups of objects) from those available for reporting (objects include hardware and software modules).
2. Selecting the events to be included in the report for each object selected.
3. Creating the report templates.
4. Creating the screen reports.
5. Creating the printed reports.
6. Exporting the printed report to a file.
7. Viewing the video archive from the screen report using the surveillance window or converter.exe utility.
8. Handling the cameras of the ATM-Intellect system (automatic banking machine surveillance system) using the X.25 protocol.

24.2 Starting and shutting-down the Report system

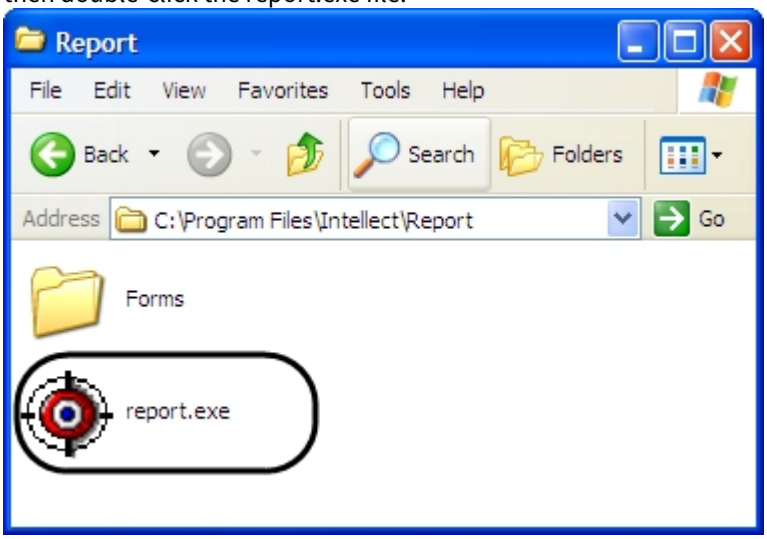
24.2.1 Starting the Report system

The Report system can be started in the following ways:

1. Using the Windows **Start** button: Click the **Start** button, then select **Programs**, then Intellect, then **Report system**.

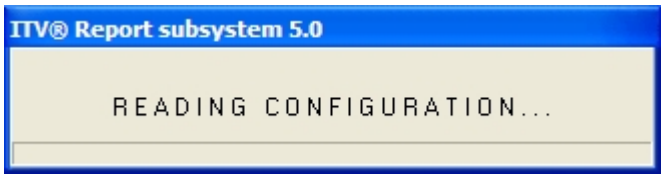


2. Using the program folder of the *Intellect* software: open the **Report** folder in the program folder of the *Intellect* system, then double-click the report.exe file.



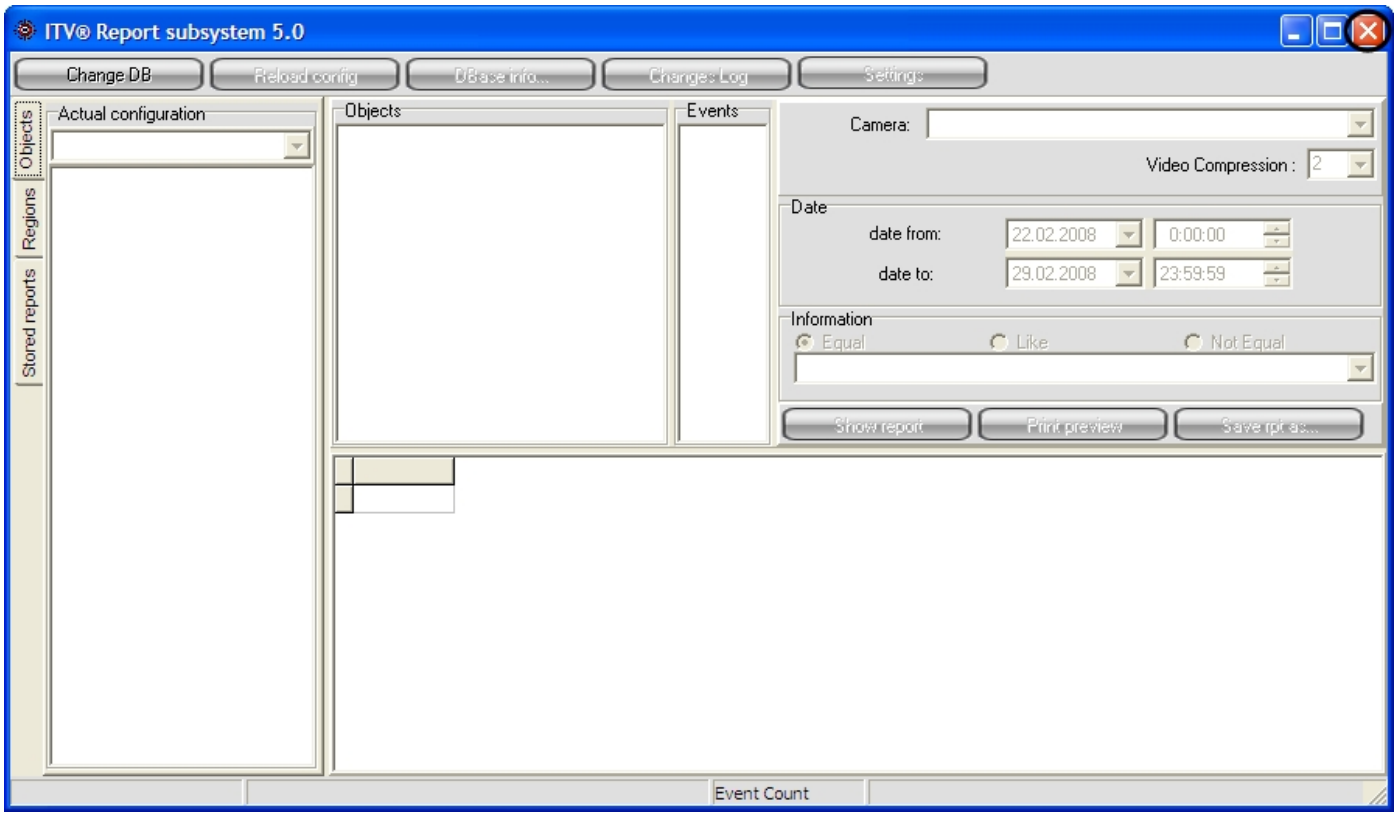
The Report system will start.

The notification window will appear, indicating that the system configuration is being read from the database.



24.2.2 Shutting-down the Report system

The Report system is shut down using the standard Windows procedure for applications shutdown. Click the **Shutdown** button in the top right corner of the window.

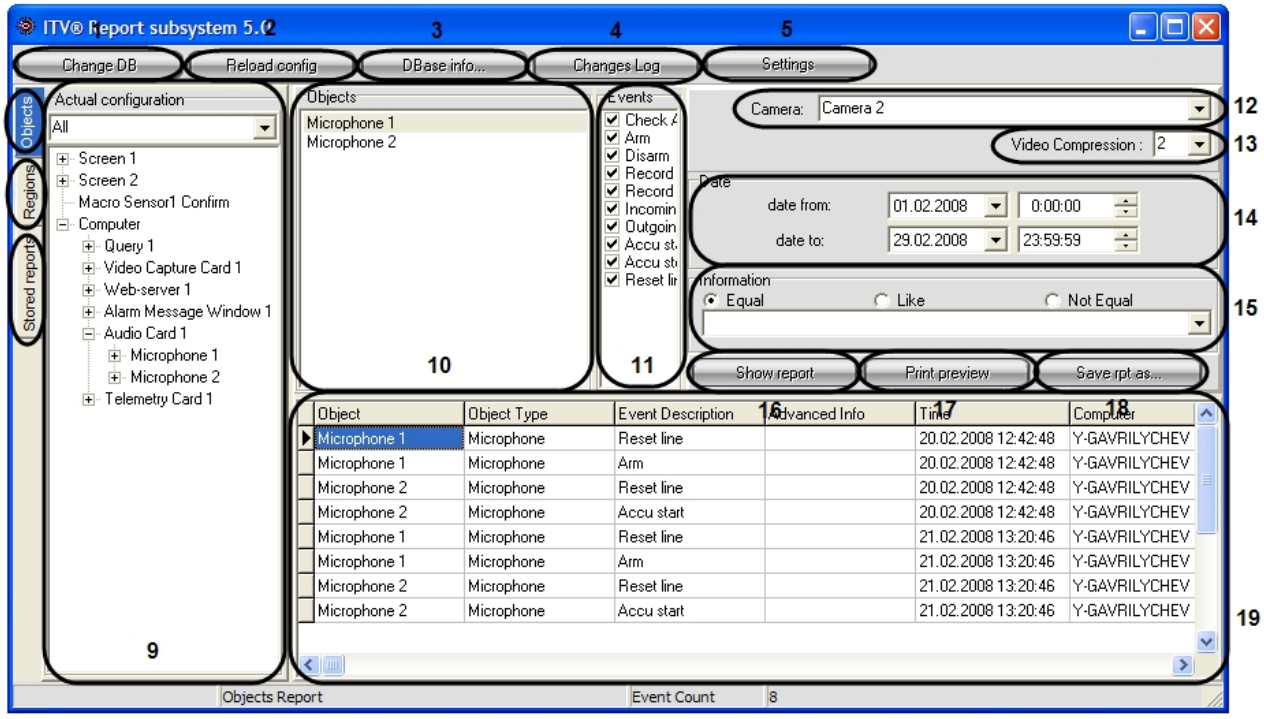


The Report system window will shutdown.

24.3 The Report window

The Report system window contains the following sections: the main control panel, the report creation panel, and the report view panel.

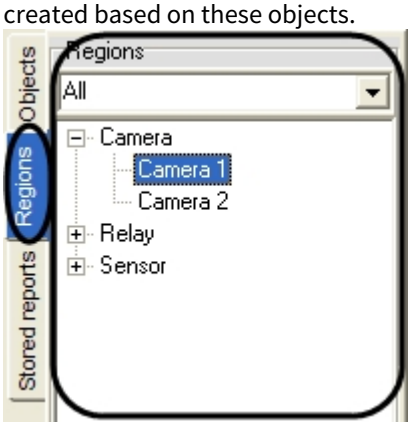
Figure below shows an example of the Report window.



The Report window includes the following interface elements (numbered according to the screenshot on the figure):

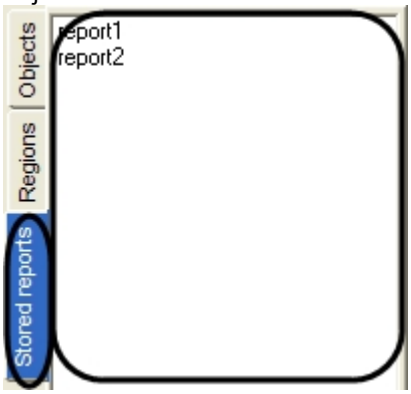
1. The **Change DB** button allows changing the current configuration database of the Intellect system.
2. The **Reload Config** button reloads the system configuration and registered events from the current database.
3. The **DBase Info** button opens the **Base Info** window containing the following information about the events archive: the dates of the first and last registered event, the archive depth and the total number of events in the database.
4. The **Changes Log** button allows viewing the information on the changes made to the *Intellect* configuration.
5. The **Settings** button opens the **OptionsForm** window allowing to introduce new Events Log parameter settings.
6. The **Object** button opens the **Actual Configuration** tab allowing to select the objects to become the sources of the events to be included in the report.
7. The **Regions** button opens the **Regions** tab allowing to select the objects in the chosen region. The reports are then created on these objects.
8. The **Shared Reports** button opens the tab for selecting the existing report templates. A report template is a list of objects and events to be included in the report.
9. The **Actual Configuration** tab allows selecting the objects to become the sources of the events to be included in the reports.
   This tab opens when the **Objects** button is clicked.

   The **Regions** button opens the **Regions tab** allowing to select the objects in the chosen region. The reports are then created based on these objects.



   The **Shared Reports** button opens the tab showing the list of all existing report templates. A report template is a list of

objects and events to be included in the report.



10. The list of selected objects to create the reports for.
11. The list of available events for the object selected in step 10. Select the events to be included in the report. By default, all events of the chosen object are selected.
12. The **Camera** list is designed for selecting the camera, archive of which is playing from the screen report form if it's required to change default camera.
13. The **Video Compression** list allows setting the compression level of the video played in the Report system.
14. The **Date** group allows specifying the time interval for the report.
15. The **Information** group allows setting the string criteria to be searched for in the **Advanced Info** column of the report.

> **Note.**
>
> In case of first start of Web-report subsystem this panel unavailable for edit. Restart the Web-report subsystem

The Information field group contains the following fields:

a. Text field. Enter the character string to be searched for.
b. **Equal** radio-button. When selected, the system looks for exact case-sensitive matches only.
c. **Like** radio-button. When selected, the system looks for the rows where the **Advanced Info** column contains the search string, case-sensitive.
d. **Not Equal** radio-button. When selected, the system looks for the rows where the **Advanced Info** column does not match the search string, case-sensitive.

16. The **Show Report** button. Creates the screen form of the report (see the Creating a screen report section).
17. The **Print Preview** button. Creates the printed report (see the Creating a printed report section).

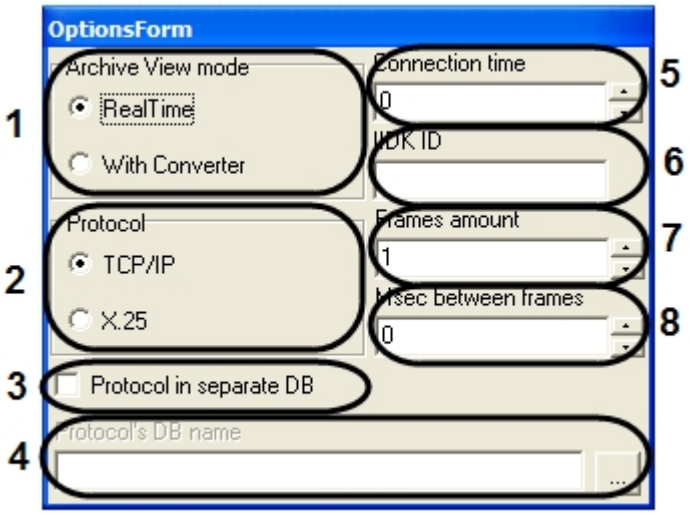
> **Note.**
>
> If the screen report has not been created before the printed report is activated, the screen report is automatically created.

18. The **Save Rpt As** button. Saves the report template, i.e. the list of objects (see p. 10) and corresponding events (see p.11).
19. The screen report panel. Shows the screen report. The panel includes the following columns:
    a. **Object** – the name of the object where the event occurred.
    b. **Object type** – the type of the object where the event occurred.
    c. **Event Description** – the name of the event registered by the system.
    d. **Advanced Info** – additional information on the event.
    e. **Time** – date and time when the event started.
    f. **Computer** - the name of the computer that registered the event.

24.3.1 The OptionsForm window

The **OptionsForm** settings window allows specifying additional parameters for the Report system: archive viewing mode, database connection, etc. To open the **OptionsForm** window, click the **Settings** button in the Report window (see The Report window section).

Figure shows the **OptionsForm** window.



The **OptionsForm** window includes the following interface elements (numbered according to the screenshot in the figure):

1. **Archive View Mode** group allows selecting the mode of playing the recordings from the video archive in the Report system:
2. The **RealTime** radio-button activates the playback via the viewing window of the *Intellect* system.

   > **Note.**
   >
   > This option is available if the *Intellect* software is currently running on the server where the archive is stored.

3. The **With Converter** radio-button activates the playback via the Converter.exe program.
4. The **Protocol** group allows to select the data exchange protocol for the connection with the videoserver:
   a. TCP/IP protocol;
   b. X.25 protocol .

   > **Note.**
   >
   > This protocol is used in the *ATM-Intellect* system (banking machine surveillance system).

5. The **Protocol in Separate DB** checkbox allows connecting a separate event database.

   > **Note.**
   >
   > This checkbox should be checked if the table with the registered events (the PROTOCOL table) is stored in a separate database outside of the *Intellect* system.

6. The **Protocol's DB Name** field allows to select the name of the database.
   To select the database, click the "**...**" button. The **Data Link Properties** window will open. Specify the database type, its pathname and access parameters (similar to changing the current database of the Report system).

   > **Note.**
   >
   > This field is enabled if the **Protocol In Separate DB** checkbox is checked.

7. The **Connection Time** field sets the waiting time for the connection with the videoserver.
8. The **IIDK_ID** field sets the id of the **IIDK Interface** object in the system settings. This object is used to receive the video feed from surveillance cameras of the *ATM-Intellect* system via the X.25 protocol.
9. The **Frames Amount** field sets the total number of frames requested from the videoserver when working via the X.25 protocol.
10. The **Msec Between Frames** field sets the time delay in milliseconds between the frames received from the banking machine archive. This parameter helps decrease the traffic in the communications channels working via the X.25 protocol.

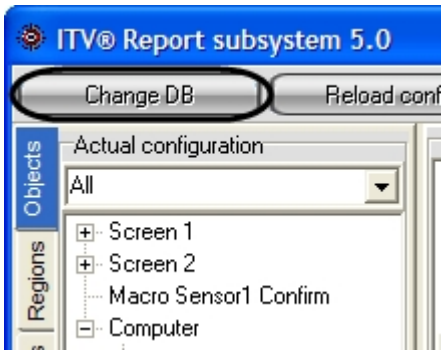
24.4 Connecting to databases

The Report system can be connected to another database of the *Intellect* system. It can also be connected to the events database, if such database exists.

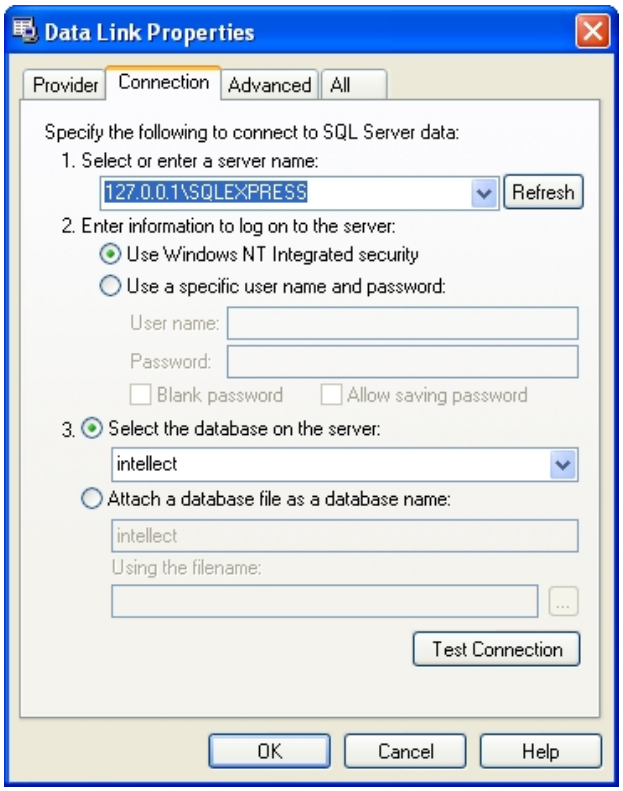
24.4.1 Connecting to the main database of the Intellect system

By default, the Report system loads the data from the main database of the *Intellect* system on the local computer. However, the database used by the Report system can be changed.

To change the main database used in the Report system, click the **Change DB** button in the Report window .



The **Data Link Properties** window will open allowing to select the name and access parameters of the database to connect to.



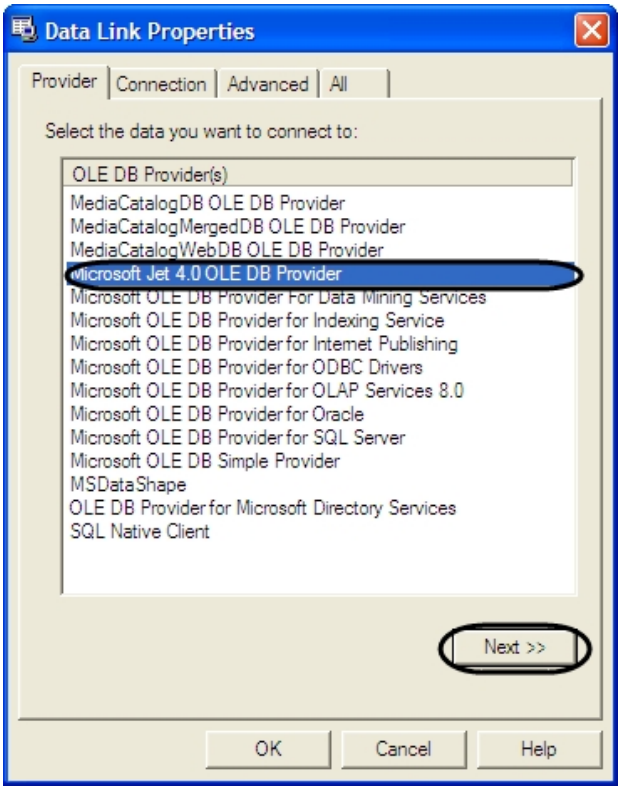
The *Intellect* system uses two types of database: SQL and Access. The connection procedure for each database type is described below.

24.4.1.1 Selecting an Access database and setting up the connection

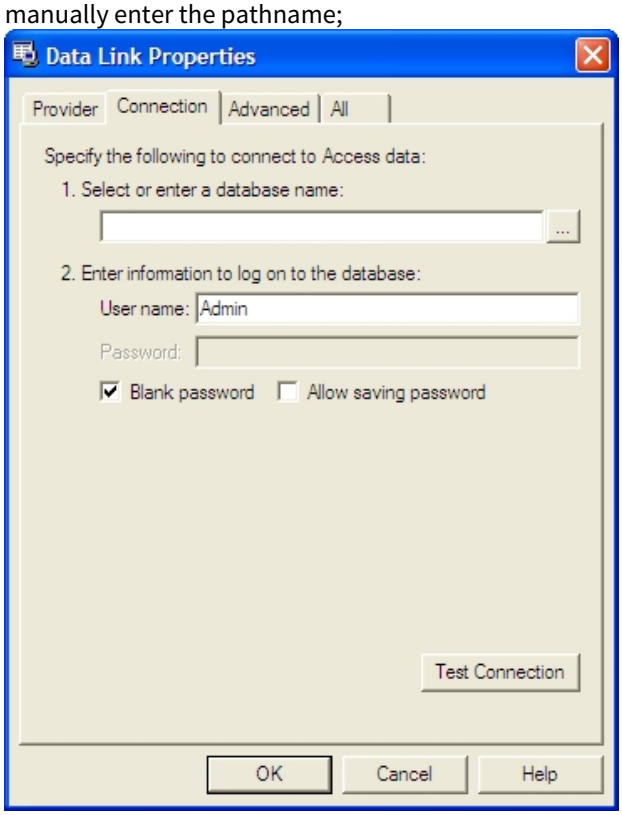
This section describes the connection to an Access database as the main *Intellect* database.

To connect to an Access database, open the **Data Link Properties** window. To set the main database in the Access format, do the following:

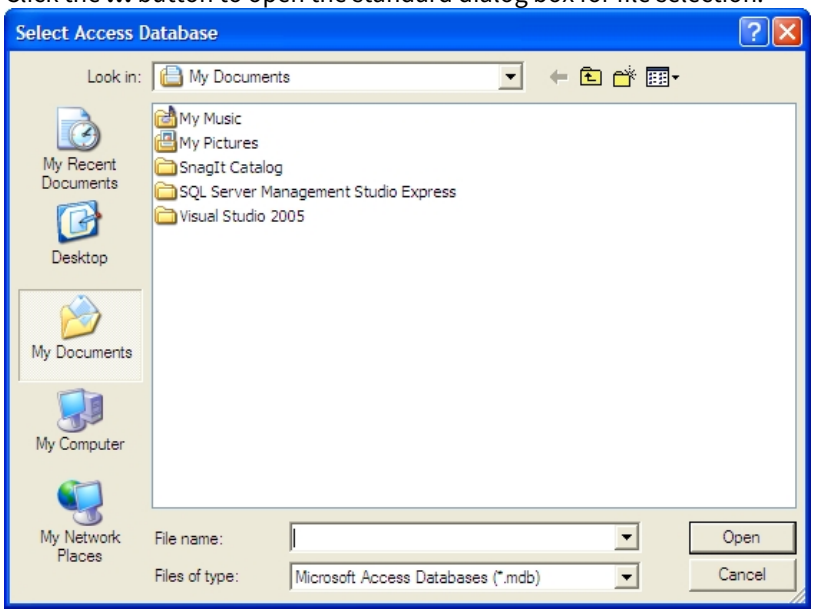
1. Select the **Microsoft Jet 4.0 OLE DB Provider** line in the **Provider** tab and click the **Next** button or move to the **Connection** tab.



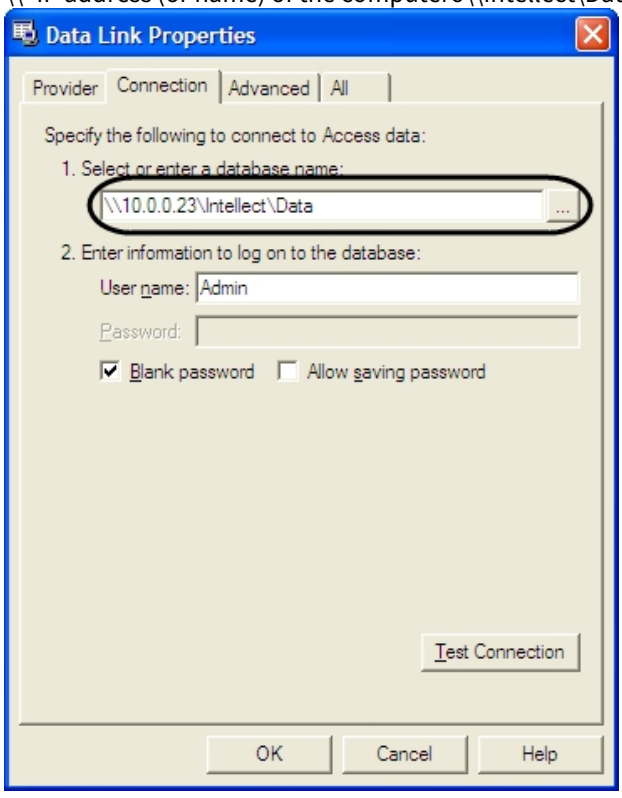
2. Select or enter the pathname of the database file in the **Select or Enter a Database Name** field of the **Connection** tab. To enter the pathname, do one of the following:
    a. manually enter the pathname;



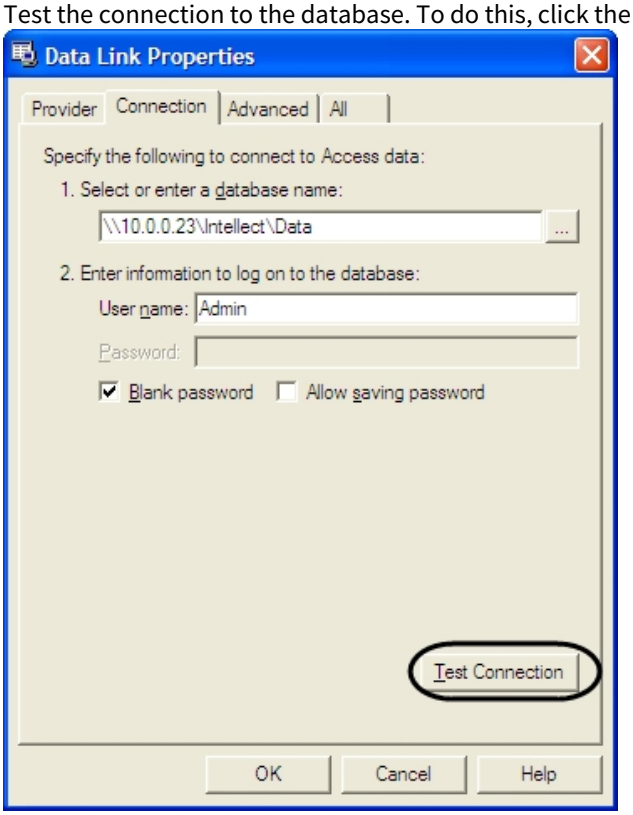
b. Click the **...** button to open the standard dialog box for file selection.



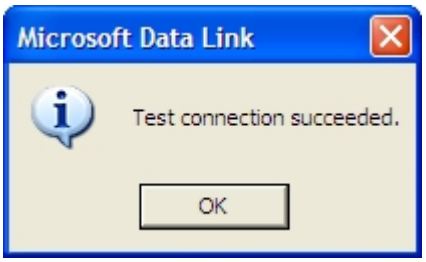
c. To connect to the main Access database located on the remote computer, the pathname should have the following format:
\\<IP address (or name) of the computerð\\Intellect\Data\intellect.mdb.



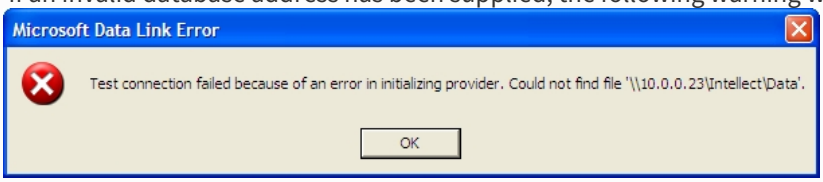
3. Test the connection to the database. To do this, click the **Test Connection** button.



4. The information box with the text **Test connection succeeded** will appear in case of successful connection.

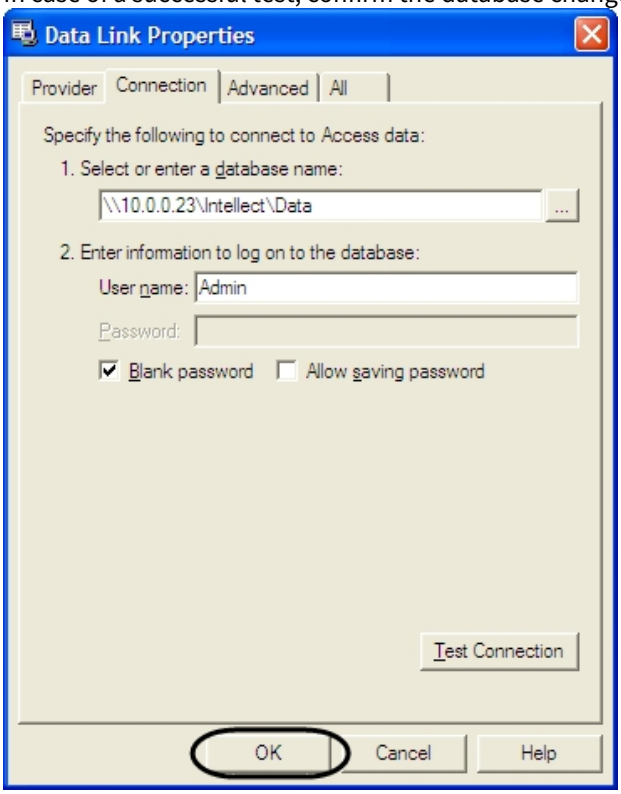


5. An information box with the error description will appear in case of a connection error.

> **Example:**
>
> If an invalid database address has been supplied, the following warning will open:
>
> 
>

> **Note.**
>
> In case of connection error, check the connection parameters in the **Provider** and **Connection** tabs.

6. In case of a successful test, confirm the database change by clicking the **OK** button.



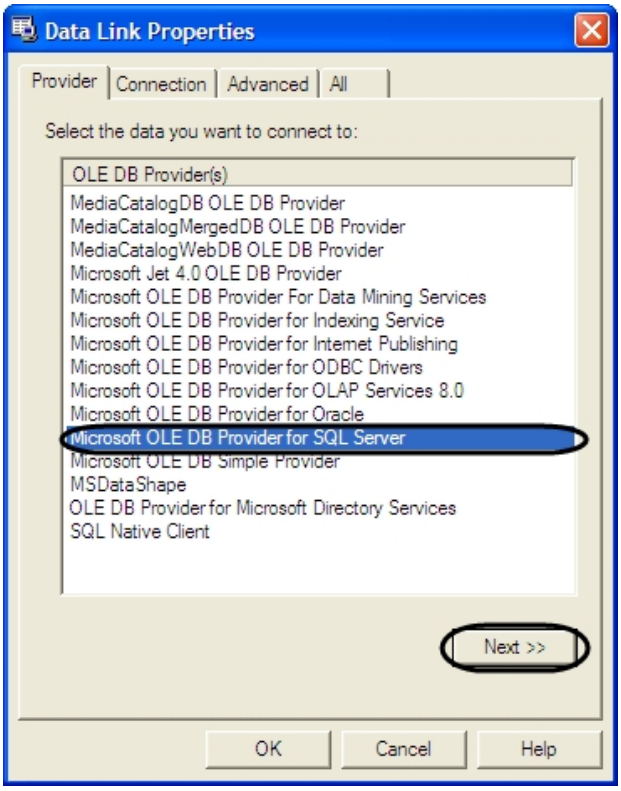
This completes the selection of the main database in Access format. The information from the selected database is now loaded into the Report system.

24.4.1.2 Selecting an SQL database and setting up its parameters

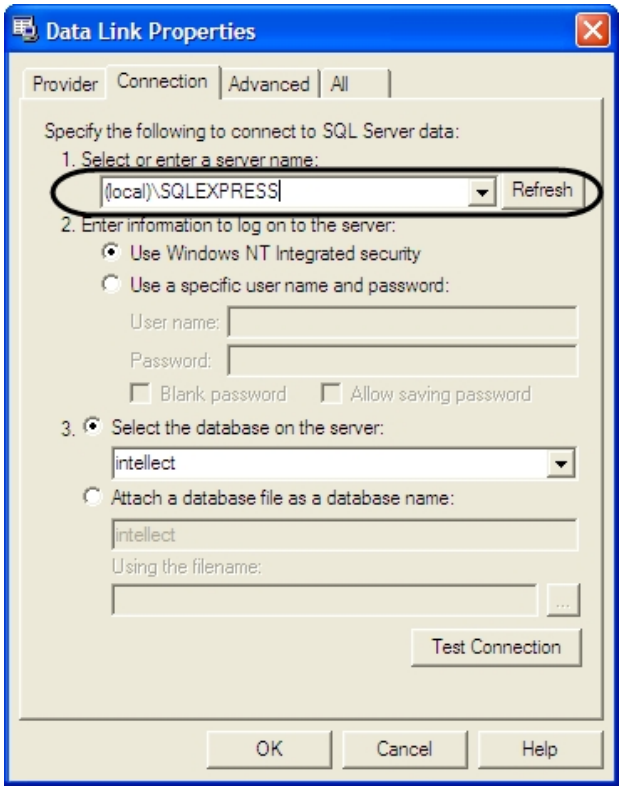
This section describes the connection to a Microsoft SQL database as the main *Intellect* database.

To connect a Microsoft SQL database, open the Data Link Properties window. To set the main database in Microsoft SQL format, do the following:

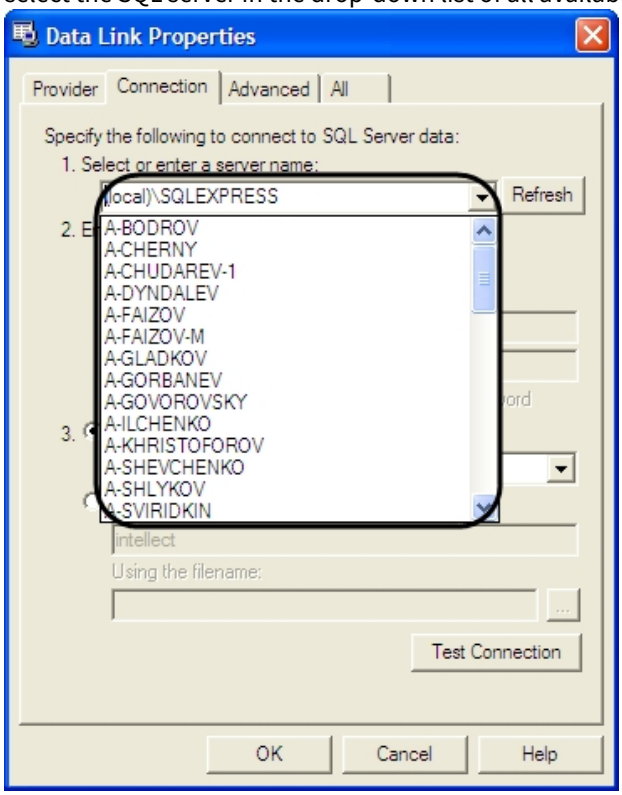
1. Select the **Microsoft OLE DB Provider for SQL Server** line in the **Provider** tab and click the **Next** button or move to the **Connection** tab.



2. Specify the name of the database SQL server in the **Connection** tab. This can be done using the **Select or Enter a Server Name** field.
   To enter the SQL server name, do one of the following:
   a. manually enter the name of the SQL server of the main *Intellect* database in the **Select or Enter a Server Name** field.



b. select the SQL server in the drop-down list of all available SQL servers. The list opens by clicking the button.



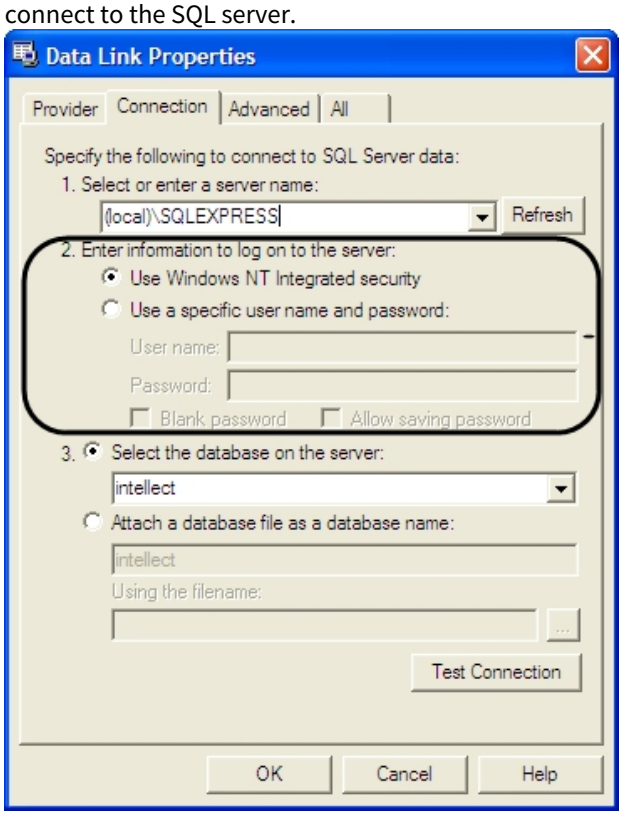
> **Note.**
>
> By default, the local server is selected named <local>\SQLEXPRESS.

> **Note.**
>
> To refresh the list of available servers, click the **Refresh** button next to the list field.

3. Specify the authorization parameters for logging onto the SQL server. The following options are available:
   a. The **Use Windows NT Integrated Security** radio-button. The Windows login information is used for authorization on the SQL server.

> **Note.**
>
> Used mostly to connect to the local SQL server.

b. The **Use Specific User name and Password** radio-button. The specific user name and password are used to connect to the SQL server.

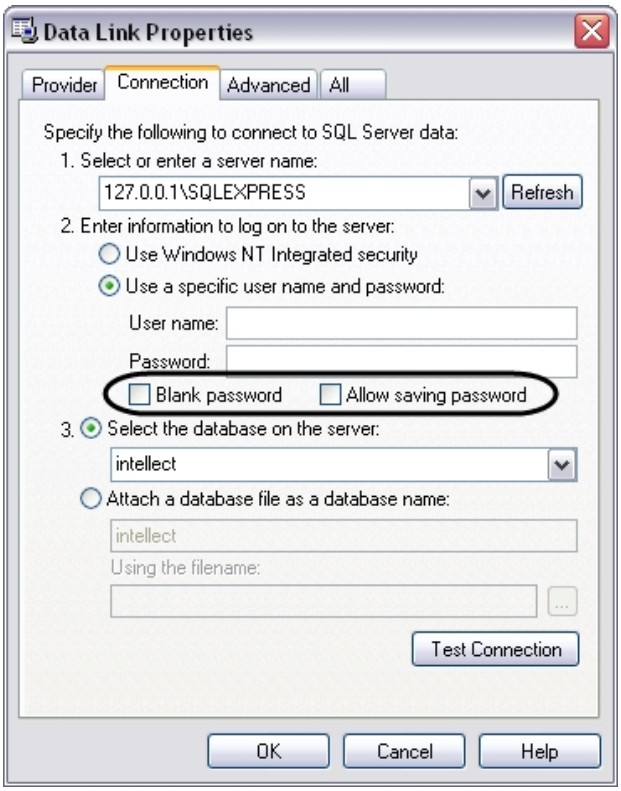


4. When the **Use Specific User name and Password** radio-button is selected, enter the information into the following fields: **User Name** and **Password**.

> **Note.**
>
> By default, the following information is set up during Intellect software installation: user name “sa”, password “axxonsoft” (see the Installing INTELLECT™ software section).

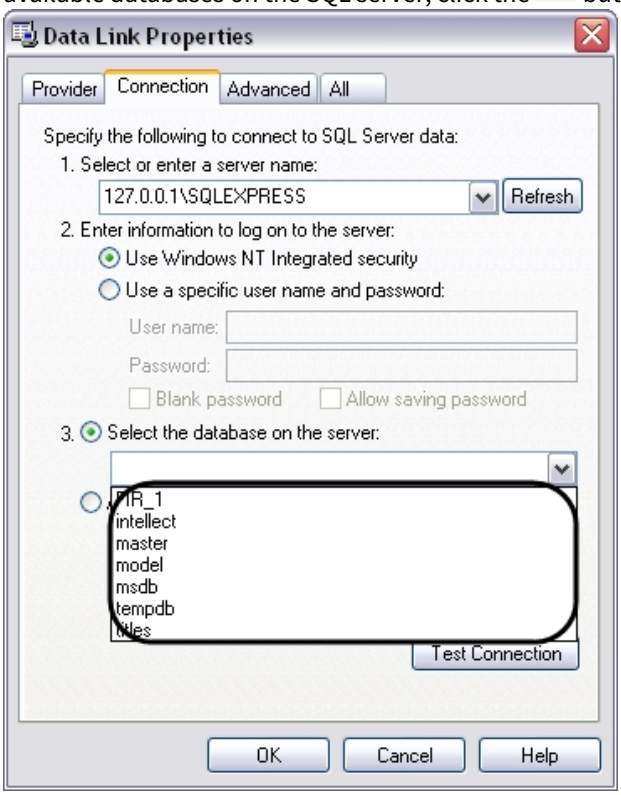
> **Note.**
>
> By default while installing the *Intellect* complex, the user(login) «sa» and Administrator password SQL Server (is registered while installing SQL Server, see Installing INTELLECT™ software) are set for authorization on SQL server

5. When the **Use Specific User name and Password** radio-button is selected, the **Blank Password** and **Allow Saving Password** checkboxes become enabled.



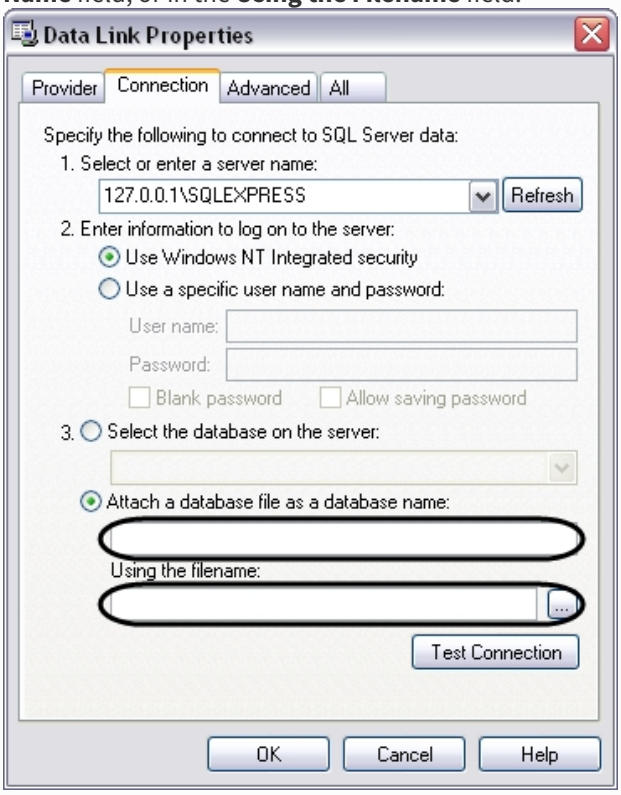
The **Blank Password** checkbox allows to enable connection to the SQL server with no password.
The **Allow Saving Password** button saves the password for the next connection to the SQL server.

6. Select the database to be used as main in the **Select the Database on the Server** drop-down list. To open the list of available databases on the SQL server, click the button.

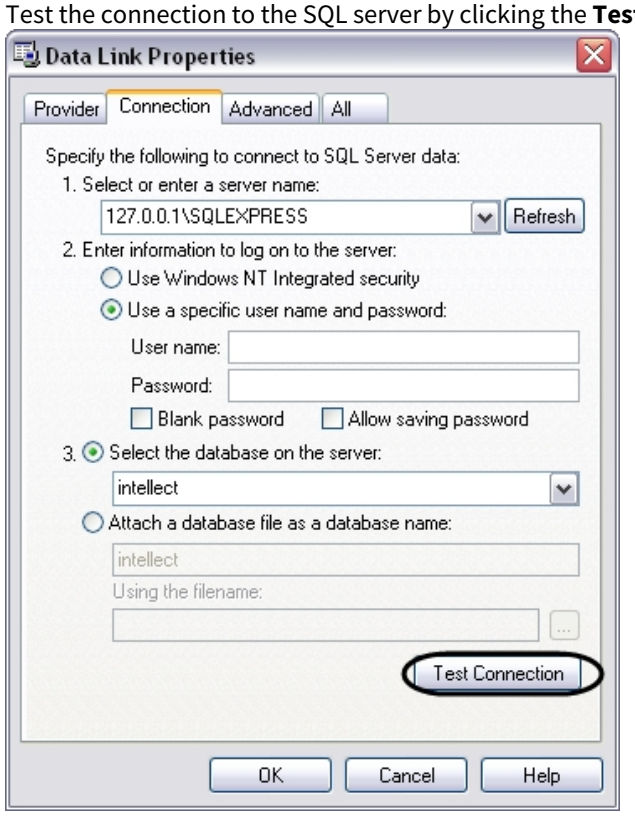


Note.

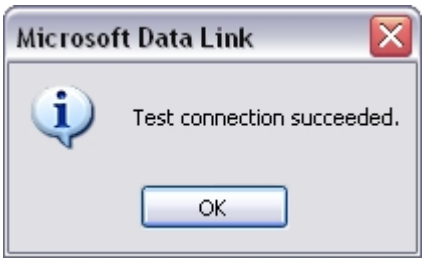
If necessary, the name of the database to connect to can be entered in the **Attach Database File** as **Database Name** field, or in the **Using the Filename** field.



7. Test the connection to the SQL server by clicking the **Test Connection** button.



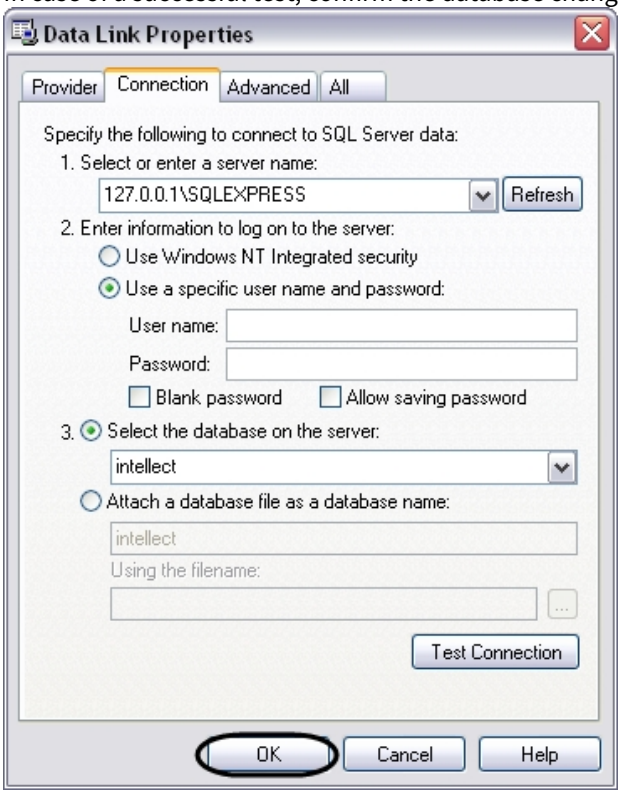
The information box showing the message "Test connection succeeded" will appear in case of successful connection.



An information box with the error description will appear in case of connection error.

> **Note.**
>
> In case of connection errors, check the connection parameters in the **Provider** and **Connection** tabs.

8. In case of a successful test, confirm the database change by clicking the **OK** button.



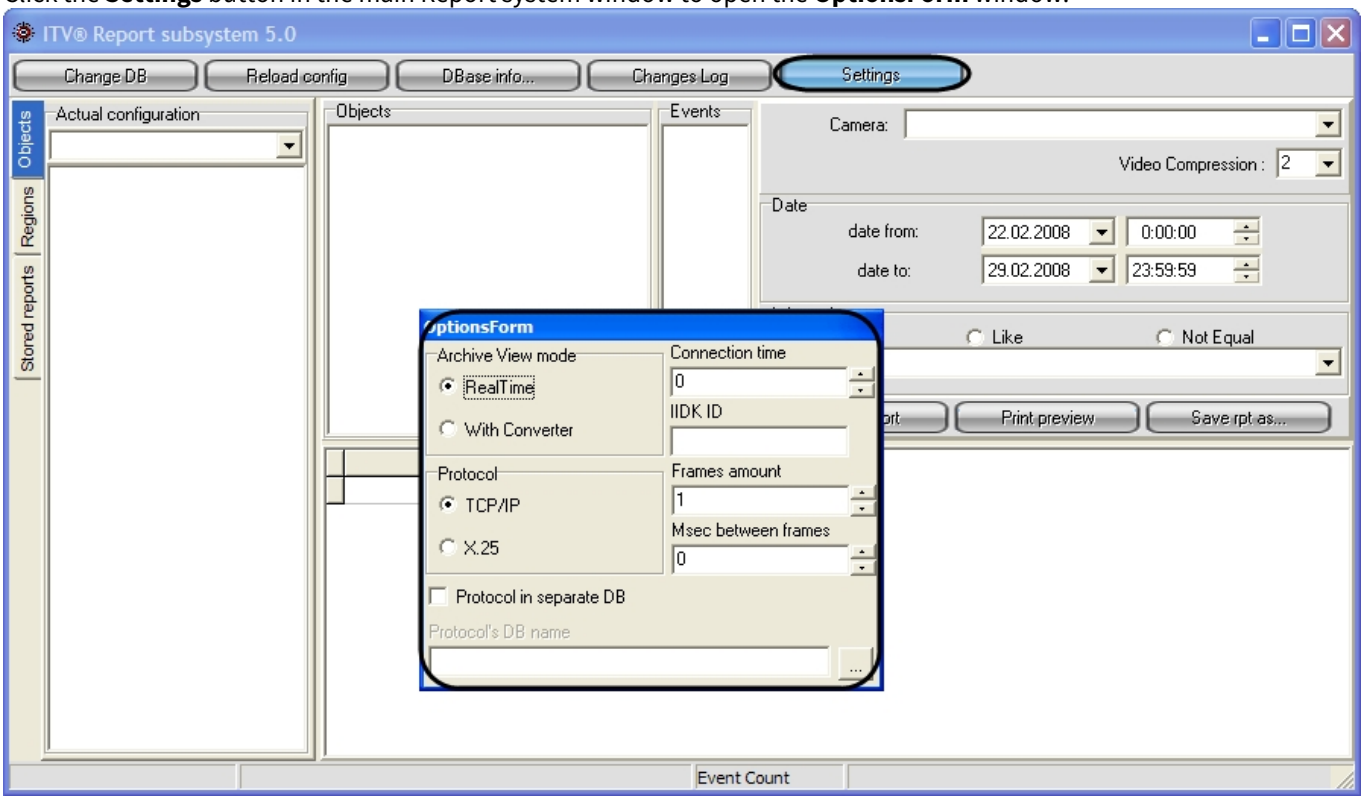
This completes the selection of the main database in Microsoft SQL format. The information from the selected database is now loaded into the Report system.

24.4.2 Connecting to the Events Log (PROTOCOL table)

By default, the information on registered events is stored in the PROTOCOL table in the main database. However, there is an option to set up the events to be logged into a separate events database, that is, the PROTOCOL table to be separate from the main database. The creation of the separate events database is described in the corresponding sections (see Extracting event protocol into an individual database).

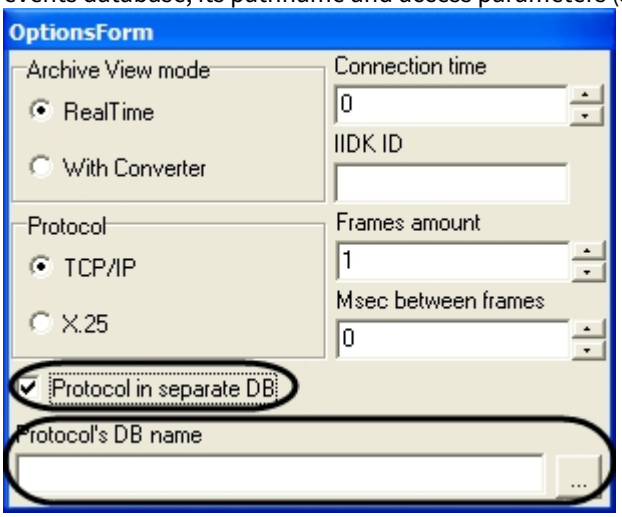
To connect the events database to the Report system, do the following:

1. Click the **Settings** button in the main Report system window to open the **OptionsForm** window.



2. Check the **Protocol in Separate DB** checkbox to enable connection to a separate event database. Specify the name of the database in the **Protocol's DB Nam**e field.

3. To select the events database, click the ... button . The **Data Link Properties** window will open. Specify the type of events database, its pathname and access parameters (similar to changing the main database of the Report system).



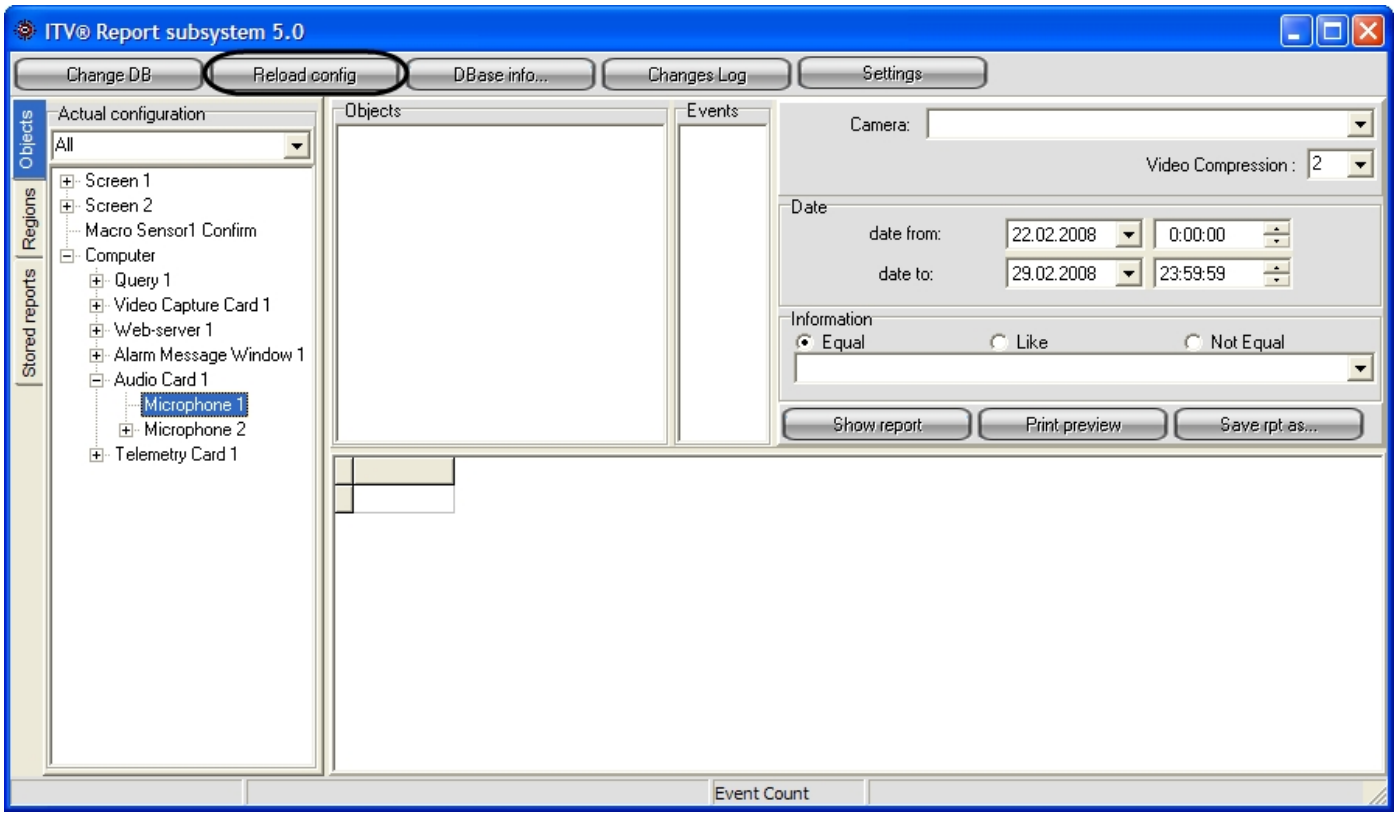
4. Press the **Escape** key on the keyboard to close the **OptionsForm** window.

This completes the selection of the events database in the Report system. The information from the selected database is now loaded into the Report system.

24.5 Manual loading of the configuration and registered events from the database

The system configuration and registered events are loaded from the database into the Report system in the following cases: Report system start-up, connection to the database, changing the database.

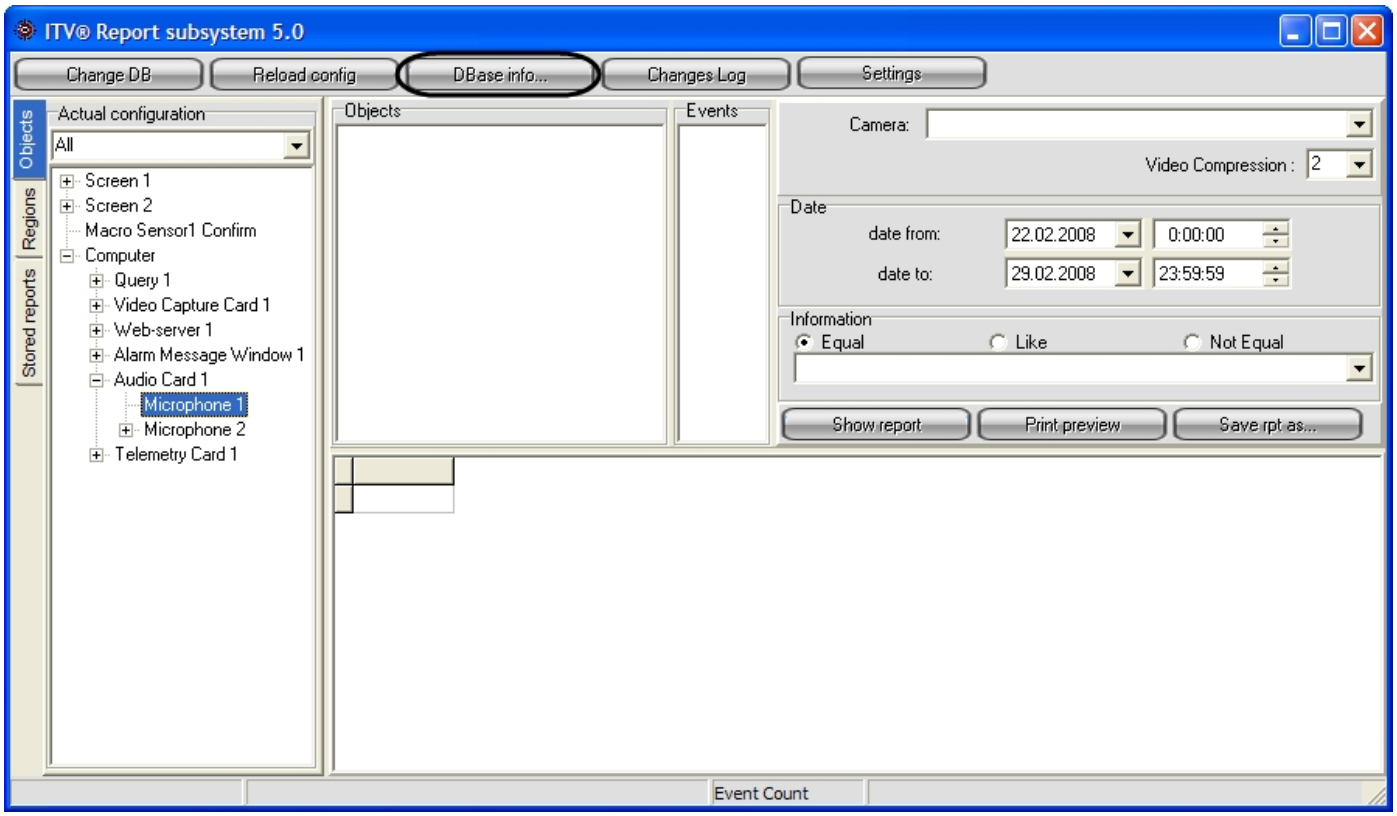
The configuration and events database can be loaded manually, as well. To reload the configuration and events database, click the **Reload Config** button on the main control panel of the Report window.



The objects tree, the regions list, the report templates list, and the registered events list will be refreshed according to the new system configuration.

24.6 Viewing the general information on the events in the database

To view the general information on the events stored in the current database, click the DBase Info button on the main control panel.



The **Base Info** information box will open showing the general information about the database.

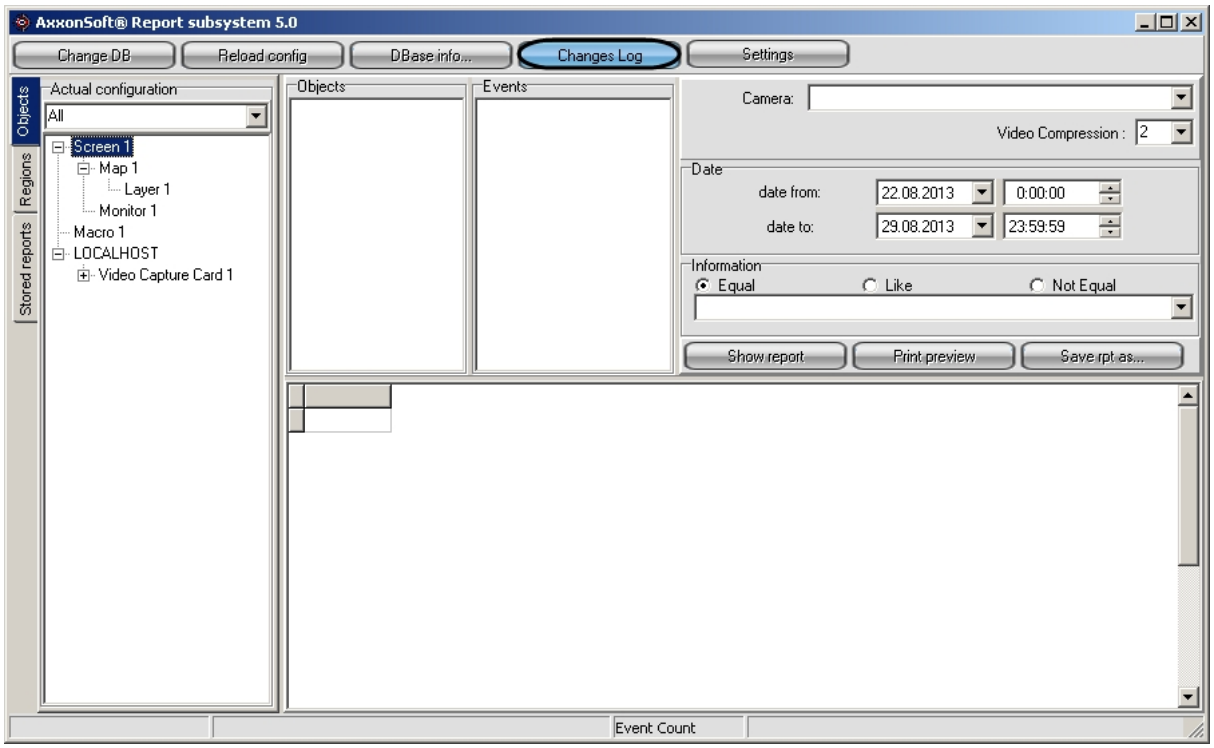
The following information is displayed:

1. The name of the current database.
2. The date of the first registered event in the current database.
3. The date of the last registered event in the current database.
4. The number of days between the first and the last event.
5. Total number of events in the database.

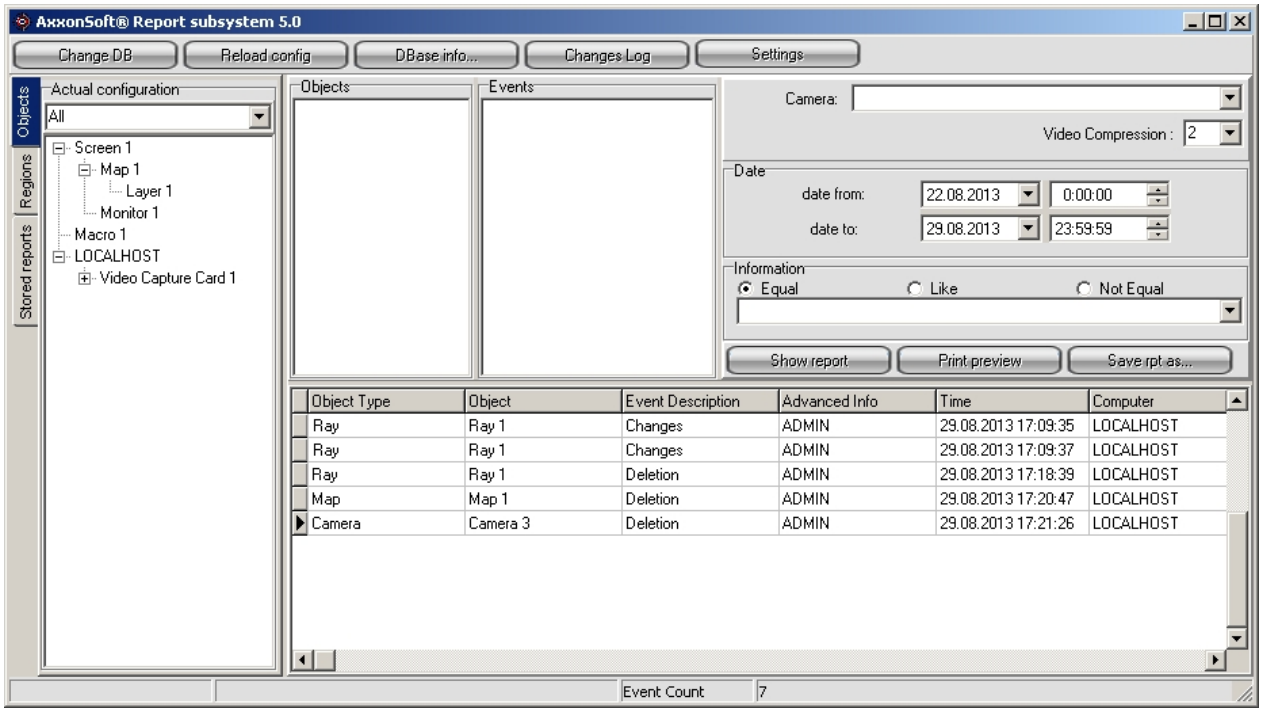
24.7 Creating the log of changes made to the system configuration

The Report system allows viewing the log of all changes made to the system configuration.

To view the configuration changes, click the **Changes Log** button on the main control panel.



The screen report section of the window will show the list of changes made to the system configuration.



The changes log includes the following columns:

1. **Object Type** —the type of the object that has been changed.
2. **Object** — the name of the object that has been changed.
3. **Event Description** — the type of the change made to the object.
4. **Advanced Info** — additional information on the change.
5. **Time** — date and time of change.
6. **Computer** — the name of the computer where the change has been made.

24.8 Using the report templates in the Report system

The report templates can be created in the Report system. The templates help automate the process of creating the screen and printed reports for a selected list of objects for particular time periods.

A report template comprises of a list of objects and events related to these objects. When the template is created, the list of objects and events is formed. To create a particular screen or printed report based on this template, only the time interval should be specified.

24.8.1 Recommendations for template creation

We do not recommend including too many objects in a template. If the template includes too many objects, the request for all events related to these objects will take a very long time to execute, or will fail.

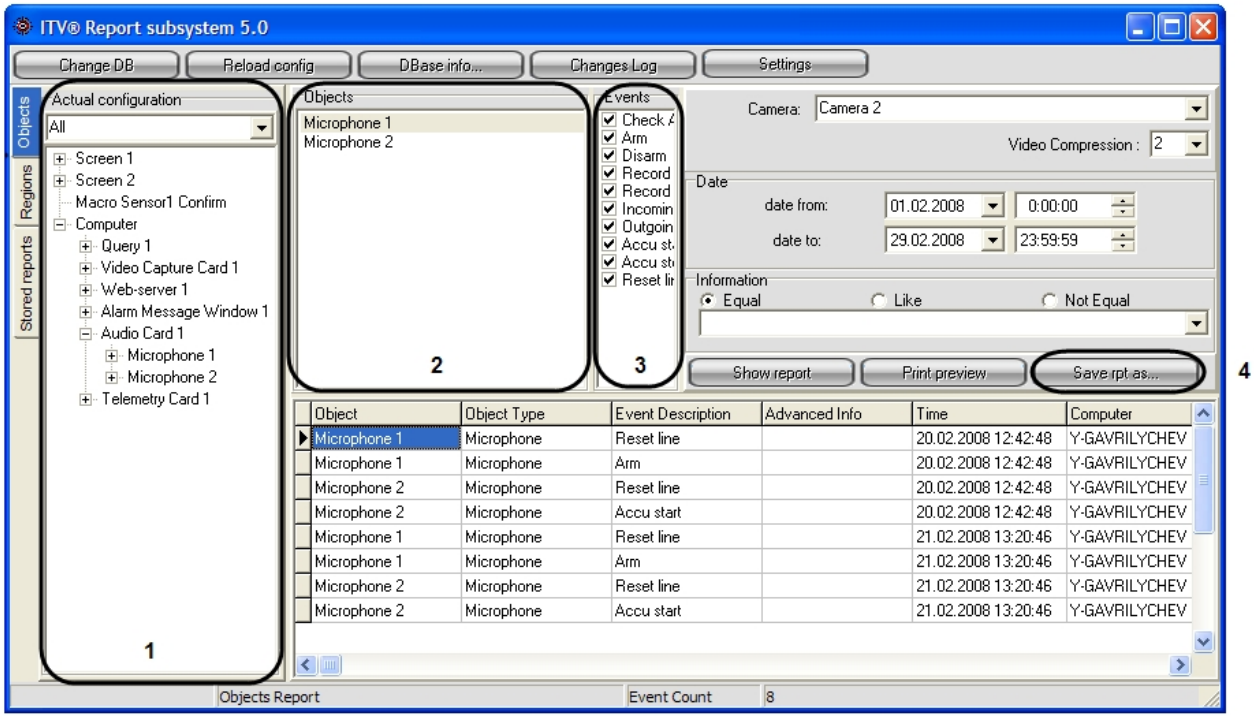
We recommend creating smaller templates that group the objects according to different regions of the protected territory.

We do not recommend including more than 200 objects in one template.

24.8.2 Creating a report template

To create a report template, the object list should be formed. This can be done using the **Objects and Regions** tabs, and the **Objects** panel. The list of events for each object can be formed using the Events panel.

The Figure shows the stages of template creation.



To create the template, do the following:

1. Click the **Objects** tab, then choose the complete objects tree or just one object type (ex., **Camera**) in the **Actual Configuration** drop-down list.

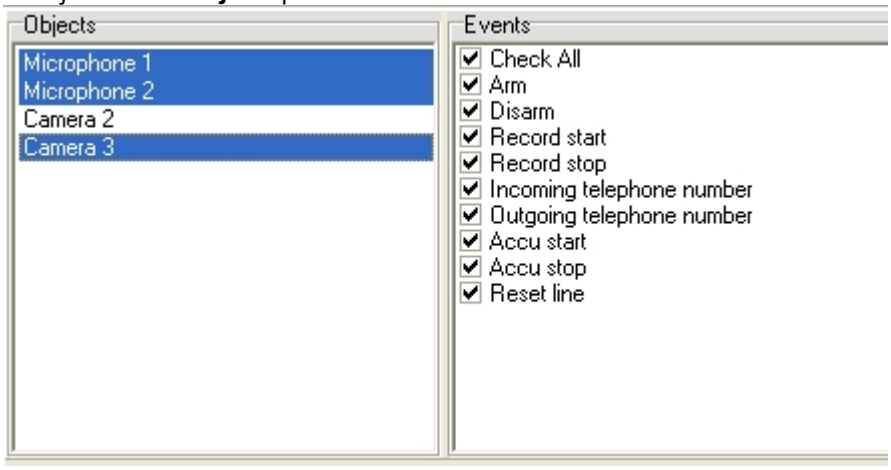
To select objects in regions, click the **Regions** tab and choose the required region type in the **Regions** drop-down list.

1. Place the required objects into the **Objects** panel. Select an object in the objects tree (**Actual Configuration** panel of the **Objects** tab or **Regions** panel of the **Regions** tab) and do one of the following:
    a. double-click the object;
    b. select the object and press Enter on the keyboard;
    c. drag the object to the **Objects** panel.

> **Note.**
>
> Only the objects with their own events can be placed onto the Object panel and thus included in the report. For example, the **Audio Card** object does not have any events of its own, so it cannot be included in the report template.

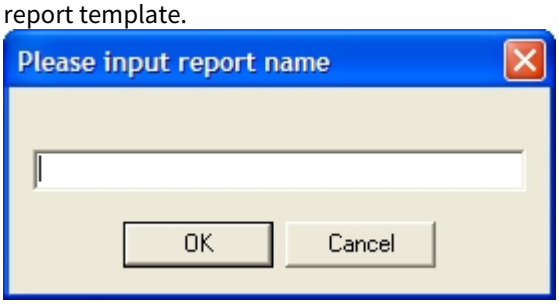
To remove the object from the report list, select the object in the **Objects** panel and press Delete on the keyboard.

2. Select the events in the **Events** panel, to be included in the report for each object in the **Objects** panel.
   By default, all events for selected objects are included. To remove particular events from the report, select an object in the **Object** panel and uncheck the checkboxes next to the events in the Events panel, which should not be included in the report template.
   To simplify editing of the events list for similar objects, a common list can be created for a group of objects. Select a group of objects in the **Objects** panel and edit the list of events. This list will relate to each of the selected objects.



> **Note.**
>
> If no events are selected in the **Events** panel for an object, then ALL events for this object will be included in the report.

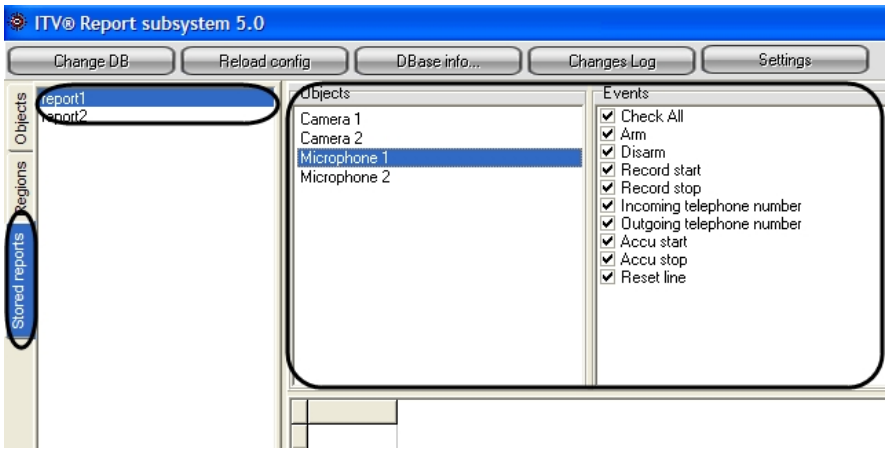
3. Click the **Save Rpt As** button. The **Please Input Report Name** dialog box will appear, allowing to specify the name of the report template.



Type in the template name and click **OK**.

This completes the creation of the report template.

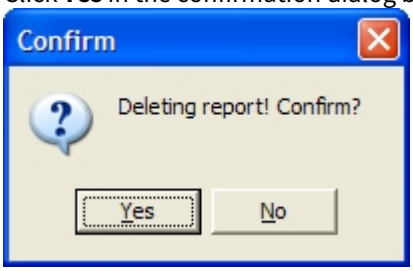
The template will appear in the objects tree of the **Shared Reports** tab. To view the template, use the **Objects** and **Events** panels. These panels are populated automatically upon template selection in the **Shared Reports** objects tree. These panels allow editing the events list and removing the objects from the list. The changes will be saved in the template.



24.8.3 Deleting the report templates

To delete the template, do the following:

1. Open the **Shared Reports** tab;
2. Select the template to be deleted;
3. Press Ctrl+Delete on the keyboard;
4. Click **Yes** in the confirmation dialog box.



This completes deletion of the report template.

24.9 Using screen and printed reports

The screen and printed reports can be created in the Report system.

A screen or printed report is a table showing the dates of the registered events, the videoservers that generated the event, and other relevant information.

The screen report allows viewing the information on the objects and events in the Report window. The screen report allows playing the recordings from the videoserver for each of the records in the report. The video archive can be played from the screen report using the surveillance window or converter.exe utility.

Note.

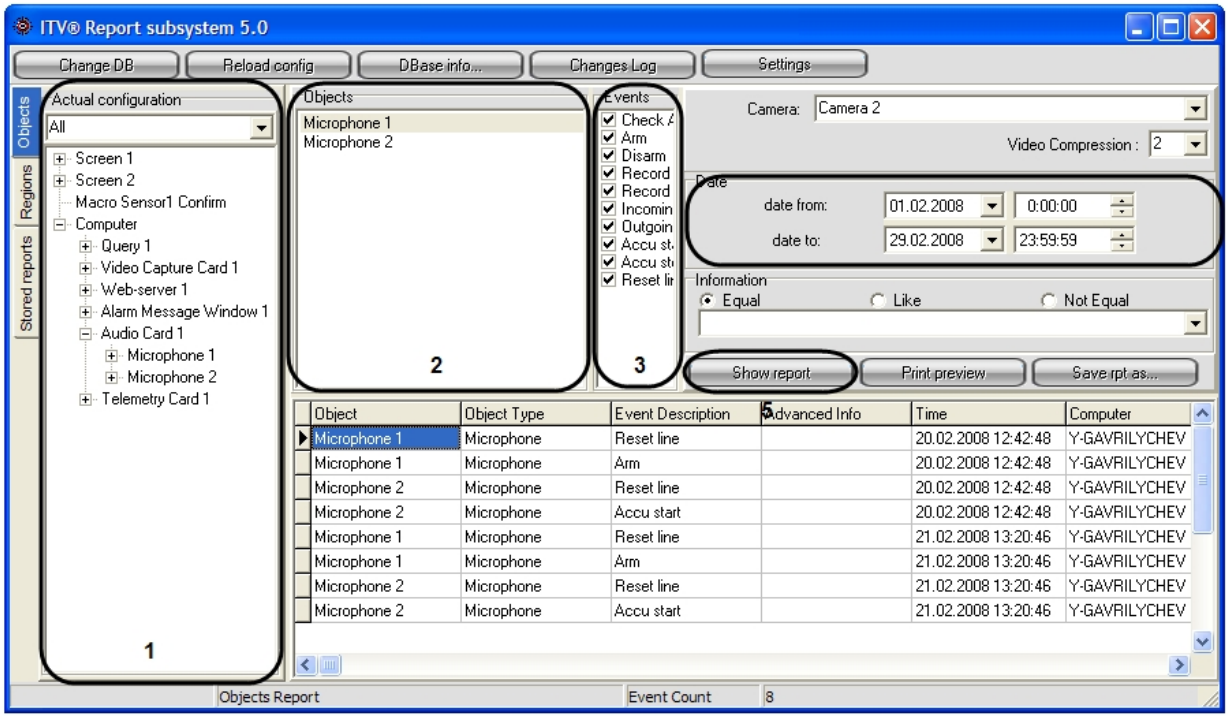
The playing of the recording in the surveillance window is possible if the *Intellect* software is running on the videoserver.

The printed report is used for printing the report or exporting it into one of the common file formats. When the printed report is created, all information about the selected objects and events is displayed in a separate window.

24.9.1 Creating a screen report

The screen report provides the means for convenient viewing of the registered events and playback of the video recordings from the videoserver archive.

Figure shows the stages of the screen report creation.



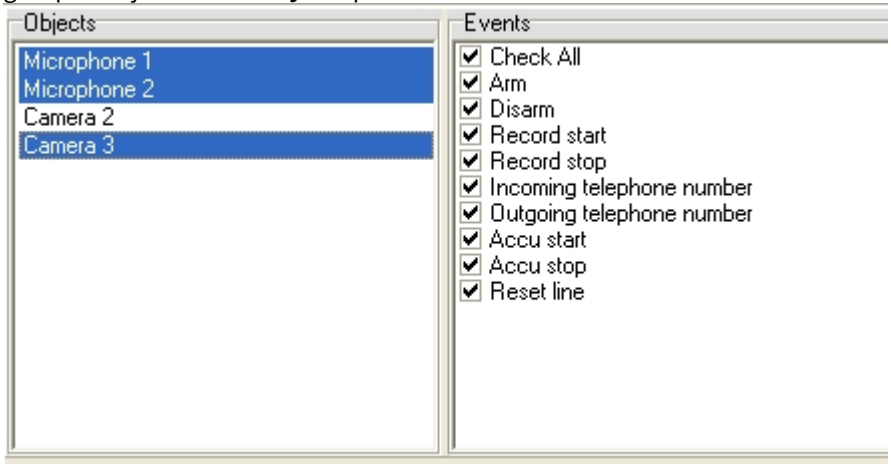
To create the screen report, do the following:

1. Click the **Objects** tab, then choose the complete objects tree or just one object type (ex., **Camera**) in the **Actual Configuration** drop-down list.
   To select objects in regions, click the **Regions** tab and choose the required region type in the **Regions** drop-down list.
2. Place the required objects into the **Objects** panel. Select an object in the objects tree (**Actual Configuration** panel of the **Objects** tab or **Regions** panel of the **Regions** tab) and do one of the following:
   a. double-click the object;
   b. select the object and press Enter on the keyboard;
   c. drag the object to the **Objects** panel.

   > **Note.**
   >
   > Only the objects with their own events can be placed onto the **Object** panel and thus included in the report. For example, the **Audio Card** object does not have any events of its own, so it cannot be included in the report template.

   To remove the object from the report list, select the object in the **Objects** panel and press Delete on the keyboard.
3. Select the events in the **Events** panel, to be included in the report for each object in the **Objects** panel.
   By default, all events for selected objects are included. To remove particular events from the report, select an object in the **Object** panel and uncheck the checkboxes next to the events in the **Events** panel, which should not be included in the report template.
   To simplify the editing of the events list for similar objects, a common list can be created for a group of objects. Select a

group of objects in the **Objects** panel and edit the list of events. This list will relate to each of the selected objects.



Note.

If no events are selected in the **Events** panel for an object, then ALL events for this object will be included in the report.

4. Specify the time period to create the report for, in the **Date** group of fields.
5. Click the **Show Report** button to create the screen report.

Note.

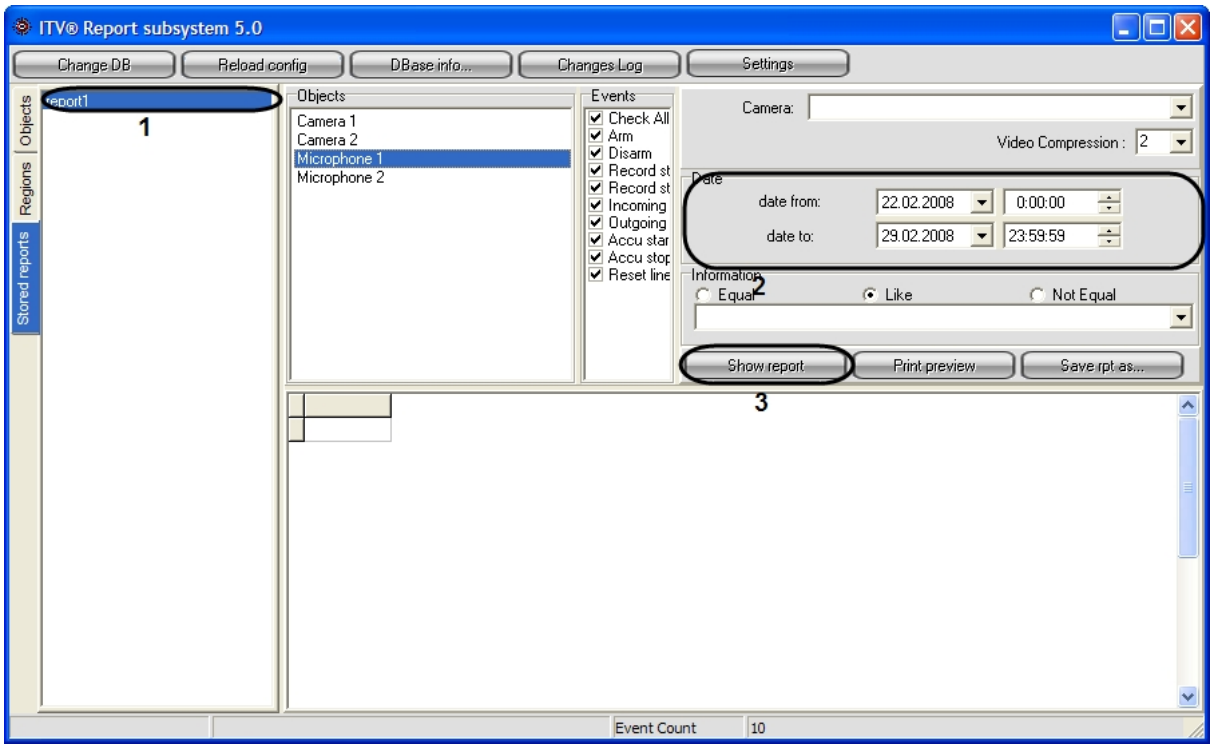
Clicking the **Show Report** button is equivalent to pressing F5 on the keyboard.

This completes the creation of the screen report. The screen report will be displayed in the lower part of the Report window.

24.9.1.1 Creating a screen report from the report template

The report templates can be created in the Report system. The templates help automate the process of creating the screen and printed reports on a selected list of objects for particular time periods.

A report template comprises of a list of objects and events related to these objects. When the template is created, a list of objects and events is formed. To create a particular screen or printed report based on this template, only the time period should be specified.



To create a screen report from the template, do the following:

1. Click the **Shared Reports** tab and select the required report template from the list.
2. Specify the time period to create the report for, in the **Date** group of fields.
3. Click the **Show Report** button to create the screen report.

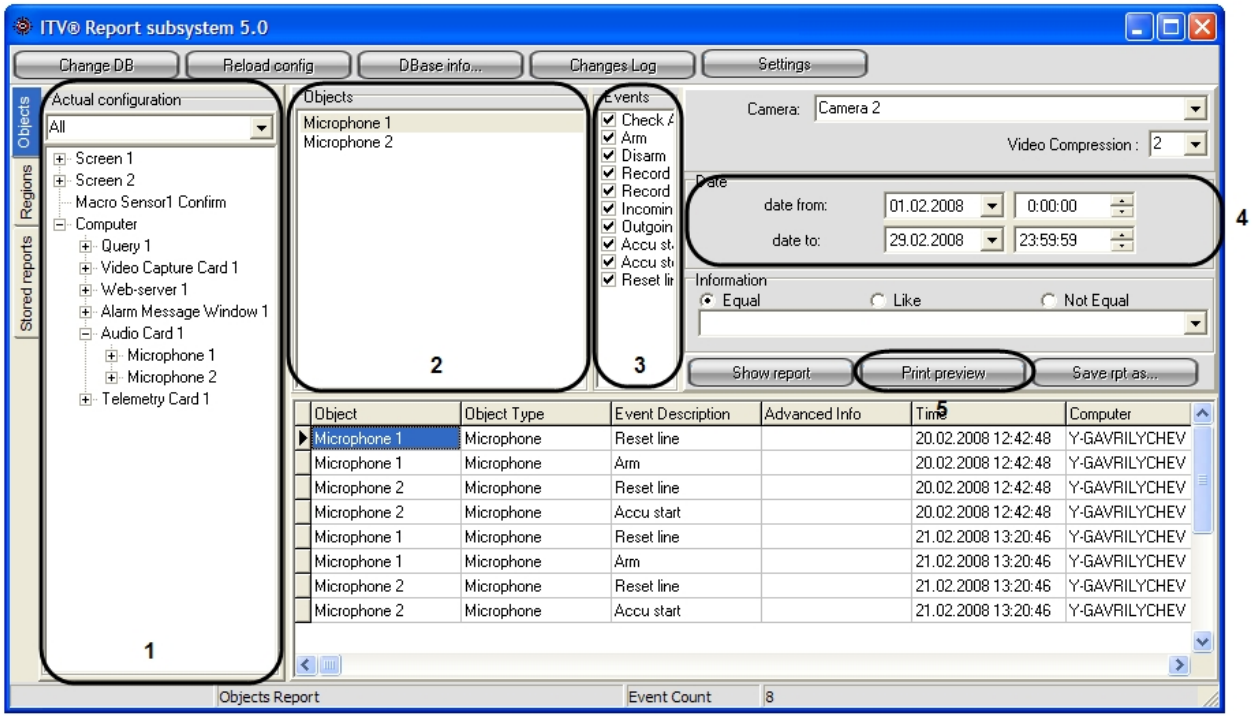
> **Note.**
>
> Clicking the **Show Report** button is equivalent to pressing F5 on the keyboard.

This completes the creation of the screen report from the template. The screen report will be displayed in the lower part of the Report window.

24.9.2 Creating a printed report

The printed report allows convenient viewing of the report in a separate window or printing the report on paper.

Figure shows the stages of creation of the printed report.

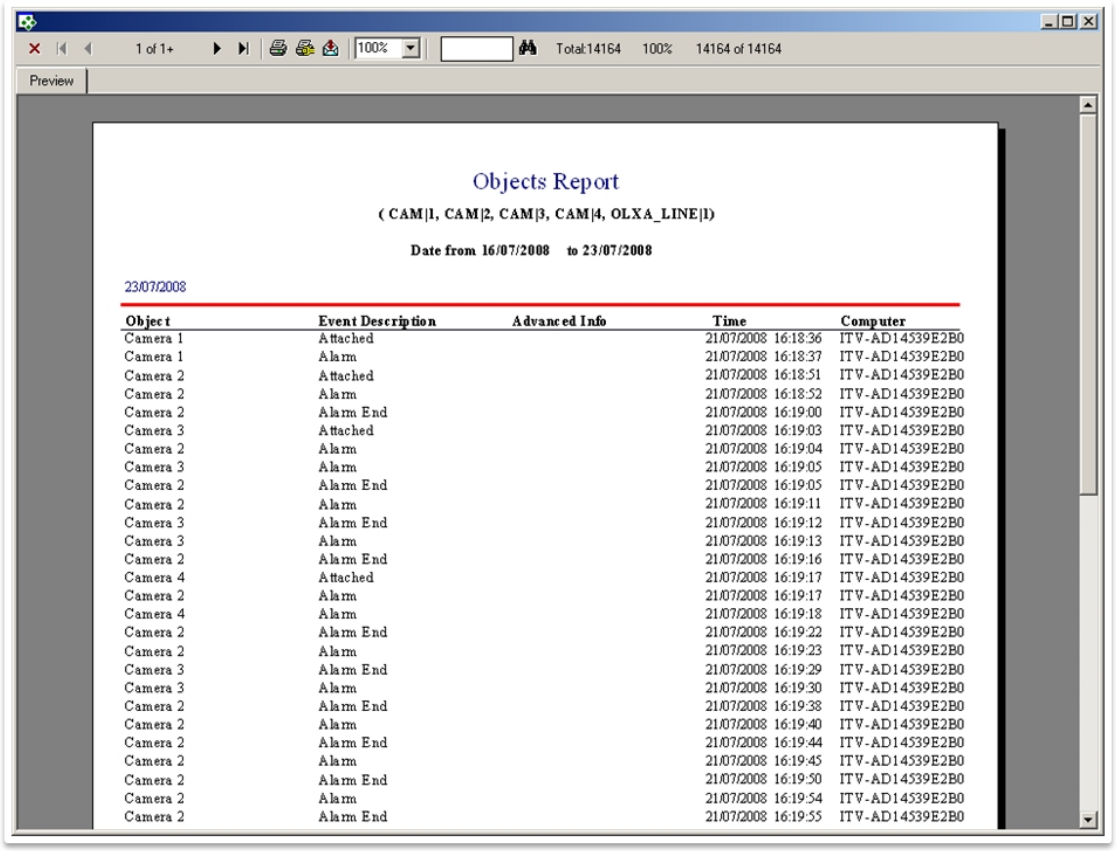


Creating a printed report is similar to the screen report creation procedure in p. 1 to 4 (see sections above).

To create a printed report, click the **Print Preview** button in p.5.

> **Note.**
>
> Clicking the **Print Preview** button is equivalent to pressing F6 on the keyboard.

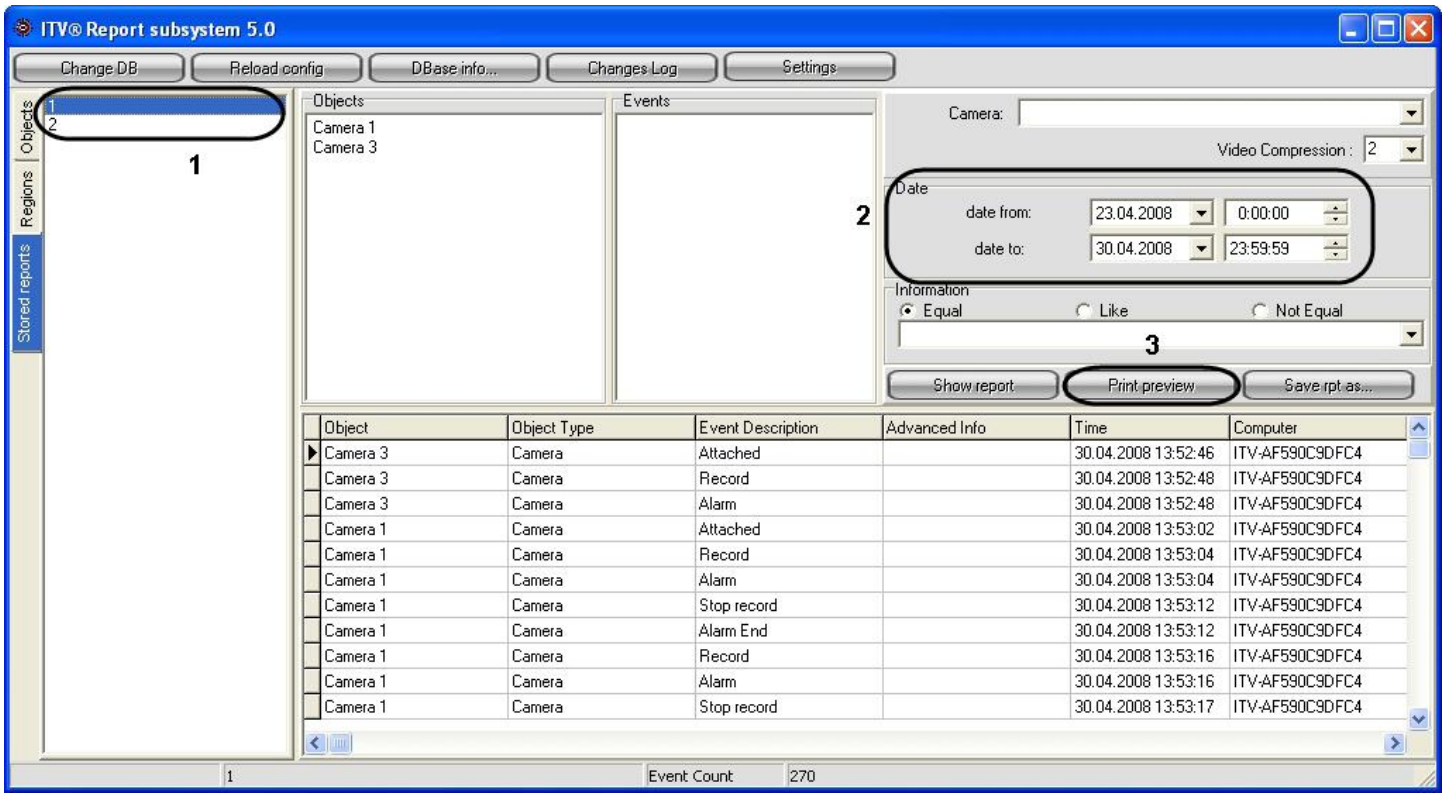
This completes the creation of the printed report. The report will open in a separate window.



24.9.2.1 Creating a printed report from a report template

The report templates can be created in the Report system. The templates help automate the process of creating the screen and printed reports on a selected list of objects for particular time periods.

A report template comprises of a list of objects and events related to these objects. When the template is created, a list of objects and events is formed. To create a particular screen or printed report based on this template, only the time period should be specified.

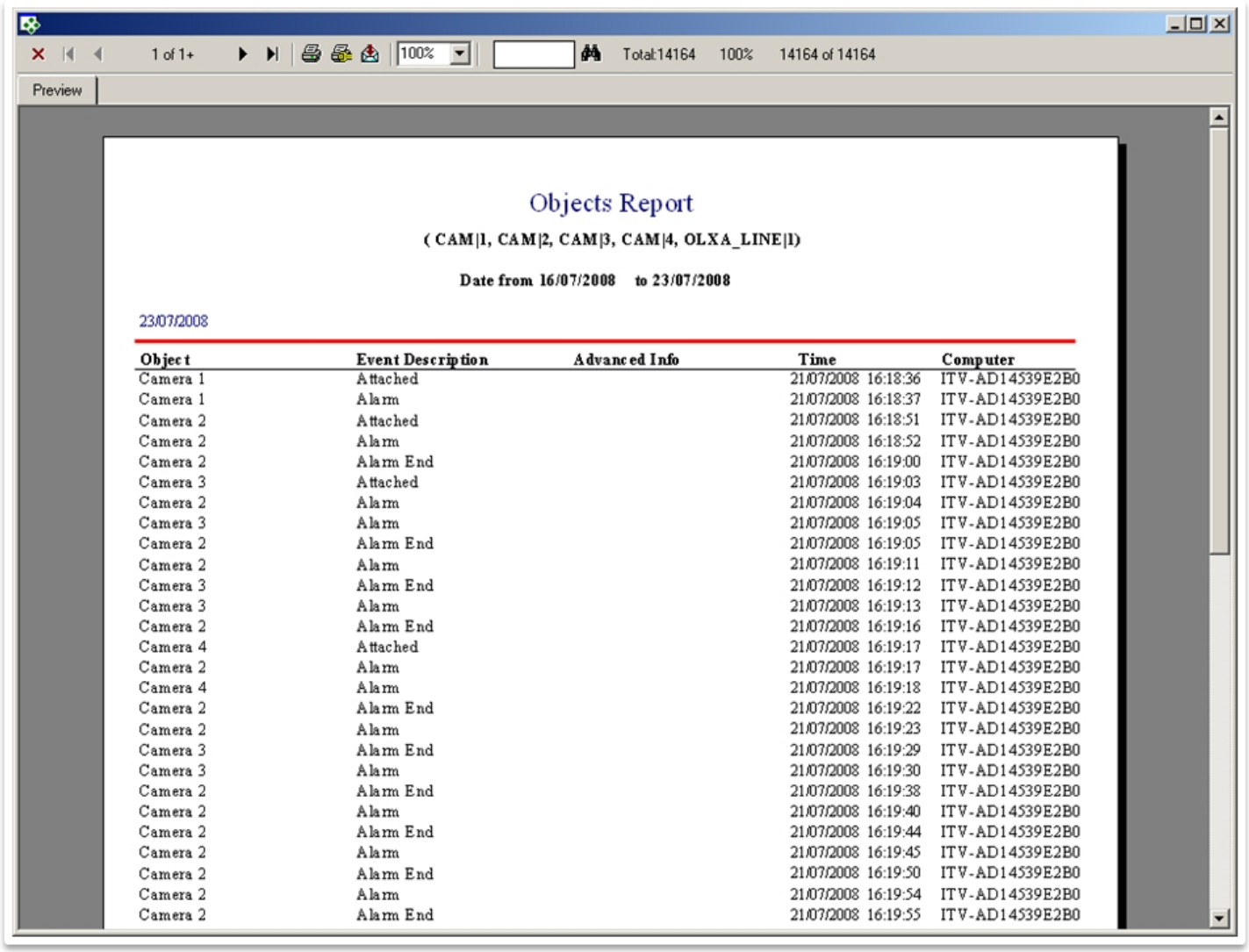


Creating a printed report is similar to the screen report creation procedure in p. 1 to 2 (see the Creating a screen report from the report template section above).

To create a printed report from the template, click the **Print Preview** button in p.3.

> **Note.**
>
> Clicking the **Print Preview** button is equivalent to pressing F6 on the keyboard.

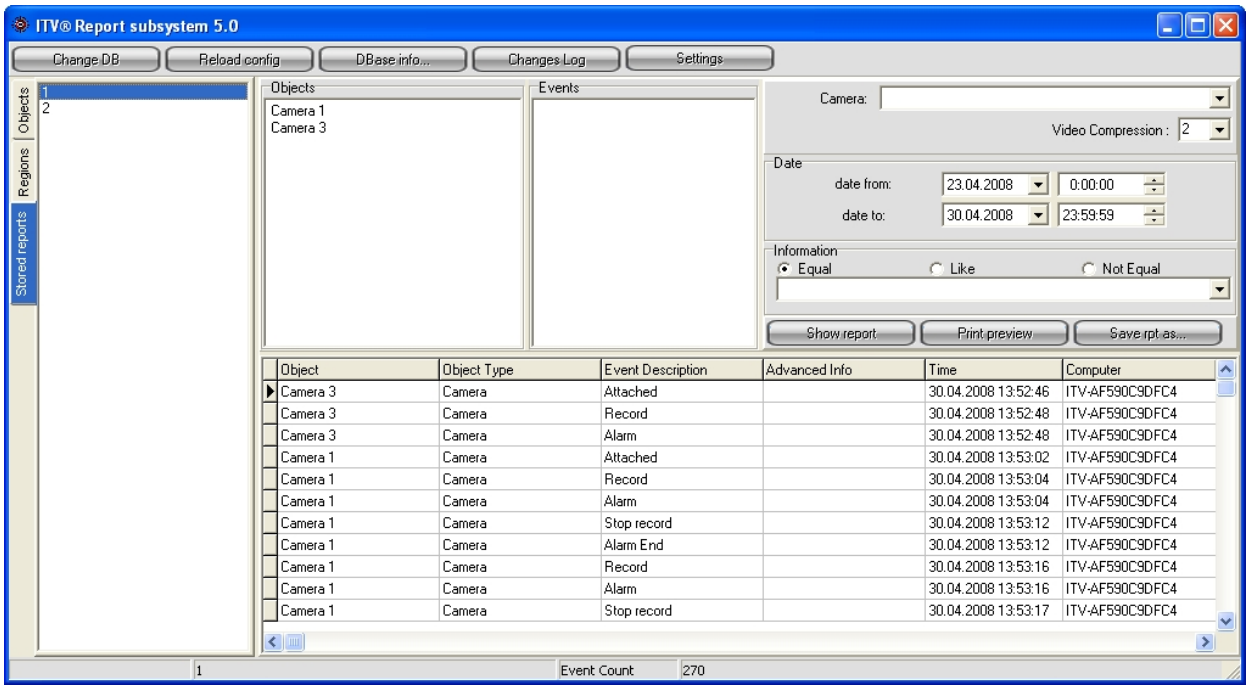
This completes the creation of the printed report from the template. The report will open in a separate window.



24.9.3 Printing the report

The report templates can be created in the Report system. The templates help automate the process of creating the screen and printed reports on a selected list of objects for particular time periods.

A report template comprises of a list of objects and events related to these objects. When the template is created, a list of objects and events is formed. To create a particular screen or printed report based on this template, only the time period should be specified.



Creating a printed report is similar to the screen report creation procedure in p. 1 to 2 (see the Creating a screen report from the report template section above).

To create a printed report from the template, click the **Print Preview** button in p.3.

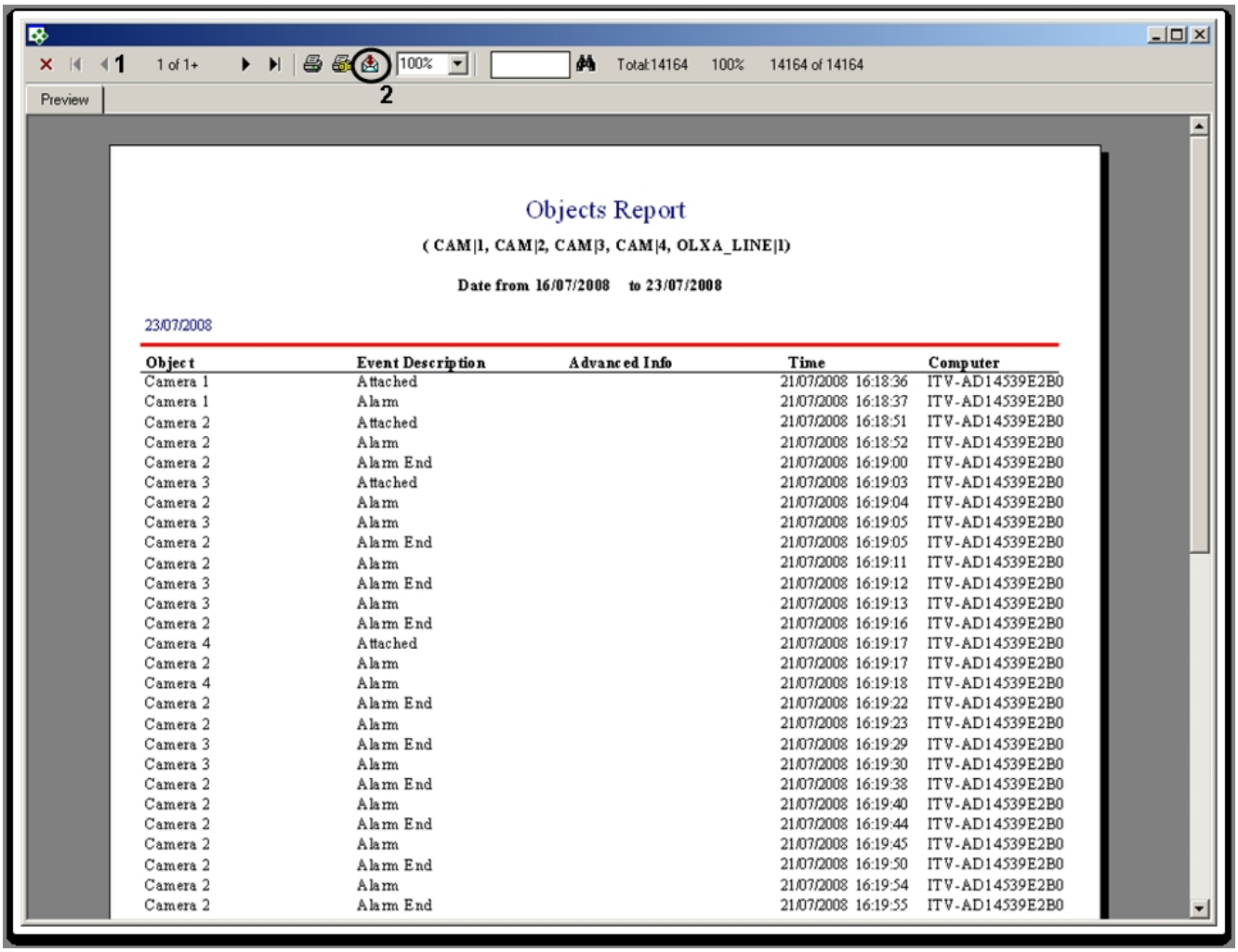
> **Note.**
>
> Clicking the **Print Preview** button is equivalent to pressing F6 on the keyboard.

This completes the creation of the printed report from the template. The report will open in a separate window.

24.9.4 Exporting the report to a file

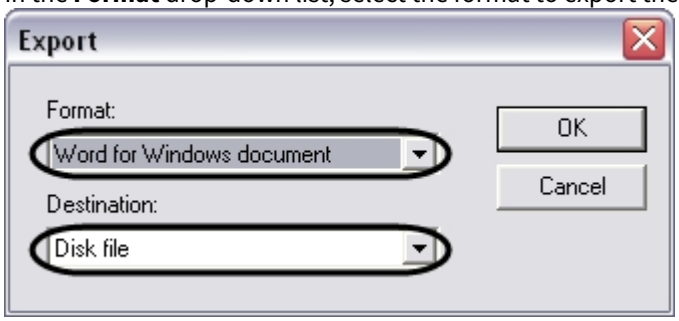
The Report system allows exporting the created report into one of the commonly used file formats.

The report to be exported opens in a separate window .



The report is exported from the printed report window. To export the report, do the following:

1. Create the printed report (see the Creating a Printed Report section).
2. Click the **Export** button in the window showing the report.
3. Specify the following in the **Export** dialog box:
   a. in the **Format** drop-down list, select the format to export the report to

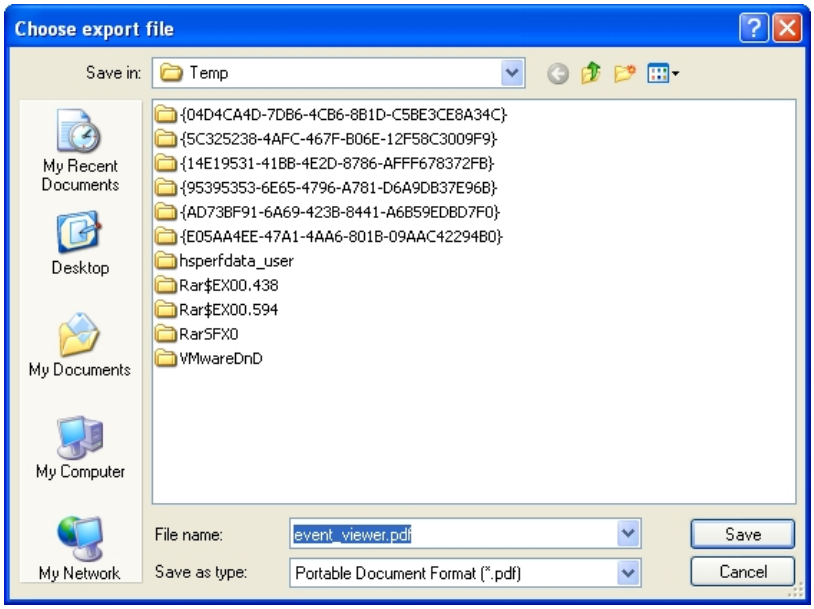


   b. in the **Destination** drop-down list, select the action to be taken. The **Destination** list contains the following options:
      i. **Application** – open the exported file in the corresponding application.
      ii. **Disk File** – save the exported file to disk in a specified format.
      iii. **Exchange Folder** – send the file to Microsoft Exchange project.
      iv. **Lotus Domino** – send the file to Lotus project.
      v. **Microsoft Mail (MAPI)** – send the file via Windows mail client.

> **Note.**

The Destination list is disabled for some formats.

4. Click the **OK** button in the Export window.
5. If **Disk File** is selected in the **Destination** list, the **Choose Export File** dialog box will appear. Select the folder and filename to save the report to.



Specify the filename and folder and click the **Save** button.

Note.

The **Choose Export File** window does not open for some file formats.

This completes the exporting of the report into a file.

24.10 Video recording playback from the Report system

The Report system allows playback of the video recordings related to a selected event from the screen report. The video playback starts from the moment the event occurred.

The recordings are played using the Converter.exe utility or the surveillance window of the corresponding camera. The playback option is selected in the Report system settings window (See the OptionsForm Window section).

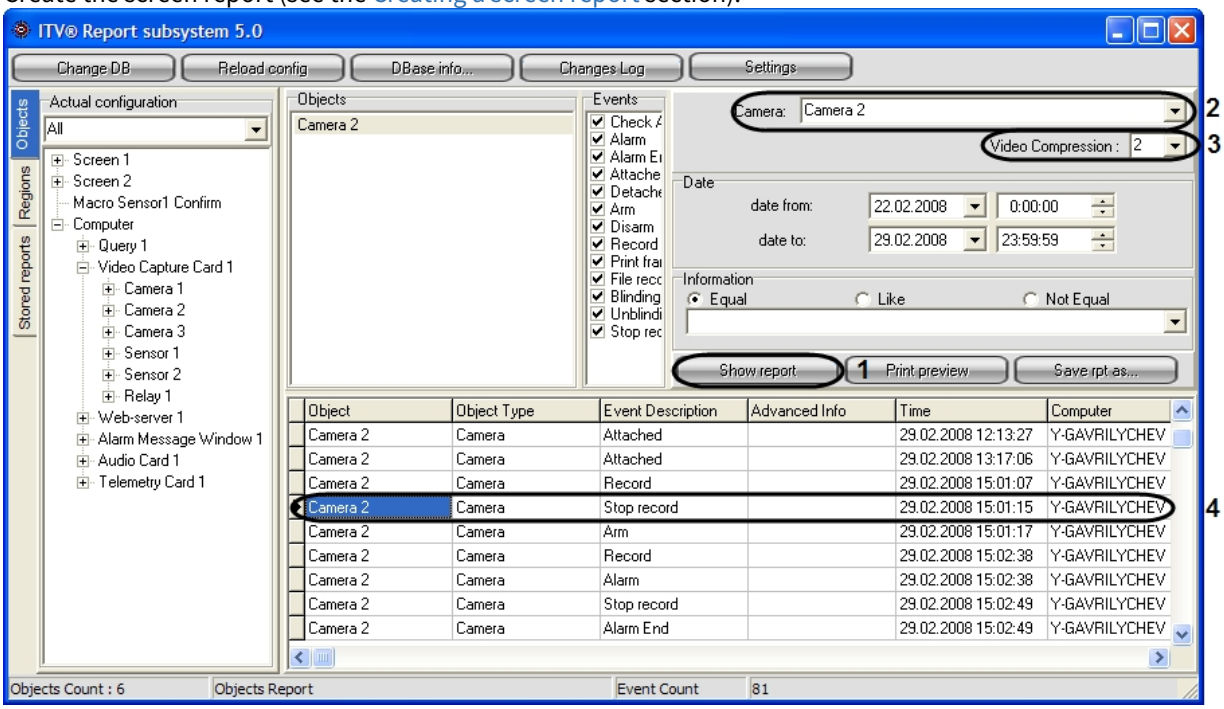
Note.

To play the video recordings directly in the surveillance window, start the *Intellect* software, and create and set up the surveillance window.

24.10.1 Playback of the video recordings from the Report system

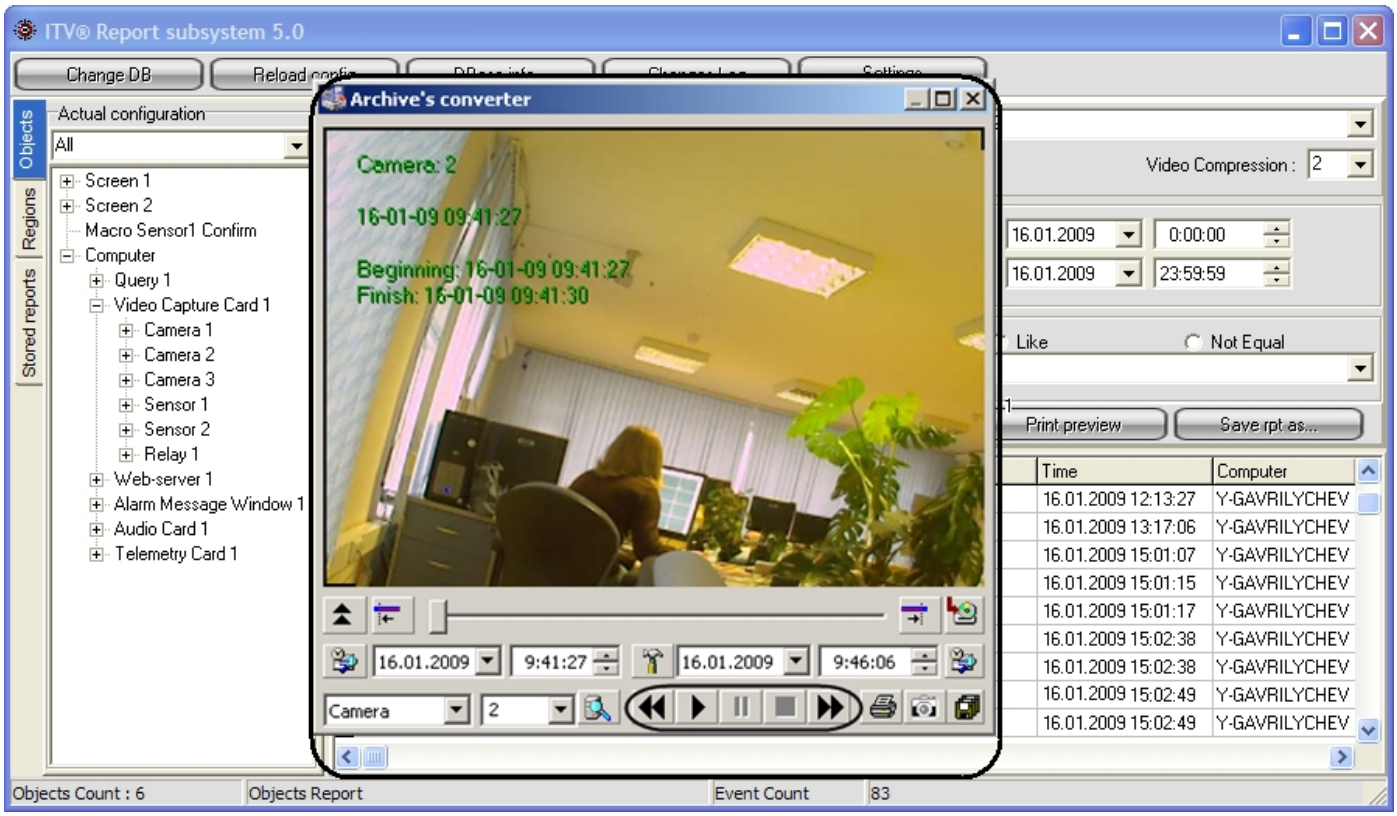
To play the video recordings from the Report system, do the following:

1. Create the screen report (see the Creating a screen report section).



2. Select the camera from the list of all camera names in the system.
   By default, only the recordings from the **Camera** objects are played from the screen report. The recording from the camera that generated the event shown in the **Event Description** column, is played. No recording is played for other objects.
   The camera whose archive will be played, should be selected in the **Camera** field.
3. Specify the compression level for the playback.
4. Double-click the event in the screen report.

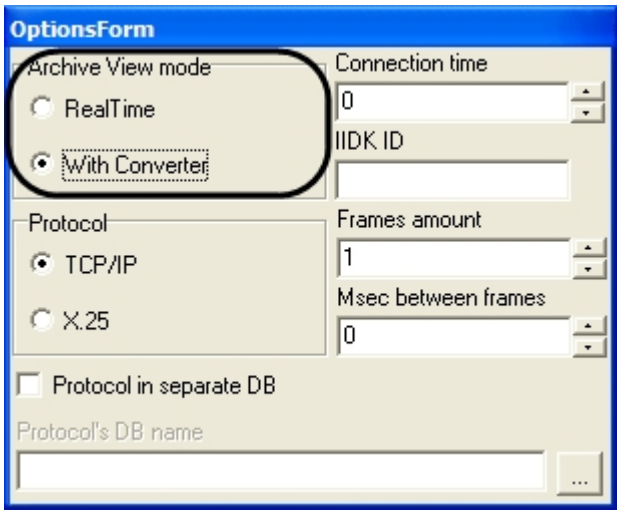
The converter.exe utility or the surveillance window will open, showing the recording for the time specified in the **Data** column of the screen report for the selected event.



24.10.2 Selecting the playback mode of video recordings

The Report system provides twoways of playing the video recordings: using the Converter.exe utility or the surveillance window of the *Intellect* system.

> **Note.**
>
> To play the video recordings in the surveillance window, the Intellect system should be running on the server where the archive is taken from.



If the **RealTime** radio-button is selected, the archive will be played in the surveillance window. If the **With Converter** radio-button is selected, the archive will be played using the Converter.exe utility.

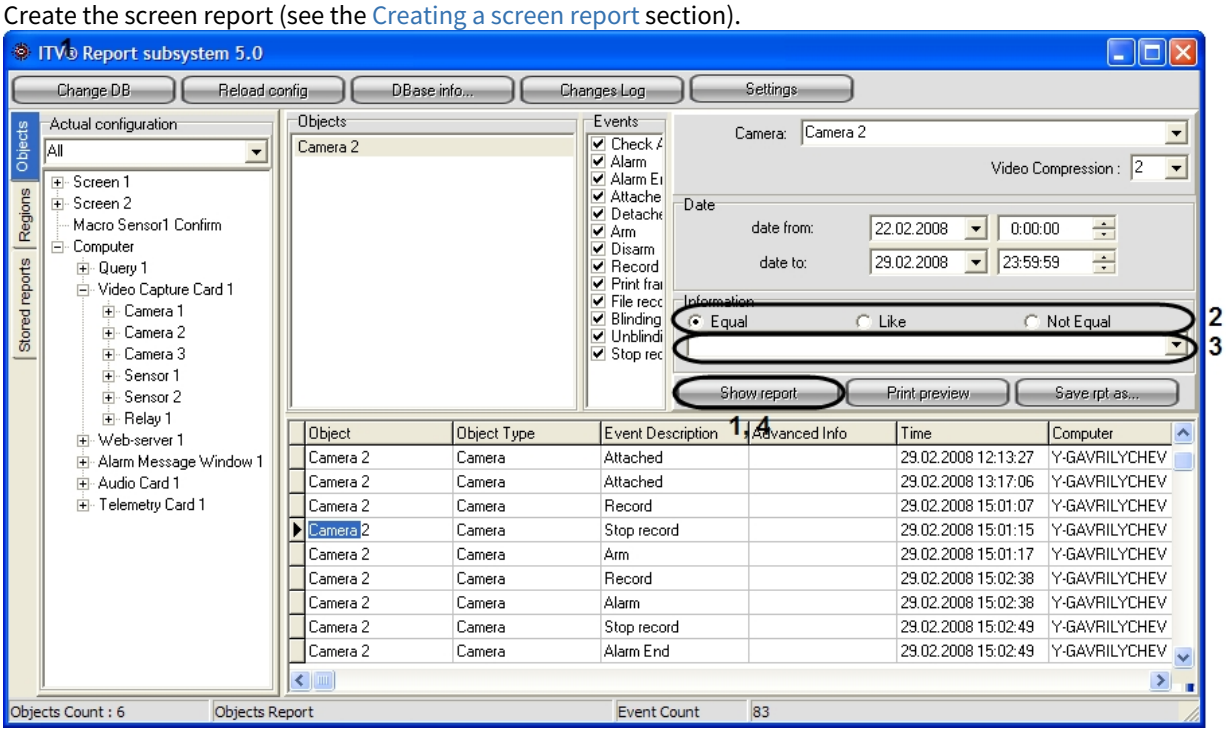
24.11 Filtering the events in the screen report according to the additional information

The Report system allows to show only the rows of the screen report containing particular additional information.

By default, the screen report contains all events that fit the report settings. To display only the rows that contain particular information, do the following:

> **Note.**
>
> The list is filtered by the **Advanced Info** column.

1. Create the screen report (see the Creating a screen report section).



2. Select the filtering method using the Information radio-buttons.

> **Note.**
>
> In case of first start of Web-report subsystem this panel unavailable for edit. Restart the Web-report subsystem

   a. **Equal** radio-button. When selected, the system looks for exact case-sensitive matches only, between the string in the Information field and the **Advanced Info** column.
   b. **Like** radio-button. When selected, the system looks for the rows where the **Advanced Info** column contains the search string, case-sensitive.
   c. **Not Equal** radio-button. When selected, the system looks for the exact case-sensitive matches, only between the string in the Information field and the **Advanced Info** column.
3. Enter the character string to filter the report by.
4. Click the **Show Report** button to run the filter.

Only the filtered rows will be displayed in the screen report.

24.12 The keyboard shortcuts list

The following keyboard shortcuts are available in the Report system:

1. All panels:
   a. F5 – creating the screen report.
   b. F6 – creating the printed report.
   c. Del – deleting an object from the **Objects** panel.

    d. Ctrl+A – selecting all objects in the list in the **Objects** panel.
2. **Objects** panel:
    a. Ctrl+F – searching the tree for an object by name or any part of the name.
    b. Enter – adding the selected object to the report.
3. The **Regions** panel:
    a. Ctrl+F – searching the tree for an object by name or any part of the name.
    b. Enter – adding the selected object to the report.
4. The **Shared Reports** panel
    a. Ctrl+Del - deleting the selected report template.

25 Administrator's Guide. Conclusion

More detailed information on the Intellect software package is presented in the documents titled:

1. Operator’s Guide.
2. The Script object. Programming using the JScript language.
3. Installing and configuring security system components guide.

If while operating the given software product you have faced difficulties and problems, you are welcome to contact us. However before addressing us, we kindly ask you to answer the following questions:

1. What is the problem?
2. When did the problem occur and what had happened before it occurred?
3. Which conditions gave rise to the problem?

Remember, that the more detailed and precise information you give us, the faster our experts will resolve your problem.

We are striving to improve the quality of our products, and hence welcome any proposals and suggestions how to improve our software and documentation.

26 Appendices

26.1 Appendix 1. Interface

General information about the System settings dialog box

26.1.1 Description of the Main control panel Interface

26.1.2 Description of the System settings dialog box

- Tabs panel
- Objects tree
- Context menu of the system object
  - The Create object function
  - The Change parameter function
  - The Camera discovery tool function
  - The Delete object function
  - The Create folder function
  - The Move to folder function
  - The Save function
  - The Find function
  - The Reconnect function
  - The Send key to all function
  - The Send key function
  - The Save configuration function
  - The Load configuration function
  - The Collapse tree function
  - The Expand tree function
- The object settings panel
- The Apply and Cancel buttons
- The elements of the System settings dialog box
- The Architecture tab
- The Hardware tab
  - The Hardware tab components
  - The Settings panel of the Computer object
  - The Settings panel of the Video capture device object
  - The Settings panel of the Camera object
  - The Settings panel of the Detection zone object
  - The Settings panel of the Audio card object
  - The Settings panel of the Microphone object
  - The Settings panel of the Telemetry Controller object
  - The Settings panel of the PTZ device object
  - The Settings panel of the Control panel object
  - The Settings panel of the Backup archive object
  - The Settings panel of the Keyboard object
  - The Settings panel of the System restart service object
  - The Settings panel of the Voice notification service object
  - The Settings panel of the Voice Message Service object
  - The Settings panel of the Voice message object
  - The Settings panel of the Short Message Service object
  - The Settings panel of the Short Message object
  - The Settings panel of the Mail Message Service object
  - The Settings panel of the Mail message object
  - The Settings panel of the Web-server object

    - The Settings panel of the RTSP Server object
    - The Settings panel of the Operator query panel object
    - The Settings panel of the Alarm Message Window object
    - The Settings panel of the Videogate object
    - The Settings panel of the Event counter object
    - The Settings panel of the Data replication service object
    - The Settings panel of the Failover service object
    - The Settings panel of the Backup audio archive object
    - The Settings panel of the Web-server 2.0 object
    - The Settings panel of the Edge storage object
    - The Settings panel of the PS-RTP server object
    - The Settings panel of the Manager of failover services object
    - The Settings panel of the ONVIF-Server object
    - The Settings panel of the ONVIF-Server Profile object
    - The Settings panel of the Telegram bot object
    - The Settings panel of the SIP-terminal object
    - The Settings panel of the SIP-device object
    - The Settings panel of the SIP-operator object
    - The Settings panel of the Address book object
    - The Settings panel of the Incident handler object
- The Interfaces tab
    - Interfaces tab components
    - The Settings panel of the Display object
    - The Settings panel of the Monitor object
    - The Settings panel of the Audio player object
    - The Settings panel of the Telemetry control panel object
    - The Settings panel of the Backup archive panel object
    - The Settings panel of the Map object
    - The Settings panel of the Layer object
    - The Settings panel of the Event viewer object
    - The Settings panel of the Operator protocol object
    - The Settings panel of the External window object
    - The Settings panel of the Scene object
    - The settings panel of the HTML Interface object
    - The settings panel of the HTML page object
    - The Settings panel of the Display manager object
    - The Settings panel of the State statistics object
    - The Settings panel of the Charts object
    - The Settings panel of the SIP-panel object
    - The Settings panel of the Incident manager object
- The Programming tab
    - The Settings panel of the Security zone object
    - The Settings panel of the Macro object
    - The Settings panel of the Program object
    - The Settings panel of the Time schedule object
    - The Settings panel of the Script object
    - The Settings panel of the Region object
    - The Settings panel of the Rule of states transition object
    - The Settings panel of the Macro event object
- The Users tab
    - The Users tab components
    - The Settings panel of the Department object
    - The Settings panel of the User object
    - The Settings panel of the User permissions object

26.1.3 Information about program

26.1.4 Description of the Main control panel Interface

As a part of the **System settings** interface window, the **Main control panel** has a fixed position and is located in the upper right corner of the **System settings** interface window.

> **Note**
>
> If the **Main control panel** is hidden, move the mouse cursor to the upper right corner of the screen to display it. By default, the **Main control panel** is displayed on the main monitor. The number of the monitor for displaying the **Main control panel** can also be set by the cur_monitor registry key (see Registry Keys Reference Guide).

Intellect **Main control panel** is small (for the purpose of saving the useful screen space) and contains only the information window and two buttons to the right of it.

Intellect **Main control panel** elements and their descriptions are given below:

1.

—**Information window** or help window. This window displays comments (brief information) to the interface elements on mouse hover, and the system error messages. If *Intellect* is running in demo mode, the text in the window says "Mode: Demo".
2. —The **Screens** button. The button is used to control virtual screens.
3. —The **Execute** button. The button is used to
   - display or hide the **System settings** interface window,
   - manually execute the macros,
   - open the system info window,
   - display or hide the **Debug window**,
   - shut down the system.

26.1.5 Description of the System settings dialog box

26.1.5.1 Tabs panel

The Tabs panel is located in the upper left corner of the **System settings** dialog box and is used for switching between the settings groups of different types of *Intellect* objects. The Tabs panel is shown in the figure.

The table below presents a list and a short description of the tabs of the **System settings** dialog box.

№	Section (tab) of the System settings dialog box	Features of the section (tab)
1	**Architecture**	The tab describes the system structure, the network settings of communication between computers and the parameters of events transmission between the computers of the distributed network
2	**Hardware**	The tab is used to connect and configure hardware and program modules. This tab is also used to connect and configure the special components of the Operator user interface—the **Operator query panel** and **Alarm message window** objects

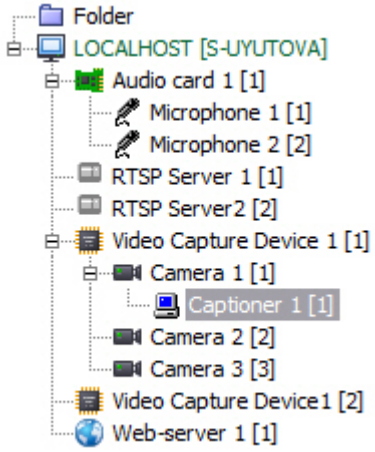
№	Section (tab) of the System settings dialog box	Features of the section (tab)
3	**Interfaces**	The tab is used to create and configure virtual screens and components of the Operator user interface—Video surveillance monitors, audio players and control panels of various devices and modules
4	**Users**	The tab is used to create user accounts (registration) of the digital video surveillance and audio monitoring system, classify the levels (rights) of their access to the system resources and assign passwords to the users
5	**Programming**	This tab is used to create macros and scripts, as well as to create time schedules, shift schedules, subdivision areas of the protected facility, access levels for the access points, which are equipped with readers

To switch from one tab to another, use the mouse. To do this, do the following:

1. Hover the mouse cursor over the tab.
2. Click the left mouse button.

26.1.5.2 Objects tree

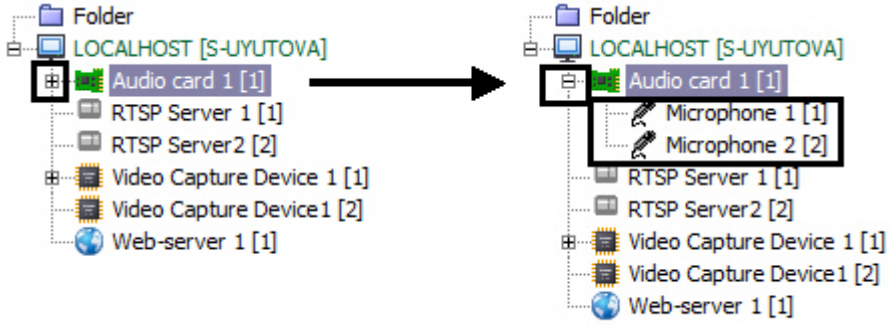
The system is based on the tree-like structure of the objects arrangement (objects tree). The objects tree is a multi-level nested list of objects.



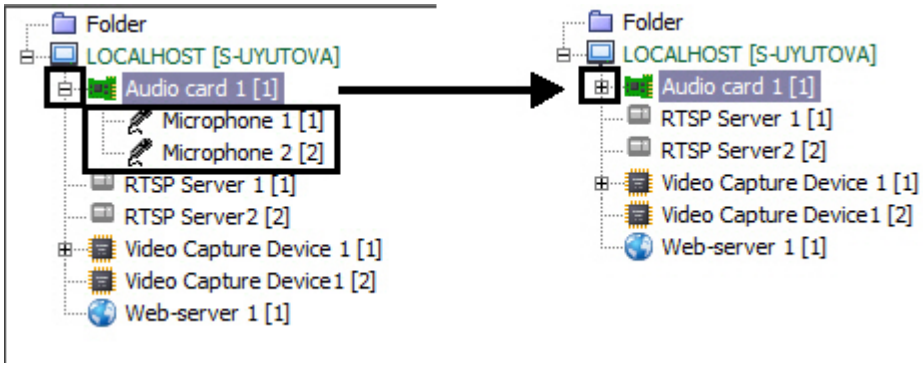
The objects structure is hierarchical. The low-order (child) objects can only be created on the basis of the higher-order (parent) object. The objects in the tree are sorted by name in the following order: Cyrillic characters, spaces, symbols, numbers, Latin characters. If folders are created in the objects tree (see The Create folder function), then the folders are located in the tree above the objects at the corresponding hierarchy level and are sorted in the same order.

The objects tree can be expanded. You can open and view the contents of all its groups (branches), collapse it, hiding the objects not required to be seen at the moment.

To get to a lower level and see the list of the child objects, click the left mouse button hovering over the **+** icon to the left of the parent object.

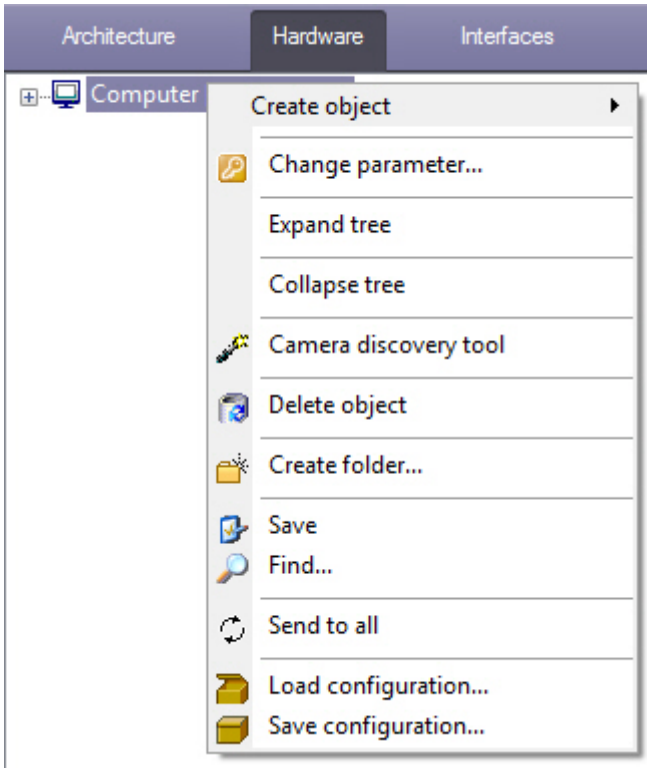


To collapse the branch of the objects tree with the child objects, click the left mouse button hovering over the - icon.



26.1.5.3 Context menu of the system object

The context menu of the system object is available when working with the objects tree. To display the menu, click the right mouse button, hovering over the name of the system object in the objects tree.



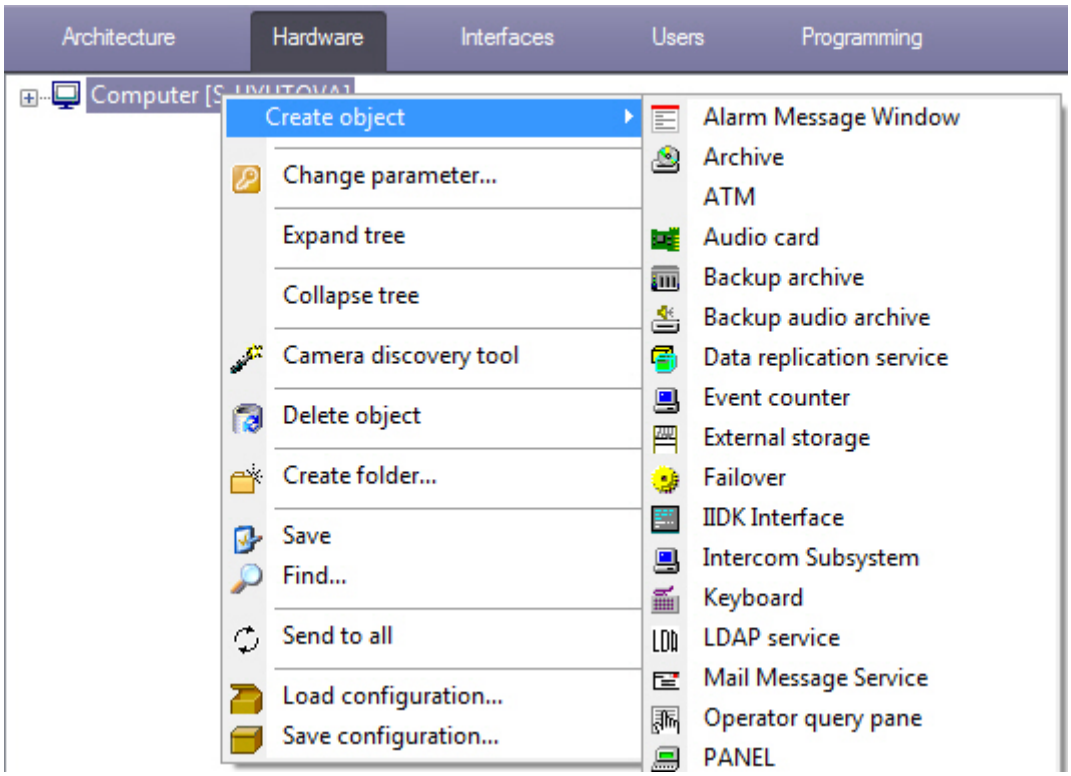
The number of the menu items varies depends on the video surveillance system complexity and object tasks. The context menu items of a system object are described below.

Note

If the Settings panel of any object is open (see Object Setting Panel), and you right-click on an empty space in the objects tree area, this panel will close and the context menu will open, and the object will be deselected in the objects tree.

26.1.5.3.1 The Create object function

The **Create object** function is used to create a new system object in the objects tree in the **Hardware** tab. The function is selected from the context menu of the parent system object.

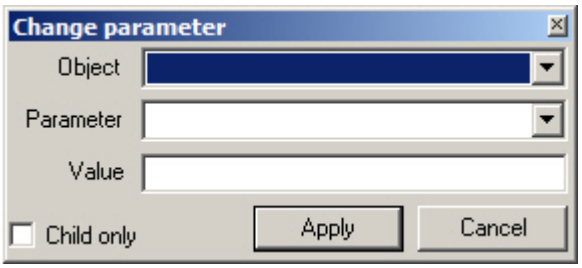


When you select the **Create object** menu item, the submenu will open with a list of the system objects. The figure shows a list of some objects that can be created on the basis of the **Computer** object.

26.1.5.3.2 The Change parameter function

The **Change parameter** function is used to group edit the parameter values of *Intellect* objects in the database. To use this function, you should know the *Intellect* database structure. This function isn't recommended to be used by beginning users.

When you select the **Change parameter** function in the context menu of the system object, the **Change parameter** dialog box will open.



From the **Object** drop-down list, select the type of the system objects, the parameter of which should be edited. This list contains only the objects that are the child objects to the object whose context menu was used to display the dialog box. To edit the parameters of the **Computer** object, select the **Change parameter** item in the context menu that opens when you right-click the area with no objects of *Intellect* objects tree.

From the **Parameter** drop-down list, select the name of the object parameter that should be changed in the *Intellect* database.

> **Attention!**
>
> The parameter will be changed for all objects of the selected type in the distributed configuration.

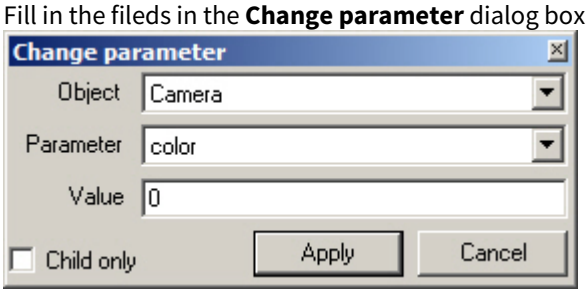
In the **Value** field, specify a new value of the parameter in the format in which it will be saved in the database. You can find out the data type of the parameter using the ddi.exe utility (see Editing intellect.dbi and intellect.ext.dbi database templates using the ddi.exe utility). You can find out the format of the parameter when viewing the *Intellect* database (see Viewing the Intellect database).

If you need to edit the parameter only of the child objects relative to the object selected in the tree, set the **Child only** checkbox. For example, this checkbox allows editing the parameter only on the computer selected in the tree.

Example. All cameras in the system should display a black-and-white video image.

For this, do the following:

1. Open the **Change parameter** dialog box from the context menu of the **Video capture device** or **Camera** object.
2. Fill in the fileds in the **Change parameter** dialog box as shown in the figure.



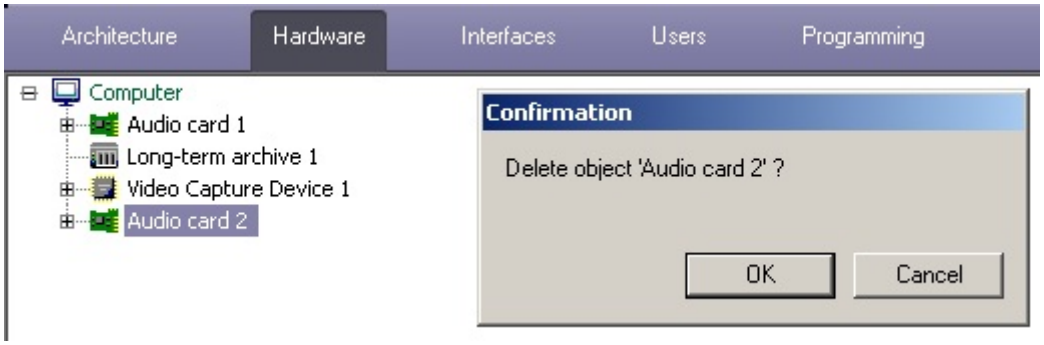
3. Click the **Apply** button.

26.1.5.3.3 The Camera discovery tool function

When you select the **Camera discovery tool** function in the context menu of the **Computer** system object, the *Camera discovery tool* utility starts. Its operation is described in Camera discovery tool.

26.1.5.3.4 The Delete object function

To delete an object from the tree, hover the mouse cursor over the object and open the context menu. Select the **Delete object** menu item. A dialog box asking you to confirm the deletion of the system object will open.



To confirm the object deletion, click the **OK** button. To cancel the deletion, click the **Cancel** button. As soon as deletion is confirmed, the system object, as well as all its child objects, will be deleted.

The delete system object function applies to all objects, including the **Computer** object, created by default when *Intellect* is installed.

> **Note**
>
> Note that after deleting a parent object, like the **Computer** object corresponding to the local computer, it will be difficult to restore it. That is why it isn't recommended deleting objects such as **Computer** created by *Intellect*.

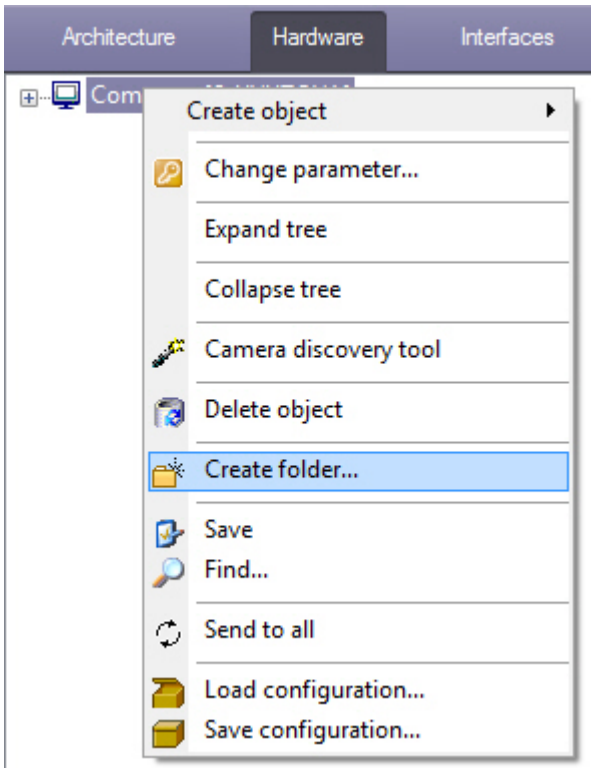
26.1.5.3.5 The Create folder function

The create folder function is used to arrange the display of the system objects in the objects tree when there are many objects of different types. The objects are grouped into folders arbitrarily. The function is available on all tabs of the **System settings** dialog box except for the **Architecture** tab.

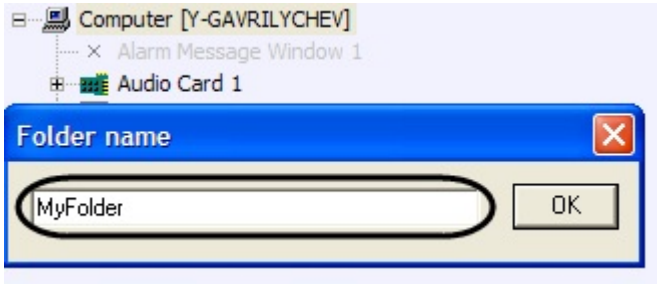
To create a folder, open the context menu of an object or a folder and select the **Create folder** item.

Note

A folder can be created on the basis of the object that has child objects or on the basis of other folder. For example, you can create a folder on the basis of the **Computer** or **Video capture device** object, but you cannot create a folder on the basis of the **Captioner** or **Detection zone** object.

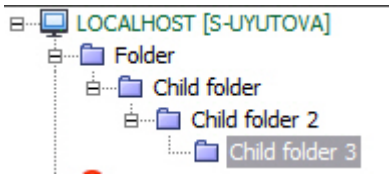


The **Folder name** dialog box for entering a folder name will open. Enter the folder name in the dialog box, click the **OK** button.



A folder will be created in the objects tree on the basis of the selected object.

To create a folder nested in another folder, select the **Create folder** item in the function menu that opens by right-clicking a previously created folder.

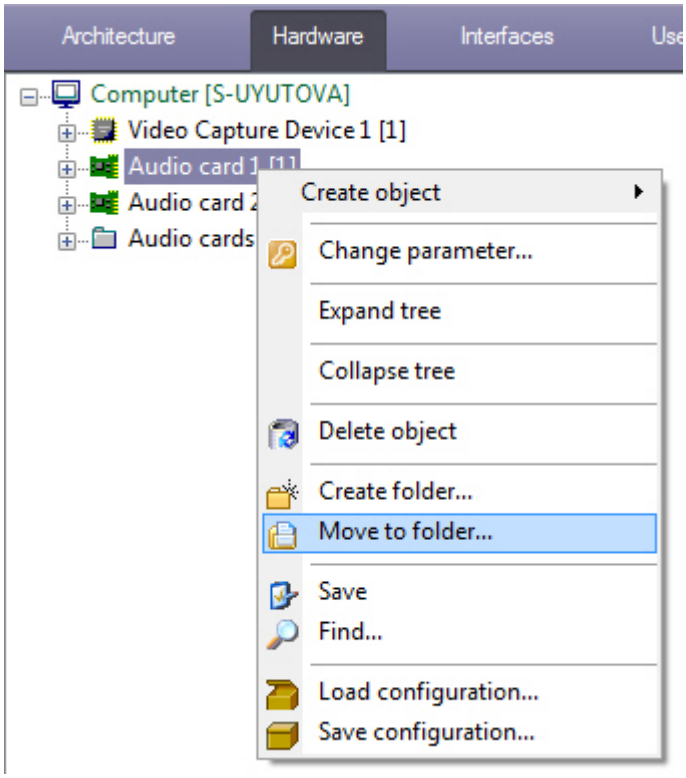


26.1.5.3.6 The Move to folder function

This function allows moving system objects to the objects tree folder.

> **Attention!**
>
> When working in a distributed system, objects are grouped into folders individually on each Server/RAW and aren't displayed on other Servers/RAWs. The folders synchronize between Servers/RAWs.
> To synchronize the contents of folders on all Servers/RAWs, set up database synchronization.

To move objects to the folder, select the object that you want to move, open the context menu and select the **Move to folder** item.



A window will open for selecting a folder, where you want move the selected system object.

To confirm the selected folder, click the **OK** button. The object will be moved to this folder.

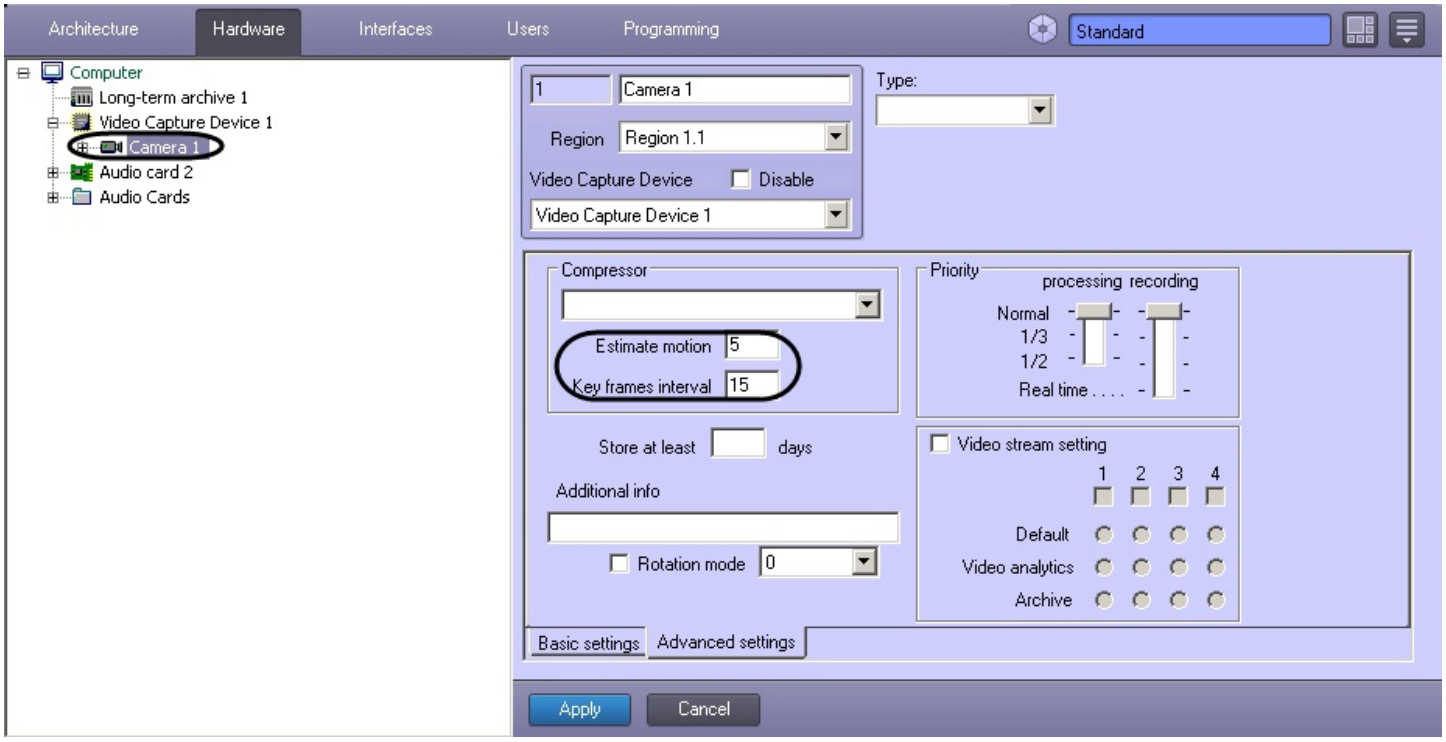
26.1.5.3.7 The Save function

Intellect allows creating objects based on a template. A template is created using the **Save** function accessible in the main function menu.

> **Note**
>
> Objects can also be copied and pasted using the Ctrl+C and Ctrl+V key combinations (see **Copy objects** in Setting procedure for system objects). If you use Ctrl+C and Ctrl+Shift+V, the object will be pasted together with its child objects.
> Once copied, object can be pasted multiple times. The copied object will be stored in the clipboard until *Intellect* restart, or until the clipboard clipping is replaced with a new copied object.

Below you can see how to create the **Camera** object by a template using the **Save** function.

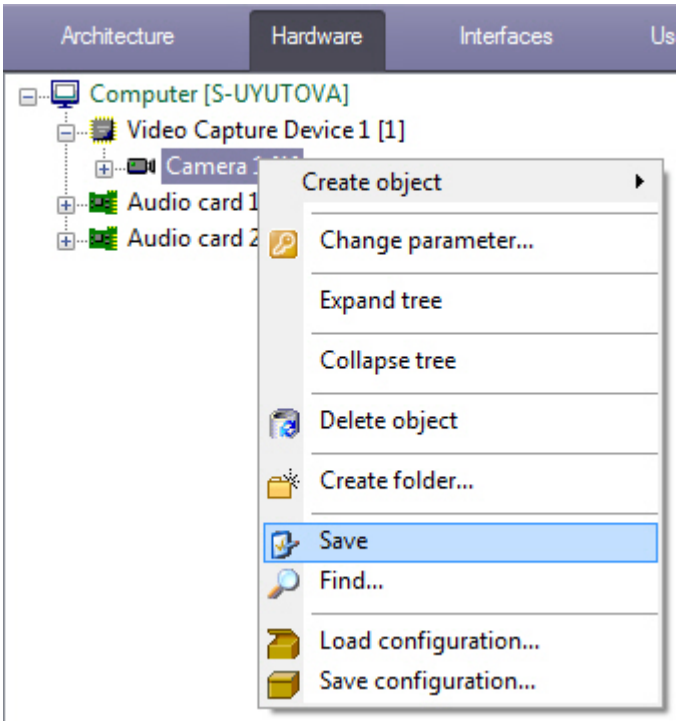
First of all, select an object that has already been created and configured, for example, the **Camera 1** object. The figure displays a settings panel with the highlighted parameters of the **Camera 1** object that were edited (differ from the default settings).



To create a template based on this object, do the following:

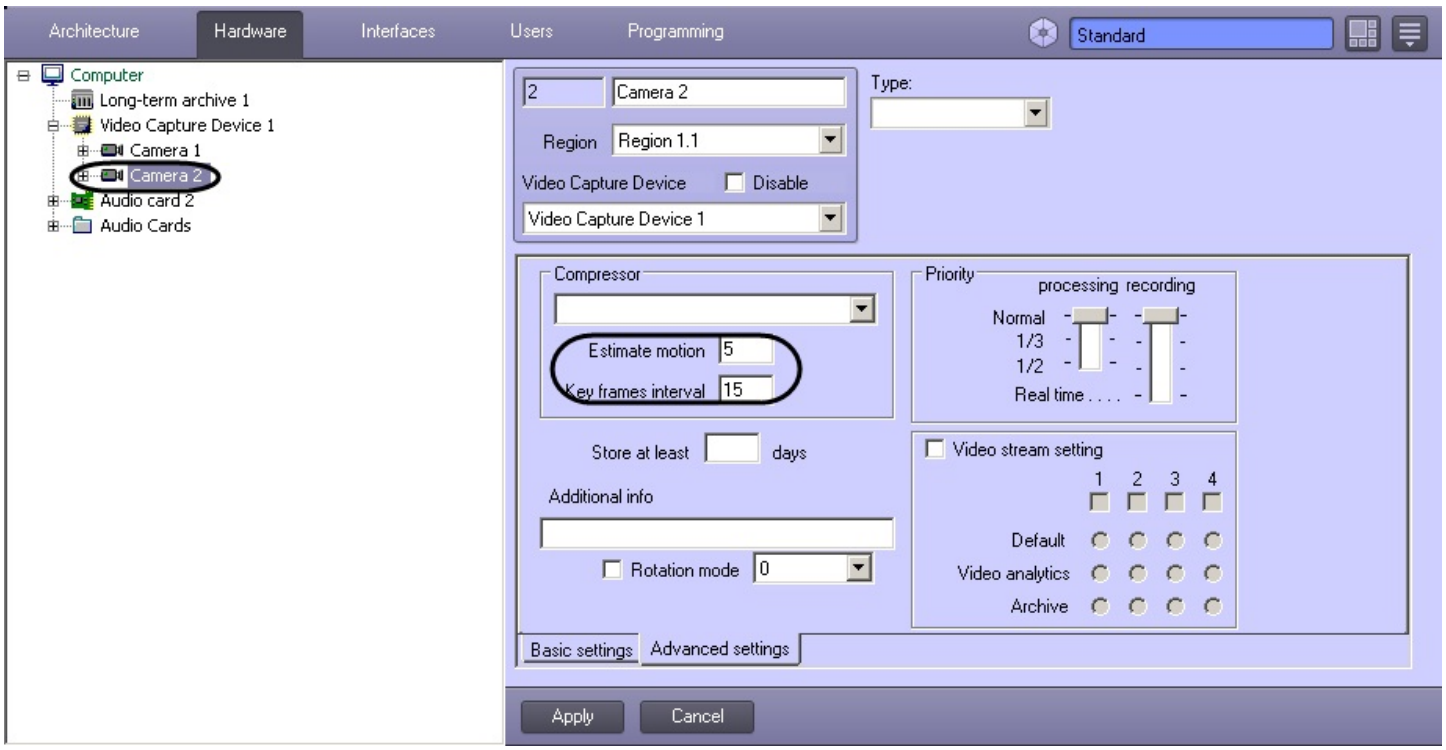
1. Open the context menu of the **Camera 1** object.

2. Select the **Save** menu item.



As a result, the template of the **Camera** object with the settings of the **Camera 1** object will be created.

Now it is necessary create the **Camera 2** object based on the **Video Capture Device 1** object (see The Create object function). By default, the newly created **Camera 2** object will have the same settings as the **Camera 1** object.

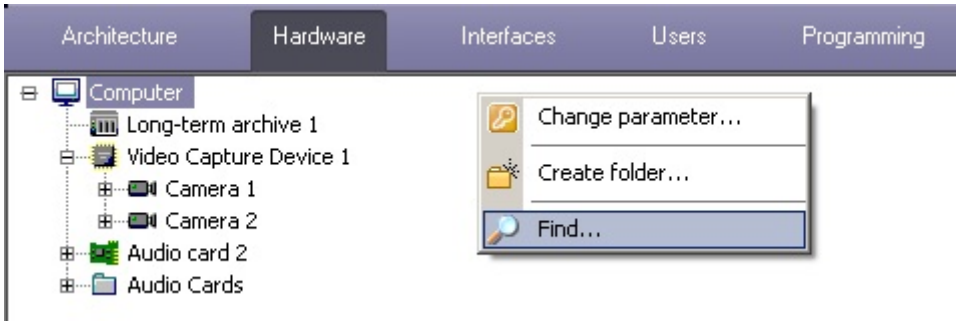


The created object template is preserved until the clipboard is cleared (for example, when you restart *Intellect*) or replaced with new content. Thus, if you continue to create the **Camera** objects, they will have the settings of the **Camera 1** object as long as the clipboard contains the saved template.

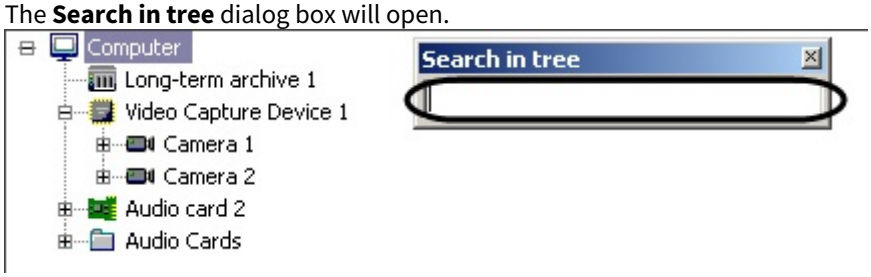
26.1.5.3.8 The Find function

The **Find** item of the menu is used to search for an object in the tree. *Intellect* has two methods of searching for an object:

1. Searching within a tree. This method is used when only an object name (type) is known. To find an object, do the following:
   a. Open the context menu of the objects tree.
   b. Select **Find** in the menu.



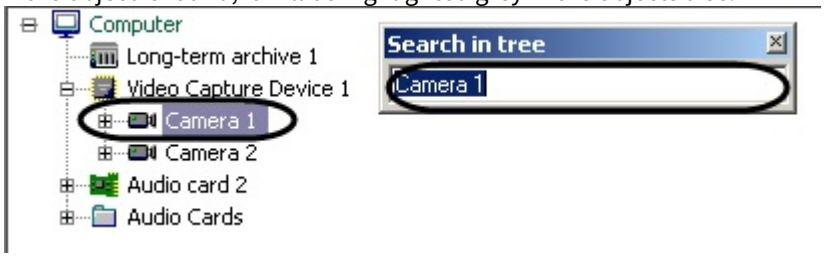
The **Search in tree** dialog box will open.



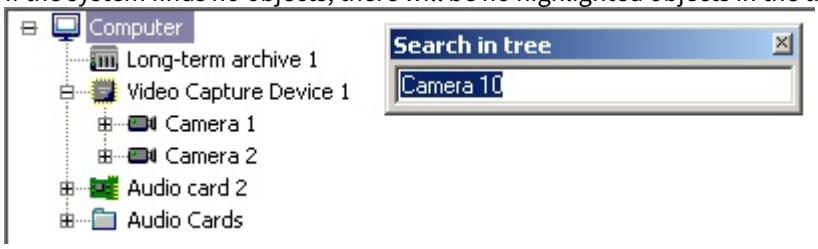
> **Note**
>
> It is also possible to open this window using the Ctrl+F key combination.

   c. Enter the name of the required object.

   d. Press **Enter** on the keyboard to start searching.
   If the object is found, it will be highlighted grey in the objects tree.



   If the system finds no objects, there will be no highlighted objects in the tree.

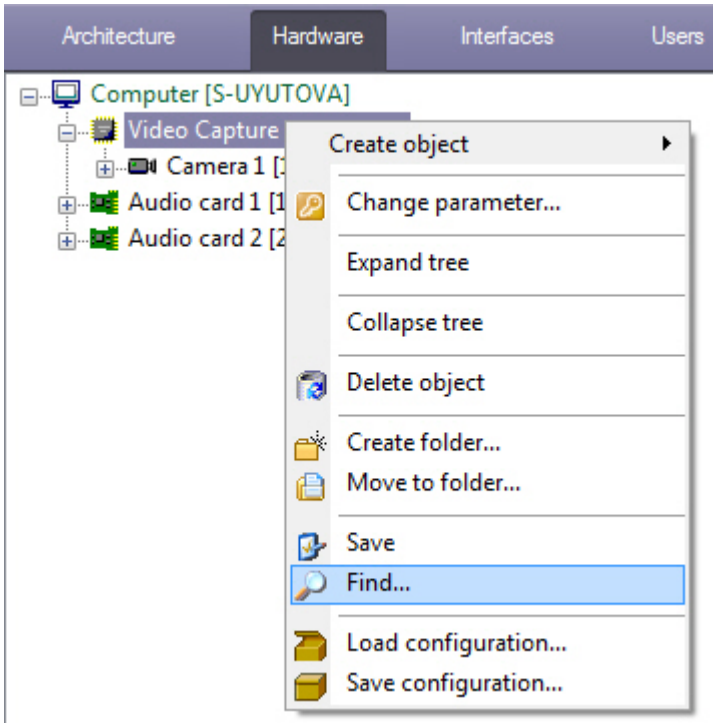


To close the window for entering the object name, when the search is complete, click the left mouse button, hovering over the window field displaying the objects tree.

2. Search from a selected object.
   To find an object, whose location in the objects tree is known approximately, do the following:
   a. Select an object in the tree, below which you want to search.

> **Note**
>
> To search for an object in the tree, it is better to select an object that is a child to the **Computer** object. Otherwise, the search will be performed down the branch of the selected object.

   b. Open the context menu of the objects tree.
   c. Select **Find** in the menu.

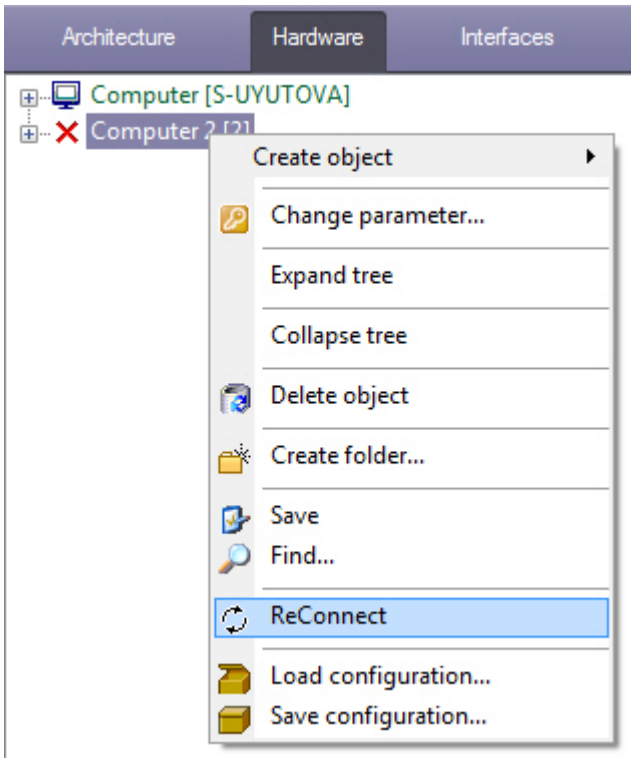


Then perform the search in the order described in the method 1.

26.1.5.3.9 The Reconnect function

This menu item appears if besides the object corresponding to the base computer, there is at least one (additional) **Computer** object ready to connect to the base computer, but the connection isn't established for some reason.

To establish a connection between two **Computer** objects, open the context menu of the additional **Computer** object ready for connection, and select the **Reconnect** menu item.

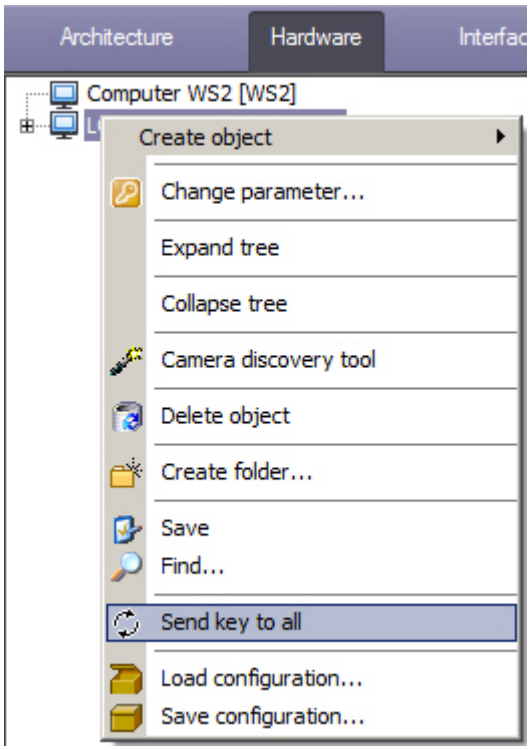


As a result, the objects of the base computer will connect to the objects of the remote computer over the network.

26.1.5.3.10 The Send key to all function

This function allows you to send the *intellect.sec* activation key that regulates the system configuration to all computers that are part of the distributed digital video surveillance and audio control system. If the system functionality was updated and a new activation key was received, you need to update it on all computers that are part of the system, using the **Send key to all** function.

This function is available only from the context menu of the **Computer** object, corresponding to the local computer that performs the administrator functions.



Note

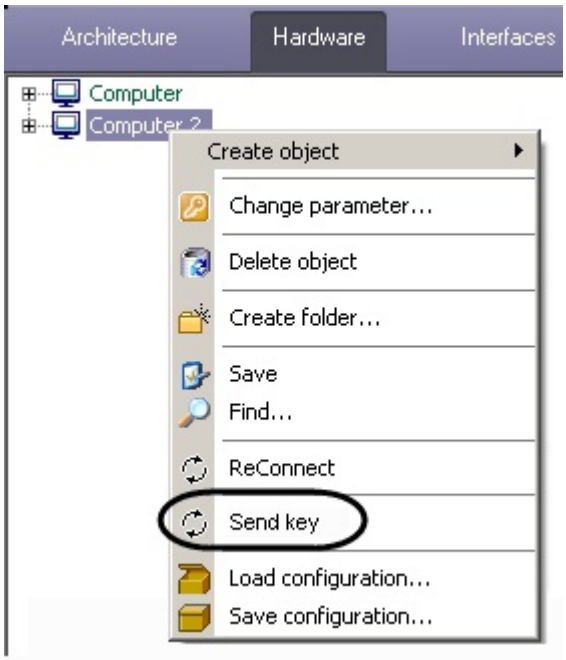
If an updated activation key isn't sent to all computers in the system in time, *Intellect* won't start after the restart, because when the activation key data is read, there will be discrepancies with the information contained in the database.

If the key is successfully applied on a particular computer in the distributed system, the "Key updated" message will be displayed in the Event Viewer. However, if the key has expired or the number of the objects in the key is less than the number of the objects created in the objects tree on the corresponding computer, then this information won't be displayed in the Event Viewer, but an error will occur the next time *Intellect* starts. See also Features of the Intellect software operation when the object limit is exceeded and What should I do if I'm getting the 'key file expired' error when running?

If the activation key cannot be applied on any computer because of the HID codes mismatch, the message "Key rejected (HID incompliance)" will be displayed in the Event Viewer. See also What should I do if I'm getting the 'Key file is not corresponding cards' error when running?

26.1.5.3.11 The Send key function

This function allows you to update the activation key on the remote computer that is a part of the system. The function is available only from the main function menu of the object, such as **Computer**, corresponding to the remote computer.



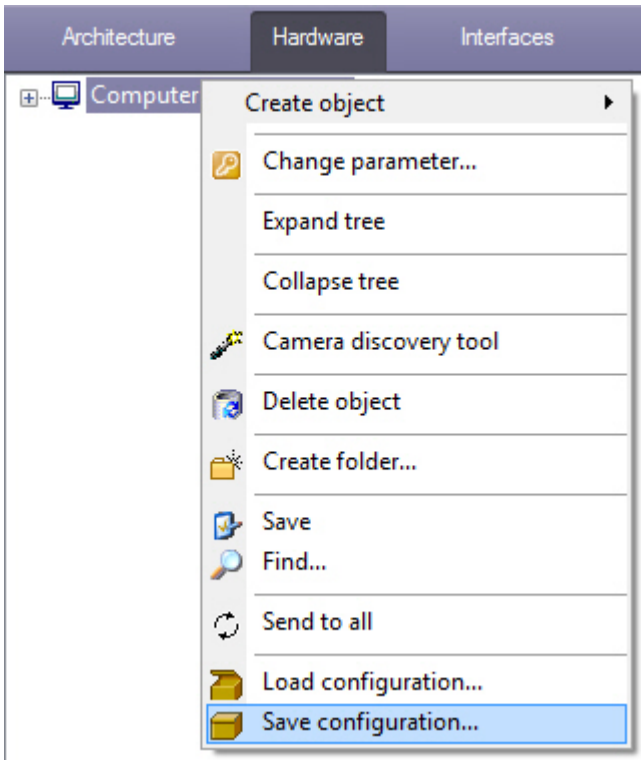
Note

If an updated activation key isn't sent to this computer in time, *Intellect* won't start after the restart, because when the activation key data is read, there will be discrepancies with the information contained in the database.

The Send key to all function

26.1.5.3.12 The Save configuration function

The **Save configuration** function allows you to save the current configuration parameters of an object to a file with the .cfg extension, so that these parameters can be used to configure other objects or to restore the configuration parameters of the current object after unexpected loss (for example, if an object is accidentally deleted).

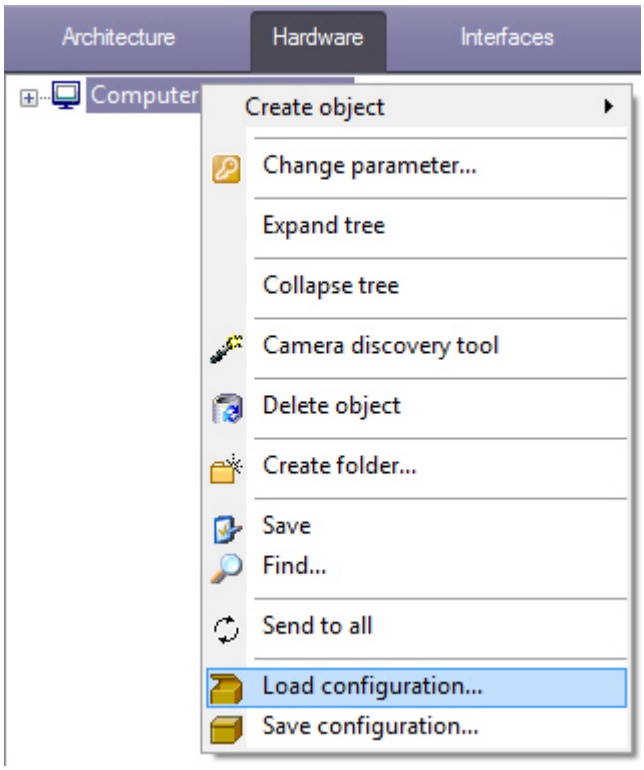


After you select the **Save configuration** menu item, the standard Windows dialog box appears, in which you can specify the name of the configuration file and where you want to save it. By default, the file name includes the name of the object type and its number, for example **CAM.1.cfg** or **GRABBER.3.cfg**.

The saved configuration can be applied to any object of the same type that was used to create the configuration file. To do so, use the **Load configuration** function (see The Load configuration function).

26.1.5.3.13 The Load configuration function

The **Load configuration** function allows you to load the configuration parameters from a file with the .cfg extension that was created using the **Save configuration** function (see Save configuration function). The configuration parameters can be applied only to the objects of the same type as an object used to create the configuration file.



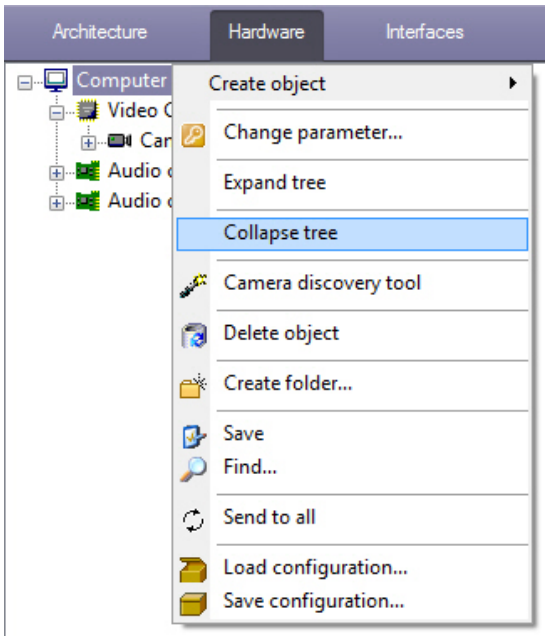
After you select the **Load configuration** menu item, a standard Windows dialog box appears, in which you can specify the necessary configuration file.

Note

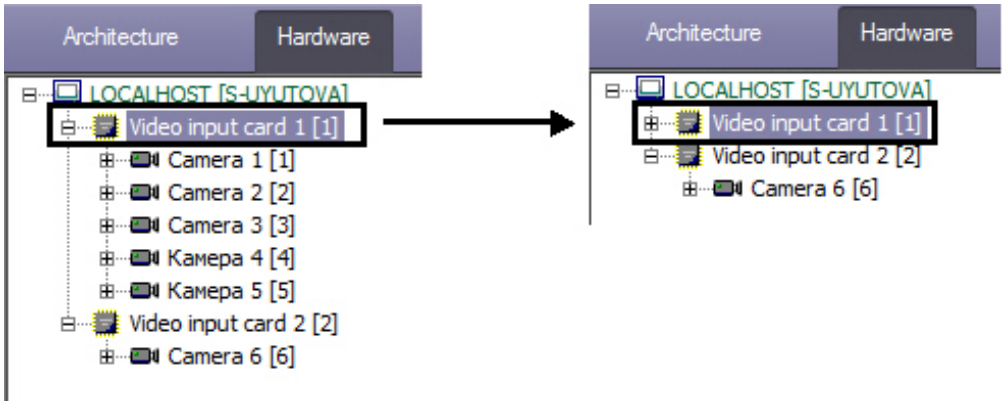
Some configuration parameters that are unique for the objects of the given type may not be applied when the configuration is loaded.
For example, the **PCI channel** parameter of the **Video Capture Device** object won't be changed according to the configuration file if there is already a **Video Capture Device** object in the objects tree that has the same **PCI channel** parameter value. For more information on allocation of the PCI channels between the **Video Capture Device** objects, see Creating and configuring the Video Capture Device object in the Installing and configuring security system components guide.

26.1.5.3.14 The Collapse tree function

The **Collapse tree** function allows you to collapse the objects tree (see Objects tree).



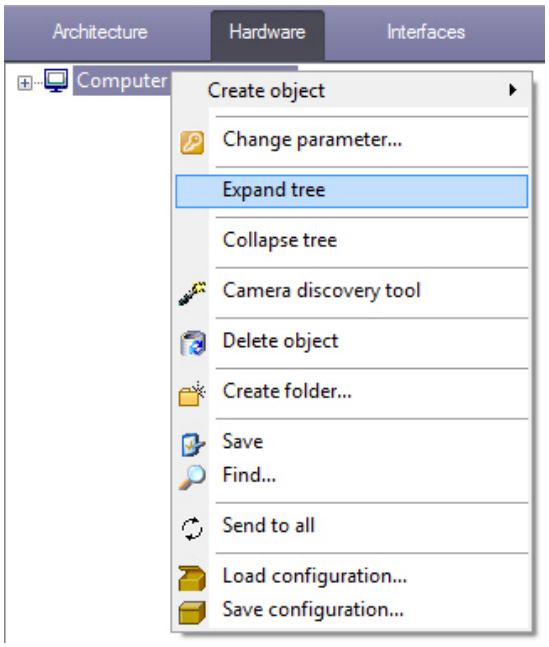
When you use this function, only the branch of the tree under the object from the function menu of which the function was called will collapse.



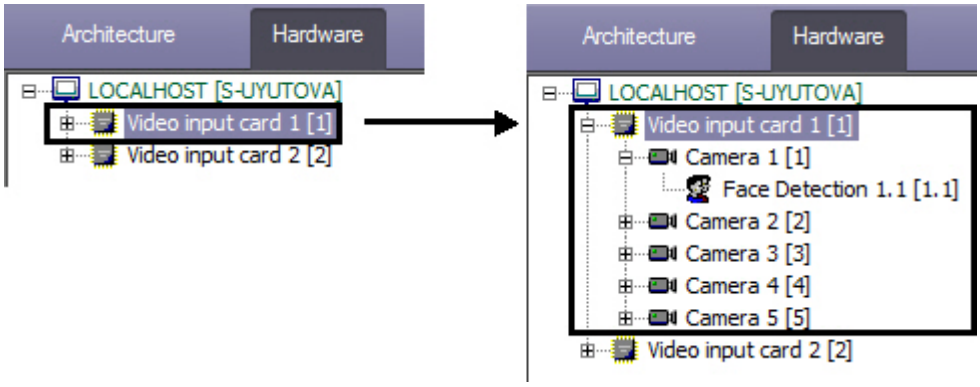
To collapse all branches of the objects tree, select the **Collapse tree** menu item holding down the Shift key.

26.1.5.3.15 The Expand tree function

The **Expand tree** function allows you to expand the branches of the objects tree (see Objects tree).



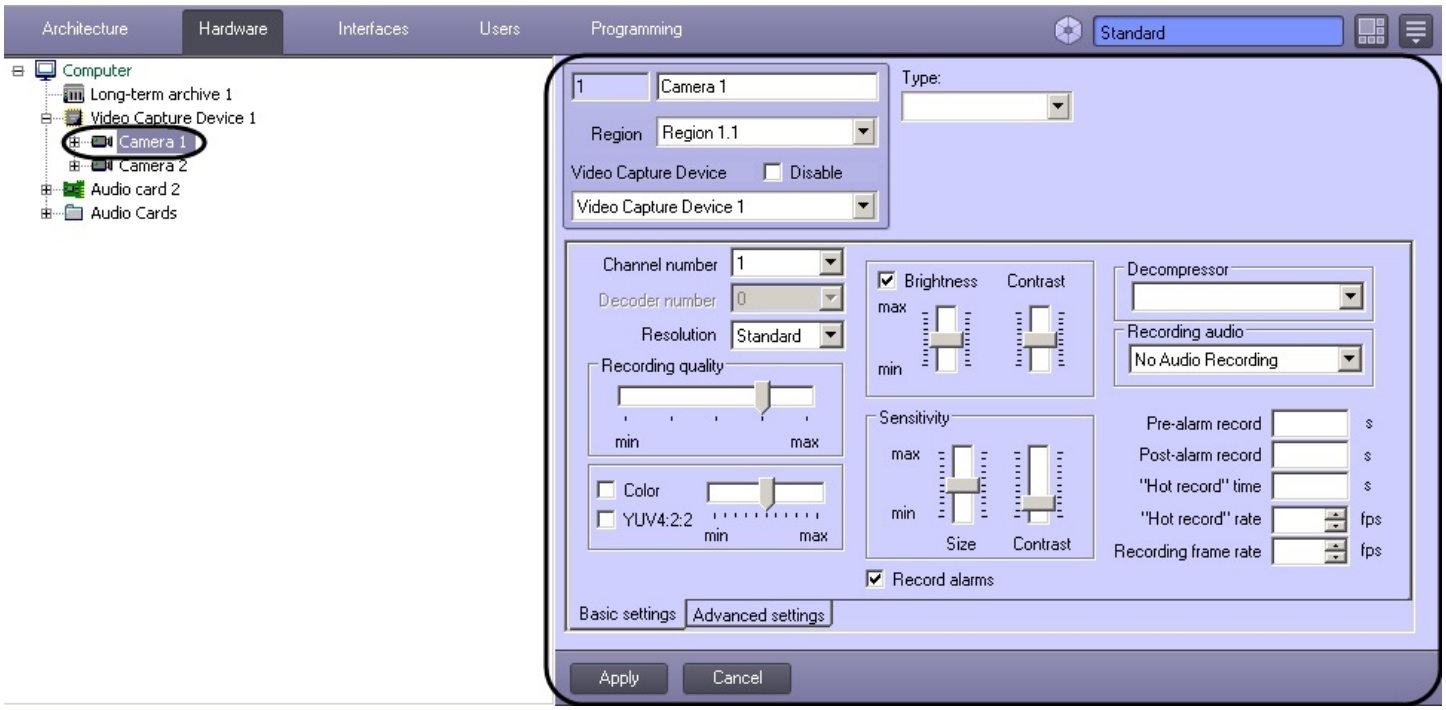
When you use this function, only the branch of the tree under the object from the function menu of which the function was called will expand.



To expand all branches of the objects tree, select the **Expand tree** menu item holding down the Shift key.

26.1.5.4 The object settings panel

The settings panel of the system object is located on the right side of the **System settings** dialog box and is used to activate and configure the object selected in the tree.

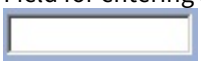


Depending on the type of the selected object, the settings panel of this object displays the necessary fields for entering the parameter values — the elements of the settings panel.

The elements of the settings panel are described below:

1. Field for entering a numerical value of the parameter

2. Field for entering a string value of the parameter



3. Checkbox

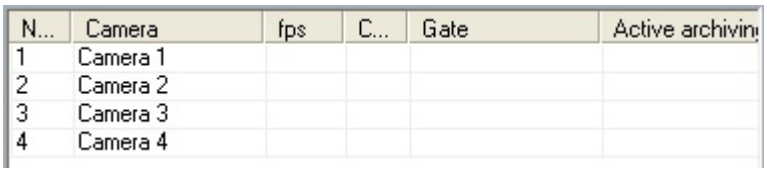
4. Radio button

5. Slider

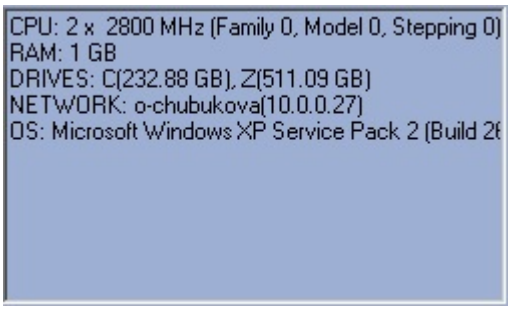
6. Drop-down list

7. Information table

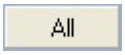
8. Table



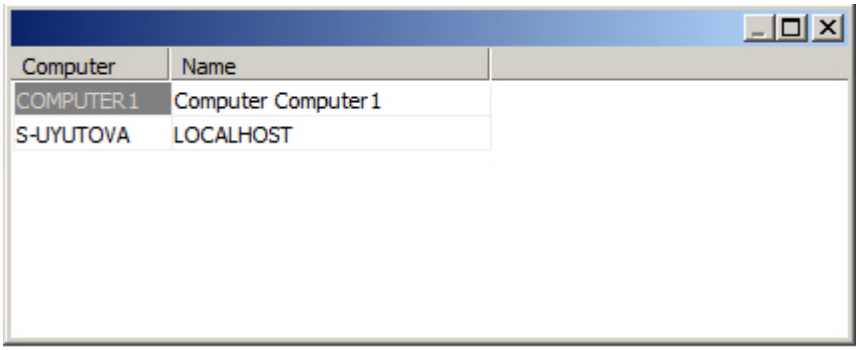
9. Information field



10. Button



11. Extended information table



Element name	Options for using the element
Field for entering a numerical value of the parameter	Enter a numerical value of the parameter. Place the mouse cursor in the field, click the left mouse button and enter the required number from the keyboard

Element name	Options for using the element
Field for entering a string value of the parameter	Enter a string value of the parameter. Place the mouse cursor in the field and enter the required number from the keyboard
Checkbox	Set/clear the checkbox. Set the checkmark in the field and clear the field by clicking it with the left mouse button
Radio button	Set the radio button to the required position. To set the radio button, click the required field with the left mouse button. Other fields get cleared automatically
Slider	Set the slider to the required position. Drag the slider cursor along the scale with the mouse
Drop-down list	Select an item from the drop-down list. The list opens when you click the **down arrow** button located on the right side of the element and looking like a triangle. To select from the list, click the required item with the left mouse button
Information table	This table has automatically filled fields. Working with the table means activating the lines (columns) using the checkbox on the left side of the table. Text fields cannot be edited. The number of lines cannot be edited. *Note. The table for selecting the hard disk for the archive storage is an exception. You can add new lines to this table when configuring recording to network disks.* When you right-click any area of the information table, a separate extended window with this information table opens (see item 11 above). This window is intended to improve the process of working with small tables. In order to set all checkboxes in the column of the information table, select a cell in this column and press Ctrl+A. In order to clear all checkboxes in the column, select a cell and press Shift +A
Table	To enter data, do the following: 1. Place the cursor in the table cell 2. Enter/select the required values in the fields/from the list in the column lines of the table. As you move to the next cell, the entered parameter values are saved in the table 3. To add new lines to the table, select any field of the filled line and press the down arrow button on the keyboard 4. To delete a line from the table, press the Ctrl+Delete key combination
Information field	The field displays information messages. It cannot be edited
Button	It starts the function corresponding to this button. To click the button with the mouse, hover the mouse cursor over the button and click the left mouse button
Extended information table	See Information table

26.1.5.5 The Apply and Cancel buttons

The **Apply** and **Cancel** buttons are located at the bottom of the **System settings** dialog box and are used to confirm or cancel the entered parameter values of the object settings.

The **Apply** button is used to save the set object identification and setting parameters. The **Cancel** button is used to return to the previous values of the object identification and setting parameters.

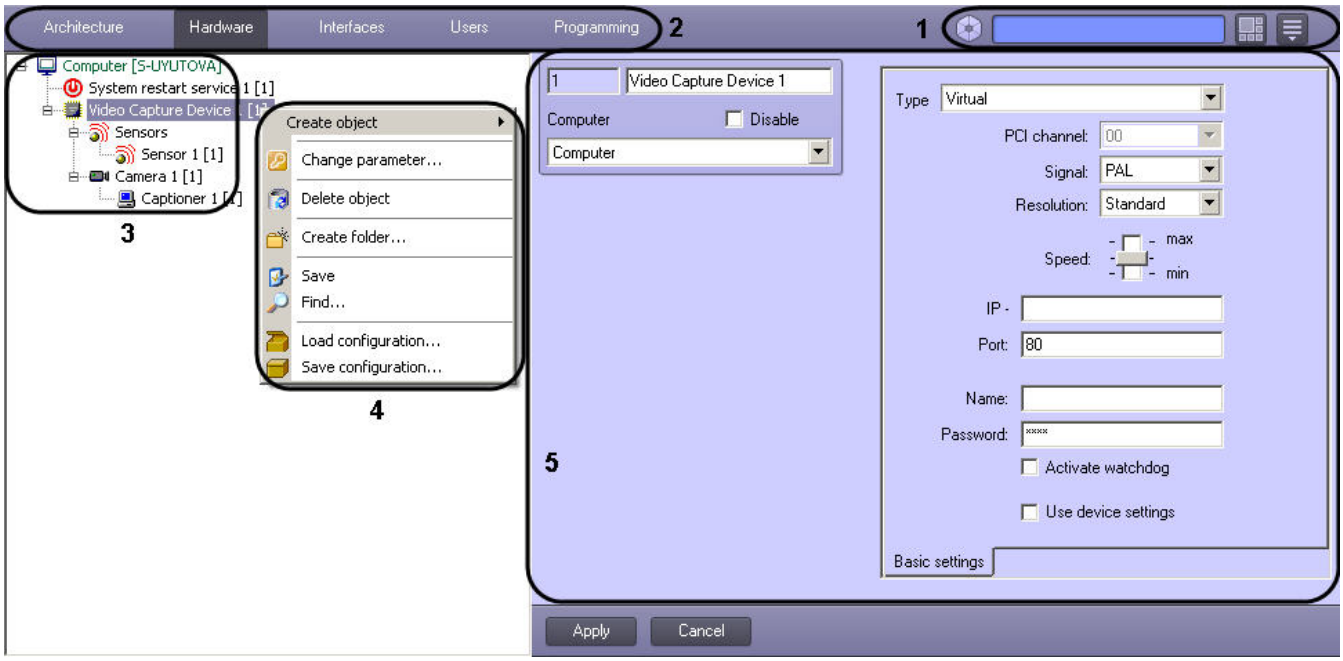
Note

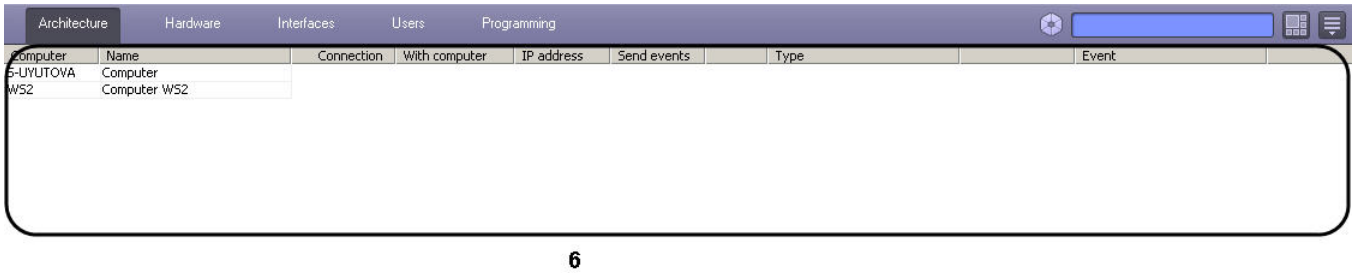
After you click the **Apply** button, you cannot cancel the actions with the **Cancel** button.

26.1.5.6 The elements of the System settings dialog box

The interface of the **System settings** dialog box consists of the following elements:

1. Main control panel.
2. Tabs panel.
3. Objects tree.
4. Context menu.
5. Objects settings panel.
6. Connection settings table.
7. The **Apply** and **Cancel** buttons.





The **System settings** dialog box contains the following tabs:

1. **Architecture**.

2. **Hardware**.
3. **Interfaces**.
4. **Users**.
5. **Programming**.

These tabs are used while creating and configuring the digital video surveillance and audio control system.

26.1.5.7 The Architecture tab

The **Architecture** tab allows you to create a distributed video surveillance and audio control system and is used to configure connection parameters and data exchange between the system components.

26.1.5.7.1 Connection settings table

The Connection settings table can be accessed from the **Architecture** tab. This table is used to configure connection between computers in the distributed system and distribute the information about the events registered in the system. The connection settings table is shown in the figure.

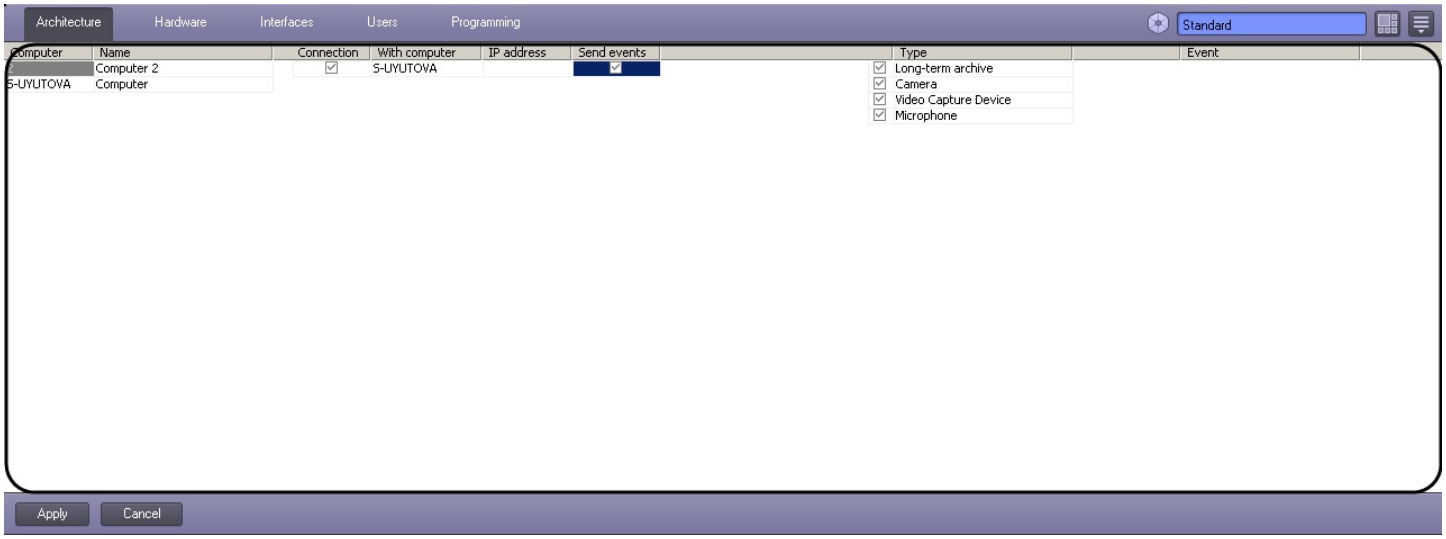


Table describes the elements of the connection settings table.

№	Column	Description	Value
1	**Computer**	Network name of the computer	Defined by the OS
2	**Name**	Computer name in the system	Set in the **Hardware** settings tab
3	**Connection**	Checkbox	If the checkbox is set—the computer is connected If the checkbox is clear—connection wasn't established
4	**With computer**	List of names of the network computers	Defined by the OS
5	**IP-address**	IP-address of the computer in the local network (if connected via the Internet, then public IP-address)	Defined by the OS or assigned manually. When the IP-address of the Server/RAW is edited, the IP-address for the current Server/RAW only is changed. For other Servers/ RAWs the IP-addresses should be changed individually. If the entered address is already assigned to a computer in the system, the address will be assigned to the computer being configured, and the corresponding warning message will be displayed. The address of the computer that previously had this address will be reset

№	Column	Description	Value
6	**Send events**	Checkbox	If the checkbox is set—there is a permission to send events to the computer it is connected to If the checkbox is clear—there is no permission to send events
7	**Type**	List of the system objects, from which the events will be transmitted to the selected computers	Defined by the list of the registered objects
8	**Event**	Checkbox in the list next to each item in the event list, corresponding to the device selected in the **Type** column	If the checkbox is set—this event will be transmitted If the checkbox is clear—this event won't be transmitted

26.1.5.8 The Hardware tab

The **Hardware** tab is used to create and configure the system objects corresponding to different types of hardware, used as components of the video surveillance and audio control system being created.

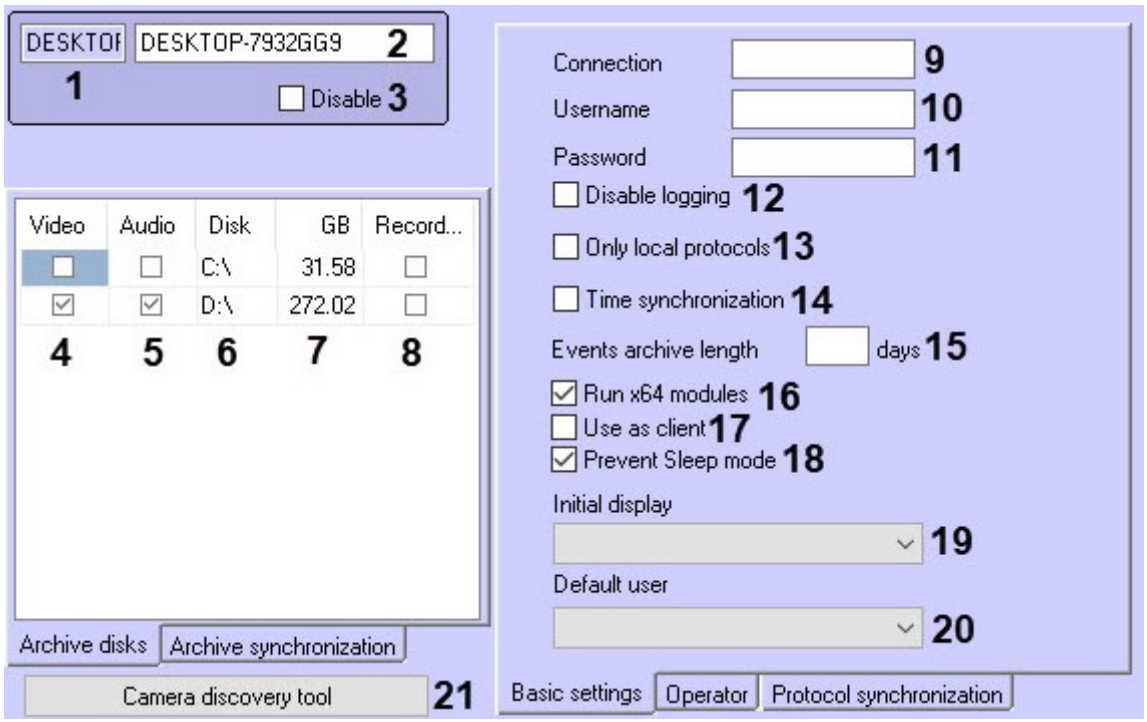
26.1.5.8.1 The Hardware tab components

The **Hardware** tab displays the tree of the system objects belonging to the Hardware group, and the settings panel of the object selected in the tree. The settings panels of each object used in the video surveillance and audio control system are described in the following sections.

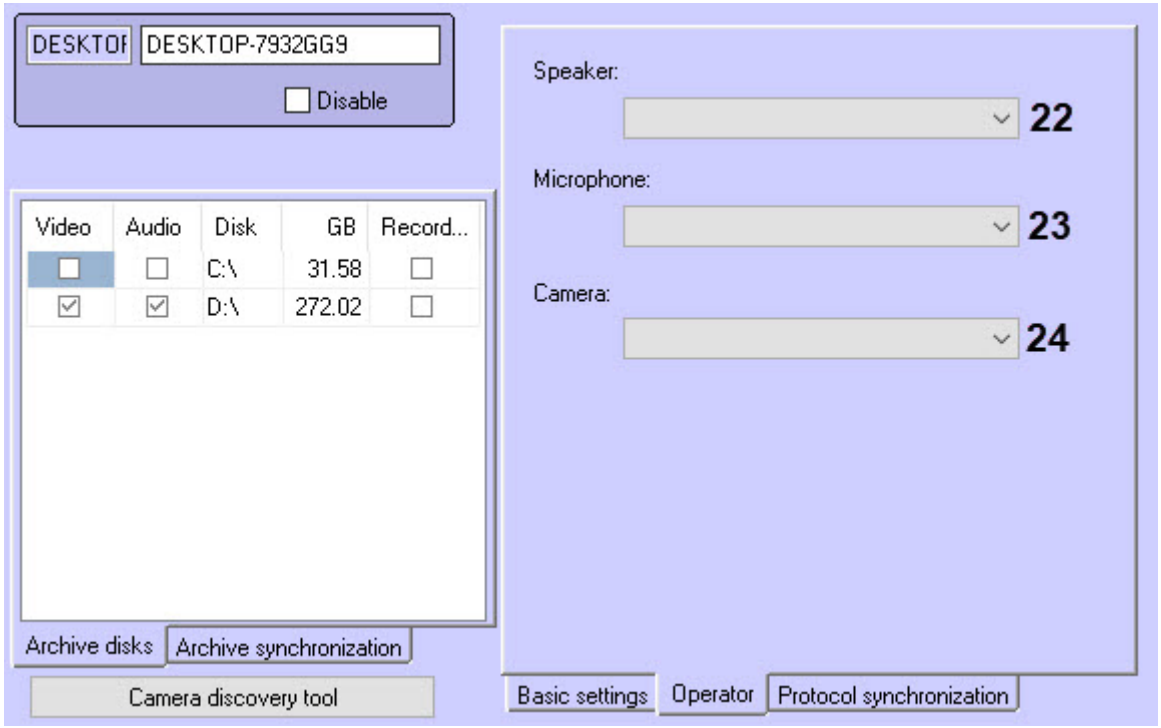
26.1.5.8.2 The Settings panel of the Computer object

The appearance of the settings panel of the **Computer** object is shown in the figures. The description of the parameters of the **Computer** object settings panel is given in the table below the figures.

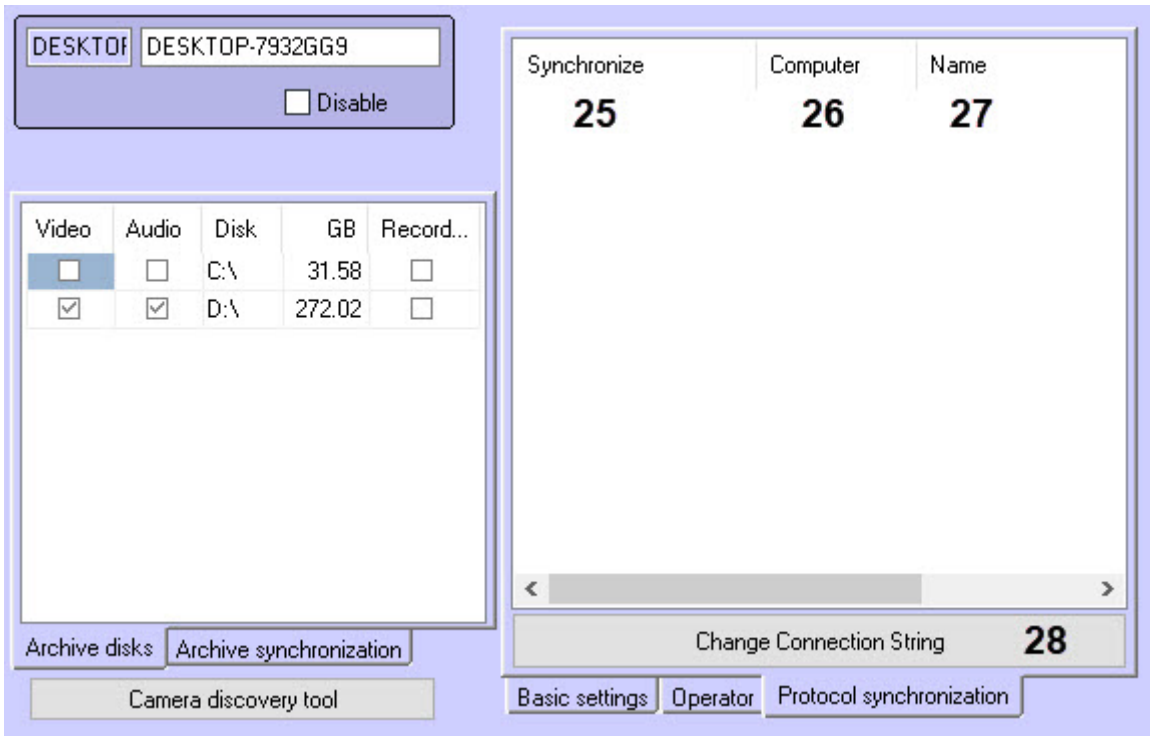
The **Archive disks** and **Basic settings** tabs:



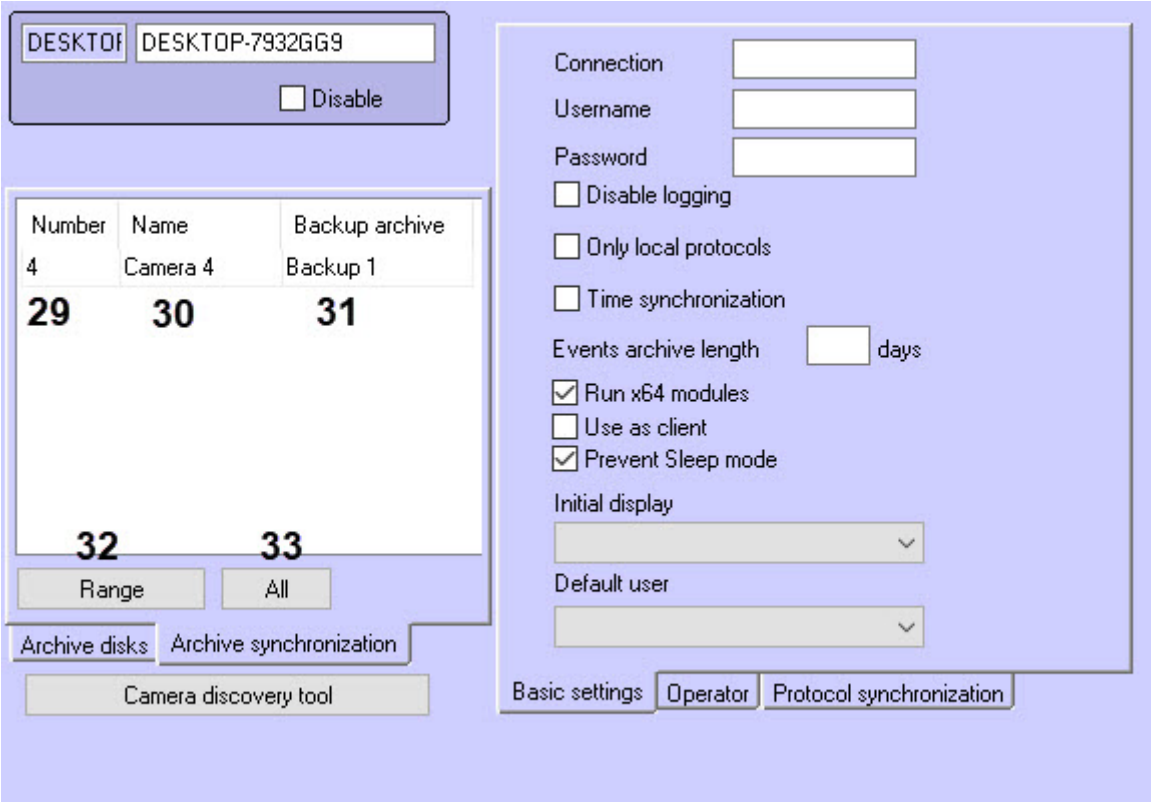
The **Operator** tab:



The **Protocol synchronization** tab:



The **Archive synchronization** tab:



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Network name***	Automatically	Displays the computer name in the local network	Numbers, letters, periods, hyphen, dash, underscore and any symbols	-	Depends on the number of the **Computer** objects registered in the system. Number of characters—from 1 to 15
2	**Name***	Enter the value in the field	Sets the name of the **Computer** object in the system	Latin, Cyrillic and service characters	Computer	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Defines the condition (enabled or disabled) of the **Computer** object in the system	Boolean type	Clear	Set—the **Computer** object is disabled and isn't used Clear—the **Computer** object is enabled and used
The **Archive disks** tab						

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Video**	Set the checkbox	Sets the disk for storing video archive from cameras and also audio archive during synchronous audio and video recording	Boolean type	Clear	Set—the disk is used for video archive storing Clear—the disk is not used for video archive storing
5	**Audio**	Set the checkbox	Sets the disk for storing audio archive from microphones	Boolean type	Clear	Set—the disk is used for audio archive storing from microphones Clear—the disk is not used for audio archive storing from microphones
6	**Disk**	Automatically, enter the value in the field	Displays the names of the local disks, accessible for storing video and audio archive, and also used to specify the network disks used for archive storing	Names of the local disks (Latin characters), names of the network disks (UNC paths)	-	Depends on the total number of the local and network disks
7	**GB**	Automatically	Displays the amount of free space on each available disk	Disk space in GB	-	Depends on the total free disk space
8	**Recording**	Automatically	Displays the current disk for the archive recording	Boolean type	Clear	Set—the archive is currently recorded on the specified disk Clear—the archive isn't currently recorded on the specified disk
The **Basic settings** tab						
9	**Connection**	Enter the value in the field	Sets the name to the modem connection used in Windows	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters). Number of characters—from 1 to 30
10	**Username**	Enter the value in the field	Sets the login of the modem connection used in Windows	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters), case-sensitive. Number of characters—from 1 to 30
11	**Password**	Enter the value in the field	Sets the password of the modem connection used in Windows	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters), case-sensitive.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Number of characters—from 1 to 30
12	**Disable logging**	Set the checkbox	Disables the event logging to the Event Viewer database on the local computer	Boolean type	Clear	Set—events aren't logged to the Event Viewer database Clear—events are logged to the Event Viewer database
13	**Only local protocols**	Set the checkbox	Enables logging to the Events Viewer database only the information about the events, registered on this computer	Boolean type	Clear	Set—only the events, registered on this computer are logged to the Events viewer database Clear—all required events are logged to the Events Viewer database
14	**Time synchronization**	Set the checkbox	Sets the time synchronization of all computers in the distributed system with the system time of this computer. Time is automatically synchronized at midnight every 24 hours or when *Intellect* is started on the Server that is the source of the time synchronization	Boolean type	Clear	Set—time is synchronized Clear—time isn't synchronized
15	**Events archive length**	Enter the value in the field	Sets the event storage period for: • events registered in the system on the local computer (Protocol table in the *Intellect* database or in a separate database) • Incident server events (table PROTOCOL_INC_SERVER in the *Intellect* database)	Days	-	More than 1
16	**Run x64 modules**	Set the checkbox	Sets the way to run the 64-bits modules	Boolean type	Up to 4.10.2 — Clear From 4.10.3 — Set	Set—when you attempt to run a module, the 64-bits module variant runs. If such a variant isn't found, the 32-bits module runs Clear—64-bits modules don't run
17	**Use as client**	Set the checkbox	Indicates that the computer is a Client in the distributed video surveillance system	Boolean type	Clear	Set—computer is used as a Client Clear—computer is used as a Server or a RAW
18	**Prevent Sleep mode**	Set the checkbox	If the checkbox is set, when *Intellect* is running, Windows OS sleep mode settings will be blocked, and the computer won't enter the sleep mode	Boolean type	Set	Set—computer doesn’t enter the sleep mode Clear—computer enters the sleep mode

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
19	**Initial display**	Select from the list	Sets the default **Display** to be displayed after starting *Intellect*. If no **Display** is selected, the last active display will be displayed after *Intellect* starts	Names of the **Display** objects registered in the system	-	Depends on total number of **Display** objects registered in the system
20	**Default user**	Select from the list	Sets a default user, i.e. the user with the rights and permissions to start *Intellect* without a password	Names of the users registered in the system	-	The list of users registered in *Intellect*
21	**Camera discovery tool**	Click the button	Access to creating, configuring and editing IP devices	-	-	-
The **Operator** tab						
22	**Speaker**	Select from the list	Allows selecting the speaker that should be use for audio signal playback (used when organizing a video surveillance system using SIP-devices — see Configuring SIP-terminal)	Names of the **Speaker** objects registered in the system	-	Depends on number of the **Speaker** objects registered in the system
23	**Microphone**	Select from the list	Allows selecting the microphone that should be used for audio signal transmission (used when organizing a video surveillance system using SIP-devices — see Configuring SIP-terminal)	Names of the **Microphone** objects registered in the system	-	Depends on number of the **Microphone** objects registered in the system
24	**Camera**	Select from the list	Allows selecting the camera that should be used for video signal transmission (used when organizing a video surveillance system using SIP-devices — see Configuring SIP-terminal)	Names of the **Camera** objects registered in the system	-	Depends on number of the **Camera** objects registered in the system
The **Protocol synchronization** tab						
25	**Synchronize**	Set the checkbox	Sets the synchronization of the local computer and remote computer Event Viewer databases	Boolean type	Clear	Set—local and remote computers Event Viewer databases are synchronized Clear—local and remote computers Event Viewer databases aren't synchronized
26	**Computer**	Automatically	Displays the network name of the remote computer with which you want to synchronize the Event Viewer database	Latin and service characters	-	Depends on the number of the **Computer** objects registered in the system
27	**Name**	Automatically	Displays the name of remote computer in the network	Latin, Cyrillic and service characters		A line containing a sequence of any characters (letters, digits, service characters), case-sensitive. Number of characters—from 1 to 60

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
28	**Change Connection String**	Click the button	Access to settings and editing the parameters of connection to the remote computer Event viewer database	-	-	-
The **Archive synchronization** tab						
29	**Number**	Select from the list	Sets the ID of the camera the archive of which should be synchronized when restoring the main Server (see also Configuring archive synchronization of main and backup Servers)	IDs of the **Camera** objects created in the objects tree of the main Server	-	Depends on the number of the **Camera** objects registered in the system
30	**Name**	Select from the list	Sets the name of the camera the archive of which should be synchronized when restoring the main Server (see also Configuring archive synchronization of main and backup Servers)	Names of the **Camera** objects created in the objects tree of the main Server	-	Depends on the number of the **Camera** objects registered in the system
31	**Backup archive**	Select from the list	Sets the **Backup archive** object configured to cooperate with the Failover service and used to synchronize the archives of the main and backup Servers (see also Configuring archive synchronization of main and backup Servers)	Names of the **Backup archive** objects registered in the system	-	Depends on the number of the **Backup archive** objects registered in the system
32	**Range**	Click the button	Opens a dialog box for adding cameras in groups	-	-	-
33	**All**	Click the button	Adds all available cameras to the table	-	-	-

26.1.5.8.3 The Settings panel of the Video capture device object

The settings panel of the **Video capture device** object is shown in the figure.

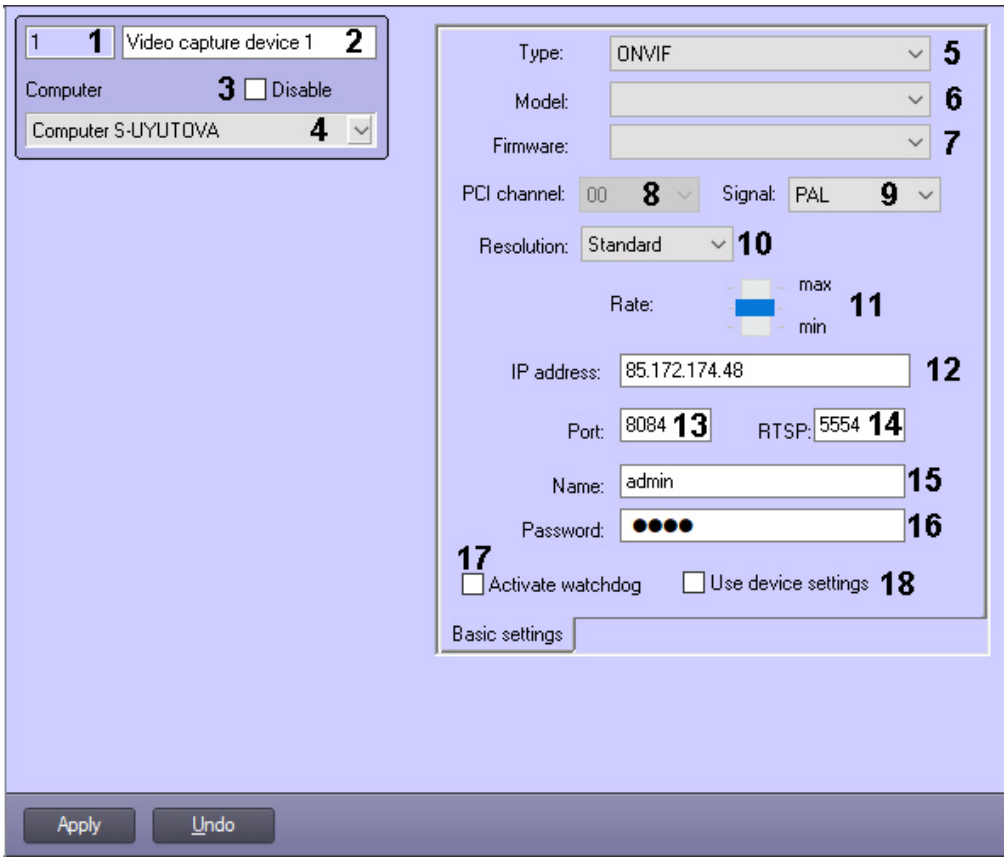


Table describes the setting parameters of the **Video capture device** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Video capture device** system object	Sequence of numbers	-	Depends on the number of the **Video capture device** objects in the system
2	**Name**	Enter the value in the field	Sets the name of the **Video capture device** object in the system	Latin, Cyrillic letters and service characters	Video capture device	A line representing a sequence of any characters (letters, digits, service characters except > and < symbols), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the status (enabled or disabled) of the **Video capture device** object in the system	Boolean type	-	Set—the **Video capture device** object is disabled and isn't in use Clear—the **Video capture device** object is enabled and is in use
4	**Computer**	Select from the list	Sets the **Computer** parent object for this **Video capture device** object	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the system

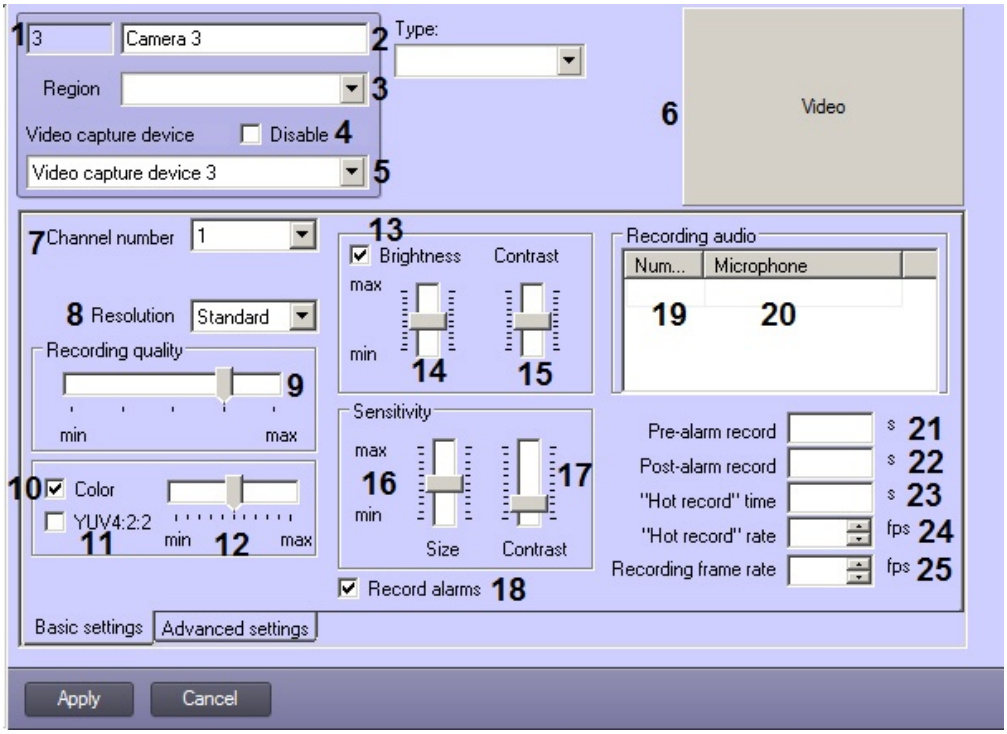
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Basic settings** group						
5	**Type**	Select from the list	Sets the type of the video capture board or the manufacturer of the IP device	Name of the types of the video capture boards and the manufacturers of the IP devices	-	Video capture boards (FS-3, FS-5, FS-6, FS-8, WS–4, WS-7/17, etc.). Network video hubs (WaveHub) Network devices (Axis, Panasonic, etc.) Virtual
6	**Model**	Select from the list	Sets the model of the IP device	Names of the models of the IP devices		Integrated models of the IP devices of the selected manufacturer
7	**Firmware**	Select from the list	Sets the firmware of the IP device	Numbers of the integrated firmware of the IP device		Integrated firmware of the selected IP device
8	**PCI channel**	Select from the list	Sets number of the PCI channel of the video capture board ADC	List of connected channels for video capture	-	From 0 to 31, depending on the number of the PCI channels on the Server and the number of installed ADCs
9	**Signal**	Select from the list	Sets the format of the incoming video signal	List of video signal formats	PAL	PAL, NTSC
10	**Resolution**	Select from the list	Sets resolution of the video frames	List of video frame resolutions	Standard	**Standard** **High** **Full** Specific values depend on the camera model
11	**Speed**	Set in the required position	Sets the frame rate of the video stream	Permissable changes of the total frame rate of the video signal transmission	Average	Depends on the capabilities of the IP-camera or video capture board. For boards with software compression: **Ma**—maximum permissable total frame rate of the video signals **Average**—half of the maximum permissable total frame rate of the video signals **Min**—one third of the maximum permissable total frame rate of the video signals
12	**IP address**	Enter the value in the field	Sets the IP address of the network device	IP address	-	A line presented as xxx.xxx.xxx.xxx Contains the values: 0.0.0.0 – 255.255.255.255

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Depends on the network settings of the IP devices registered in the system When configuring getting live video from the ECHD Server, specify the following line in the field <ECHD Server address>:<GUID cameras in the system>:<external account>
13	**Port**	Enter the value in the field	Sets the connection port of the network IP device	Nonnegative integer	-	From 0 to 65535 Depends on the network settings of the IP device
14	**RTSP**	Enter the value in the field	Sets the RTSP connection port of the network IP device	Nonnegative integer	-	From 0 to 65535 Depends on the network settings of the IP device
15	**Name**	Enter the value in the field	Set the user name to connect to the network IP device	-	-	Depends on the network settings of the IP device
16	**Password**	Enter the value in the field	Sets the password to connect to the network IP device	-	-	Depends on the network settings of the IP device
17	**Activate watchdog**	Set the checkbox	Activates the Windows reset function, when *Intellect* main modules freeze	Boolean type	Clear	Set—the reset funcion of Windows OS is enabled Clear—the reset funcion of Windows OS is disabled
18	**Use device settings**	Set the checkbox	Allows using the settings specified in the Web-Server or other software of the IP device	Boolean type	Clear *Note. When creating the **Video capture device** object using the Camera discovery tool, the value of the checkbox depends on the settings configured in the Wizard*	Set—the settings of the IP device are used Clear—the settings of *Intellect* are used

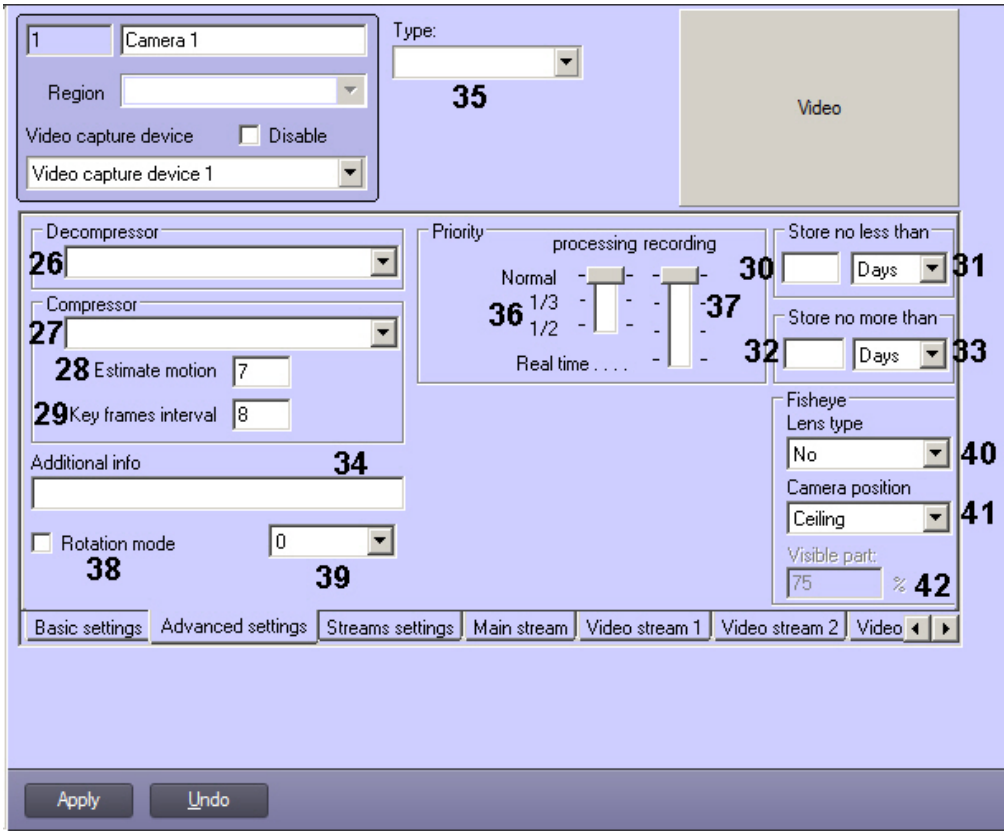
26.1.5.8.4 The Settings panel of the Camera object

The settings panel of the **Camera** object is shown in the figures.

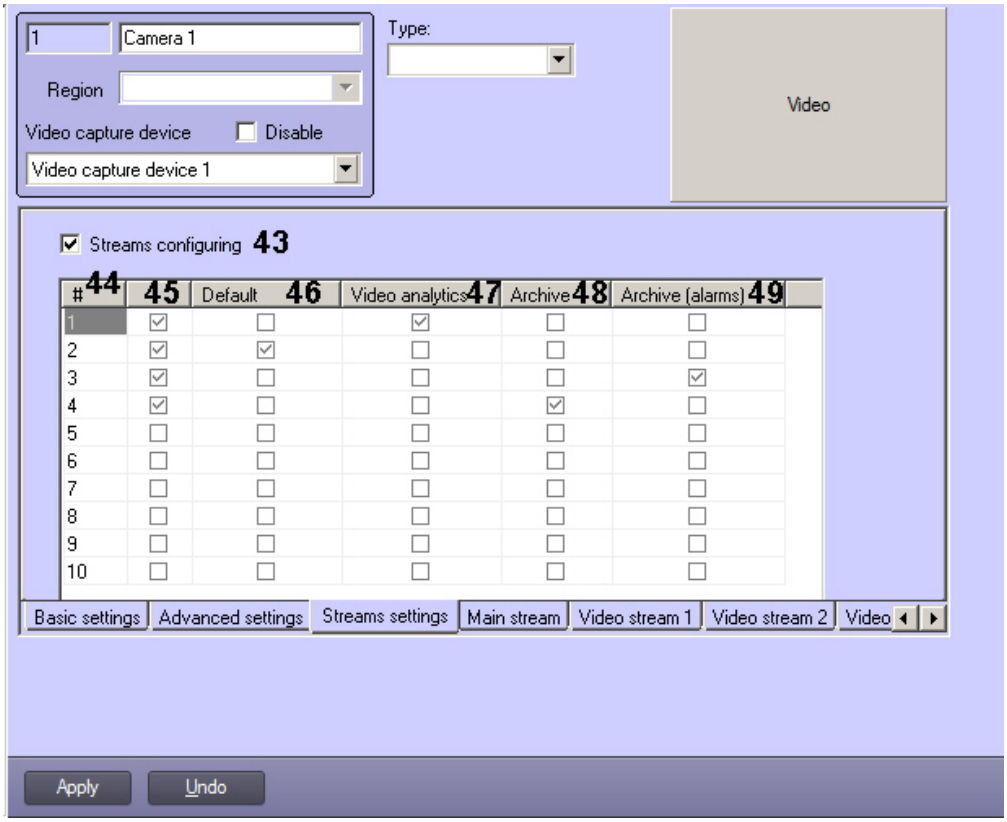
The **Basic settings** tab:



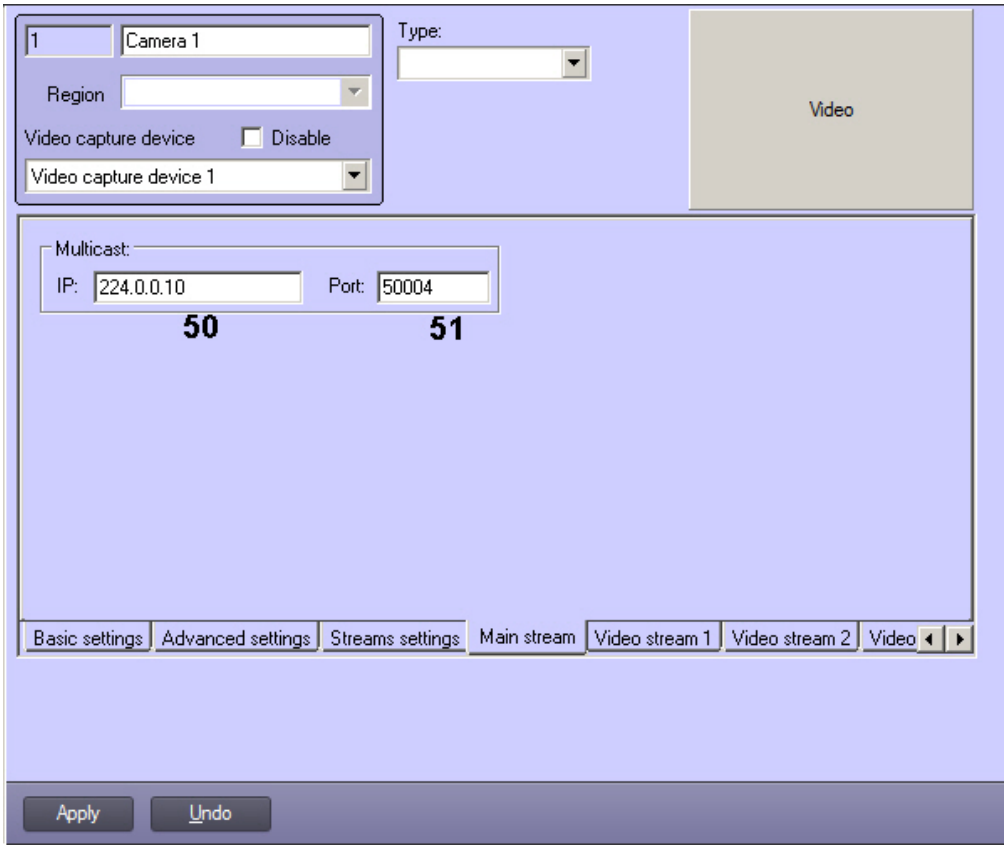
The **Advanced settings** tab:



The **Streams settings** tab:



The **Main stream** tab:



The **Video stream** tab:

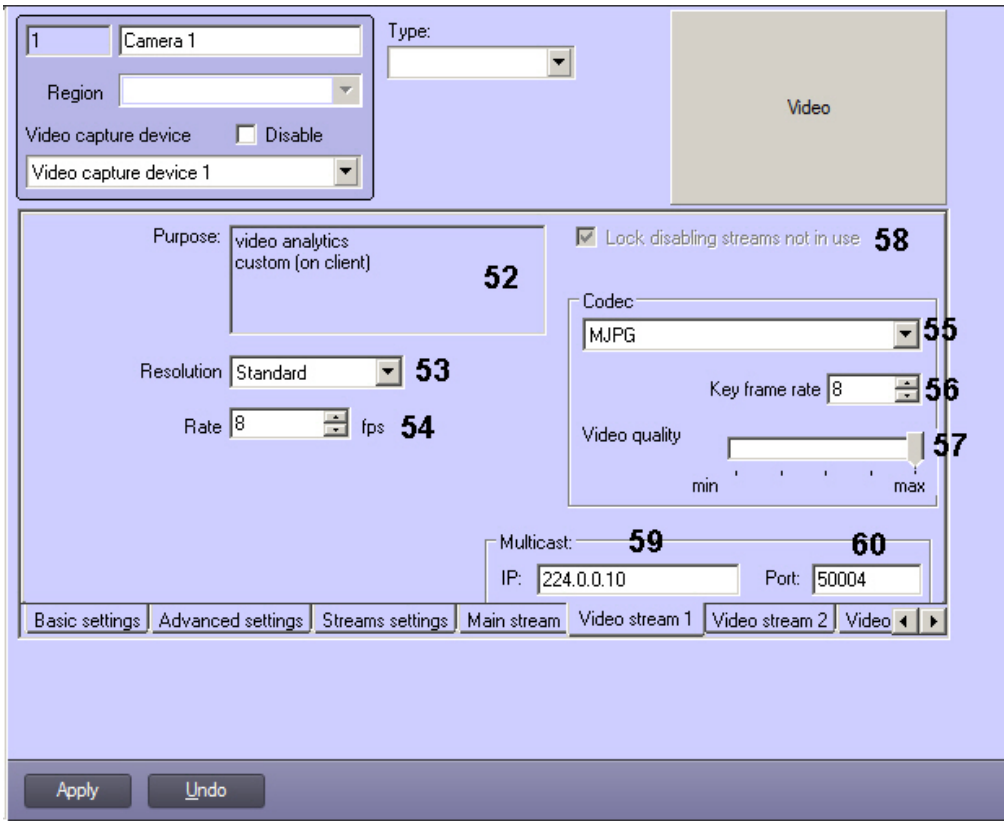


Table describes the setting parameters of the **Camera** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Camera** system object in the system	Sequence of numbers	-	From 1 to FaceCamOffset. By default, FaceCamOffset = 50000. The FaceCamOffset value is set using the same-name registry key (see Registry keys reference guide)
2	**Name**	Enter the value in the field	Sets the name of the **Camera** object in the system	Latin, Cyrillic and service characters	Camera	A line containing a sequence of any characters (letters, digits, service characters except > and < symbols), case-insensitive. Number of characters—from 1 to 60
3	**Region**	Select the value from the list	Sets the **Region** structural element, to which this **Camera** object belongs	Name of the **Region** objects registered in the system	Region	Depends on the number of the **Region** objects registered in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Disable**	Set the checkbox	Sets the status (enabled or disabled) of the **Camera** object in the system	Boolean type	Clear	Set—the **Camera** object is disabled and isn't in use Clear—the **Camera** object is enabled and is in use
5	**Video capture device**	Select the value from the list	Sets the **Video capture device** parent object for this **Camera** object	Name of the **Video capture device** objects registered in the system	Name of the **Video capture device** parent object	Depends on the number of the **Video capture device** objects in the system
6	**Video**	Left-click	Displays video image with the configured settings. When holding down the Shift key on the keyboard, opens the Web-Server page of the IP device in the default browser (doesn't work with Internet Explorer)	Video image	-	-
The **Basic settings** tab						
7	**Channel number**	Select the value from the list	Sets the number of the channel used to connect a video camera to the video capture board. Corresponds to the number of the BNC connector of the interface cable	Sequence of numbers	1	Depends on the type of the video capture board. Maximum 16 channels
8	**Resolution**	Select the value from the list	Sets the resolution of the video image frame	List of resolutions of the video image frame	Standard	**Standard** **High** **Full** Specific values and their application depend on the camera model. If you want to use video streams with the exact resolution, it is better to use the **Streams configuring** setting (see parameter 43 and following)
9	**Recording quality**	Set the slider in the required position	Sets the quality of the recorded frame. The value is inverse to the video signal compression level	-	Above average	**Min**—maximum compression level and the lowest video signal quality **Max**—the lowest compression level and the highest video signal quality
10	**Color**	Set the checkbox	Set the type of the video image received from the camera (color or black and white)	Boolean type	Set	Set—the image from the video camera is in color Clear—the image from the video camera is black and white

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
11	**YUV 4:2:2**	Set the checkbox	Sets the format of the color representation of the video signal	Boolean type	Clear	Set—the video signal is represented in the YUV 4:2:2 format Clear—the video signal is represented in the YUV 4:2:0 format
12	**Color**	Set the slider in the required position	Sets the color saturation of the color video image	From the maximum color saturation to a black and white video image	Average	**Max**—corresponds to the maximum color saturation of the video image **Min**—corresponds to the black and white video image
13	**Brightness – Contrast**	Set the checkbox	Sets the mode for adjusting brightness and contrast of the video image	Types of modes for adjusting brightness and contrast of the video image	Automatic	Automatic (Position ☐)—**Brightness** and **Contrast** parameters are set automatically Manual (Position ■)—**Brightness** and **Contrast** parameters are set manually Manual setting with automatic optimization (Position ☑)—**Brightness** and **Contrast** parameters are set manually, followed by automatic optimization
14	**Brightness**	Set the slider in the required position	Sets the brightness of the video image	From the maximum brightness (white video image) to minimum brightness (black video image)	Average	**Max**—corresponds to the maximum brightness of the video image **Min**—corresponds to the minimum brightness of the video image
15	**Contrast**	Set the slider in the required position	Set the contrast of the video image	-	Average	**Max**—corresponds to the maximum contrast of the video image **Min**—corresponds to the minimum contrast of the video image
16	**Size**	Set the slider in the required position	Sets the minimum size of an object at which the main motion detection tool triggers	% of the screen height	Average	**Min**—0% of the video surveillance window size **Max**—100% of the video surveillance window size

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
17	**Contrast**	Set the slider in the required position	Set the minimum contrast of an object at which the motion detection tool triggers	-	Less than average	**Max**—correspond to maximum contrast of the object **Min**—corresponds to the minimum contrast of the object
18	**Record alarms**	Set the checkbox	Starts automatic video signal recording on the alarms from the camera	Boolean type	Set	Set—automatic video signal recording on the alarm from the camera is enabled Clear—automatic video signal recording on the alarm from the camera is disabled
19	**Number**	Select the value from the list	Sets the number of the microphone, the audio from which should be recorded simultaneously with the video signal from the camera	Numbers of the **Microphone** objects registered in the system	-	Depends on the number of the **Microphone** objects registered in the system
20	**Microphone**	Select the value from the list	Sets the name of microphone, the audio from which should be recorded simultaneously with video signal from the camera	Names of the **Microphone** objects registered in the system	-	Depends on the number of the **Microphone** objects registered in the system
21	**Pre-alarm record**	Enter the value in the field	Set the time period that precedes the alarm record, during which the prehistory of the event is recorded	Time in seconds (s)	-	Recommended time—from 0 to 20
22	**Post-alarm record**	Enter the value in the field	Sets the time period, during which the video is recorded after an alarm was registered	Time in seconds (s)	-	Recommended time—from 0 to 20
23	**"Hot record" time**	Enter the value in the field	Sets the time period from the moment the alarm is registered or recording begins, during which the video is recorded at the frame rate set in the **"Hot record" rate** field	Time in seconds (s)	-	Recommended time—from 0 to 30
24	**"Hot record" rate**	Enter the value in the field/ select from the list	Sets the frame rate of the alarm hot recording	FPS	-	Depends on the capabilities of the camera Recommended value—from 0 to 20

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
25	**Recording frame rate**	Enter the value in the field/ select from the list	Sets the frame rate of the video signal recording	FPS	-	Depends on the capabilities of the camera Recommended value—from 1 to 25 for PAL; from 1 to 30 for NTSC
The **Advanced settings** tab						
26	**Decompressor**	Select the value from the list	Sets the technology using which the compressed video stream will be decompressed when displaying the video signal on the monitor *Note. By default the parameter is not available for editing. To change the value of this parameter set the 1 value for the EnableCodecSettings registry key (see Registry keys reference guide)*	List of available decompressors	No	BOSCH FfmpegAllInOneDecoder H263IppDecoder H264InterlacedIppDecoder H264IppDecoder MJPEGIpp Motion Wavelet 3.5 Motion Wavelet 7.1 MPEG2IppDecoder MPEG4IppDecoder MxPEG Mobotix RGB24toYUV420 StreamLabs VWV WMVIppDecoder
27	**Compressor**	Select the value from the list	Sets the algorithm of the video stream compression *Note. By default the parameter is not available for editing. To change the value of this parameter set the 1 value for the EnableCodecSettings registry key (see Registry keys reference guide)*	List of available algorithms	No	Depends on the camera model
28	**Estimate motion**	Enter the value in the field	Sets the threshold of the camera sensivity to motion depending on the change of the object brightness. The delta frame of the video signal is formed according to this criterion	Sequence of numbers	7	From 2 to 255
29	**Key frames interval**	Enter the value in the field	Sets the rate of the key frames	Sequence of numbers	8	Depends on the capabilities of the camera
The **Store no less than** group						
30	**Store no less than**	Enter the value in	Set the time period for keeping the video archive from the camera and audio archive (in case of synchro recording) on the	Day or hour depending on the value	-	More than 1

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
		the field	Server. The parameter allows storing the large archive for the selected camera using the archive of other cameras *Note. It is recommended to set the **Store no less than** parameter for no more than 30% of cameras, as this setting is only advisory. If there isn't enough space for the archive recording, the setting will be ignored and the recording won't stop anyway.* *If more than 10 cameras are created in the system, then when setting this parameter for more than 30% of cameras in the system, after you click the **Apply** button, a corresponding warning message will appear. It can be disabled using the NotifyAbout_arch_days registry key (see Registry keys reference guide)*	selected in the drop-down list		
31	**Store no less than**	Select the value from the list	Sets the units for time period specified in the **Store no less than** field	List of available time units	Days	Days Hours
The **Store no more than** group						
32	**Store no more than**	Enter the value in the field	Sets the time period for storing the camera archive. When it is expired, the camear archive should be deleted *Note. The archive can be deleted before the specified time if it is required for loop recording*	Day or hour depending on the value selected in the drop-down list	-	More than 1
33	**Store no more than**	Select the value from the list	Sets the units for time period specified in the **Store no more than** field	List of available time units	Days	Days Hours
Not in groups						
34	**Additional info**	Enter the value in the field	Sets the information displayed on the video surveillance monitor above the camera name. This information is added to the export file and when the frame is printed, as well as to the event log	Line not longer than 100 characters	Blank line	Latin and Cyrillic letters, numbers
35	**Type**	Select the value from the list	Sets the type of the camera. The setting affects the type of the icons used to represent the camera on the map	List of available camera types	-	Fisheye PTZ Standard
36	**Processing priority**	Set the slider in the required position	Sets the priority of the video signals processing by ADC	Order of video signals processing	Normal	**Normal**—normal video signals processing order **1/3**—1/3 processing order **1/2**—1/2 processing order

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
37	**Recording priority**	Set the slider in the required position	Set the priority of video signals processing by ADC in the recording mode	Order of video signals processing in the recording mode	Normal	**Normal**—normal video record order **1/3**—1/3 processing order **1/2**—1/2 processing order **Real time**—all ADC resourses are used for video signals recording
38	**Rotation mode**	Set the checkbox	Enables the rotation the the video image displayed on the **Video surveillance monitor**	Boolean type	Clear	Set—rotation is enabled Clear—rotation is disabled
39	**Rotate on**	Select the value from the list	Specifies the angle of video image rotation when the rotation mode is enabled	Sequence of numbers	0	0, 90, 180, 270
40	**Lens type**	Select the value from the list	Sets the type of lens to use	Supported lens types	No	**No**—select if there are neither fisheye nor panomorph lens on the camera **Standard fisheye lens**—select if there is a fisheye lens on the camera **Autocalibration**—select if there is a fisheye lens on the camera and the video conversion parameters should be automatically determined to eliminate artifacts **A0*V, A1UST, A8TRT, B0QQV, B4QQV, B5SST, B6SST**—types of panomorph lenses
41	**Camera position**	Select the value from the list	Sets the position of the camera	Supported camera position options	Ceiling	**Ceiling** **Wall** **Floor**
42	**Visible part**	Enter the value into the field	Determines what part of the frame will be visible on the **Video surveillance monitor** after the conversion	Percentage	75% for the **Ceiling** position 66% for the **Wall** position *Note. The default value may not be displaye*	0-100

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
					d in the field	
The **Streams settings** tab						
43	**Streams configuring**	Set the checkbox	Enables the video signal multistream feature	Boolean	Clear	Set—video signal multistreaming is enabled; different streams can be used for analytics, archiving, and display Clear—video signal multistreaming is disabled; a single stream is used for analytics, archiving, and display
44	**#**	Automatically	Displays the number of the stream	Integer	-	1-10
45	**Enabled ***	Set the checkbox	Sets the used camera streams	Boolean	Clear	Set—the stream is in use Clear—the stream is not in use
46	**Default**	Set the checkbox	Sets the video stream that will be used in the following cases: 1. to display video locally and on the remote clients; 2. to send the video stream to the remote clients and to the Videogate that will record this video stream; 3. in cases when video request doesn't specify the stream	List of available streams	Clear	Set—the stream is used by default Clear—the stream isn't used by default
47	**Video analytics**	Set the checkbox	Sets the video stream used for video analytics. This stream will be used by the base motion detection tool, zone detection tools, tracking detection tool, face detection tool (if an external recognizer isn't used). The **Default** stream is used for the LPR server, face detection tool (if an external recognizer is used), and the detection tools that are part of the *Detector Pack.* The **Archive**/**Archive (alarms)** stream is used for the long-term archive	List of available streams	Clear	Set—the stream is used for video analytics Clear—the stream isn't use for video analytics
48	**Archive**	Set the checkbox	Sets the video stream that is recorded to the archive not upon alarm, but continuously	List of available streams	Clear	Set—the stream is used for archive recording Clear—the stream isn't used for archive recording
49	**Archive (alarms)**	Set the checkbox	Sets the video stream recorded to the archive upon alarm	List of available streams	Clear	Set—the stream is used for archive recording upon alarm

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the stream isn't used for archive recording upon alarm
The **Main stream** tab						
50	**IP**	Enter the value in the field	Sets the IP address from which the client will receive the video data from the ONVIF Server in the **Multicast** mode	IP address	224.0.0.10	224.0.0.0 - 239.255.255.255
51	**Port**	Enter the value in the field	Sets the port for transmitting the video data in the **Multicast** mode	Sequence of numbers	Depends on the number of video cameras and streams in the system	Any valid unused port numbers. The number of ports is determined by the system administrator
The **Video stream** tab						
52	**Purpose**	-	Provides information about the use of the video stream	String	Depends on the video stream designated purpose	Latin and Cyrillic characters, numbers
53	**Resolution****	Select the value from the list	Sets the video stream resolution	List of supported resolutions of the video image frame	Standard	**Standard** **High** **Full** Particular values depend on the camera model
54	**Speed****	Enter the value in the field	Sets the frame rate of the video stream	Frame rate in FPS	25	Depends on the capabilities of the camera
55	**Codec****	Select the value from the list	Sets the technology used to encode and decode the video stream	List of supported codecs	Depends on the camera model	Depends on the camera model
56	**Key frame rate****	Enter the value in the field	Sets the key frames rate	Sequence of numbers	8	Depends on the capabilities of the camera

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
57	**Video quality****	Set the slider in the required position	Sets the frame quality	-	Maximum	**Min**—maximum compression and minimum video signal quality **Max**—minimum compression and maximum video signal quality
58	**Lock disabling streams not in use**	Set the checkbox	This checkbox should be set if the purpose is not specified for the configured stream but it is used for recording on a macro or a script	Boolean	Clear	Set—if the stream purpose isn't specified, the stream is in the sleep mode and it cannot be used for recording on a macro or a script Clear—if the stream purpose isn't specified, it can be used for recording on a macro or a script
59	**IP**	Enter the value in the field	Sets the IP address from which the client will receive the video data from the ONVIF Server in the **Multicast** mode	IP address	224.0.0.10	224.0.0.0 - 239.255.255.255
60	**Port**	Enter the value in the field	Sets the port for transmitting the video data in the **Multicast** mode	Sequence of numbers	Depends on the number of cameras and streams in the system	Any valid unused port numbers. The number of ports is determined by the system administrator

* Name of the interface element isn't displayed on the settings panel.

** Similar settings on the **Basic Settings** and the **Advanced settings** tabs, as well as on the settings panel of the **Video capture device** object, are ignored.

26.1.5.8.5 The Settings panel of the Detection zone object

The **Detection zone** object is used to register and configure intelligent video detectors. The settings panel of the **Detection zone** object is shown in the figure:

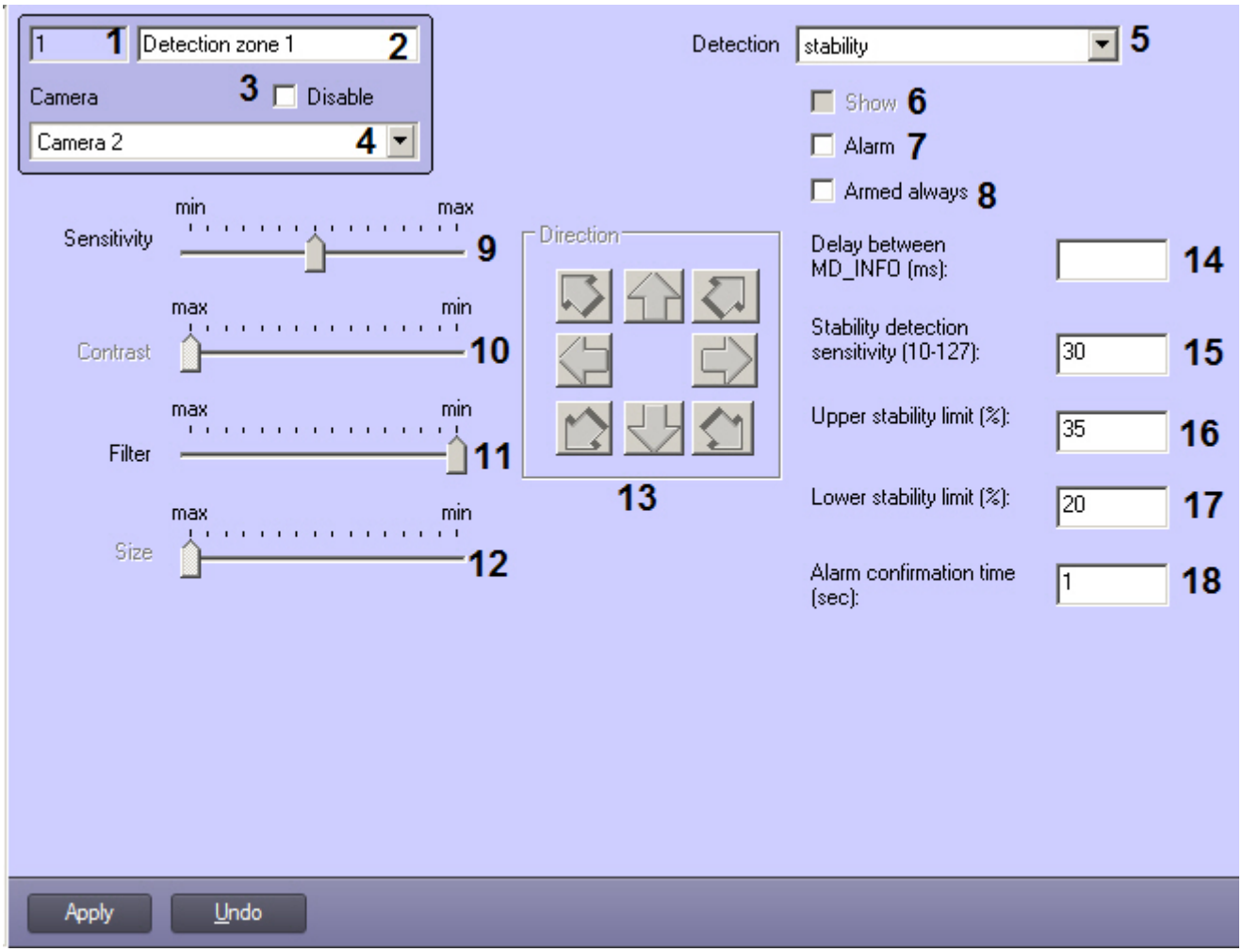


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Detection zone** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Detection zone** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Detection zone** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Detection zone** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic characters and service characters	Detection zone	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Detection zone** object (enabled or disabled) in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Detection zone** is disabled and isn't used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the **Detection zone** object is enabled and is used
4	**Camera**	Select the value from the list	Sets the **Camera** parent object of the digital video surveillance system with the distributed architecture, to which the given **Detection zone** object belongs	Name of the **Camera** objects registered in the system	Name of the **Camera** parent object	Depends on the number of the **Camera** objects in the digital video surveillance system with the distributed architecture
5	**Detection**	Select the value from the list	Used to set the type of the used detector	List of names of the detectors in the system	Motions	Motion Focus Stability Background change Blind Cover Infrared
6	**Show**	Set the checkbox	Sets the display of the frame border of an object in the camera field of view This parameter is active only with the following detectors are selected from the **Detection** list: motion, infrared.	Boolean type	Clear	Set—the object frame border is displayed in the camera field of view Clear—the object frame border is not displayed in the camera field of view
7	**Alarm**	Set the checkbox	Enables alarm generation on camera and automated recording of the video signal from the camera with the alarm received from the selected detector	Boolean type	Clear	Set—on alarm received from the selected detector, an alarm is generated on the camera and automated recording of the video signal is performed Clear—alarm is not generated on the camera and automated recording of the video signal is not performed on the alarm received from the selected detector
8	**Armed always**	Set the checkbox	Sets the state of the selected detector as **Always armed** permanently	Boolean type	Clear	Set—the detector is always in the Always armed state Clear—the Operator can disarm the detector
9	**Sensitivity**	Set the slider in the required position	The setting depends on the type of the selected detector: **Motion detection tool** The value of this parameter corresponds to the minimum value of the averaged brightness of the moving object, at which the detection tool will trigger only at its motion, and not at the video signal noise (including snow, rain, etc.). The HIGHER the sensitivity	-	Average	-

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			value, the more sensitive the detection tool is. **Focus detection tool** The value of this parameter characterizes the minimum degree of accuracy loss, expressed in the difference between the average number of outlines and the number of outlines in the incoming frame at which the detection tool should trigger. **Stability detection tool** The value of this parameter characterizes the minimum degree of reduction in the resolution of the frame, expressed in the difference between the average number of outlines and the number of outlines in the incoming frame at which the detection tool should trigger. **Background change detection tool** This parameter characterizes the deviation of the integral brightness of the frame from the average value at which the detection tool should trigger. **Blind detection tool** This parameter corresponds to the rate of illumination of the video expressed in the difference between the positions of medians of the brightness chart of the incoming frame and the reference illumination frame at which the detection tool should trigger. **Cover detection tool** This parameter corresponds to the rate of narrowing of the brightness chart of the frame, i.e. estimation of the frame filling with gray color, at which the detection tool should trigger. **Infrared detection tool** The value of this parameter corresponds to the minimum value of the averaged brightness of the moving object, at which the detection tool will trigger at its motion			
10	**Contrast**	Set the slider in the required position	Sets the minimum contrast of the object at which the detection tool triggers at its motion. The HIGHER the specified contrast value, the more different the neighboring b/w elements should be, so that the detection tool considers them as different objects. It is not applicable for all detector types	-	Average	-
11	**Filter**	Set the slider in the required position	The setting depends on the type of the selected detector: **Motion detection tool, Infrared detection tool** The value of this parameter corresponds to the threshold of color processing of objects, at which the detection tool should trigger. The HIGHER the filtering, the more different the neighboring elements (pixels) of the image should be, so that the detection tool considers them as different objects.	-	Minimum	-

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			Background change detection tool, Stability detection tool The value of this parameter corresponds to the contrast threshold of the detected object. It is not applicable for all detector types			
12	**Size**	Set the slider in the required position	The setting depends on the type of the selected detector. The value of this parameter corresponds to the minimum size of the detection object relatively to the frame sizes. It is not applicable for all detector types	-	Average	-
13	Direction of search*	Press the arrow buttons	Sets the direction of search for the motion detector	8 possible directions to object movement in the frame	All directions are selected: up, down, to the left, to the right, up and to the left, up and to the right, down and to the left, down and to the right	Up, down, to the left, to the right, up and to the left, up and to the right, down and to the left, down and to the right
14	**Delay between MD_INFO (ms)**	Enter the value into the field	Sets the time period in milliseconds between the MD_INFO events from the CAM_ZONE object in the Event Viewer (if the MD_INFO event is enabled in ddi)	Non-negative integer	0 (not set)	>=0
15	**Stability detection sensitivity (10-127)**	Enter the value into the field	**Stability detection tool** Sets the threshold of difference between the brightness of the pixel in the current frame and the background	Non-negative integer	30	10-127
16	**Upper stability limit (%)**	Enter the value into the field	**Stability detection tool** Sets the maximum permissible percentage of the stabilized frame pixels that differ from the background by more than the value in the **Stability detection sensitivity** field. When exceeded, the alarm verification process starts	Non-negative integer	35	0-100%
17	**Lower stability limit (%)**	Enter the value into the field	**Stability detection tool** Sets the maximum permissible percentage of the stabilized frame pixels that differ from the background by more than the value in the **Stability detection sensitivity** field. Below the value, the frame is considered stable	Non-negative integer	20	0-100%
18	**Alarm confirmation time (sec)**	Enter the value into the field	**Stability detection tool** Sets the time period in seconds during which the **Upper stability limit** must be exceeded to generate an alarm	Non-negative integer	1	>0

*Name of the element is not displayed in the settings panel of the given object.

26.1.5.8.6 The Settings panel of the Audio card object

The **Audio card** object is used to register and configure in *Intellect* audio signal digitization devices installed on the Server.

The settings panel of the **Audio card** object is shown in figure.

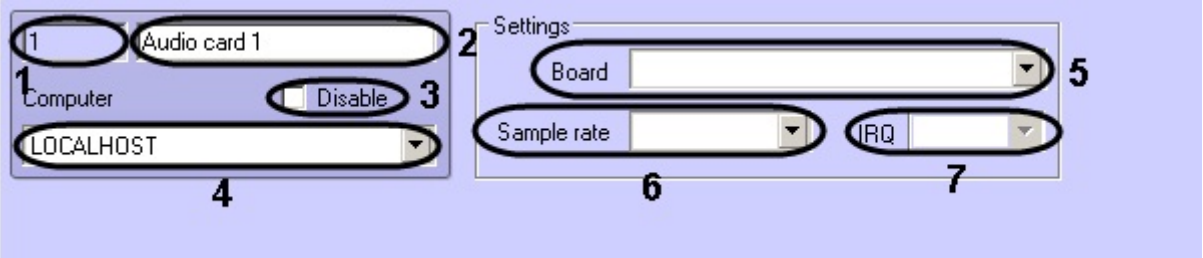


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Audio card** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Audio card** object in the digital video surveillance system with the distributed architecture	Sequence of numbers	-	Depends on the number of the **Audio card** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Audio card** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic characters and service characters	Audio card	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Audio card** object (enabled or disabled) in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Audio card** object is disabled and isn't used Clear—the **Audio card** object is enabled and is used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Audio card** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**Board**	Select the value from the list	Sets the type of the device for sound digitization. Digitization devices include various sound cards, such as SoundBlaster, ADC of the video capture cards, USB devices for the audio signal digitization	List of the types of the devices for sound digitization	Not defined	Depends on the number of audio signal digitization devices installed on the Server. For sound cards such as **SoundBlaster**—the name of the card. For the ADC of the video capture cards—the name of the video capture card,

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						including the number of the audio channel. For the USB devices—the name of the video capture card, including the number of the audio channel. For network devices—the type of the network device: **AX**, **IpCamAxis**
6	**Sample rate**	Select the value from the list	Sets the frequency rate at which the device digitizes the audio signal	Hz	For audio cards such as SoundBlaster—8000 For the ADC of the video capture cards—8000	For audio cards such as **SoundBlaster**, the frequency range of the digitization depends on the type of the audio card. 48000 is the maximum value for any card. For the ADC of the video capture cards—8000, 16000, 32000. For the USB devices, the frequency range of the digitization depends on the type of the used device, 48000 is the maximum value
7	**IRQ**	Not used	-	-	-	-

*Name of the element is not displayed in the settings panel of the given object.

26.1.5.8.7 The Settings panel of the Microphone object

The settings panel of the **Microphone** object is shown in the figure.

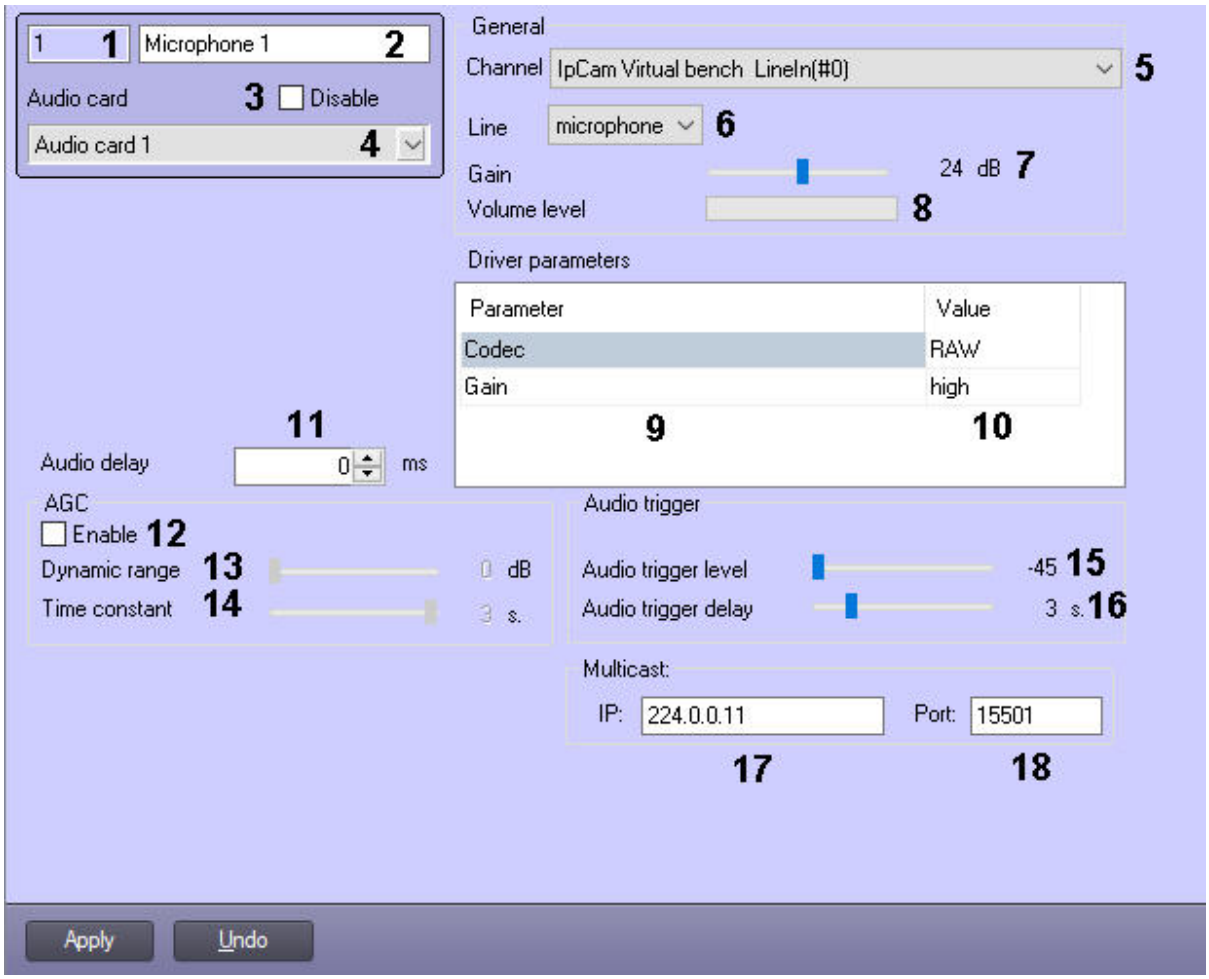


Table describes the settings parameters of the **Microphone** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **Microphone** object in the system	Sequence of numbers	-	Depends on the number of the **Microphone** objects in the system
2	Name	Enter the value into the field	Sets the name of the **Microphone** object in the system	Latin, Cyrillic characters and service characters	Microphone	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Microphone** object (enabled or disabled) in the system	Boolean type	Clear	Set—the **Microphone** object is disabled and isn't used Clear—the **Microphone** object is enabled and is used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Audio card**	Select the value from the list	Sets the **Audio card** parent object for the given **Microphone** object	Name of the **Audio card** objects registered in the system	Name of the **Audio card** parent object	Depends on the number of the **Audio card** objects in the system
The **General** group						
5	**Channel**	Select the value from the list	Sets the number of the channel for the audio signal input according to the number of the RCA-F connector to which the microphone is connected	Right, left chanel	0	Depends on the type of the audio signal digitization card. For AxxonSoft ADC of the audio signal digitization cards and audio cards such as SoundBlaster: 0—Left channel 1—Right channel
6	**Line**	Select the value from the list	Sets the source of audio signal	Type of the audio signal source	Microphone	**Microphone**—audio signal comes from the microphone **Phone**—audio signal comes from the telephone line
7	**Gain**	Set the slider into the required position	Sets the audio signal power gain	Sound power in decibels (dB)	24	From 0 to 45
8	**Volume level**	Automatically	Displays the power volume of the incoming audio signal	Sound power in decibels (dB)	-	From 0 to 45
The **Driver parameters** group						
9	**Parameter**	Automatically	Displays the available parameters of the IP device driver	-	-	Depends on the connected IP device
10	**Value**	Select the value from the list	Sets the values of the IP device parameters	-	-	Depends on the connected IP device and parameter
Not in group						
11	**Audio delay**	Enter the value into the field using the **up** and **down** buttons	Sets the delay in milliseconds between the receiving of audio signal from the audio input device and its output to the speaker or its recording to the archive simultaneously with the video signal. This parameter is used if the video image comes delayed or advanced, and the sound is ahead or behind it	Sequence of numbers	0	-10000 – 10000

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **AGC** group (set using the Olkha sound cards: Olkha-9P, Olkha-10LP, Olkha-12U, Olkha-14)						
12	**Enable**	Set the checkbox	Enables the automatic adjustment of audio signal gain	Boolean type	Clear	Set—automatic adjustment of audio signal gain is enable Clear—automatic adjustment of audio signal gain is disabled
13	**Dynamic range**	Set the slider into the required position	Set the level of audio signal power after the automatic adjustment	Sound power in decibels (dB)	0	From 0 to 45
14	**Time constant**	Set the slider into the required position	Sets the time period, during which the audio signal is brought to the set power level with automatic adjustment	Time in seconds (s)	3	From 0.1 to 6
The **Audio trigger** group						
15	**Audio trigger level**	Set the slider into the required position	Sets the level of the sound power, above which the recording of the audio signal (registration of alarm) starts automatically	Sound power in standard units	-45	-45—audio trigger is off From -44 to 0—audio trigger is on
16	**Audio trigger delay**	Set the slider into the required position	Sets the time period, during which the audio signal is post-recorded after the end of the alarm event	Time in seconds (s)	3	From 1 to 16
The **Multicast** group						
17	**IP**	Enter the value into the field	Sets the IP address from which the client will receive the audio data from the ONVIF Server in the **Multicast** mode	IP address	224.0.0.10	224.0.0.0 - 239.255.255.255
18	**Port**	Enter the value into the field	Sets the port for transmitting the audio data in the **Multicast** mode	Sequence of numbers	Depends on the number of cameras and streams in the system	Any valid unused port numbers. The number of ports is determined by the system administrator

26.1.5.8.8 The Settings panel of the Telemetry Controller object

The **Telemetry Controller** object is used to register and configure in *Intellect* the serial (COM) ports used for connecting the PTZ devices.

The settings panel of the **Telemetry Controller** object is shown in the figure.

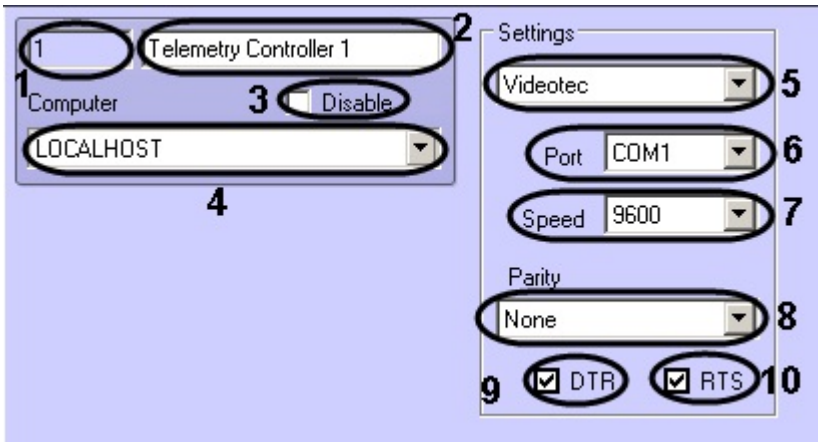


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Telemetry Controller** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Telemetry Controller** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Telemetry Controller** objects in the igital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Telemetry Controller** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic characters and service characters	Telemetry Controller No.	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters — from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Telemetry Controller** object (enabled or disabled) in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Telemetry Controller** object is disabled and isn't used Clear—the **Telemetry Controller** object is enabled and is used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Telemetry Controller** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital system with the distributed architecture
The **Settings** group						
5	Controller type*	Select the value from the list	Sets the data communication protocol with the PTZ device via the serial (COM) port. Data communication protocols are supplied by the PTZ devices manufacturers	Name of the PTZ devices integrated in the system	Videotec	Corresponds to the list of the PTZ devices integrated in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
6	**Port**	Select the value from the list	Sets the number of the computer COM port, used to connect the PTZ devices	List of the available COM ports	COM1	Depends on the number of COM ports on the Server or Remote Administrator's workstation. If a non-null value is selected, then the local COM port has a higher priority than other devices when processing the PTZ device commands. Otherwise, the COM port priority is set by default
7	**Speed**	Select the value from the list	Sets the data communication speed via the COM port	kB/s	9600	From 300 to 256000
8	**Parity**	Select the value from the list	Sets the parity check mode for the data transfer via the COM port	List of parity check names and modes	None	Even, Odd, None, Mark, Space
9	**DTR**	Set the checkbox	Sets the power supply to the PTZ device via the output of the DTR COM port	Boolean type	Set	Set—the power will be supplied via the DTR port output Clear—the power will not be supplied via the DTR port output
10	**RTS**	Set the checkbox	Sets the power supply to the PTZ device via the output of the RTS COM port	Boolean type	Set	Set—the power will be supplied via the RTS port output Clear—the power will not be supplied via the RTS port output

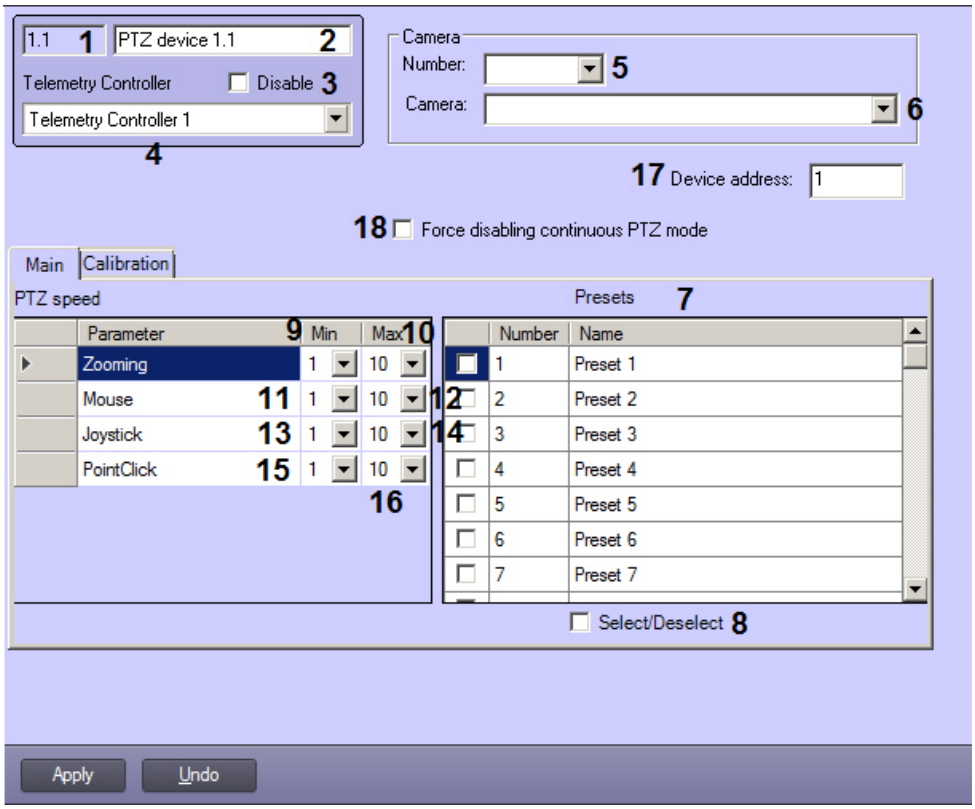
*Name of the element is not displayed in the settings panel of the given object.

26.1.5.8.9 The Settings panel of the PTZ device object

The **PTZ device** object is used to register and configure the PTZ device in *Intellect*.

The settings panel of the **PTZ device** object is shown in the figure.

The **Main** tab.



The **Calibration** tab.

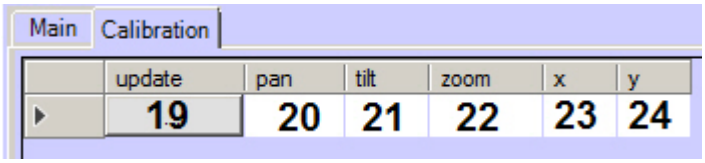


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **PTZ device** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **PTZ device** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **PTZ device** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **PTZ device** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic characters and service characters	PTZ device	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters — from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **PTZ device** object (enabled or disabled) in the digital video surveillance system	Boolean type	Clear	Set—the **PTZ device** object is disabled and isn't used Clear—the **PTZ device** object is enabled and is used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			with the distributed architecture			
4	**Telemetry Controller**	Select the value from the list	Sets the **Telemetry Controller** parent object of the digital system with the distributed architecture, to which the given **PTZ device** object belongs	Name of the **PTZ device** objects registered in the system	Name of the **Telemetry Controller** parent object	Depends on the number of the telemetry controllers in the digital system with the distributed architecture
The **Camera** group						
5	**Number**	Select the value from the list	Set the identification number of the video camera, where the PTZ device is installed	Sequence of numbers	Not defined	Depends on the number of video cameras in the digital video surveillance system with the distributed architecture
6	**Camera**	Select the value from the list	Matches the PTZ device with the video camera, where it is installed. The parameter is used by the **Video surveillance monitor** and the **Telemetry panel** to control the PTZ devices of the video cameras	Name of the **Camera** objects registered in the system	No	Depends on the number of the **Camera** objects in the digital video surveillance system with the distributed architecture
7	**Presets**	Set the checkbox	Selects the presets that should be displayed in the **Telemetry control panel**	Boolean type	Clear	Up to 355 presets can be enabled. The maximum number depends on the device, see Appendix 6. Maximum number of presets for IP devices. Set—the preset name is displayed in the **Telemetry control panel** Clear—the preset name isn't displayed in the **Telemetry control panel**
	Name	Enter the value into the field	Sets the preset name to display on the **Telemetry control panel**	Latin, Cyrillic characters and service characters	Preset	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive
8	**Select/Deselect**	Set the checkbox	Sets/clears the checkboxes next to all the elements in the **Presets** table	Boolean type	Clear	Set—select all presets Clear—deselect all presets
The **PTZ speed** group						
9	**Min**	Enter the value into the field	Sets the minimum possible speed of optical zoom on the PTZ device	Speed in standard units	0	1 – 10

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
10	**Max**	Enter the value into the field	Sets the maximum possible speed of optical zoom on the PTZ device	Speed in standard units	0	1 – 10
The **Mouse** group						
11	**Min**	Enter the value into the field	Sets the minimum possible rotation speed of the PTZ devices from the **Video surveillance monitor**	Speed in standard units	0	1 – 10
12	**Max**	Enter the value into the field	Sets the maximum possible rotation speed of the PTZ devices from the **Video surveillance monitor**	Speed in standard units	0	1 – 10
The **Joystick** group						
13	**Min**	Enter the value into the field	Sets the minimum possible rotation speed of the PTZ devices using the joystick	Speed in standard units	0	1 – 10
14	**Max**	Enter the value into the field	Sets the maximum possible rotation speed of the PTZ devices using the joystick	Speed in standard units	0	1 – 10
The **Point&Click** group						
15	**Min**	Enter the value into the field	Sets minimum possible rotation speed of the PTZ device in the direction of the mouse click (Point&Click)	Speed in standard units	0	1 – 10
16	**Max**	Enter the value into the field	Sets maximum possible rotation speed of the PTZ device in the direction of the mouse click (Point&Click)	Speed in standard units	0	1 – 10
Not in the groups						
17	**Device address**	Enter the value into the field	Sets the address of the PTZ device installed via hardware (with jumpers on the PTZ device board) or software (with a special software for the PTZ devices firmware upgrade)	Sequence of numbers	1	Integer from 1 to 255. Depends on the PTZ device protocol
18	**Force disabling continuous PTZ mode**	Set the checkbox	Sets the PTZ control mode: continuous or discrete	Boolean type	0	0—the continuous PTZ control mode is enabled

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						1—the discrete PTZ control mode is enabled
The **Calibration** tab						
19	**update**	Click the button	Gets data on the current camera position and display them in the **pan, tilt, zoom** fields	-	-	-
20	**pan**	Automatically on clicking the **update** button	Panoraming of the PTZ device	Integer	-	Depends on the model of the connected PTZ device
21	**tilt**	Automatically on clicking the **update** button	Tilt of the PTZ device	Integer	-	Depends on the model of the connected PTZ device
22	**zoom**	Automatically on clicking the **update** button	Scaling (zooming) of the PTZ device	Sequence of numbers	-	Depends on the model of the connected PTZ device
23	**x**	Enter the value into the field	The X coordinate of the point on the map corresponding to the selected position of the camera		-	Depends on the map size
24	**y**	Enter the value into the field	The Y coordinate of the point on the map corresponding to the selected position of the camera		-	Depends on the map size

*Name of the element is not displayed in the settings panel of the given object.

26.1.5.8.10 The Settings panel of the Control panel object

The **Control panel** object is used to register and configure a specialized control panel used to manage the PTZ devices in *Intellect*.

The settings panel of the **Control panel** object is shown in the figure.

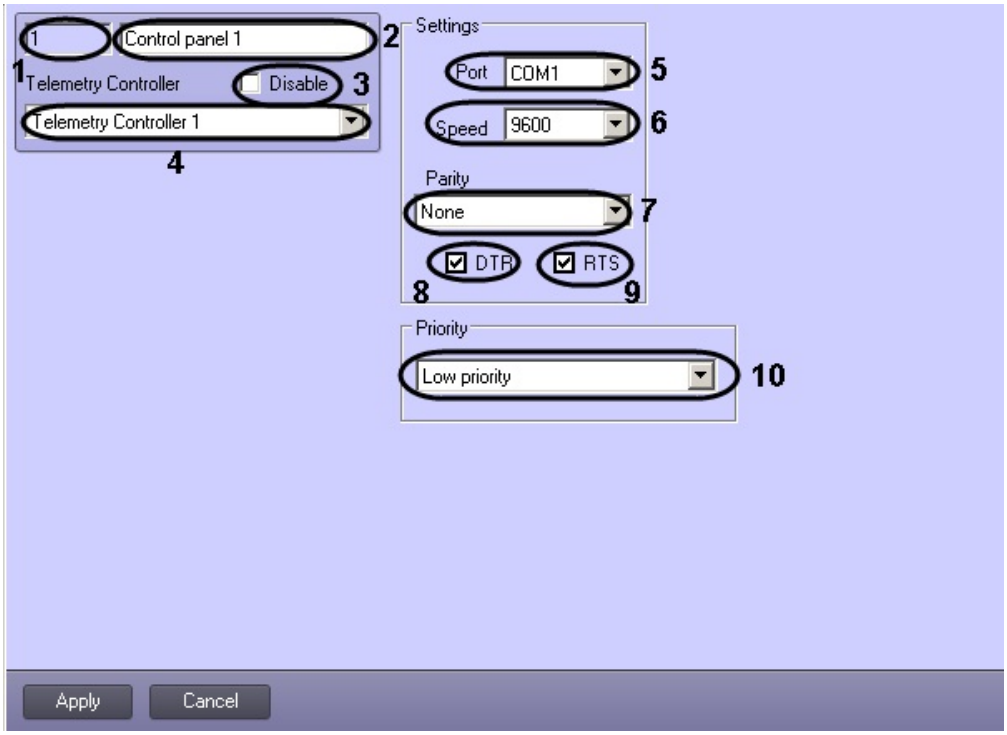


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Control panel** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Control panel** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Control panel** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Control panel** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic characters and service characters	Control panel	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters — from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Control panel** object (enabled or disabled) in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Control panel** object is disabled and isn't used Clear—the **Control panel** object is enabled and is used
4	**Telemetry Controller**	Select the value from the list	Sets the **Telemetry Controller** parent object of the digital system with the distributed architecture, to which the given **Control panel** object belongs	Name of the **Telemetry Controller** objects registered in the system	Name of the **Telemetry Controller** parent object	Depends on the number of telemetry controllers in the digital video surveillance system with the distributed architecture
The **Settings** group						

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
5	**Port**	Select the value from the list	Sets the number of the computer serial (COM) port used to connect the **Control panel**	List of available COM ports	COM1	Depends on the number of COM ports on the Server or Remote Administrator's workstation
6	**Speed**	Select the value from the list	Sets the data communication speed of the serial (COM) port	Kb/s	9600	From 300 to 256000
7	**Parity**	Select the value from the list	Sets the parity check mode for the data transmission over the serial (COM) port	List of the parity check modes	None	Even, Odd, None, Mark, Space
8	**DTR**	Set the checkbox	Sets whether or not the power should be supplied to the **Control panel** via the output of the DTR serial (COM) port	Boolean type	Set	Set—the power will be supplied via the DTR port output Clear—the power will not be supplied via the DTR port output
9	**RTS**	Set the checkbox	Sets whether or not power should be supplied to the Control panel via the output of the RTS serial (COM) port	Boolean type	Set	Set—the power will be supplied via the RTS port output Clear—the power will not be supplied via RTS port output
10	**Priority**	Select the value from the list	Sets the priority of the PTZ devices control using the **Control panel**	Names of priorities used to control the PTZ devices	Low	**Control prohibited**—the PTZ device cannot be controlled using the **Control panel** **Low**—the PTZ device can be controlled after it is controlled by the devices with the standard or high priority **Standard**—the PTZ device can be controlled after it is controlled by the device with the high priority **High**—the PTZ device is controlled first

*Name of the element is not displayed in the settings panel of the given object.

26.1.5.8.11 The Settings panel of the Backup archive object

The settings panel of the **Backup archive** object is shown in the figure.

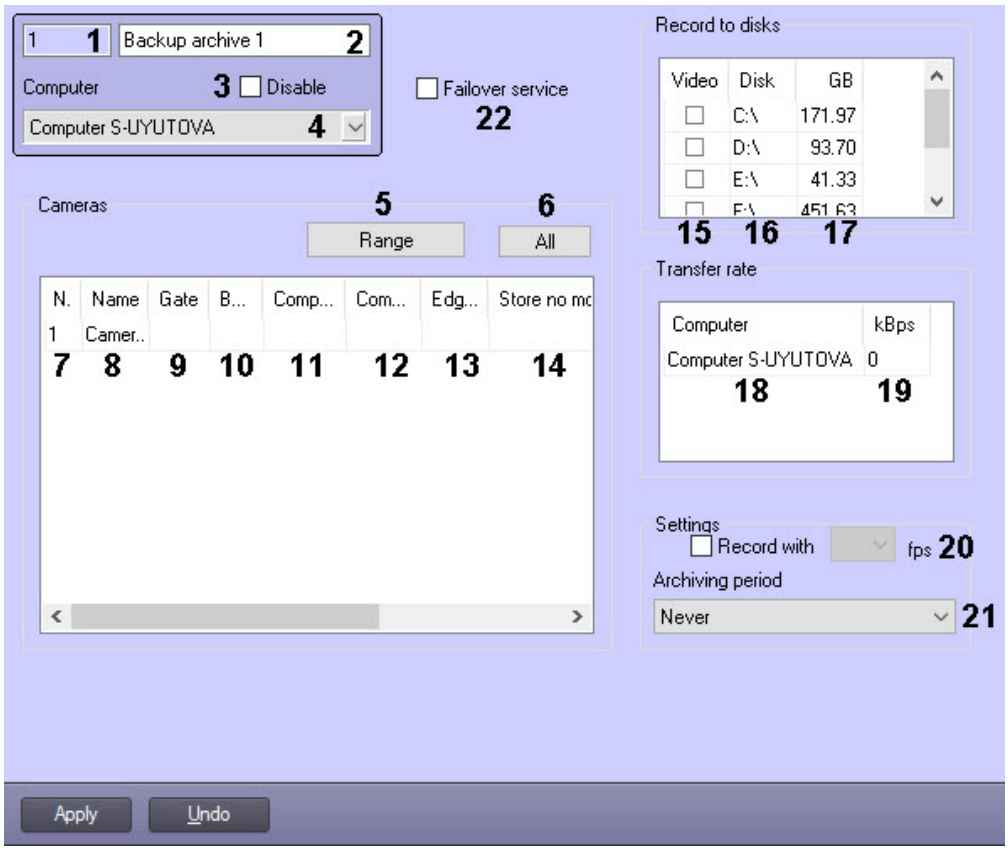


Table describes the setting parameters of the **Backup archive** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Backup archive** object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Backup archive** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Backup archive** object in the system	Latin, Cyrillic and service characters	Backup archive	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Backup archive** object (enabled or disabled) in the system	Boolean type	Clear	Set—the **Backup archive** object is disabled and isn't used Clear—the **Backup archive** object is enabled and is used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object for the given **Backup archive** object	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the system
The **Cameras** group						

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
5	**Range**	Click the button	Access to the complex selection of video cameras for copying the video archive to the **Backup archive**	-	-	-
6	**All**	Click the button	Selection of all cameras registered in the system for copying the video archive to the **Backup archive**	-	-	-
7	**Number**	Select the value from the list	Sets the number of the camera for copying the video archive to the **Backup archive**	Sequence of numbers	-	Depends on the number of the cameras registered in the system
8	**Camera**	Select the value from the list	Sets the name of the camera for copying the video archive to the **Backup archive**	Names of the cameras registered in the system	-	Depends on the number of the cameras registered in the system
9	**Gate**	Select the value from the list	Sets the **Videogate** object through which the video archive from the selected camera is transferred to the **Backup archive**	Names of the **Videogate** objects registered in the system	-	Depends on the number of the **Videogate** objects registered in the system
10	**Backup archive**	Select the value from the list	Sets the **Backup archive** object which transfers the video archive from the selected camera to the given **Backup archive**	Names of the B**ackup archive** objects registered in the system	-	Depends on the number of **Backup archive** objects registered in the system
11	**Compression**	Select the value from the list	Sets the level of the video signal compression to write to the **Backup archive**	Sequence of numbers	-	In order of increasing the compression level 0, 1, 2, 3, 4, 5 0—no compression 5—maximum compression
12	**Compressor**	Select the value from the list	Sets the algorithm of the video stream compression used for the video signal recompression when writing to the **Backup archive**. If the compressor is specified, the value should be selected in the **Compression** list	List of available algorithms	-	MJPEG, Motion Wavelet 3.5, MPEG4
13	**External storage**	Select the value from the list	Set the **External storage** object used for the archive import from the external storage of the IP device	Names of the **External storage** objects registered in the system	-	Depends on the number of the **External storage** objects registered in the system
14	**Store no more than (hours)**	Enter the value into the field	Sets the time period in hours after which the records should be deleted from the **Backup archive**	Non-negative integer	-	>0
The **Record to disks** group						
15	**Video**	Set the checkbox	Sets the disks to store the **Backup archive**	Boolean type	Clear	Set—the disk is used to store the **Backup archive**

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the disk isn't used to store the **Backup archive**
16	**Disk**	Automatically	Displays the names of the local (network, USB) disks, available for storing the **Backup archive**	Names of the available disks (Latin characters)	-	Depends on the total number of the available disks
17	**GB**	Automatically	Displays the amount of free space on each available disk	Disk space in GB	-	Depends on the amount free disk space
The **Transfer rate** group						
18	**Computer**	Automatically	Sets the list of computers from which the archive is transferred to the **Backup archive**	Names of the competers in the hardware tree	-	Depends on the number of the **Computer** objects created in the system and on the list of the cameras selected for transferring the archive
19	**kBps**	Enter the value into the field	Sets the maximum data transfer speed from this computer to the **Backup archive** via the LAN	kbyte/s	100	Depends on the bandwidth of the local network and resources of the computers 0—the video archive data transfer speed is unlimited
The **Settings** group						
20	**Record with**	Set the checkbox	Enables the decimation of the video archive for transferring it to the **Backup archive**	Boolean type	Clear	Set—the decimation is enabled Clear—the decimation is disabled
	Record with	Select the value from the list	Sets the frame rate of the video archive when decimating	Frame/s	-	1, 2, 3, 4, 6, 8, 12, 25
21	**Archiving period**	Select the value from the list	Sets the schedule of copying the video archive to the **Backup archive**	Name of the **Time schedule** objects registered in the system Never Always	Never	**Never**—video archive won't be copied to the **Backup archive** **Always**—video archive is always copied to the **Backup archive** **Connection lost**—the video archive is copied to the **Backup archive** from the external storage when the connection is restored **Time schedule**—video archive is copied to the **Backup archive** according to the time schedule
22	**Failover service**	Set the checkbox	Enables the cooperation of the **Backup archive** with the Failover service (see also	Boolean type	Clear	Set—the *Backup archive* module is used to synchronize the archives of

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			Configuring archive synchronization of main and backup Servers)			the main and backup Servers in the Failover mode Clear—the *Backup archive* module operates as usual

26.1.5.8.12 The Settings panel of the Keyboard object

The **Keyboard** object is used to register and configure a special keyboard in *Intellect*. The keyboard is used for the operational control of the major functions of the digital video surveillance system with the distributed architecture based on *Intellect*.

The settings panel of the **Keyboard** object is shown in the figure.

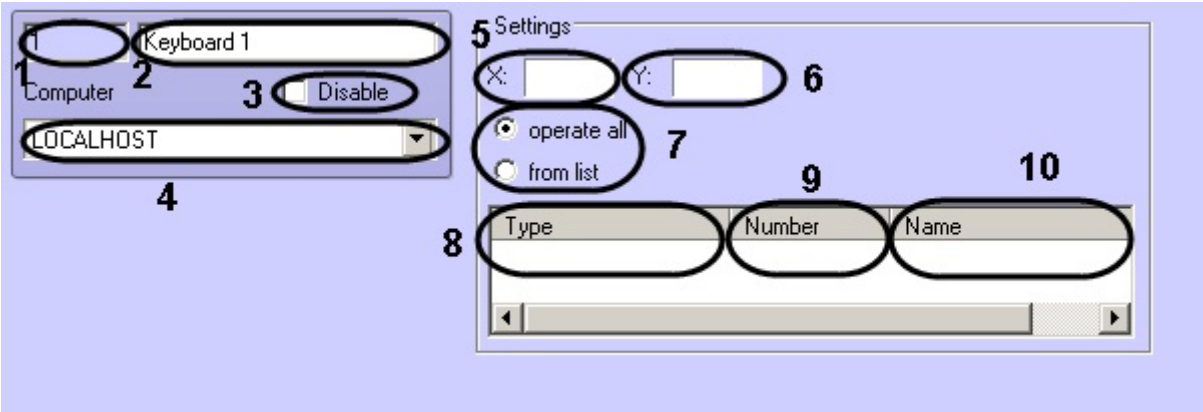


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Keyboard** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Keyboard** object in the digital video surveillance system with the distributed architecture	Sequence of numbers	-	From 1 and above. Depends on the number of the **Keyboard** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Keyboard** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Keyboard	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive Number of symbols – from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Keyboard** object (enabled or disabled) in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set – the **Keyboard** object is disabled and isn't used Clear – the **Keyboard** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the	Name of the **Computer** objects registered in the system	Name of the **Computer**	Depends on the number of the **Computer** objects in the digital video surveillance

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			given **Keyboard** object belongs		parent object	system with the distributed architecture
The **Settings** group						
5	**X**	Enter the value into the field	Sets the coordinate on the horizontal X axis of the upper left corner of the object selection window, to which the given command refers	% of the screen width	Not defined	From 0 to 100
6	**Y**	Enter the value into the field	Sets the coordinate on the vertical Y axis of the upper left corner of the object selection window, to which the given command refers	% of the screen height	Not defined	From 0 to 100
7	Control devices*	Set the required radio button	Sets the interface objects, which will be controlled using the **Keyboard**	Types of control devices	Operate all	**Operate all** – the Operator can control all interface objects according to the settings in the configuration file of the **Keyboard** **From list** – the Operator can control only those interface objects, which are sepcified in the list below
8	**Type**	Select the value from the list	Sets the type of the interface object, which can also be controlled using the **Keyboard**	Name of the object types registered in the system	Not defined	Depends on the number of the interface object types created in the digital video surveillance system with the distributed architecture
9	**Number**	Select the value from the list	Sets the identification number of the interface object, which can also be controlled using the **Keyboard**	Sequence of numbers	Not defined	Depends on the number of the created devices of the type selected in item 8 in the digital video surveillance system with the distributed architecture
10	**Name**	Automatically	Indicates the name of the device selected in item 9	Name of the objects of the selected type registered in the system	Not defined	Depends on the number of the created devices, of the type selected in item 8 in the digital video surveillance system with the distributed architecture

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.13 The Settings panel of the System restart service object

The settings panel of the **System restart service** object is shown in the figure.

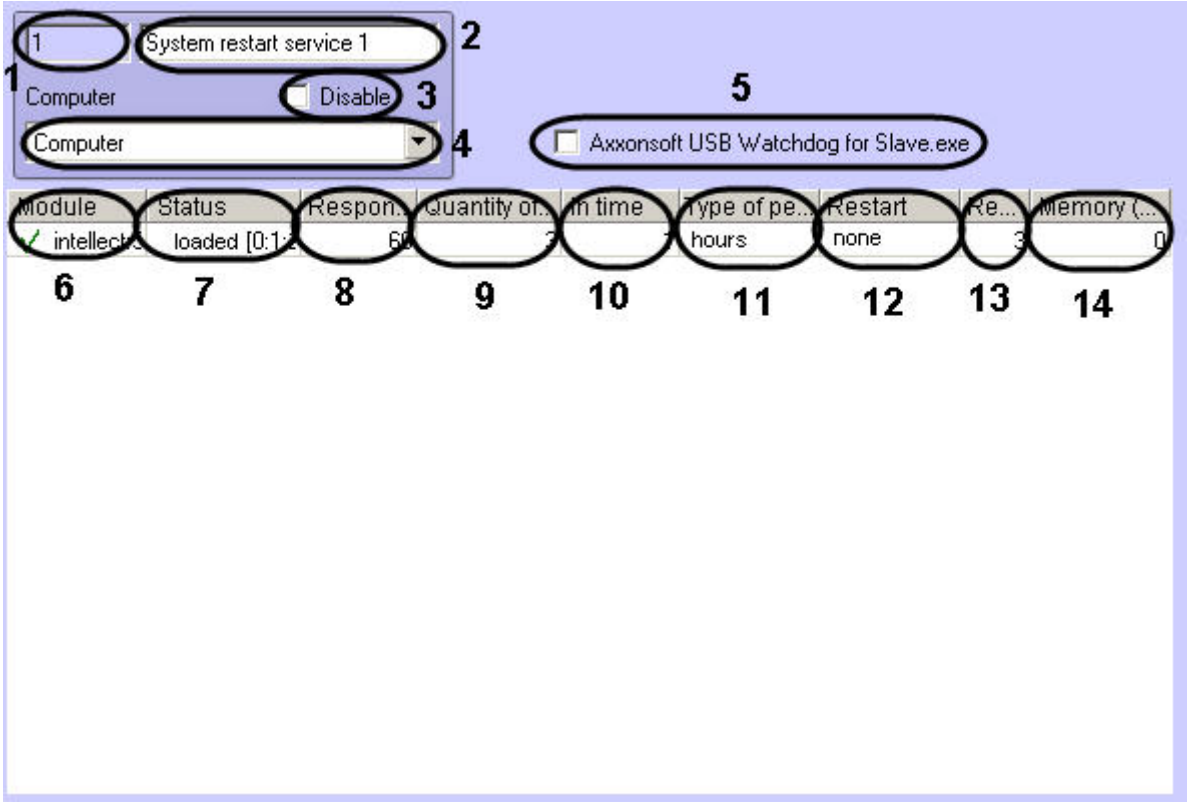


Table describes the setting parameters of the **System restart service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **System restart service** object in the system	Sequence of numbers	-	From 1 and above. Depends on the number of the **System restart service** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **System restart service** object in the system	Latin, Cyrillic and service characters	System restart service	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **System restart service** object in the system	Boolean type	Clear	Set—the **System restart service** object is disabled and isn't used Clear—the **System restart service** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object in the system, to which the given **System restart service** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Name of the **Computer** parent object (the **System restart service** object cannot be edited remotely)

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
5	**Axxonsoft USB Watchdog for Slave.exe**	Set the checkbox	Activates the system of the computer automatic restart when the slave.exe. process isn't active	Boolean type	Clear	Set—the system of automatic restart is activated Clear—the system of automatic restart is deactivated
Table of the performance monitoring of Intellect modules						
6	**Module**	Automatically	Displays the list of the modules running on the computer	Names of the running modules	-	Depends on the number of the modules registered in the system
7	**Status, hours**	Automatically	Displays the current state of the modules	Names of the current states of the modules	-	**loaded**—module runs **unloaded** (red field)—no response from the module after the waiting time expires **unloaded** (no coloring)—module is unloaded *Note. The time of the module run time since the last restart is displayed in the HH:MM:SS format in the square brackets*
8	**Response time, s**	Enter the value into the field	Sets the time interval in seconds of the module response time. If there is no response after the specified time, the system can be restarted	Non-negative integers	60	From 0 and above
9	**Quantity of restarts**	Enter the value into the field	Sets the maximal quantity of restarts for a period of time, specified in the **In time** and **Type of period** columns	Non-negative integers	3	From 0 and above
10	**In time**	Enter the value into the field	Set period of time during which the maximum quantity of the system restarts can be performed	Non-negative integers	1	From 0 and above
11	**Type of period**	Select the value from the list		Names of time period units	hours	**hours**—the time period is measured in hours **days**—the time period is measured in days
12	**Restart**	Select the value from the list	Sets the type of the system restart	Names of the possible types of restart	none	**none**—restart isn't performed **module**—module restart is performed **core**—*Intellect* core restart is performed
13	**Remains of restarts**	Automatically	Displays the quantity of the remaining restarts for the period specified in the **In time** and **Type of period** columns	Non-negative integers	-	Depends on the maximum quantity of restarts and on the number of restarts that were performed for a current time period

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
14	**Memory (Mb)**	Enter the value into the field	Sets the module memory consumption threshold above which the module should be restarted	Non-negative integers	0	From 0 and above

26.1.5.8.14 The Settings panel of the Voice notification service object

The **Voice notification service** object is used for the registration of the program module, which supports the voice notification of the security system operators upon occurrence of certain events.

The settings panel of the **Voice notification service** object is shown in the figure.

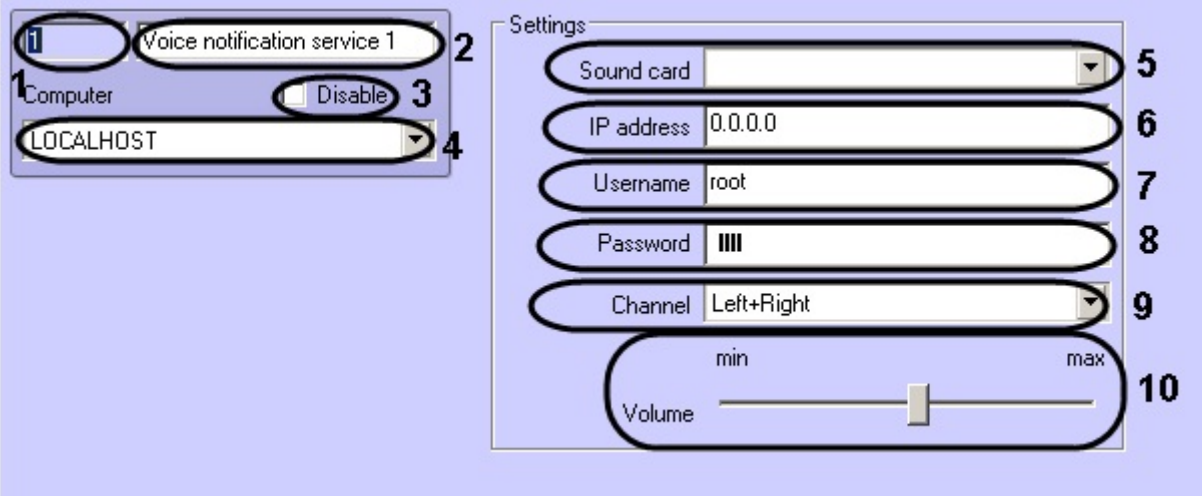


Table describes the setting parameters corresponding to the elements of the settings panel of the **Voice notification service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Voice notification service** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Voice notification service** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name to the **Voice notification service** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Voice notification service	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Voice notification service** object in the digital video surveillance	Boolean type	Clear	Set—the **Voice notification service** object is disabled and isn't used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			system with the distributed architecture			Clear—the **Voice notification service** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Voice notification service** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**Sound card**	Select the value from the list	Sets the device to which the audio signal is sent for processing during voice notification	Names of the types of the audio devices registered in the system	Name of the installed sound card	Name of the installed sound card—specifies the audio card on the Server or on the Remote Administrator's workstation, which processes the audio signal for the voice notification **LinuxHub**—specifies the LinuxHub type of the device on which the audio signal of the voice notification will be played back **Axis**—specifies the Axis type of the device on which the audio signal of the voice notification will be played back
6	**IP address**	Enter the value into the field	Sets the IP address of the LinuxHub and Axis devices. *Note. This field is active, if LinuxHub or Axis item was selected in the **Sound card** parameter*	Sequence of numbers	0.0.0.0	Expression like: xxx.xxx.xxx.xxx From 0.0.0.0 to 255.255.255.255 depending on the local network settings
7	**Username**	Enter the value into the field	Sets the username used to connect to the LinuxHub and Axis devices. *Note. This field is active, if LinuxHub or Axis item was selected in the **Sound card** parameter*	Latin characters, digits and service characters.	root	A line containing a sequence of any characters (letters, digits, service characters), case-sensitive. Number of characters—from 1 to 60
8	**Password**	Enter the value into the field	Sets the password used to connect to the LinuxHub and Axis devices. *Note. This field is active, if LinuxHub or Axis item was selected in the **Sound card** parameter*	Latin characters, digits and service characters.	root	A line containing a sequence of any characters (letters, digits, service characters), case-sensitive. Number of characters—from 1 to 60

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
9	**Channel**	Select the value from the list	Sets a channel in the Server sound card to playback the audio signal	Name of the audio channel to which the sound is transmitted	Left+Right	**Left+Right**—the sound notification signal is transmitted to both channels of the sound card **Left**—the sound notification signal is transmitted to the left channel of the sound card **Right**—the sound notification signal is transmitted to the right channel of the sound card
10	**Volume**	Set the slider into the required position.	Sets the volume of the audio signal, transmitted to the sound card. *Note. This parameter is active, if the sound card was selected in the **Sound card** parameter*	dB	24 dB	Min—0 Max—45

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.15 The Settings panel of the Voice Message Service object

The **Voice Message Service** is used for registration of the program module, which supports transmission of voice messages over the telephone lines. This service provides automatic redial of the specified telephone numbers and playback of the audio files.

The settings panel of the **Voice Message Service** object is shown in the figure.

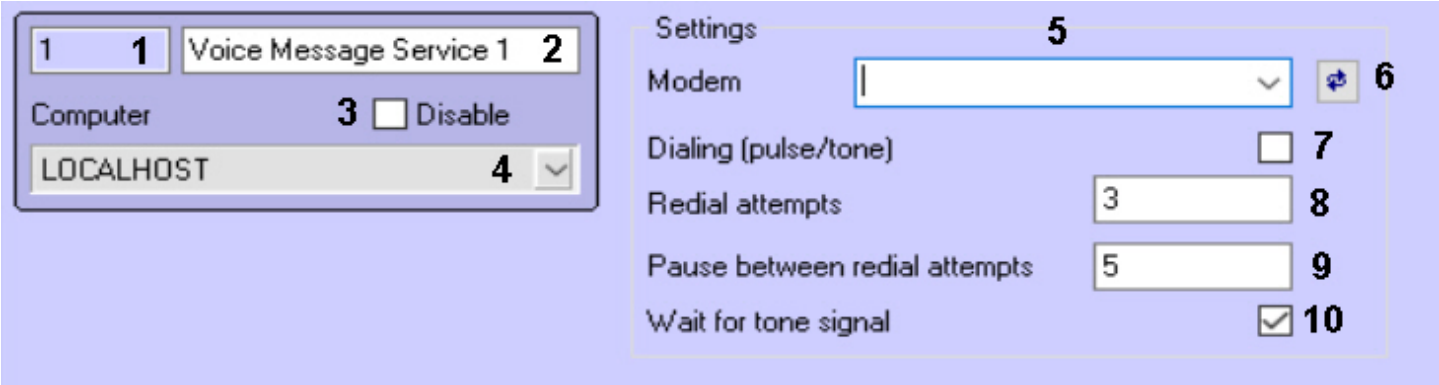


Table describes the setting parameters corresponding to the elements of the settings panel of the **Voice Message Service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Voice Message Service** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Voice Message Service** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Displays the name of the **Voice Message Service** object in the	Latin, Cyrillic and service characters	Voice Messages Service	A line containing a sequence of any characters (letters, digits, service

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			digital video surveillance system with the distributed architecture			characters except > and < characters), case-insensitive Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Voice Messages Service** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Voice Message Service** object is disabled and isn't used Clear—the **Voice Message Service** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Voice Message Service** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**Modem**	Select the value from the list	Sets the voice modem used for transmitting the voice messages	Name of the voice modem registered in Windows OS	Not defined	Depends on the number of the connected voice modems
6	**-**	Click the button	All connected devices are scanned to identify the voice modems and put them in the **Modem** list	-	-	-
7	**Dialing (pulse/ tone)**	Set the checkbox	Sets number dialling mode: pulse or tone	Boolean type	Clear	Set—tone dialling Clear—pulse dialling
8	**Redial attempts**	Enter the value into the field	Sets the maximum number of redial attempts to establish a connection	Sequence of numbers	5	From 1 to 10 (recommended—from 1 to 5)
9	**Pause between redial attempts**	Enter the value into the field	Sets a length of a pause between redial attempts	from	3	Recommended—from 30 to 120
10	**Wait for tone signal**	Set the checkbox	Enables the tone signal wait function before redialling the number	Boolean type	Set	Set—waiting for a tone signal before number redial is required Clear—waiting for a tone signal before number redial isn't required

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.16 The Settings panel of the Voice message object

The **Voice message** object is used to create a voice message that can be sent over the telephone lines.

The settings panel of the **Voice message** object is shown in the figure.

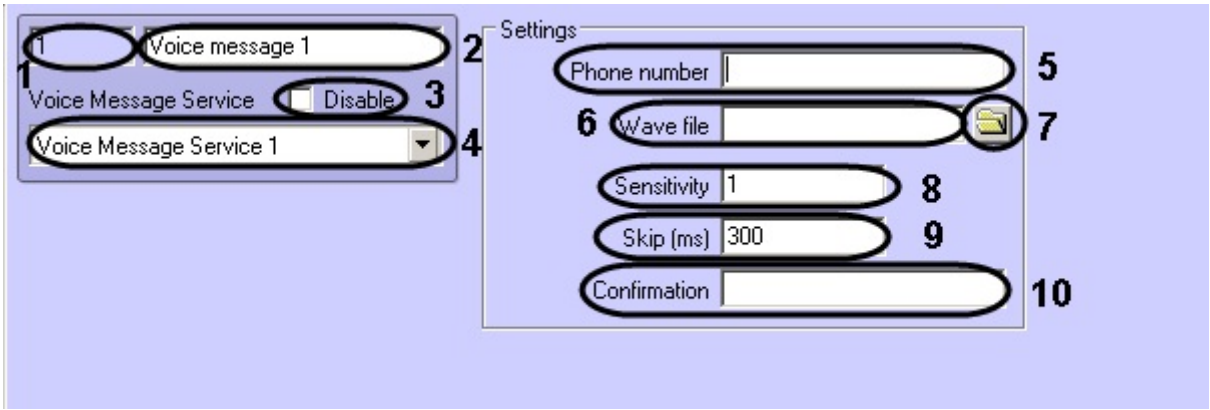


Table describes the setting parameters corresponding to the elements of the settings panel of the **Voice message** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Voice message** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Voice message** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Voice messages** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Voice message	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Voice message** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Voice messages** object is disabled and isn't used Clear—the **Voice message** object is enabled and used
4	**Voice Messages Service**	Select the value from the list	Sets the **Voice Messages Service** parent object of the digital system with the distributed architecture, to which the given **Voice message** object belongs	Name of the **Voice Messages Service** objects registered in the system	Name of the **Voice Messages Service** parent object	Depends on the number of the **Voice Message Service** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**Phone number**	Enter the value into the field	Sets the phone number of the voice message recipient	Sequence of numbers	Not defined	A line, containing a sequence of digits. Depends on the used voice modem
6	**Wave file**	Enter the value into the field	Sets the path to the audio file, which will be played back, when the recipient picks up the phone	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
7	**File picker**	Click the button	Sets the path to the audio file, which will be played back when the recipient picks up the phone, by selecting a file directly from the standard file selection menu	-	-	-
8	**Sensitivity**	Enter the value into the field	Sets the maximum noise level in the phone handset, which prevents false identification of the noise as a reply of the voice message recipient	Sequence of numbers	1	From 1 to 10
9	**Skip (ms)**	Enter the value into the field	Sets the delay time between redial attempts	ms	300	More than 1
10	**Confirmation**	Enter the value into the field	Sets a digital code, which the recipient should enter to confirm the voice message reception	Sequence of numbers	Not defined	A line, containing a sequence of digits. Number of characters—from 1 and above

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.17 The Settings panel of the Short Message Service object

The **Short Message Service** object is used to register and configure the program module, which supports the short message (SMS) transmission to mobile phones via cellular communication.

The settings panel of the **Short Message Service** object is shown in the figure.

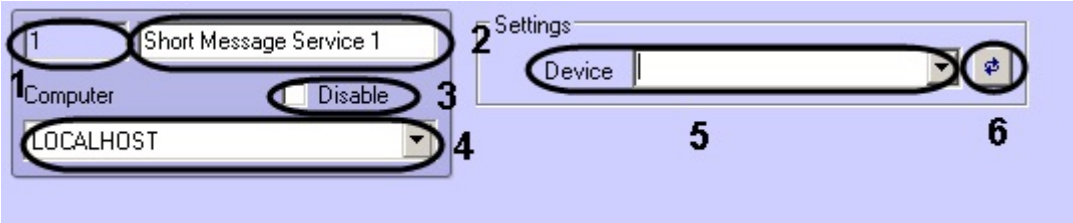


Table describes the setting parameters corresponding to the elements of the settings panel of the **Short Message Service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Short Message Service** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Short Message Service** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Short Message Service** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Short Message Service	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Short Message Service** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Short Message Service** object is disabled and isn't used Clear—the **Short message service** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Short Message Service** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object.	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**Device**	Select the value from the list	Sets the GSM device used to send short messages (SMS)	Names of the GSM devices registered in Windows OS	Not defined	Depends on the number of the connected GSM devices
6	Device picker*	Click the button	Scans the connected devices to find the GSM devices and put them on the **Devices** list	-	-	-

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.18 The Settings panel of the Short Message object

The **Short Message** object is used to create a short message (SMS) that can be sent to a mobile phone via cellular communication.

The settings panel of the **Short Message** object is shown in the figure.

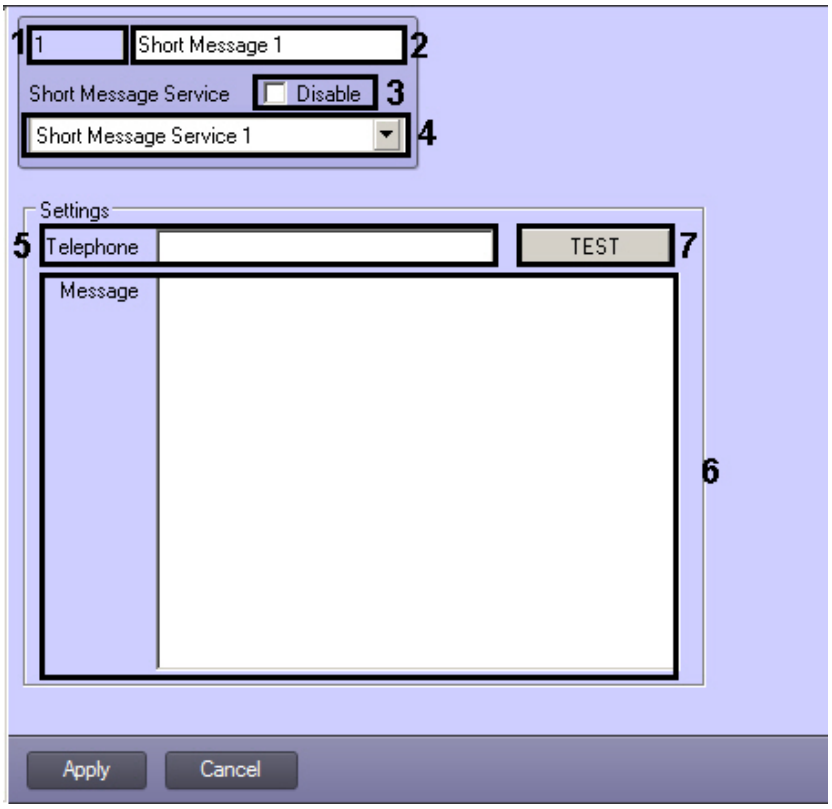


Table describes the setting parameters corresponding to the elements of the settings panel of the **Short Message** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Short Message** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Short Message** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Short Message** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Short Message	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Short Message** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Short Message** object is disabled and isn't used Clear—the **Short Message** object is enabled and used
4	**Short Message Service**	Select the value from the list	Sets the **Short Message Service** parent object of the digital system with the distributed architecture, to which the given **Short Message** object belongs	Name of the **Short Message Service** objects registered in the system	Name of the **Short Message Service** parent object	Depends on the number of the **Short Message Service** objects in the digital video surveillance system with the distributed architecture

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Settings** group						
5	**Telephone**	Enter the value into the field	Sets a mobile phone number of the short message (SMS) recipient	Sequence of numbers	Not defined	Number in the international format. Multiple numbers are listed separated by a semicolon. Example: +79061234567;+79271112233
6	**Message**	Enter the value into the field	Sets a text of the short message (SMS), which will be sent via cellular communication	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 60
7	**TEST**	Click the button	Forced sending of the short message to the specified number	-	-	-

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.19 The Settings panel of the Mail Message Service object

The **Mail Message Service** object is used to register the program module, which supports e-mail message transmission to the e-mail boxes of the remote system users.

The settings panel of the **Mail Message Service** object is shown in the figure.

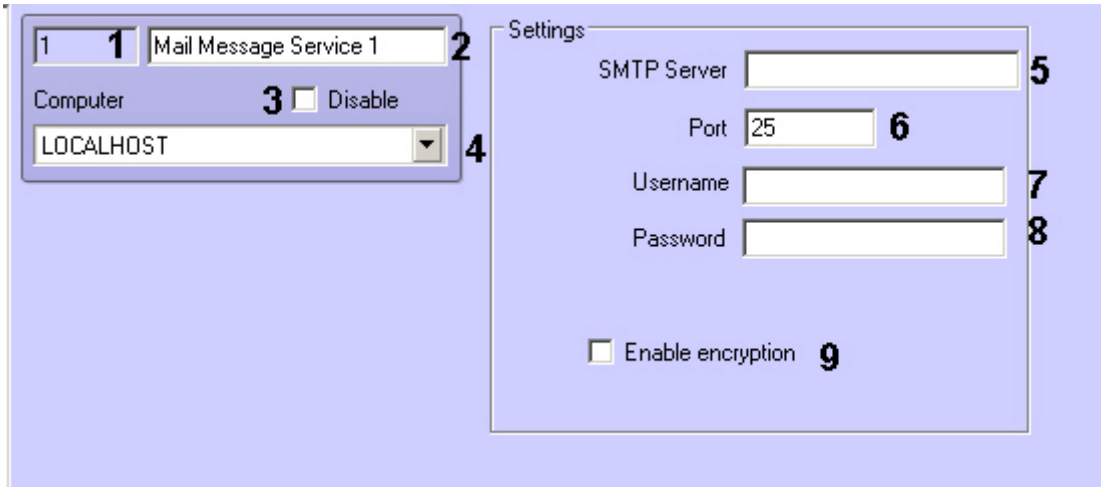


Table describes the setting parameters corresponding to the elements of the settings panel of the **Mail Message Service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Mail Message Service** object in the	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Mail Message Service** objects in the digital video

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			digital video surveillance system with the distributed architecture			surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Mail Message Service** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Mail Message Service	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Mail Message Service** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Mail Message Service** object is disabled and isn't used Clear—the **Mail Message Service** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Mail Message Service** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**SMTP Server**	Enter the value into the field	Sets the SMTP Server address used for sending the e-mail messages	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 100
6	**Port**	Enter the value into the field	Sets the number of the SMTP Server port used for sending the e-mail messages	Sequence of numbers	25	Determined by the system administrator
7	**Username**	Enter the value into the field.	Sets the username (login) for authorization on the SMTP Server. Username matches the unique name of the e-mail box on the mail server	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-sensitive. Number of characters—from 1 to 100
8	**Password**	Enter the value into the field.	Sets the password for authorization on the SMTP Server	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-sensitive. Number of characters—from 1 to 100
9	**Enable encryption**	Set the checkbox	Enables the TLS encryption	Boolean type	Clear	Set—encryption is enabled

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—encryption is disabled

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.20 The Settings panel of the Mail message object

The **Mail message** object is used to create an e-mail message that is sent to the e-mail boxes of the remote system users.

The settings panel of the **Mail message** object is shown in the figure.

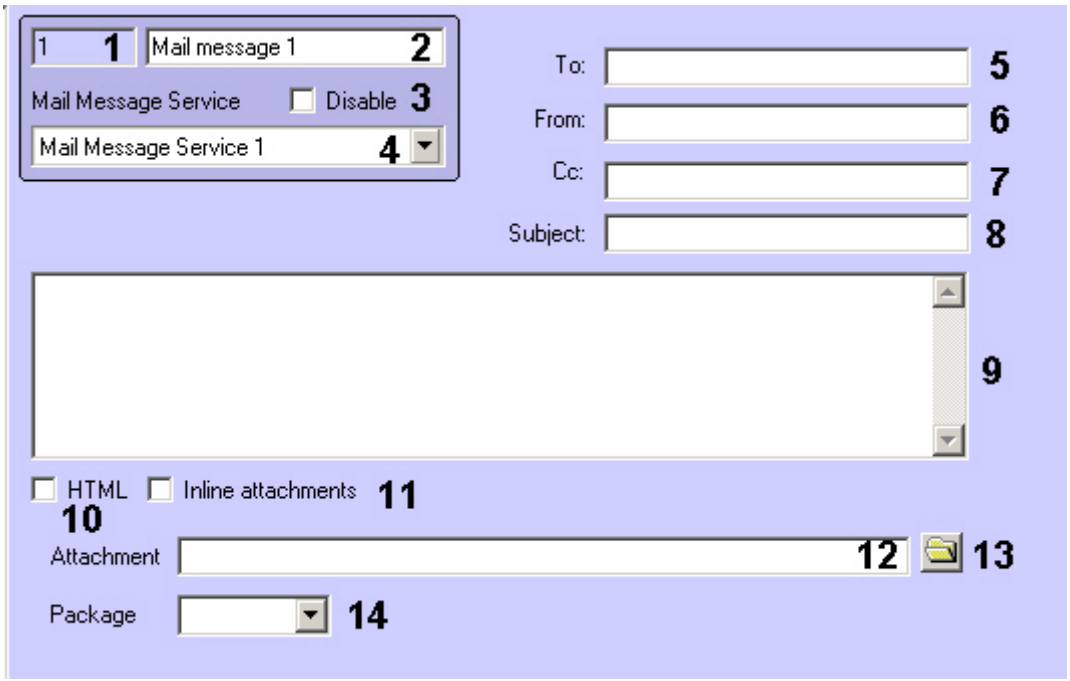


Table describes the setting parameters corresponding to the elements of the settings panel of the **Mail message** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Mail message** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Mail message** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Mail message** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Mail message	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Mail message** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Mail message** object is disabled and isn't used Clear—the **Mail message** object is enabled and used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Mail Message Service**	Select the value from the list	Sets the **Mail Message Service** parent object, to which the given **Mail message** object belongs	Name of the **Mail Message Service** objects registered in the system	Name of the **Mail Message Service** parent object	Depends on the number of the **Mail Message Service** objects in the digital video surveillance system with the distributed architecture
The **Settings** group						
5	**To**	Enter the value into the field	Sets the e-mail box address of the mail message recipient	Latin and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 30
6	**From**	Enter the value into the field	Sets the e-mail box address of the mail message sender	Latin and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 30
7	**Cc**	Enter the value into the field	Sets the e-mail box address of the mail message copy recipient	Latin and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 60. If you want to send the mail message copy to several e-mail addresses, enter the e-mail addresses separated by a comma
8	**Subject**	Enter the value into the field	Sets the subject of the mail message	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 60
9	Text message*	Enter the value into the field	Sets the text content of the mail message	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 250
10	**HTML**	Set the checkbox	Enables the HTML formatting in the mail message text	Boolean type	Clear	Set—the HTML formatting is applied Clear—the HTML tags are displayed as text
11	**Inline attachments**	Set the checkbox	Excludes the attachments from the **Attachment** section in the mail message. The attachments are displayed in the body of the mail message only	Boolean type	Clear	Set—the attachments are excluded from the **Attachment** section and displayed in the body of the mail message only (if mentioned) Clear—the attachments are included both in the body of the mail message (if mentioned) and

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						in the **Attachment** section of the mail message
12	**Attachment**	Enter the value into the field	Sets a path to the file, which will be attached to the mail message	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 250
13	File picker*	Click the button	Sets a path to the file, which will be attached to the mail message by selecting the file using the standard file selection menu	-	-	-
14	**Package**	Select the value from the list	Sets the compression format for archiving the file attached to the mail message	Names of the archive type	Empty field	Empty field—the file attached to the mail message is sent without compression GZIP—a file attached to the mail message is sent compressed in the gzip format

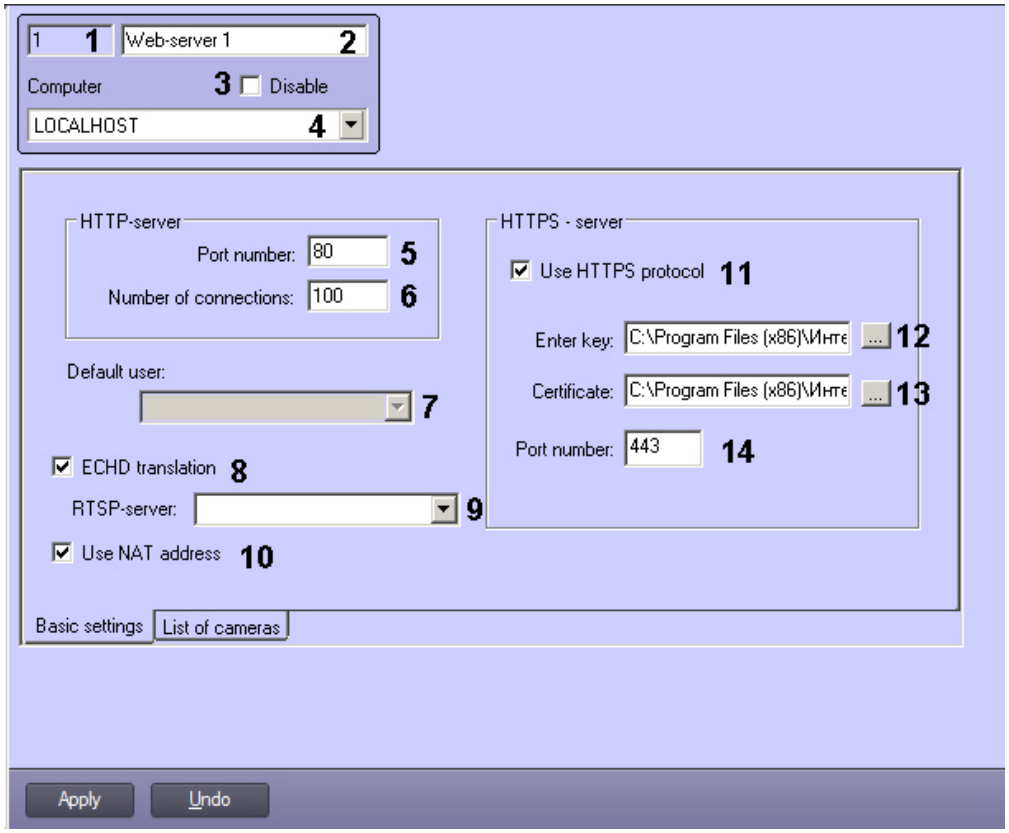
*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.21 The Settings panel of the Web-server object

The **Web-server** object is used for video surveillance via the Internet browser and the TCP/IP communication environment.

The settings panel of the **Web-server** object is shown in the figure.

The **Basic settings** tab.



The **List of cameras** tab.

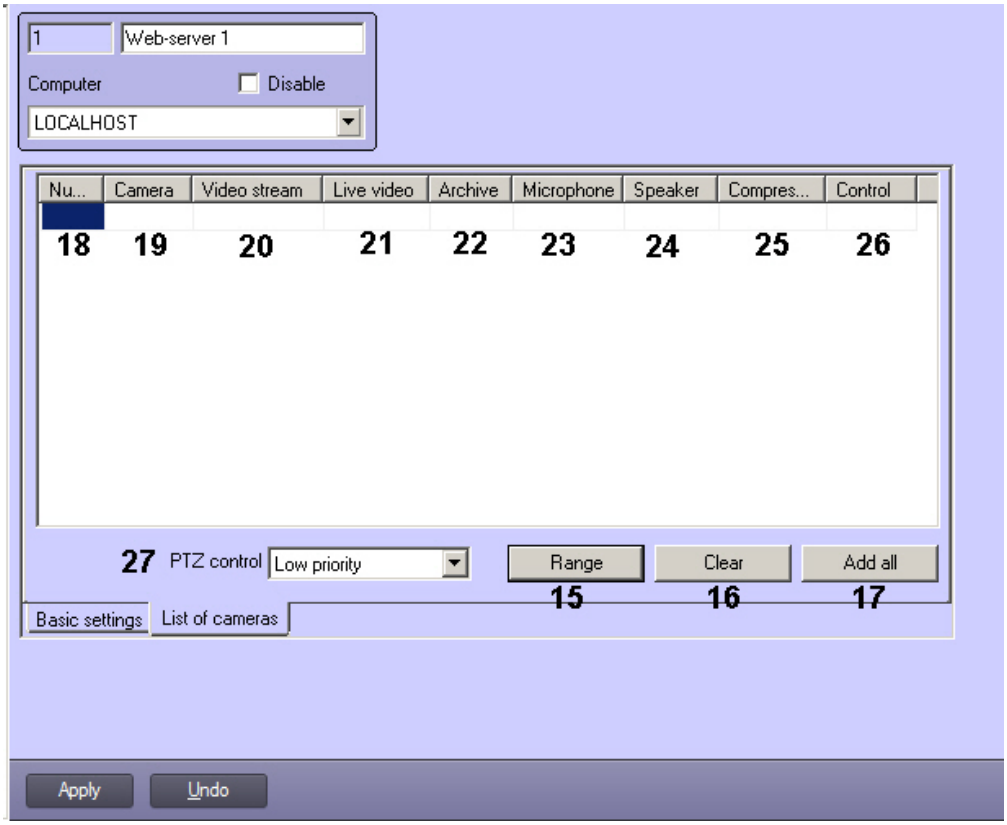


Table describes the setting parameters corresponding to the elements of the settings panel of the **Web-server** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Web-server** object in the digital video surveillance system with the distributed architecture	Sequence of numbers	-	From 1 and above. Depends on the number of the **Web-server** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Web-server** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Web-server	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Web-server** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Web-server** object is disabled and isn't used Clear—the **Web-server** object is enabled and used

4	**Compute r**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Web-server** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **HTTP-server** group						
5	**Port number**	Enter the value into the field	Sets the number of the port used by the HTTP-server (used for video surveillance via the Web-browser, including via the Internet)	Sequence of numbers	80	Any valid unused port numbers. The number of ports is determined by the system administrator.
6	**Number of connectio ns**	Enter the value into the field	Sets the maximum possible number of connections to the Server via the *Web-server* module. Each request to view the video signal from each camera and each request to control all PTZ devices regadless of their number is considered as a connection	pcs	100	Any integer. If 0 value is specified on the Video Monitor of the *Web-server* module, video signals won't be displayed
Not in a group						
7	**Default user**	Select the value from the list	Sets the user with rights and authority to conduct the video surveillance from the Remote workstation using the *Web-server* module	Names of the users registered in the system and added to the rights	Not defined	Depends on the number of the users registered in *Intellect*
8	**ECHD translatio n**	Set the checkbox	Enables to use the http requests used for integration with ECHD	Boolean type	Clear	Set—requests used for integration with ECHD are run for the **Camera** objects on the basis of which the **ECHD channel** objects are created Clear—requests used for integration with ECHD are not run
9	**RTSP-server**	Select the value from the list	Sets the RTSP server to process the ECHD requests	Names of the **RTSP-server** obje cts registered in the system	Not defined	Depends on the number of the **RTSP-server** objects in the digital video surveillance system with the distributed architecture
10	**Use NAT address**	Set the checkbox	Enables the router address substitution in the ECHD requests	Boolean type	Clear	Set—when requesting the URL of streams via the HTTP API, the IP address of the router specified in the settings panel of the **RTSP-Server** object is substituted in the response to the request Clear—when requesting the URL of streams via the HTTP API, the IP address of the Server in its local network is returned in response to the request

The **HTTPS-server** group						
11	**Use HTTPS protocol**	Set the checkbox	Enables the HTTPS protocol when transmitting data via the Web-server	Boolean type	Clear	Set—the HTTPS protocol is used Clear—the HTTPS protocol isn't used
12	**Enter key**	Enter the value into the field	Key for data transmission via the HTTPS protocol	Latin, Cyrillic and service characters	C:\Program Files (x86)\Intellect\Modules\SSL\ssl_internal.key	Depends on the location of data encryption key when transmitting data via the HTTPS protocol
13	**Certificate**	Enter the value into the field	Certificate for data transmission via the HTTPS protocol	Latin, Cyrillic and service characters	C:\Program Files (x86)\Intellect\Modules\SSL\ssl_internal.cert	Depends on the location of certificate file when transmitting data via the HTTPS protocol
14	**Port number**	Enter the value into the field	Sets the number of the port used for HTTPS-server (used for video surveillance in the web browser and in the Internet)	Sequence of numbers	443	Any available unused port numbers. The number of ports is specified by the system administrator
The **List of cameras** tab						
15	**Range**	Click the button	Opens the dialog box for complex selection of video cameras	-	-	-
16	**Clear**	Click the button	Clears the list of the added video cameras	-	-	-
17	**Add all**	Click the button	Adds to the list of video cameras all **Camera** objects created in the system	-	-	-
18	**Number**	Select the value from the list	Sets the number of the camera the video from which is transmitted to the remote workstation using the *Web-server* module	Identifiers of the **Camera** objects registered in the system	Not defined	Depends on the number of the video cameras in the digital video surveillance system with the distributed architecture
19	**Camera**	Select the value from the list	Sets the name of the camera the video from which is transmitted to the remote workstation using the *Web-server* module	Names of the **Camera** objects registered in the system	Not defined	Depends on the number of the cameras in the digital video surveillance system with the distributed architecture
20	**Video stream**	Select the value from the list	Sets the number of the video stream used for displaying in the Web-server interface	Numbers of video streams enabled on the camera and the By default value	By default	Depends on the number of the enabled streams on the camera
21	**Live video**	Select the value from the list	Sets the source of live video that is displayed in the Web-server interface	Available means to get live video	Server	**Server**—live video is received from the Server to which the camera is connected

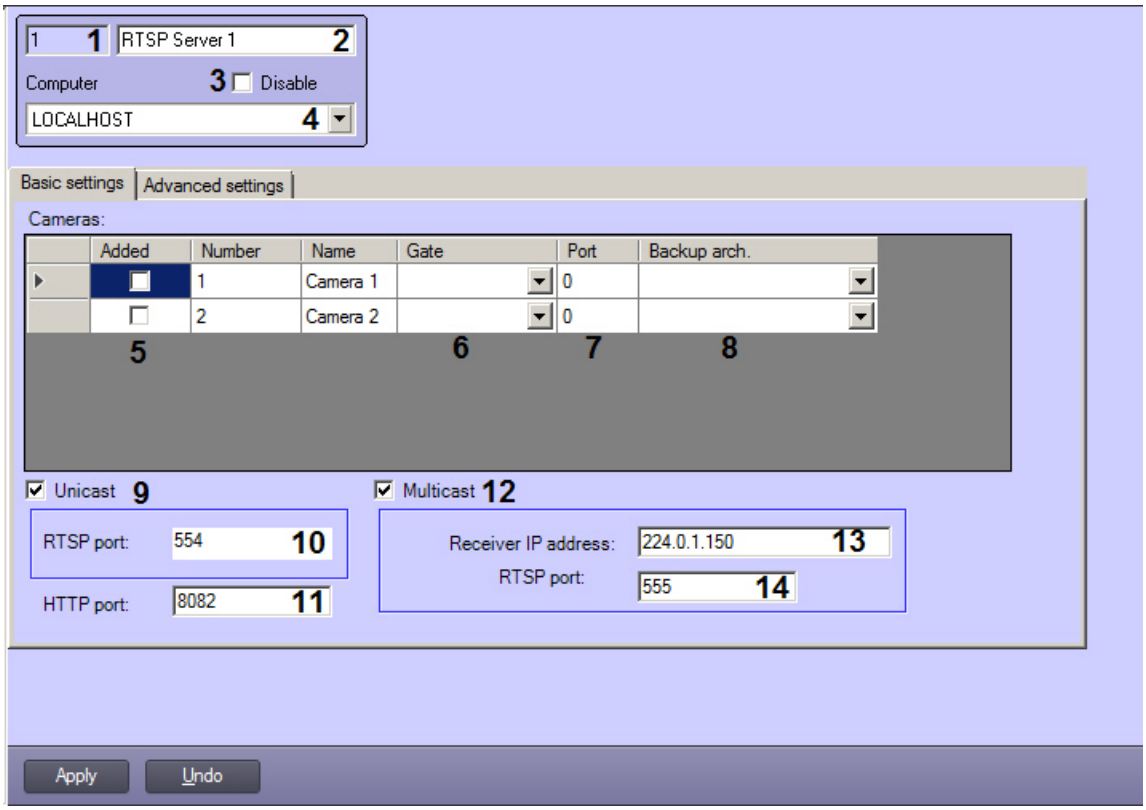
						Videogate—live video is received from the Videogate. If a camera is not configured to transmit video through the Videogate, then this item is unavailable in the list
22	**Archive**	Select the value from the list	Sets the source of the archive video that is displayed in the Web-server interface	Available means to get archive video	Server	**Server**—archive video is received from the Server to which the camera is connected **Videogate**—archive video is received from the Videogate. If a camera is not configured to transmit video through the Videogate, then this item is unavailable in the list. **Backup archive**—archive video is received from the Backup archive
23	**Microphone**	Select the value from the list	Sets the name of microphone associated with the camera, the sound from which will be transmitted through the Web-server	Names of the **Microphone** objects registered in the system	Not defined	Depends on the number of the **Microphone** objects in the digital video surveillance system with the distributed architecture
24	**Speaker**	Select the value from the list	Sets the name of the speaker associated with the camera which will be used to playback the sound received from the client	Names of the **Speaker** objects registered in the system	Not defined	Depends on the number of the **Speaker** objects in the digital video surveillance system with the distributed architecture
25	**Compression**	Select the value from the list	Sets the compression level of the video signal transmitted to the remote workstations using the *Web-server* module. Increasing the level of compression leads to deterioration of the video signal quality	Reference compression levels	Not defined	Not defined, 1 – 5. Value 1 corresponds to the minimum compression level, 5—to maximum compression level. If the compression level is not specified, video signal is transmitted with the same compression level as set for recording and transmitting video
26	**Control**	Select the value from the list	Sets the camera control (arm/disarm, PTZ, recording to the archive) according to the user rights	Boolean type	Enabled	Enabled—camera control according to the user rights is enabled Disabled—camera control is disabled regardless of the user rights
27	**PTZ control**	Select the value from the list	Set the prioritiy for the PTZ control in video surveillance using the web browser	Names of the PTZ control priorities	Low priority	**Forbidden**—option of the PTZ control in web browser is disabled **Low priority**—low priority of control **Medium priority**—medium priority of control **High priority**—high priority of control

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.22 The Settings panel of the RTSP Server object

The settings panel of the **RTSP Server** object is shown in the figure.

The **Basic settings** tab.

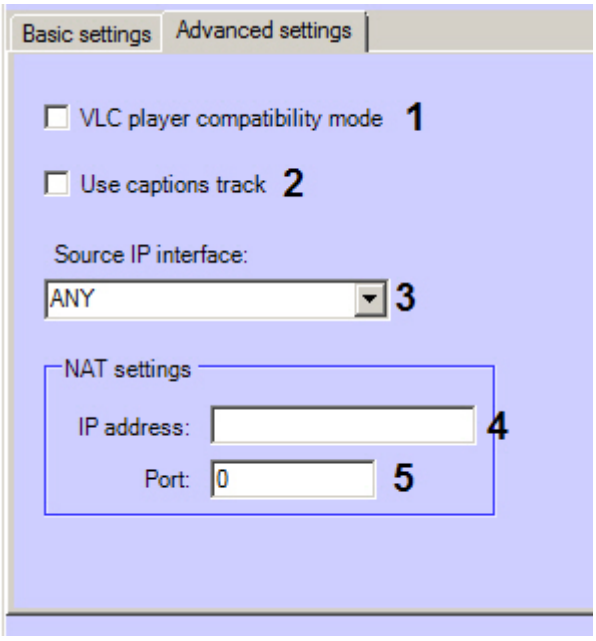


Tables describe the setting parameters of the **RTSP Server** system object.

№	Parameter	Method for setting the parameter value	Parameter description
1	Identification number*	Automatically	Displays the identification number of the **RTSP Server** object in the digital video surveilla
2	Name*	Enter the value into the field	Sets the name of the **RTSP Server** object in the digital video surveillance system
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **RTSP Server** object in the digital video surveill
4	**Computer**	Select the value from the list	Sets the **Computer** parent object to which the given **RTSP Server** object belongs
The **Basic settings** tab			
5	**Cameras**	Set the checkbox	Specifies the cameras the video signals from which should be transmitted to remote worl
6	**Gate**	Select the value from the list	Specifies the **Videogate** through which video is received from the camera

№	Parameter	Method for setting the parameter value	Parameter description
7	**Port**	Enter the value into the field	Sets the port via which a video signal from the camera will be transmitted. *Note. This column is available only if is the **Multicast** checkbox is set (12).* *Specified ports are not addressed directly. Use the RTSP port to get video from all cameras i*
8	**Backup arch.**	Select the value from the list	Specifies the **Backup archive** from which the archive is received for the camera
9	**Unicast**	Set the checkbox	Enables the "unicast" transmitting mode
10	**RTSP port**	Enter the value into the field	Sets the port via which the video signal will be transmitted
11	**HTTP port**	Enter the value into the field	Sets the port which should be used for transmitting the video signal via the http protocol
12	**Multicast**	Set the checkbox	Enables the video transmission via different RTSP ports. The **Multicast** mode allows reducing the Server load by reducing the amount of the trans
13	**Receiver IP address**	Enter the value into the field	Sets the IP address from which the video will be transmitted in the **Multicast** mode
14	**RTSP port**	Enter the value into the field	Sets the port number via which the video signal will be transmitted in the **Multicast** mod protocol, it is necessary to specify this port. The system forwards the request to the port

The **Advanced settings** tab.



№	Parameter	Method for setting the parameter value	Parameter description

1	**VLC player compatibility mode**	Set the checkbox	Enables sending the current time to VLC Media Player inste
2	**Use captions track**	Set the checkbox	Enables sending the video captions along with video image
3	**Source IP interface**	Select the value from the list	Sets the name of the network interface that should be usec
The **NAT settings** group			
4	**IP address**	Enter the value into the field	Sets the IP address of the router that performs the NAT tran
5	**Port**	Enter the value into the field	Sets the port of the router that performs the NAT transmiss

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.23 The Settings panel of the Operator query panel object

The **Operator query panel** object is used to perform user specified functions and contains a custom set of elements. The elements are configured by the *Intellect* administrator using the *ArpEdit* utility (see User's Manual for ArpEdit).

The settings panel of the **Operator query panel** object is shown in the figure.

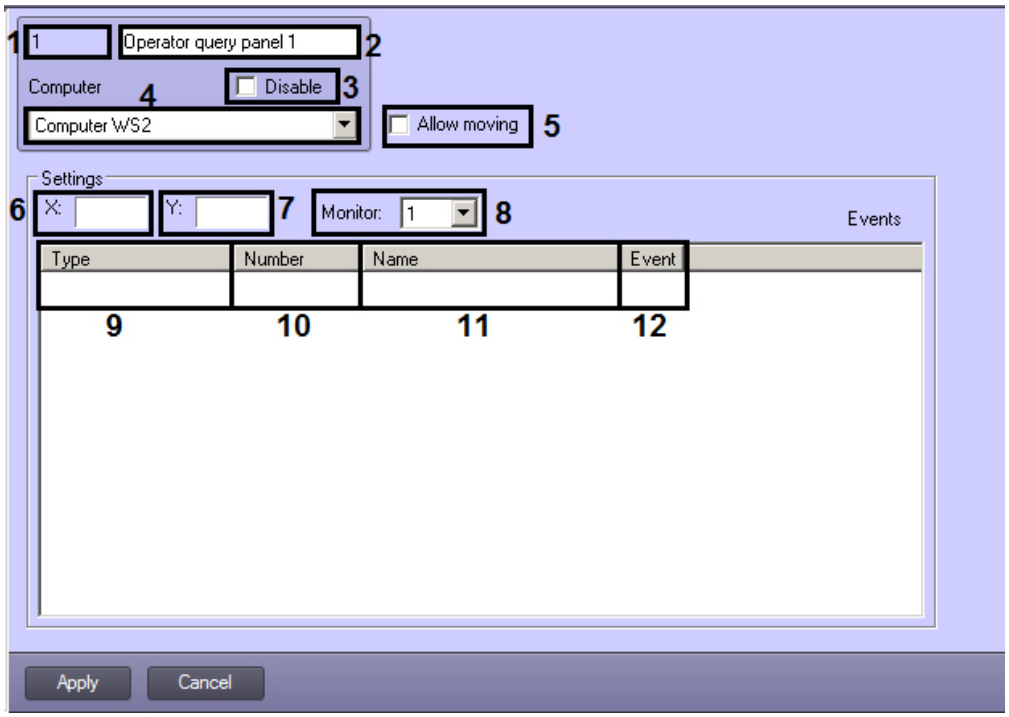


Table describes the setting parameters corresponding to the elements of the settings panel of the **Operator query panel** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identifier*	Enter the value into the field	File name used to control certain PTZ device. The file name is usually the same	Latin, Cyrillic and service characters	-	A line containing a sequence of characters (Latin and service characters, digits), case-insensitive.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			as the name of the PTZ device			Number of characters—from 1 to 16
2	Name*	Enter the value into the field	Sets the name of the **Operator query panel** object in the digital video surveillance system with the distributed architecture. The object name is usually the same as the name of the PTZ device	Latin, Cyrillic and service characters	Operator query panel	A line containing a sequence of characters (Latin and service characters, digits, except > and < characters), case-insensitive. Number of characters—from 1 to 16
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Operator query panel** object	Boolean type	Clear	Set—the **Operator query panel** object is disabled and isn't used Clear—the **Operator query panel** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Operator query panel** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
5	**Allow moving**	Set the checkbox	Allows moving the **Operator query panel** around the screen using the mouse	Boolean type	Clear	Set—moving is allowed Clear—moving isn't allowed
The **Settings** group						
6	**X**	Enter the value into the field	Sets the coordinate in the horizontal X axis of the upper left corner of the **Operator query panel** on the screen	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed Video Monitors
7	**Y**	Enter the value into the field	Sets the coordinate in the vertical Y axis of the upper left corner of the **Operator query panel** on the screen	% of the screen height	Not defined	From 0 to M*100, where M is the number of the installed Video Monitors
8	**Monitor**	Select the value from the list	Sets the number of the computer monitor for which the coordinates are set	Sequence of numbers	1	1–16
9	**Type**	Select the value from the list	Sets the object type that calls the **Operator query panel**	Types of the objects registered in the system	Not defined	Depends on the number of the object types created in the digital video surveillance system with the distributed architecture
10	**Number**	Select the value from the list	Sets the number of the object that calls the **Operator query panel**	Sequence of numbers	Not defined	Depends on the number of the objects created in the digital video surveillance

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						system with the distributed architecture
11	**Name**	Automatically	Sets the name of the object that calls the **Operator query panel**	Names of the objects of the selected type registered in the system	Not defined	Depends on the number of the objects types created n the digital video surveillance system with the distributed architecture
12	**Event**	Select the value from the list	Sets the name of the event that calls the **Operator query panel**	Names of the event types for the selected type of devices	Empty	Empty – the **Operator query panel** isn't called List of the available events depends on the selected object

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.24 The Settings panel of the Alarm Message Window object

The **Alarm Message Window** object is used to display an interface box with the text message about alarm events that were initiated by the *Intellect* digital video surveillance system.

The settings panel of the **Alarm Message Window** object is shown in the figure.

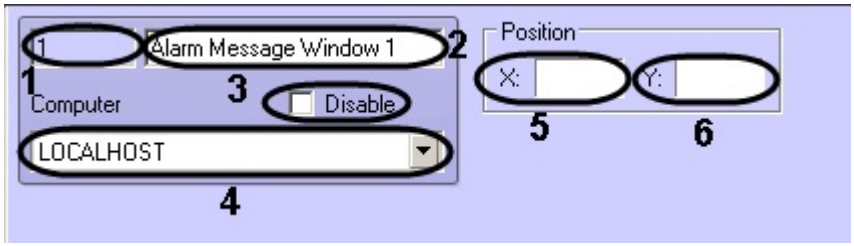


Table describes the setting parameters corresponding to the elements of the settings panel of the **Alarm Message Window** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Alarm Message Window** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Alarm Message Window** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Alarm Message Window** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Alarm Message Window	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Alarm Message Window** object in the digital video surveillance system with	Boolean type	Clear	Set—the **Alarm Message Window** object is disabled and isn't used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			the distributed architecture			Clear—the **Alarm Message Window** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Alarm Message Window** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
5	**X**	Enter the value into the field	Sets the coordinate in the horizontal X axis of the upper left corner of the **Alarm Message Window** on the screen	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed Video Monitors
6	**Y**	Enter the value into the field	Sets the coordinate in the vertical Y axis of the upper left corner of the **Alarm Message Window** on the screen	% of the screen height	Not defined	From 0 to M*100, where M is the number of the installed Video Monitors

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.25 The Settings panel of the Videogate object

The settings panel of the **Videogate** object is shown in the figure.

Table describes the setting parameters of the **Videogate** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Videogate** system object	Sequence of numbers	-	Depends on the number of the **Videogate** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Videogate** object in the system	Latin, Cyrillic and service characters	Videogate	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Videogate** object in the system	Boolean type	Clear	Set—the **Videogate** object is disabled and isn't used Clear—the **Videogate** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object for the given **Videogate** object	Name of the **Computer** objects	Name of the **Computer**	Depends on the number of the **Computer** objects in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
				registered in the system	parent object	
5	**All**	Click the button	Selects all video cameras registered in the system for transmitting the video signals through the Videogate	-	-	-
6	**Range**	Click the button	Gives the access to the complex selection of video cameras for transmitting video signals through the Videogate	-	-	-
7	**Number**	Select the value from the list	Sets the number of the video camera for transmitting video signals through the Videogate	Sequence of numbers	-	Depends on the number of the video cameras registered in the system
8	**Name**	Select the value from the list	Sets the name of the video camera for transmitting video signals through the Videogate	Names of the cameras registered in the system	-	Depends on the number of the video cameras registered in the system
9	**Stream for archive**	Select the value from the list	Set the video stream to record the archive of the *Videogate* module	Names of streams transmitted by the Server	-	Depends on the number of the video streams configured on the Server
10	**Compression**	Select the value from the list	Sets the level of video signal compression for transmitting through the Videogate. If the value is set, the additional consumption of the Server resources occurs	Sequence of numbers	-	In order of increasing the compression level 0, 1, 2, 3, 4, 5. 0—no compression 5—maximum compression
11	**Compressor**	Select the value from the list	Sets the algorithm to compress the video stream used to recompress the video signal when transmitted through the Videogate. If the compressor is specified, you should select the value in the **Compression** drop-down list	List of the available algorithms	-	MJPEG, Motion Wavelet 3.5, MPEG4. If the **Compression** level is specified, but the **Compressor** isn't selected, the Motion Wavelet algorithm is used
12	**fps**	Enter the value into the field	Sets the video signal frame rate for transmitting through the Videogate	Sequence of numbers	-	No more than the rate of the video signal digitizing by the video capture card. No less than 0.01
13	**Critical rate**	Enter the value into the field	Sets the minimum permissible rate of the video signal frames arrival to the Videogate to control the transmission of the video signal through the local network	Sequence of numbers	-	No more than the frame rate of the video signal that is transmitted to the Videogate
14	**Gate**	Select the value from the list	Sets the **Videogate** object from which the video signal from the selected camera has to be transmitted to the given Videogate. ***Attention!*** *The selected* ***Videogate*** *object must differ from the configured one, otherwise there will be no video transmission via the Videogate*	Names of the **Videogate** objects registered in the system	-	Depends on the number of the **Videogate** objects registered in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
15	**Backup archive**	Select the value from the list	Sets the **Backup archive** object, from which the archive from the selected camera has to be transmitted to the given **Videogate**	Names of the **Backup archive** objects registered in the system	-	Depends on the number of the **Backup archive** objects registered in the system
16	**Store no more than (hours)**	Enter the value into the field	Sets the time period in hours after which it is necessary to delete the recordings of the corresponding camera from the Videogate	Sequence of numbers	-	>0
17	**Video**	Set the checkbox	Sets the disk for storing the archive of the video signals, transmitted through the Videogate	Boolean type	Clear	Set—the disk is used for storing the archive of the *Videogate* module Clear—the disk isn't used for storing the archive of the *Videogate* module
18	**Disk**	Automatically	Displays the names of the local (network, USB) disks, available for storing the archive of the *Videogate* module	Names of the available disks (Latin characters)	-	Depends on the total number of the availabe disks
19	**GB**	Automatically	Displays the information about free space on every available disk	Disk space in GB	-	Depends on the amount of free disk space
20	**Constant recording**	Set the checkbox	Enables constant recording on all video cameras added to the Videogate	Boolean type	Clear	Set—constant recording is enabled on all video cameras added to the Videogate Clear—recording is enabled on the video cameras that are configured for recording on the Server
21	**Active cameras**	Set the checkbox	Enables recording only on the video cameras the video stream from which is requested and displayed on the **Video surveillance monitor**	Boolean type	Clear	Set—recording is enabled on the video cameras the video stream from which is requested (displayed) on the **Video surveillance monitor** Clear—recording is enabled on the video cameras that are configured for recording on the Server

26.1.5.8.26 The Settings panel of the Event counter object

The **Event counter** object is used to register and count events of a certain type, occurring at the specified objects and registered by *Intellect.*

The settings panel for the **Event counter** object is shown in the figure.

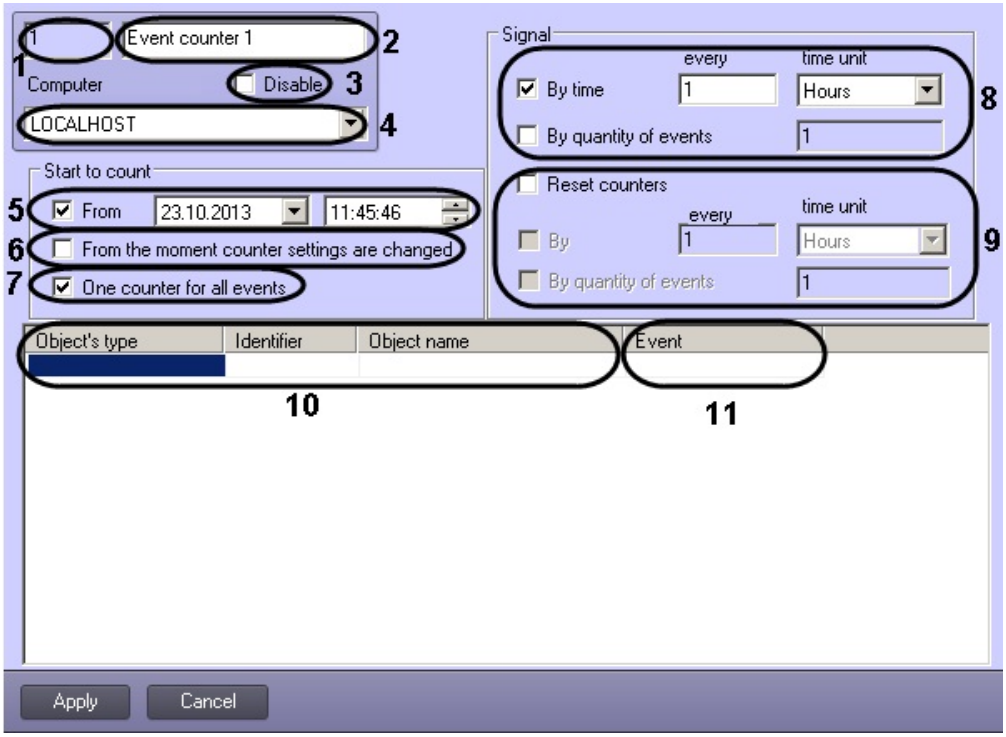


Table describes the setting parameters corresponding to the elements of the settings panel of the **Event counter** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Event counter** object in the digital video surveillance system with the distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Event counter** objects in the digital video surveillance system with the distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Event counter** object in the digital video surveillance system with the distributed architecture	Latin, Cyrillic and service characters	Event counter	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Event counter** object in the digital video surveillance system with the distributed architecture	Boolean type	Clear	Set—the **Event counter** object is disabled Clear—the **Event counter** object is enabled
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture, to which the given **Event counter** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Start to count** group						
5	**From** (activation)	Set the checkbox	Allows setting manually the date and time of the count start	Boolean type	Set	Set—the date and time of the count start are set manually

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the date and time of the count start are set at the date and time, when the **Event counter** object was last modified
	From (date)	Enter the value into the field or select the value from the drop-down list	Sets the date of the count start	DATE:MONTH:YEAR	Current system date	09.1752 – 12.9999
	From (time)	Enter the value into the field	Sets the time of the count start	HOURS:MINUTES:SECONDS	Current system time	00:00:0 – 23:59:59
6	**From the moment counter settings are changed**	Set the checkbox	Sets the date and time of the count start at the date and time, when the **Event counter** object was last modified	Boolean type	Clear	Set—the date and time of the count start are set at the date and time, when the **Event counter** object was last modified Clear—the date and time of the count start are set manually
7	**One counter for all events**	Set the checkbox	Sets the same counter for all events presented in the **Objects and events** group of the given **Event counter** object	Boolean type	Set	Set—only one counter will be used for counting all events specified in the **Objects** group Clear—different events are counted by different counters (each event is counted by a separate counter)
The **Signal** group						
8	**By time** (activation)	Set the checkbox	Enables regular notification in a set period of time	Boolean type	Set	Set—the notification by time is enabled Clear—the notification by time is disabled (notification by quantity of events is enabled)
	By time (every)	Enter the value into the field	Sets the notification period as a time interval. Notification is performed regardless of count start time at 00 minutes 00 seconds of every hour (or at 00 hours 00 minutes 00 seconds of every day, depending on the **time unit** settings)	Sequence of numbers	0	0 – 2147483648
	By time (time unit)	Select the value from the list	Sets a time unit for the notification	Line	Hours	Hours Days
	By quantity of events (activation)	Set the checkbox	Enables a regular notification about events starting from the set one	Boolean type	Clear	Set—the notification by quantity of events is enabled Clear—the notification by quantity of events is disabled (the notification by time is enabled)

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
	By quantity of events (quantity of events)	Enter the value into the field	Sets the number of event starting from which the notification will be performed. Example: if the parameter has the value 5, then notification will be performed by every event starting from 5 (5, 6, 7, 8, etc.)	Sequence of numbers	0	0 – 2147483648
The **Reset counters** group						
9	**By** (activation)	Set the checkbox	Enables a cyclic counter reset in a set time period	Boolean type	Set	Set—a cyclic reset in a set time period is enabled Clear—a cyclic reset in a set time period is disabled (By quantity of events (a cyclic reset by quantity of events is enabled)
	By (every)	Enter the value into the field	Sets a reset period as a time interval. Reset is performed regardless of the time of the count start at 00 minutes 00 seconds of every hour (or at 00 hours 00 minutes 00 seconds of every day, depending on the **time unit** settings)	Sequence of numbers	0	0 – 2147483648
	By (time unit)	Select the value from the list	Sets a time unit for the counters reset	Line	Hours	Hours Days
	By quantity of events (activation)	Set the checkbox	Enables a counter reset when it reaches a specified number of event	Boolean type	Clear	Set—a cyclic reset upon reaching a specified number of events is enabled Clear—a cyclic reset upon reaching a specified number of events is disabled (a cyclic reset by time is enabled)
	By quantity of events (quantity of events)	Enter the value into the field	Sets a reset period for counters by quantity of events	Sequence of numbers	0	0 – 2147483648
The **Objects and events** group						
10	**Object's type**	Select the value from the list	Sets the type of object for which the events are counted	Names of the types of objects registered in the system	Not set	Depends on the types of objects registered in the digital video surveillance system with the distributed architecture
	Identifier	Select the value from the list	Sets the identification number of an object of the selected type for which the events are counted	Sequence of numbers	Not set	Depends on the number of objects of the given type in the digital video surveillance system with the distributed architecture
	Object name	Automatically	Displays the identification number of the selected object	Latin, Cyrillic and	Not set	Object name with the specified identifier

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
				service characters		
11	**Event**	Select the value from the list	Sets an event that should be counted	Latin, Cyrillic and service characters	Not set	Depends on the types of objects registered in the digital video surveillance system with the distributed architecture

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.27 The Settings panel of the Data replication service object

The **Data replication service** object is used for archive replication on the unconnected Servers.

The settings panel of the **Data replication service** object is shown in the figure.

Table describes the setting parameters corresponding to the elements of the settings panel of the **Data replication service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Replicator's status**	Select the value from the list	Sets role of the Server in replication—whether it is a data source or a data receiver	Names of the existing roles in replication	Export	**Export**—Server is the source **Target**—Server is the data receiver
2	**Target disk**	Select the value from the list	Sets the removable storage used to move the data	Letters of the disks connected to the Server	-	Depends on the number of disks connected to the Server

26.1.5.8.28 The Settings panel of the Failover service object

The **Failover service** object is used to ensure the operation of the distributed system in the failover mode.

The settings panel of the **Failover service** object is shown in the figure.

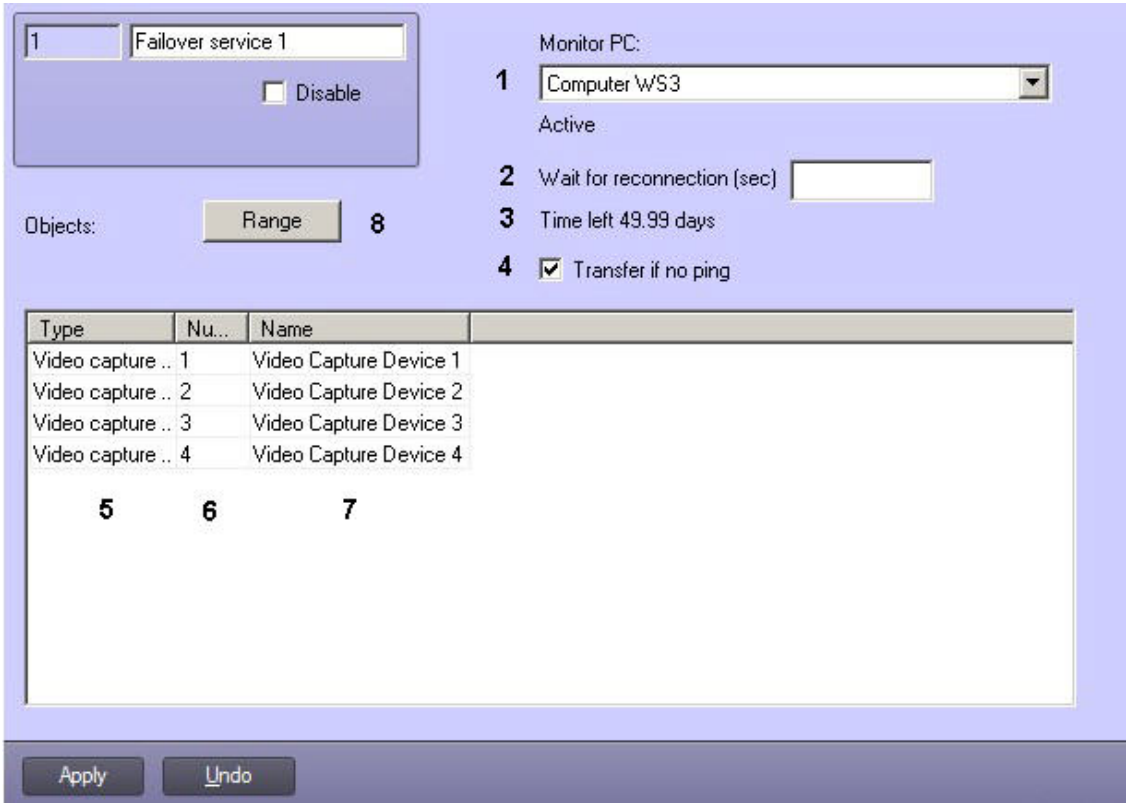


Table describes the setting parameters corresponding to the elements of the settings panel of the **Failover service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Monitor PC**	Select the value from the list	Sets the name of the Server the state of which will be monitored by the object	Names of the **Computer** objects registered in the system	-	Depends on the number of the **Computer** objects registered in the system
2	**Wait for reconnection (sec)**	Enter the value into the field	Sets the time period in seconds after which the configuration will be transferred to the backup Server after the loss of connection	Sequence of numbers	-	From 0 to 65535
3	**Time left __ days**	Automatically	Displays the period of time in days remaining to restore the configuration from the backup Server to the main Server and restore the license	Days	0.00	From 0.00 to 50.00
4	**Transfer if no ping**	Set the checkbox	Specifies if it is necessary to transfer the configuration without the ping from the main monitored Server	Boolean type	Clear	Set—the configuration is transferred if there is no ping Clear—ping isn't taken into account when transferring the configuration
5	**Type**	Select the value from the list	Sets the object type in the configuration of the monitored Server that should be transferred to the	Types of objects registered on the basis of the main Server	-	Depends on the configuration created on

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			backup Server in case of connection loss			the basis of the main Server
6	**Number**	Select the value from the list	Sets the identifier of the object of the selected type that should be transferred to the backup Server in case of connection loss	Identifiers of the objects of the selected type that are present in the configuration of the monitored Server	-	Depends on the number of the objects of the selected type in the configuration of main Server
7	**Name**	Automatically	Sets the name of the object that should be transferred to the backup Server in case of connection loss	Names of the objects of the selected type that are present in the configuration of the monitored Server	-	Depends on the configuration created on the basis of the main Server
8	**Range**	Click the button	Opens the dialog box for the complex selection of the monitored objects	-	-	-

26.1.5.8.29 The Settings panel of the Backup audio archive object

The settings panel of the **Backup audio archive** object is shown in the figure.

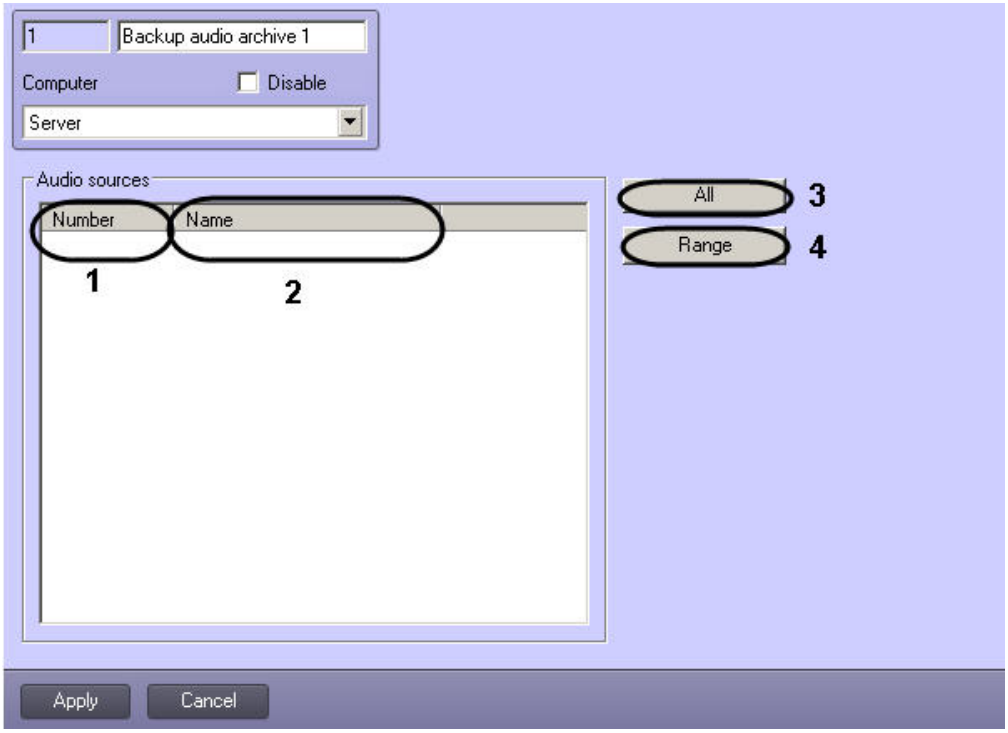


Table describes the setting parameters corresponding to the elements of the settings panel of the **Backup audio archive** object.

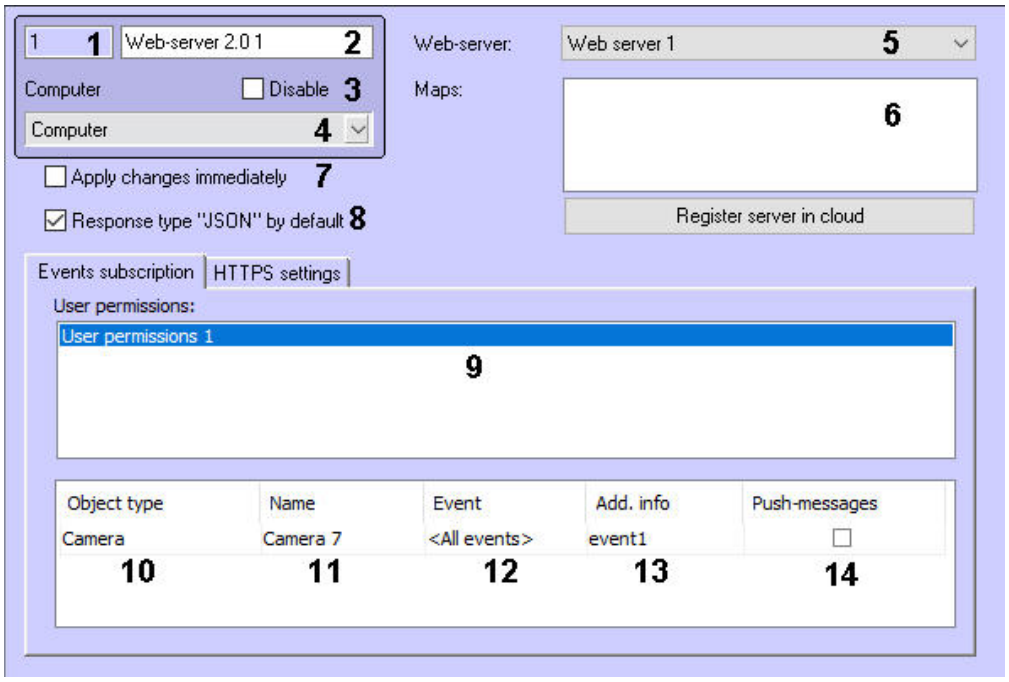
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Number**	Select the value from the list	Sets the number of the **Microphone** object to copy the video archive	Sequence of numbers	-	Depends on the number of the **Microphone** objects

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						registered in the system
2	**Name**	Automatically	Sets the name of the **Microphone** object to copy the video archive	Names of the **Microphone** objects registered in the system	-	Depends on the number of the **Microphone** objects registered in the system
3	**All**	Click the button	Adds all **Microphone** objects created in the system to the list	-	-	-
4	**Range**	Click the button	Opens the window for the complex adding of the microphones to the list of the **Backup audio archive**	-	-	-

26.1.5.8.30 The Settings panel of the Web-server 2.0 object

The settings panel of the **Web-server 2.0** system object is shown in the figures.

The **Events subscription** tab:



The **HTTPS settings** tab:

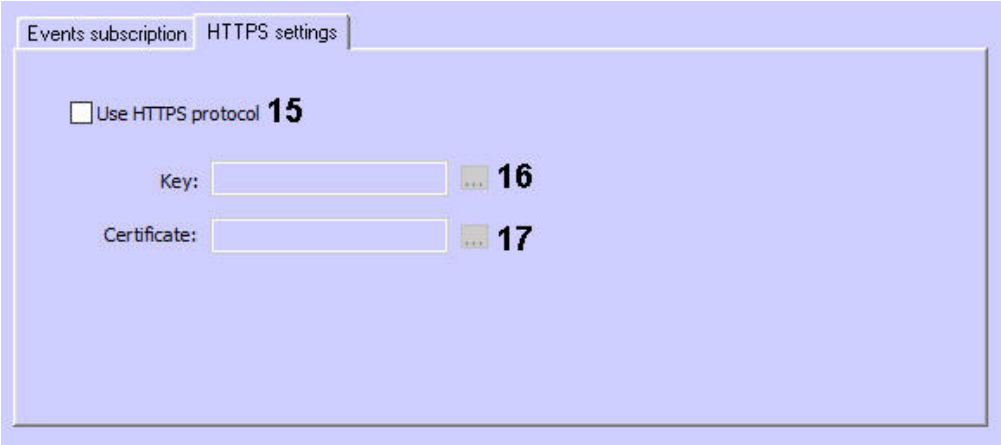


Table describes the setting parameters of the **Web-server 2.0** system object.

No.	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Web-server 2.0** system object in the system	Sequence of numbers	-	Depends on the number of the **Web-server 2.0** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Web-server 2.0** object in the system	Latin, Cyrillic and service characters	Web-server 2.0	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Web-server 2.0** object in the system	Boolean	Clear	Set—the **Web-server 2.0** object is disabled and isn't used Clear—the **Web-server 2.0** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object for the given **Web-server 2.0** object	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the system
5	**Web-server**	Select the value from the list	Sets the **Web-server** object whose settings will be used for the *Web-server 2.0* operation	Names of the **Web-server** objects registered in the system	-	Depends on the number of the **Web-server** objects registered in the system
6	**Maps**	Set the checkbox	Sets the list of Maps used by the *Web-server 2.0* module and available on the mobile clients	Names of the **Map** objects registered in the system	No maps is selected	Depends on the number of the **Map** objects registered in the system
7	**Apply changes immediately**	Set the checkbox	Enables the function to apply the changes to the user rights immediately	Boolean type	Clear	Set—the **Web-server 2.0** object will immediately apply the changes to the user rights

						Clear—when user rights are changed, access rights are not changed in the **Web-server 2.0** object until the **Apply** button is clicked on the settings panel of the **Web-server 2.0** object or *Intellect* is restarted
8	**Response type "JSON" by default**	Set the checkbox	Sets the default HTTP API response type	Boolean type	Clear	Set—the response is sent in the JSON format if the format is not specified explicitly in the request Clear—the response is sent in the XML format if the format is not specified explicitly in the request
9	**User permissions**	Select the value from the list	Sets the **User permissions** object for which the events filter is configured	Names of the **User permissions** objects registered in the system	-	Depends on the number of the **User permissions** objects registered in the system
10	**Object type**	Select the value from the list	Sets the type of objects the events from which are sent to the clients	Names of the types of objects registered in the system that are included in the selected user rights	-	Depends on the selected user rights
11	**Name**	Select the value from the list	Sets the name of object the events from which are sent to the clients	Names of the objects of the selected type that are registered in the system	-	Depends on the number of objects of the selected type that are registered in the system
12	**Event**	Select the value from the list	Sets the event type that should be sent to the clients	Names of the events that are available for the objects of the selected type	-	Depends on the selected object type
13	**Add. info**	Enter the value into the field	You can enter the additional information about the event that should be sent into the field	Latin, Cyrillic and service characters	-	-
14	**Push-messages**	Set the checkbox	Specifies whether to send push messages to the clients about the events of the selected type	Boolean	Clear	Set—push-messages are sent Clear—push-messages aren't sent
15	**Use HTTPS protocol**	Set the checkbox	Enables the use of the HTTPS protocol when transferring data via the Web-server 2.0	Boolean	Clear	Set—the HTTPS protocol is used Clear—the HTTPS protocol isn't used
16	**Key**	Enter the value into the field	Sets the path to the key file for transferring data over the HTTPS protocol	Latin, Cyrillic and service characters	No	Depends on the location of the key for encrypting data when transferring data over the HTTPS protocol
17	**Certificate**	Enter the value into the field	Sets the path to the certificate file for transferring data over the HTTPS protocol	Latin, Cyrillic and service characters	No	Depends on the location of the certificate file when transferring data over the HTTPS protocol

26.1.5.8.31 The Settings panel of the Edge storage object

The **Edge storage** object is used for viewing the video archive in the edge storages on IP devices.

The **Edge storage** object settings panel is shown in the figure.

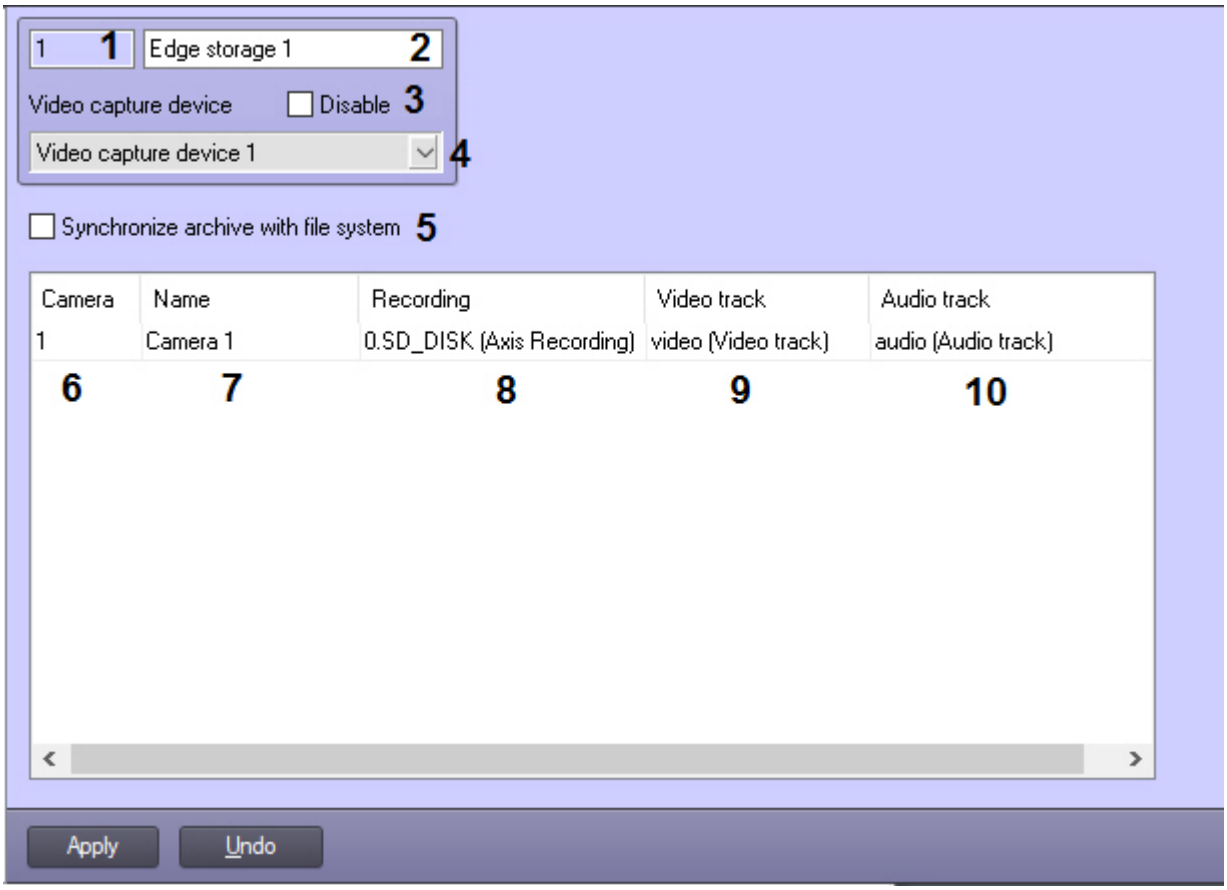


Table describes the settings parameters corresponding to the elements of the **Edge storage** settings panel.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **Edge storage** system object	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Edge storage** objects in the digital video surveillance system with the distributed architecture
2	Name	Enter the value into the field	Sets the name of the **Edge storage** object in the system	Latin, Cyrillic letters and service characters	Edge storage <ID>	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Edge storage** object in the system	Boolean type	Clear	Set—the **Edge storage** object is disabled and isn't used Clear—the **Edge storage** object is enabled and used
4	**Video capture device**	Select the value from the list	Sets the **Video capture device** parent object for	Name of the **Video capture device**	Name of the **Video capture**	Depends on the number of the **Video capture device** objects in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			the given **Edge storage** object	objects registered in the system	**device** parent object	
5	**Synchronize archive with file system**	Set the checkbox	Enables importing the archive from the edge storage to the *Intellect* file system	Boolean type	Clear	Set—archive import is enabled Clear—archive import is disabled
6	**Camera**	Select the value from the list	Sets the number of the **Camera** object used for archive viewing	Sequence of numbers	-	Depends on the number of cameras registered in the system
7	**Name**	Automatically	Displays the name of the **Camera** object	Name of the **Camera** objects registered in the system	-	Depends on the number of the **Camera** objects registered in the system
8	**Recording**	Select the value from the list	Sets the recording in the device which corresponds to one data source	Name of recordings supported by the device	-	Depends on the number of recordings supported by the device
9	**Video track**	Automatically	Sets the channel of the video data within recording	Name of the video tracks within recording	-	Depends on the number of video tracks within recording
10	**Audio track**	Select the value from the list	Sets the channel of the audio data within recording	Name of the audio tracks within recording	-	Depends on the number of audio tracks within recording

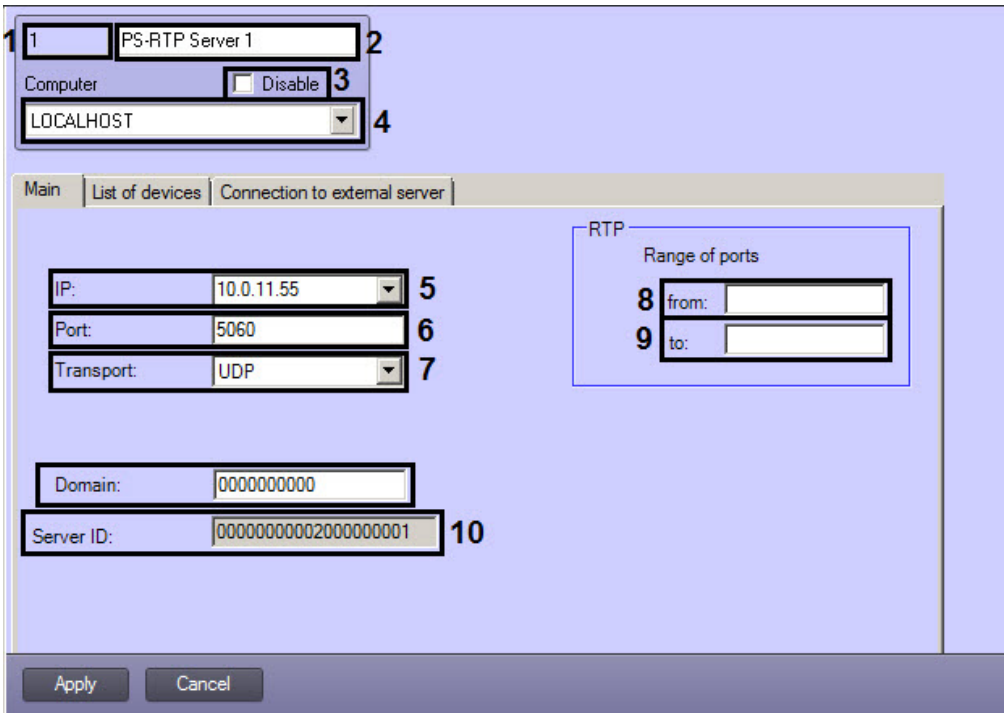
26.1.5.8.32 The Settings panel of the PS-RTP server object

Attention!

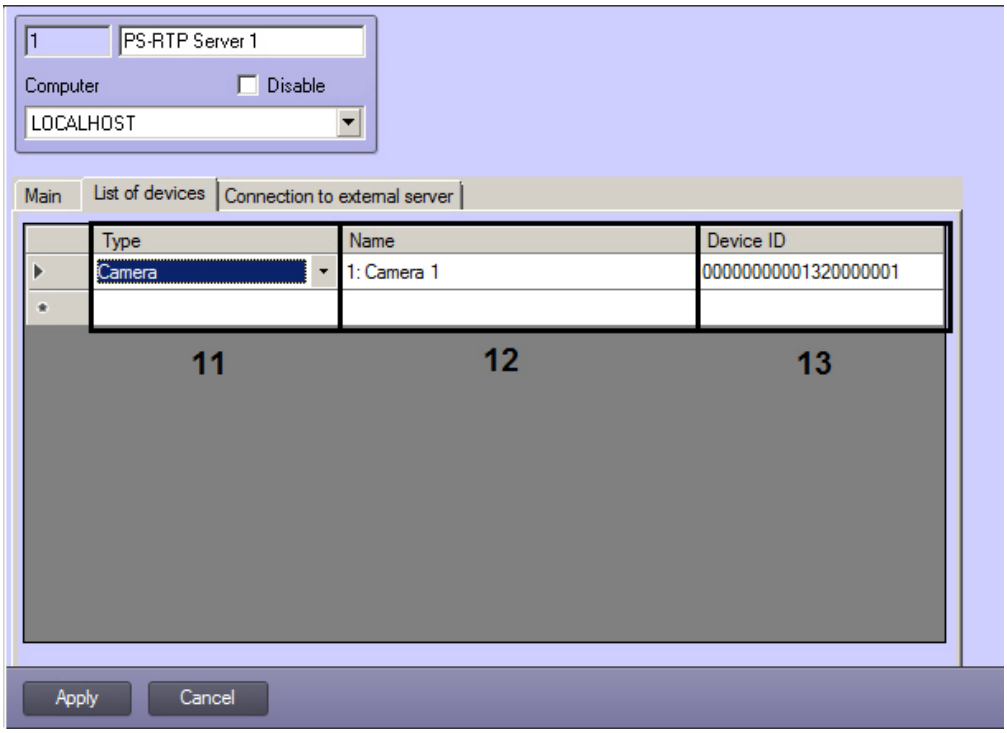
The PS-RTP Server object was excluded from *Intellect* since the version 4.11.3.

The settings panel of the **PS-RTP Server** object is shown in the figures.

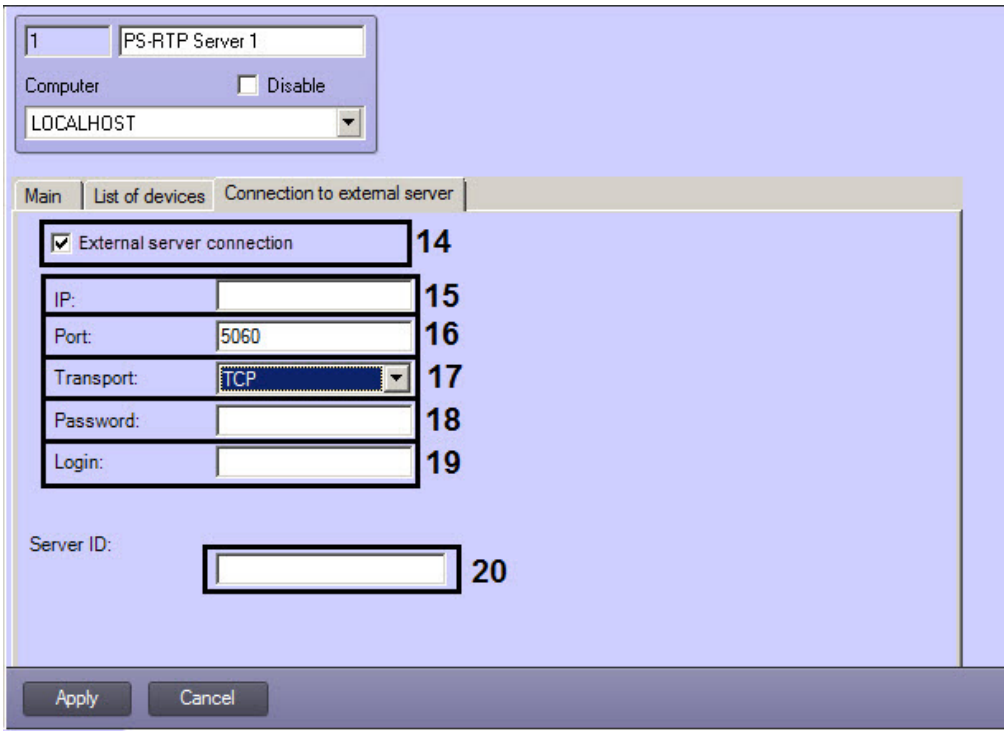
The **Main** tab.



The **List of devices** tab.



The **Connection to external server** tab.



The table describes the setting parameters of the **PS-RTP Server** system object.

№	Parameter	Method of setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **PS-RTP Server** object in the system	Sequence of numbers	-	Depends on the number of the **PS-RTP Server** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **PS-RTP Server** object	Latin, Cyrillic and service characters	**PS-RTP Server**	A line containing a sequence of any characters (letters, digits, service characters except for the > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (disabled or enabled) of the **PS-RTP Server** object	Boolean type	Clear	Set—the **PS-RTP Server** object is disabled and isn't used Clear—the **PS-RTP Server** object is enabled and used
4	**Computer**	Select the value from the list	Sets the **Computer** parent object of the digital system with the distributed architecture to which the given **PS-RTP Server** object belongs	Names of the **Computer** objects registered in the system	The name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with the distributed architecture
The **Main** tab						
5	**IP**	Select the value from the list	Sets the IP address of the network interface using which the third-party software will control the devices registered in *Intellect* via the GB28181 protocol	IP address	Depends on the parameters of the network connection	Depends on the parameters and the number of the network connections

6	**Port**	Enter the value into the field	Number of the port through which the third-party software will be connected via the GB28181 protocol	Sequence of numbers	5060	0–65535
7	**Transport**	Select the value from the list	Transport protocol for the data transmission	Supported transport protocols	UDP	UDP, TCP
8	**from**	Enter the value into the field	Lower limit of the RTP port range	Sequence of numbers	-	0–65535
9	**to**	Enter the value into the field	Upper limit of the RTP port range	Sequence of numbers	-	0–65535
10	**Server ID**	Automatically	The identifier of the *Intellect* Server that is used by the third-party software to connect to the RS-RTP Server via the GB28181 protocol	-	-	-
The **List of devices** tab						
11	**Type**	Select the value from the list	The type of object to be controlled via the GB28181 protocol	Names of the types of objects in *Intellect* objects tree	-	Depends on the number of the objects created in *Intellect* objects tree
12	**Name**	Select the value from the list	The name of the object to be controlled via the GB28181 protocol	Names of the objects in *Intellect* objects tree	-	Depends on the number of the objects created in *Intellect* objects tree
13	**Device ID**	Automatically	The identifier of the device that will be used in the third-party software to control objects via the GB28181 protocol	-	-	-
The **Connection to external server** tab						
14	**External server connection**	Set the checkbox	Defines if *Intellect* connects to the external supserver using the **PS-RTP Server** object via the GB28181 protocol	Boolean type	Clear	Set—the external server connection is enabled Clear—the external server connection is disabled
15	**IP**	Enter the value into the field	IP address of the supserver	IP address	-	000.000.000.000 – 255.255.255.255
16	**Port**	Enter the value into the field	Port used to connect to the external server	Sequence of numbers	5060	0–65535
17	**Transport**	Select the value from the list	Transport protocol used to connect to the external server	Supported transport protocols	-	TCP, UPD

18	**Password**	Enter the value into the field	Password used to connect to the external server	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters
19	**Login**	Enter the value into the field	Username used to connect to the external server	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters
20	**Server ID**	Enter the value into the field	The identifier of the supserver via the GB28181 protocol	Sequence of numbers	-	00000000000000000000 – 99999999999999999999

26.1.5.8.33 The Settings panel of the Manager of failover services object

The **Manager of failover services** object is used to control the maximum number of the active Failover services in the distributed system.

The settings panel of the **Manager of failover services** object is shown in the figure.

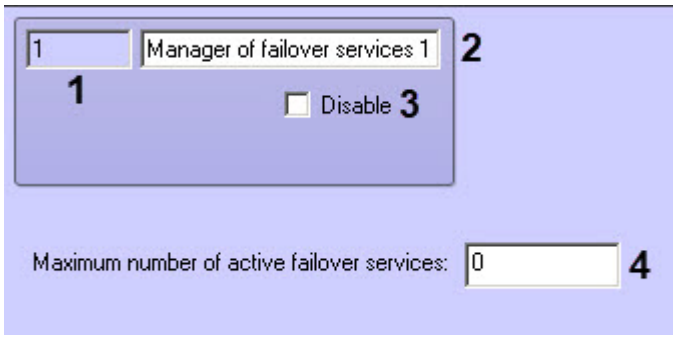


Table describes the setting parameters corresponding to the elements of the settings panel of the **Manager of failover services** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Manager of failover services** system object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Manager of failover services** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Manager of failover services** object in the system	Latin, Cyrillic and service characters	Manager of failover services	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Manager of failover services** object in the system	Boolean type	Clear	Set—the **Manager of failover services** object is disabled and isn't used Clear—the **Manager of failover services** object is enabled and used
4	**Maximum number of active**	Enter the value into the field	Sets the maximum number of inactive Servers above which the migration of the configuration should be stopped	>=0	0	0—the maximum number of the active Failover services is unlimited

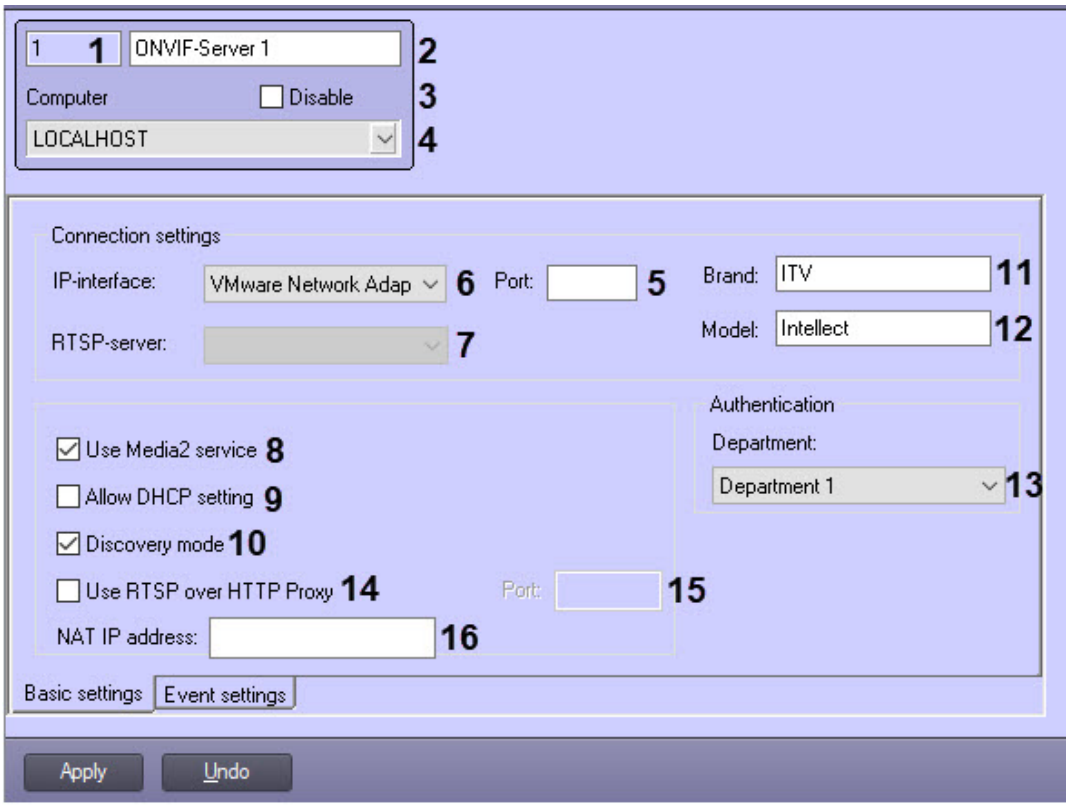
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
	failover services		until one of the busy Failover services is released			>0—the maximum number of the active Failover services is limited by the specified value

26.1.5.8.34 The Settings panel of the ONVIF-Server object

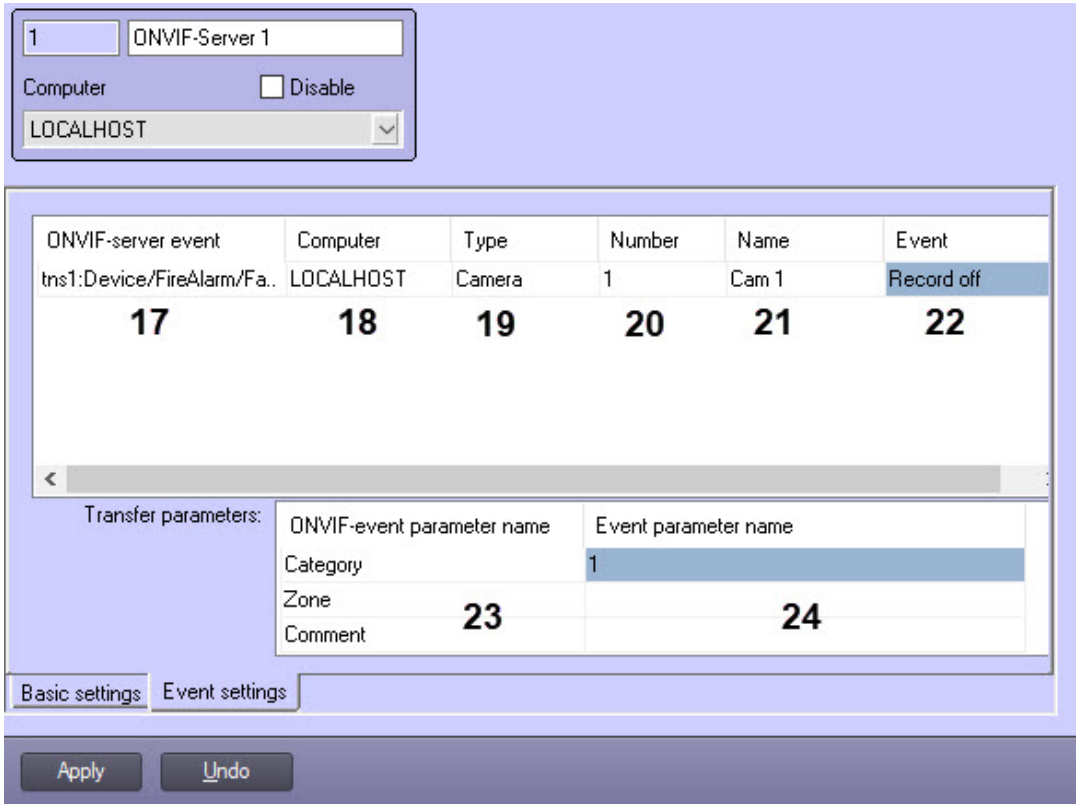
The **ONVIF-Server** object is used to transmit *Intellect* video signal via the ONVIF protocol.

The settings panel of the **ONVIF-Server** object is shown in the figure.

The **Basic settings** tab.



The **Event settings** tab.



The table describes the setting parameters of the **ONVIF-Server** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **ONVIF-Server** objects in the digital video surveillance system with distributed architecture
2	Name	Enter the value into the field	Sets the name of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	ONVIF-Server	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **ONVIF-Server** object is disabled and not in use. Clear—the **ONVIF-Server** object is enabled and in use.
4	**Computer**	Select the value from the list	Sets the **Computer** parent object in the digital system with distributed architecture to which the given **ONVIF-Server** object belongs	Names of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the computers in the digital video surveillance system with distributed architecture

The **Basic settings** tab

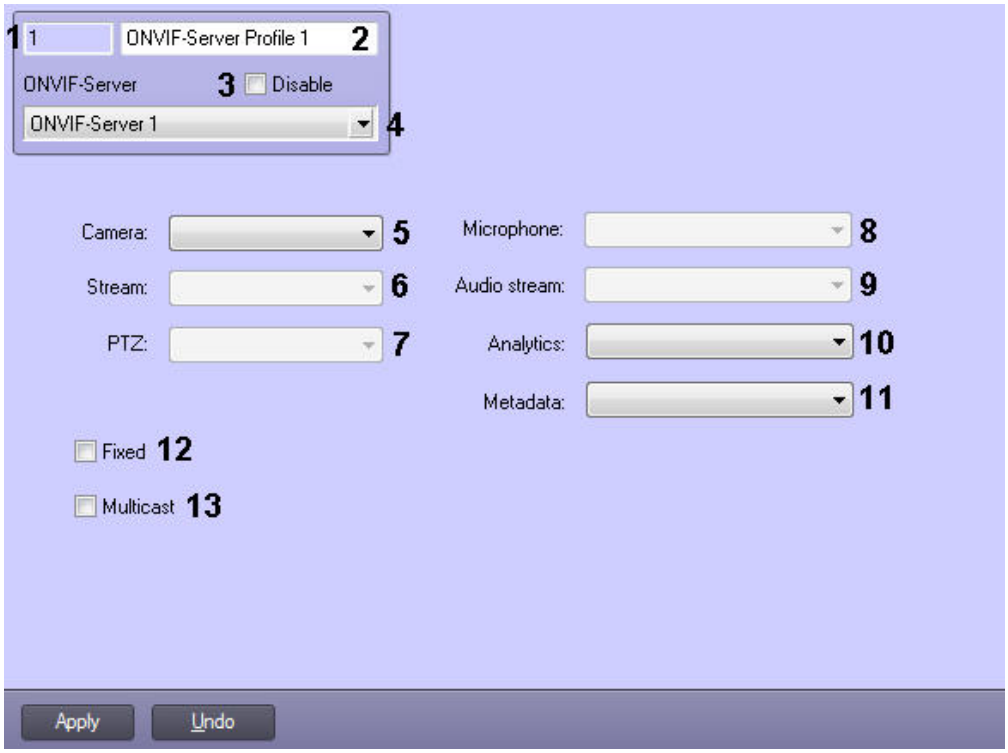
5	**Port**	Specify the value in the field	Sets the port number used to connect to the Server	Integer greater than 0	-	1– 65535
6	**IP-interface**	Select the value from the list	Sets the network interface (network adapter) used to connect to the Server	List of available network interfaces	-	The list of values depends on the network adapters available in the system
7	**RTSP-server**	Select the value from the list	Sets the **RTSP-server** object the settings of which will be applied by the **ONVIF-Server** object while transmitting the video signal	Names of the **RTSP-server** objects registered in the system	-	Depends on the number of the **RTSP-server** objects created in *Intellect*
8	**Use Media2 service**	Set the checkbox	Enables the ONVIF 2.X standard instead of ONVIF 1.X	Boolean type	Clear	Set—the ONVIF 2.X standard is used. The video is transmitted in the H264, H265, MJPEG or MPEG4 formats Clear—the ONVIF 1.X standard is used. The video is transmitted in the MPEG, MJPEG or H264 formats
9	**Allow DHCP setting**	Set the checkbox	Enables the DHCP support	Boolean type	Clear	Set—DHCP is used Clear—DHCP isn't used
10	**Discovery mode**	Set the checkbox	Enables the WS-Discovery mode	Boolean type	Set	Set—the WS-Discovery mode is enabled Clear—the WS-Discovery mode is disabled
11	**Brand**	Enter the value into the field	Sets the name of the brand that will be displayed in the third-party clients that support the video transmission via the ONVIF protocol	Latin, Cyrillic and service characters	ITV	A line containing a sequence of any characters (letters, digits and service characters)
12	**Model**	Enter the value into the field	Sets the name of the model that will be displayed in the third-party clients that support the video transmission via the ONVIF protocol	Latin, Cyrillic and service characters	Intellect	A line containing a sequence of any characters (letters, digits and service characters)
13	**Department**	Select the value from the list	Sets the department in which the users will be created when they are added via the *ONVIF-Server* interface	Names of the **Department** objects registered in the system	-	Depends on the number of the departments registered in *Intellect*
14	**Use RTSP over HTTP Proxy**	Set the checkbox	Redirects all RTSP-Server and ONVIF-Server requests to the specified port for the operation behind NAT	Boolean type	Clear	Set—the RTSP-Server and ONVIF-Server requests are redirected to the specified port Clear—the RTSP-Server and ONVIF-Server requests are transmitted to the port specified in the **Connection settings** group (see item 5 above)
15	**Port**	Enter the value into the field	Sets the port number for the RTSP-Server and ONVIF-Server requests redirection for the operation behind NAT	Integer greater than 0	-	1– 65535
16	**NAT IP address**	Enter the value into the field	Sets the IP address that the ONVIF Server will use in responses to Clients if the Clients are behind NAT	IP address	-	Depends on the network settings behind NAT

The **Event settings** tab						
17	**ONVIF-server event**	Select the value from the list	Sets the ONVIF-server event according to the ONVIF specification	List of available events	-	According to the ONVIF specification
18	**Computer**	Select the value from the list	Sets the **Computer** object on the basis of which the object is created that is the event source in *Intellect*	Names of the **Computer** objects registered in the system	-	Depends on the number of the computers in the digital video surveillance system with distributed architecture
19	**Type**	Select the value from the list	Sets the event type which is the event source in *Intellect*	Names of the object types registered in the system	-	Depends on the number of the created objects in the digital video surveillance system with distributed architecture
20	**Number**	Select the value from the list	Sets the object number which is the event source in *Intellect*	Sequence of numbers	-	Depends on the number of the created objects in the digital video surveillance system with distributed architecture
21	**Name**	Automatically	Sets the object name which is the event source in *Intellect*	Names of the object of the selected type registered in the system	-	Depends on the number of the created objects in the digital video surveillance system with distributed architecture
22	**Event**	Select the value from the list	Sets the event name in *Intellect*	Event names received from the objects of the selected type	-	Depends on the object type
23	**ONVIF-event parameter name**	Automatically	Sets the ONVIF-event parameter name according to the specification	Parameter names of the selected ONVIF-event	-	According to the ONVIF specification
24	**Event parameter name**	Enter the value into the field	Sets the event parameter name in *Intellect*	Event parameter names in *Intellect*	-	Depends on the object type

26.1.5.8.35 The Settings panel of the ONVIF-Server Profile object

The **ONVIF-Server Profile** object is used to configure the ONVIF device channel.

The settings panel of the **ONVIF-Server Profile** object is shown in the figure.



The table describes the setting parameters of the **ONVIF-Server Profile** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **ONVIF-Server** objects in the digital video surveillance system with distributed architecture
2	**Name**	Enter the value into the field	Sets the name of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	ONVIF-Server	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **ONVIF-Server** object is disabled and isn't used Clear—the **ONVIF-Server** object is enabled and used
4	**ONVIF-Server**	Select the value from the list	Sets the **ONVIF-Server** parent object in the digital system with distributed architecture to which the given **ONVIF-Server Profile** object belongs	Names of the **ONVIF-Server** objects registered in the system	Name of the **ONVIF-Server** parent object	Depends on the number of the **ONVIF-Server** objects in the digital video surveillance system with distributed architecture
5	**Camera**	Automatically	Sets the **Camera** object corresponding to the **ONVIF-Server Profile** object	Names of the **Camera** objects registered in the system	-	Depends on the number of the **Camera** objects in the digital video surveillance system with distributed architecture

6	**Stream**	Automatically	Sets the video camera stream that is transmitted via the given **ONVIF-Server Profile** object	List of available video camera streams	-	Depends on the number of the activated video camera streams
7	**PTZ**	Automatically	Sets the **PTZ** object, used for the PTZ control of the camera, corresponding to the **ONVIF-Server Profile** object	List of **PTZ** objects corresponding to the selected **Camera** object	-	Depends on the number of the **PTZ** objects created and configured in the system
8	**Microphone**	Automatically	Sets the **Microphone** object corresponding to the selected **Camera** object	List of the **Microphone** objects corresponding to the selected **Camera** object	-	Depends on the number of the **Microphone** objects created and configured in the system
9	**Audio stream**	Automatically	Sets the audio stream to be synchronously transmitted with video signal	List of available audio streams	-	Depends on the number of the available audio streams
10	**Analytics**	Automatically	Sets the stream to transmit analytics	List of available streams	-	Depends on the number of available streams
11	**Metadata**	Automatically	Sets the stream to transmit metadata	List of available streams	-	Depends on the number of available streams
12	**Fixed**	Set the checkbox	Disables deleting the **ONVIF-Server Profile** object using the driver	Boolean type	Clear	Set—the **ONVIF-Server Profile** object cannot be deleted using the driver Clear—the **ONVIF-Server Profile** object can be deleted using the driver
13	**Multicast**	Set the checkbox	Enables video transmission via the ONVIF-Server in the multicast mode	Boolean type	Clear	Set—video can be transmitted in the multicast mode. *Note. There are some extra actions needed besides setting the checkbox in order to enable video transmission in the multicast mode—see* Configuring getting video using ONVIF-Server module. Clear—video cannot be transmitted in the multicast mode.

26.1.5.8.36 The Settings panel of the Telegram bot object

The **Telegram bot** object is used for sending messages to Telegram.

The settings panel of the **Telegram bot** object is shown in the figure.

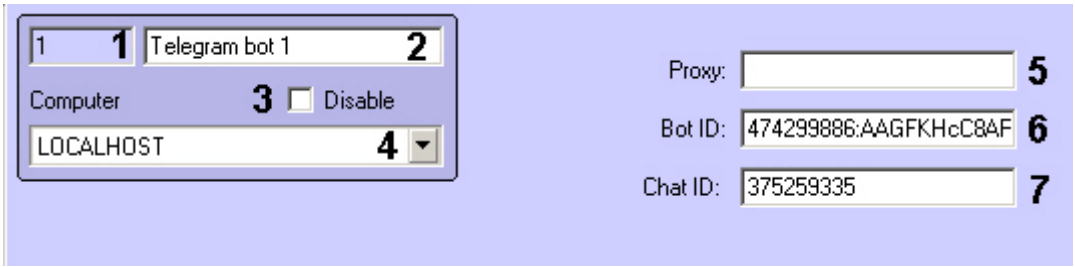


Table describes the setting parameters corresponding to the elements of the settings panel of the **Telegram bot** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Telegram bot** object in the digital video surveillance system with distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Telegram bot** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Telegram bot** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	Telegram bot	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Telegram bot** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Telegram bot** object is disabled and isn't used Clear—the **Telegram bot** object is enabled and used
4	**Computer**	Select the value from the list	Defines the **Computer** parent object, to which the given **Telegram bot** object belongs	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the digital video surveillance system with distributed architecture
The **Settings** group						
5	**Proxy**	Enter the value into the field	Sets the proxy server for sending the message	Latin and service characters	Not defined	A line containing a sequence of any characters (letters, digits, service characters). Number of characters—from 1 to 60
6	**Bot ID**	Enter the value into the field	Sets the bot identifier in Telegram	Latin and service characters	Not defined	A line containing a sequence of any characters (letters, digits, service characters). Number of characters—from 1 to 60
7	**Chat ID**	Enter the value into the field	Sets the chat identifier in Telegram	Latin and service characters	Not defined	A line containing a sequence of any characters (letters, digits, service characters). Number of characters—from 1 to 60

* Name of the element isn't displayed in the settings panel of the given object.

26.1.5.8.37 The Settings panel of the SIP-terminal object

The settings panel of the **SIP-terminal** object is shown in the figure.

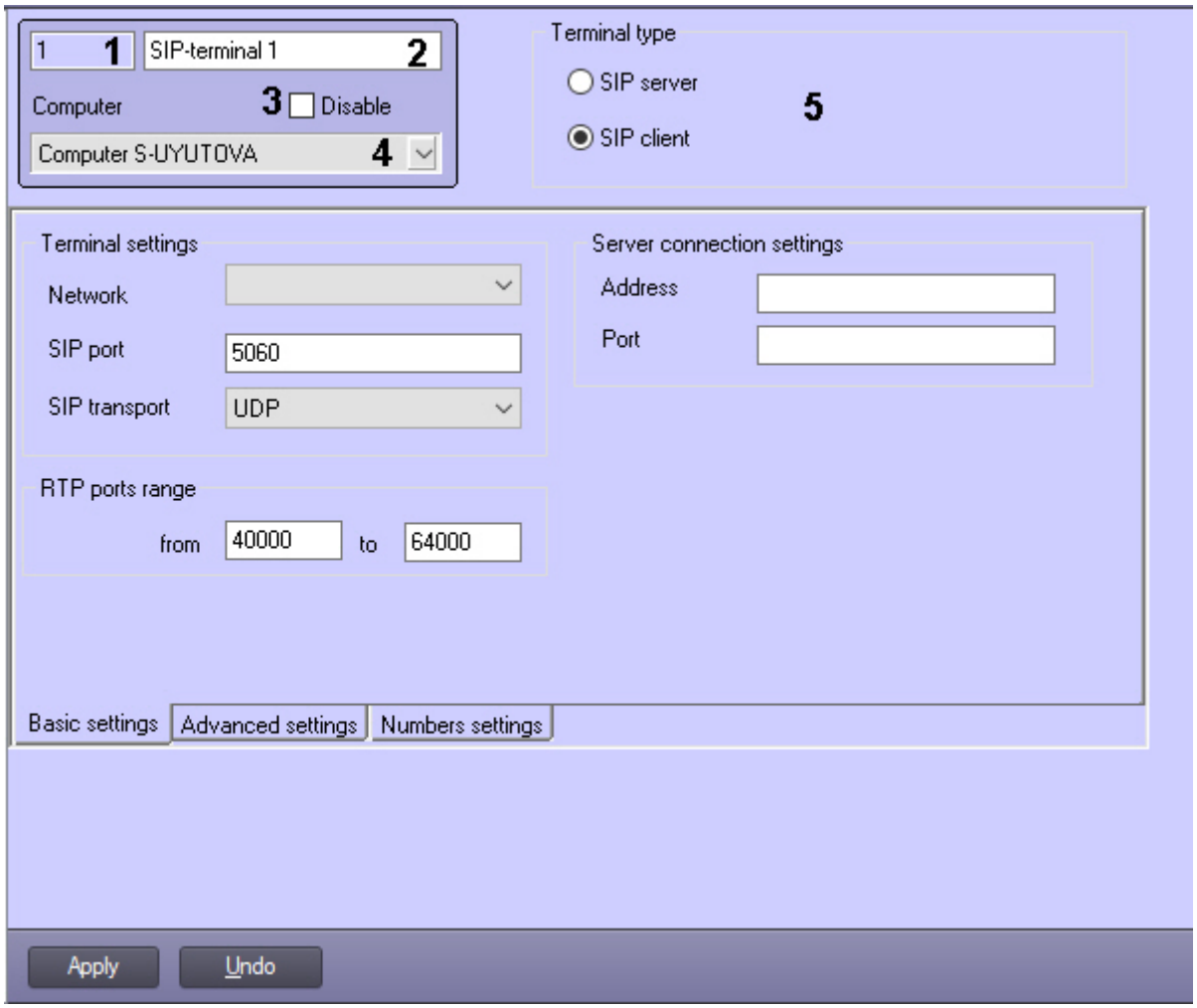


Table describes the setting parameters of the **SIP-terminal** system object.

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **SIP-terminal** system object	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **SIP-terminal** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **SIP-terminal** object in the system	Latin, Cyrillic and service characters	SIP-terminal	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **SIP-terminal** object in the system	Boolean type	Clear	Set—the **SIP-terminal** object is disabled and isn't used Clear—the **SIP-terminal object** is enabled and used

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
4	**Computer**	Select the value from the list	Sets the **Computer** parent object for the given **SIP-terminal** object	Name of the **Computer** objects registered in the system	Name of the **Computer** parent object	Depends on the number of the **Computer** objects in the system
5	**Terminal type**	Set the required radio button	Sets the SIP-terminal type	Supported SIP-terminal types	SIP server	**SIP server**—the SIP-terminal acts as a server, any SIP-clients can be connected to it **SIP client**—the SIP-terminal acts as a client, it can be connected to any SIP-server

The **Basic settings** tab.

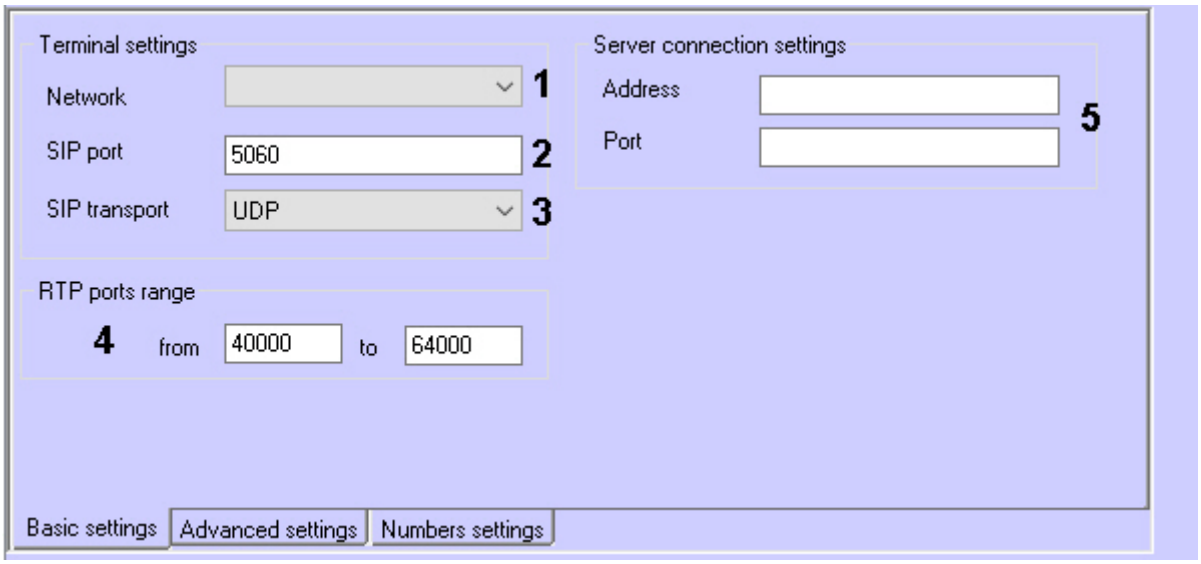


Table describes the setting parameters of the **Basic settings** tab.

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
1	**Network**	Select the value from the list	Sets the IP address of the network adapter that will be used to connect to the network in which the SIP-clients are located	IP address	Default network adapter	The list of the available network adapters of the computer
2	**SIP port**	Enter the value into the field	Sets the port number which will receive the data from the clients via the SIP protocol	Sequence of numbers	5060	0–65535
3	**SIP transport**	Select the value from the list	Sets the used transport layer protocol	Supported transport layer protocols	UDP	TCP UDP
4	**RTP ports range, from** and **to** fields	Enter the value into the field	Sets the RTP ports range	Sequence of numbers	from 40000 to 64000	0–65535

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
5	**Address**	Enter the value into the field	For the **SIP client** terminal type only. Sets the IP address of the SIP server	IP address	-	1.0.0.0–255.255.255.255
	Port	Enter the value into the field	For the **SIP client** terminal type only. Sets the port for the SIP server connection	Sequence of numbers	-	0–65535

The **Advanced settings** tab.

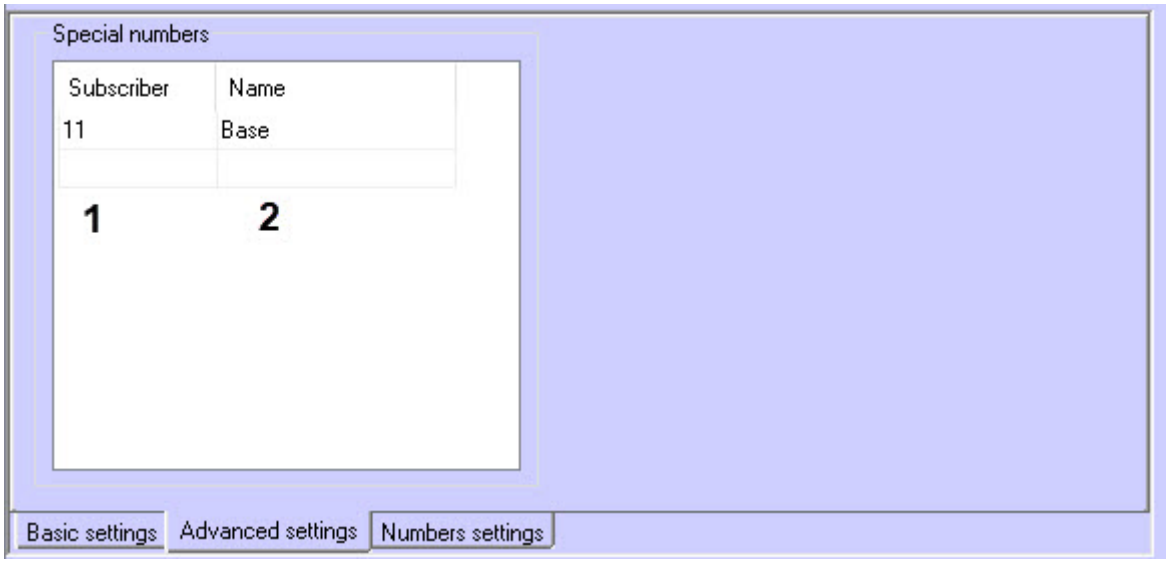


Table describes the setting parameters of the **Advanced settings** tab.

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
1	**Subscriber**	Enter the value into the field	Sets the SIP server special number	Sequence of numbers	-	>=0
2	**Name**	Enter the value into the field	Sets the name of the SIP server special number	Latin, Cyrillic letters and service characters	-	A line containing a sequence of any characters

The **Numbers settings** tab.

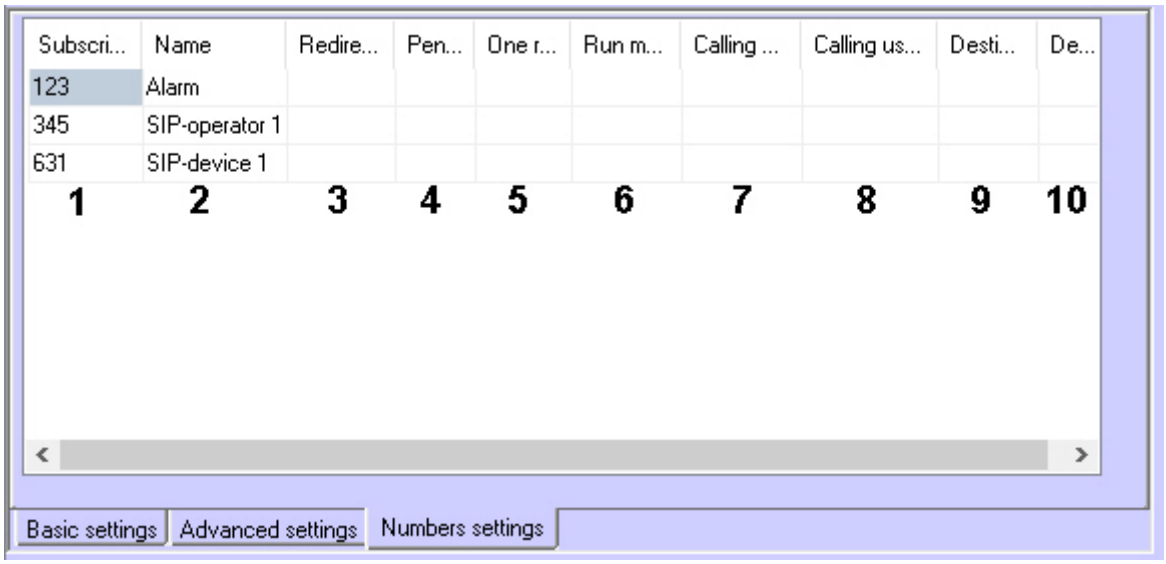


Table describes the setting parameters of the **Numbers settings** tab.

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
1	**Subscriber**	Automatically	Displays the numbers of all devices and operators registered on the SIP-terminal, as well as special numbers	-	-	-
2	**Name**	Automatically	Displays the names of the corresponding devices, operators, and special numbers	-	-	-
3	**Redirecting**	Enter the value into the field	Sets the number or numbers to which the corresponding subscriber's calls should be forwarded to	Sequence of numbers	-	Numbers of all devices and operators registered on the SIP-terminal, as well as special numbers. If you want to specify several numbers, use a semicolon as a separator, for example, 234;12;0983
4	**Pending, s**	Enter the value into the field	Sets the time period in seconds, during which it is necessary to wait for a response from the subscriber	Sequence of numbers	-	>0
5	**One responder**	Set the checkbox	Enables a group call (forwarded to several numbers) ending after one of the recipients answers	Boolean type	Clear	Set—a group call is ended for all recipients after the response of any operator or a device Clear—the group call is not ended after the answer of the first or subsequent operators and/or devices, i.e. all recipients can join the call
6	**Run macro**	Select the value from the list	Sets the **Macro** object which should be run when calling the subscribe	Name of the **Macro** objects registered in the system	-	Depends on the number of the **Macro** objects in the system
7	**Calling number multicast (video)**	Enter the value into the field	Sets the IP address for transmitting the video stream	IP address	-	1.0.0.0–255.255.255.255

№	Parameter	Method for setting the parameter value	Description	Representation	Default value	Value range
			from the calling device in the multicast mode			
8	**Calling number multicast (audio)**	Enter the value into the field	Sets the IP address for transmitting the audio stream from the calling device in the multicast mode	IP address	-	1.0.0.0–255.255.255.255
9	**Destination number multicast (video)**	Enter the value into the field	Sets the IP address for transmitting the video stream from the destination device in the multicast mode	IP address	-	1.0.0.0–255.255.255.255
10	**Destination number multicast (audio)**	Enter the value into the field	Sets the IP address for transmitting the audio stream from the destination device in the multicast mode	IP address	-	1.0.0.0–255.255.255.255

26.1.5.8.38 The Settings panel of the SIP-device object

The settings panel of the **SIP-device** object is shown in the figures below.

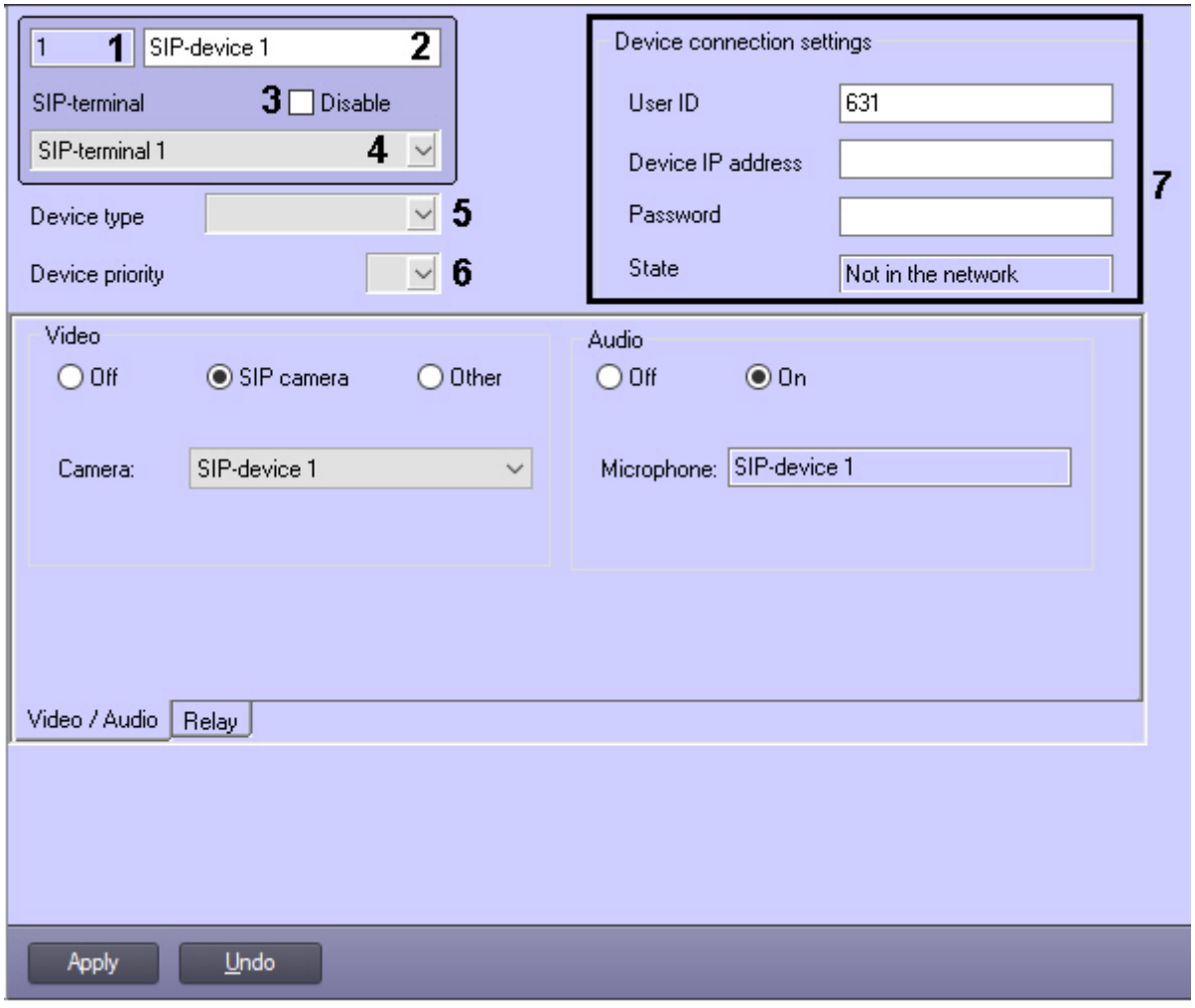


Table describes the setting parameters of the **SIP-device** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **SIP-device** object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **SIP-device** objects in the system
2	**Name**	Enter the value into the field	Sets a name of the **SIP-device** object in the system	Latin, Cyrillic and service characters	SIP-terminal	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **SIP-device** object in the system	Boolean type	Clear	Set—the **SIP-device** object is disabled and isn't used Clear—the **SIP-device** object is enabled and used
4	**SIP-terminal**	Select the value from the list	Sets the **SIP-terminal** parent object for the given **SIP-device** object	Name of the **SIP-terminal** objects registered in the system	Name of the **SIP-terminal** parent object	Depends on the number of the **SIP-terminal** objects in the system
5	**Device type**	Select the value from the list	Sets the icon type to display the device on the Map	Names of the available icon types	-	No value touch panel speaker camera microphone default
6	**Device priority**	Select the value from the list	Sets the priority of a call from this device in the incoming calls window of the SIP panel	Sequence of numbers	-	0–10 The lower the number, the higher the priority and, accordingly, the higher the display in the list. If the field is left blank, then the priority is considered to be minimal. Calls from devices with the same priority will be sorted by the time of the call
The **Device connection settings** group						
7	**User ID**	Enter the value into the field	Sets the SIP-device identification number, i.e. the number to call it	Sequence of numbers		>=0
	Device IP address	Enter the value into the field	For the **SIP-server** terminal type only. Sets the SIP-device IP address	IP address		1.0.0.0–255.255.255.255
	Password	Enter the value into the field	For the **SIP-server** terminal type only.	Latin, Cyrillic and service characters		A line containing a sequence of any characters (letters, digits, service characters)

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			The password specified on the SIP-device			
	State	Automatically	For the **SIP-server** terminal type only. Displays the SIP-device state	-	-	-

The **Video / Audio** tab (only for the **SIP-server** terminal type).

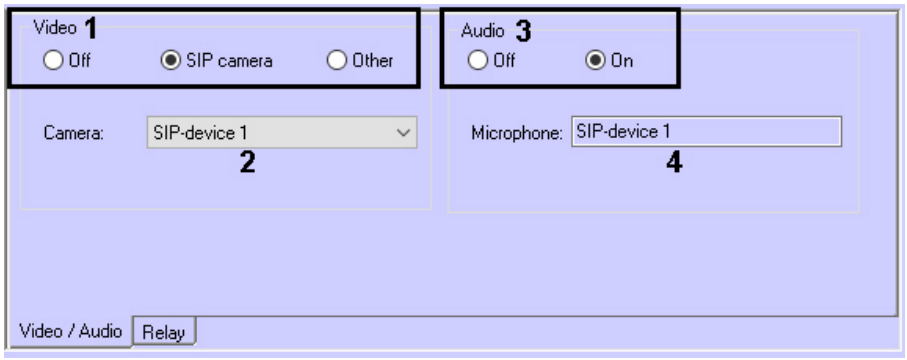


Table describes the setting parameters of the **Video / Audio** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Video**	Set the required radio button	Sets the video camera used for calls	Supported options of camera usage	Off	**Off**—the video is not used during the call **SIP camera**—a SIP-device camera connected via the SIP protocol is used **Other**—any other camera from the *Intellect* hardware tree selected from the **Camera** drop-down list is used
2	**Camera**	Select the value from the list	Sets any video camera used for calls	Name of the **Camera** objects registered in the system	-	Depends on the number of the **Camers** objects in the system
3	**Audio**	Set the required radio button	Enables or disables the audio during a call	Supported options of audio usage	Off	**Off**—the audio is not used during the call **On**—the microphone of the SIP-device is used during the call
4	**Microphone**	Automatically	Displays the name of the **Microphone** object corresponding to the SIP-device	-	-	-

The **Relay** tab (only for the **SIP-server** terminal type).

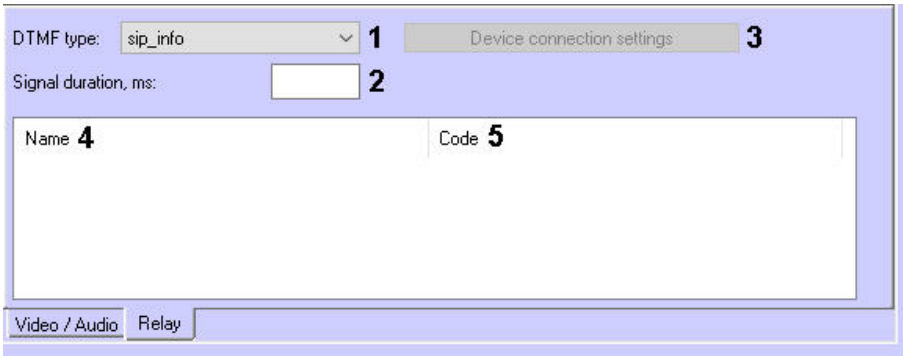


Table describes the setting parameters of the **Relay** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**DTMF type**	Select the value from the list	Sets the type of the tone DTMF signal	Supported signal types	sip_info	**sip_info**—signals are transmitted in the INFO message of the SIP protocol **sip_notify**—signals are transmitted in the NOTIFY message of the SIP protocol **in_band**—the signal is transmitted as normal sound in an audio stream **http_bas**—signals are transmitted via the HTTP protocol separately from the voice stream
2	**Signal duration, ms**	Enter the value into the field	Sets the time period in milliseconds during which the DTMF signal should be sent	Sequence of numbers		>0
3	**Device connection settings**	-	Opens a pop-up window of connection settings when the **http_bas** type of tone is selected	-	Inactive by default	-
4	**Name**	Enter the value into the field	Sets the name of the command that will be displayed on the SIP-panel	Latin, Cyrillic and service characters		A line containing a sequence of any characters (letters, digits, service characters)
5	**Code**	Enter the value into the field	Sets the unique command code	Sequence of numbers or HTTP request (for **http_bas**)		A line containing a sequence of numbers or HTTP request

The **Device connection settings** pop-up window.

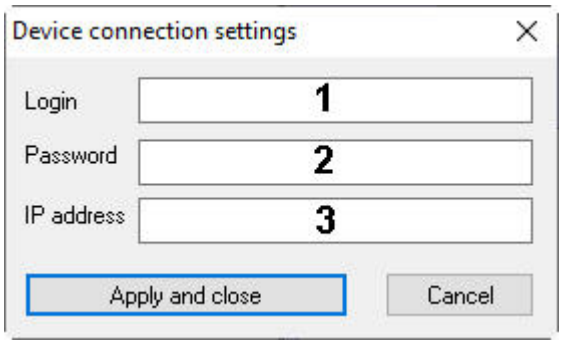


Table describes the fields of the **Device connection settings** window.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Login**	Enter the value into the field	Sets the user name to connect to the SIP-device (BasIP)	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters)
2	**Password**	Enter the value into the field	Sets the password to connect to the SIP-device (BasIP)	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters)
3	**IP address**	Enter the value into the field	Sets the IP address of the SIP-device (BasIP)	IP address	-	1.0.0.0–255.255.255.255

26.1.5.8.39 The Settings panel of the SIP-operator object

The settings panel of the **SIP-operator** object is shown in the figures below.

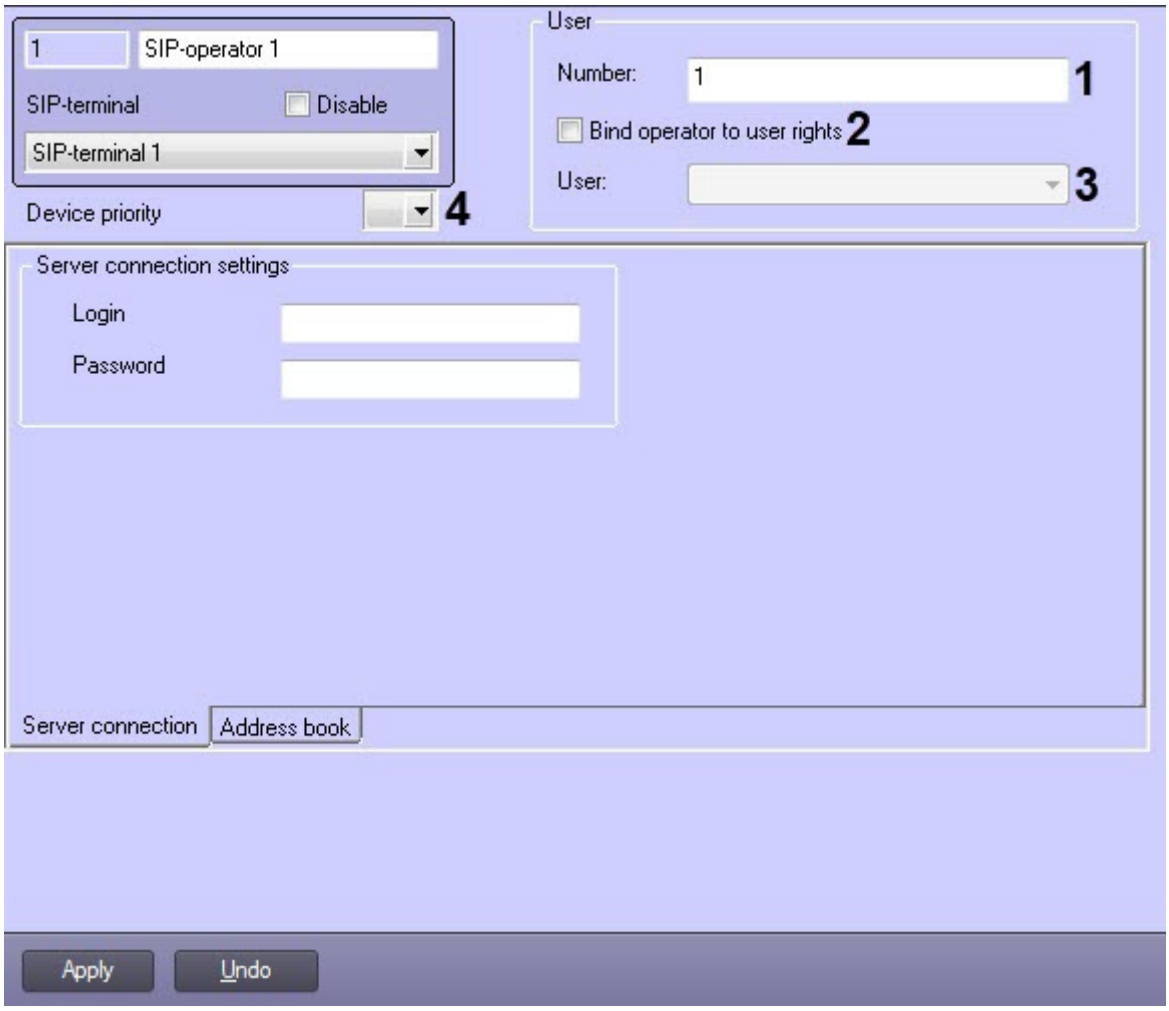


Table describes the setting parameters of the **SIP-operator** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Number**	Enter the value into the field	Sets the identification number of the operator to which you can call	Numbers, letters, periods, hyphen, dash and underscore	-	>=0
2	**Bind operator to user rights**	Set the checkbox	Enables binding of a SIP-operator to *Intellect* user rights. Activates the **User** drop-down list. *Note. It is used when the **User rights** are selected by default on the operator's SIP-panel*			Set—binding of a SIP-operator to *Intellect* user rights is enabled Clear—binding of a SIP-operator to *Intellect* user rights is disabled
3	**User**	Select the value from the list	Sets the user under which it is necessary to register in *Intellect*	Name of the **User** objects registered in the system		Depends on the number of the **User** objects in the system
4	**Device priority**	Select the value from the list	Sets the priority of a call from this operator in the incoming calls window of the SIP-panel	Sequence of numbers	No	0–10

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						The lower the number, the higher the priority and, accordingly, the higher the display in the list. If the field is left blank, then the priority is considered to be minimal. Calls from operators with the same priority will be sorted by the time of the call

The **Server connection** tab (only for the **SIP-client** terminal type).

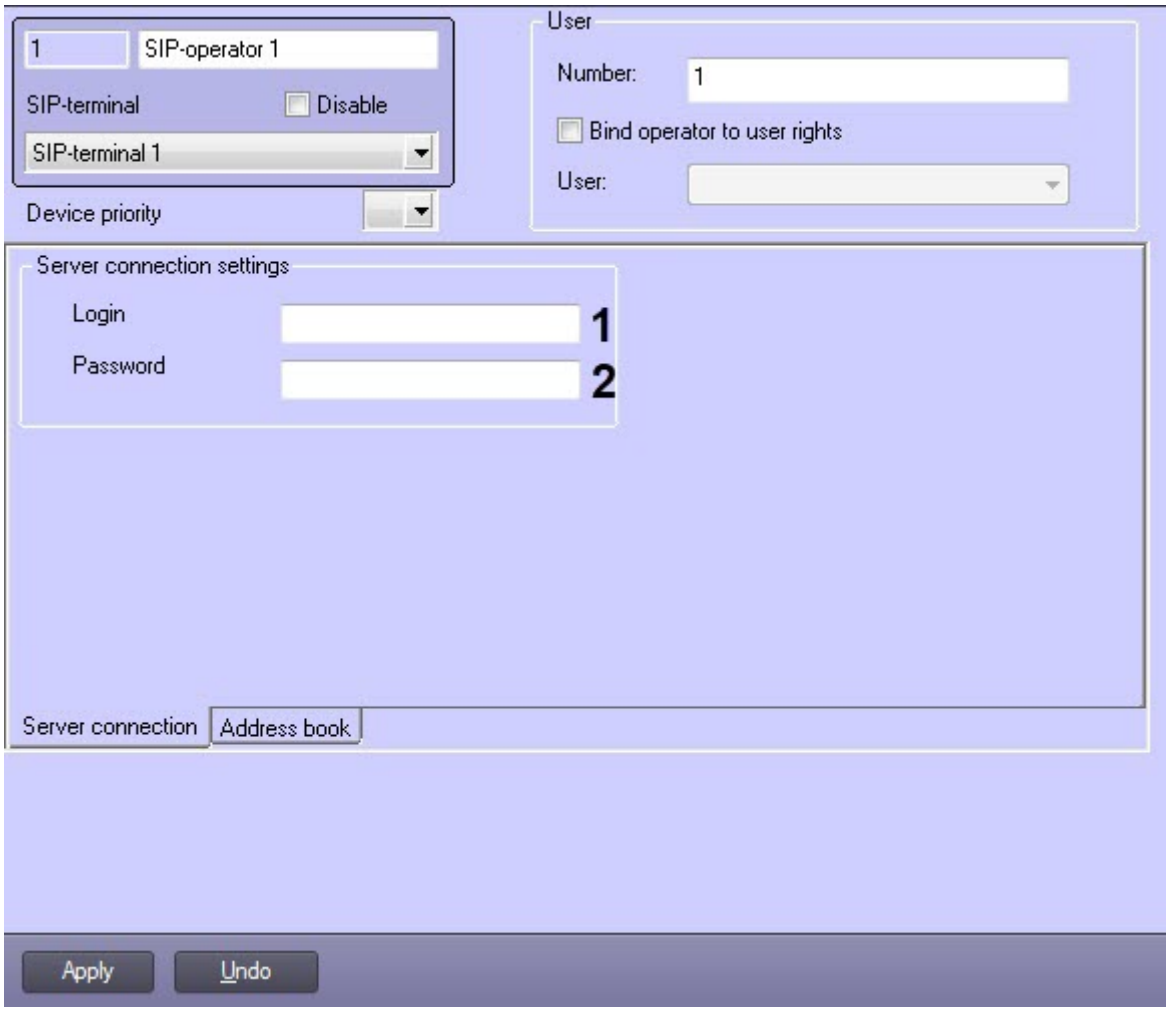


Table describes the setting parameters of the **Server connection** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Login**	Enter the value into the field	Sets the login for connecting to the SIP-server	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters)

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
2	**Password**	Enter the value into the field	Sets the password for connecting to the SIP-server	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters (letters, digits, service characters

The **Address book** tab.

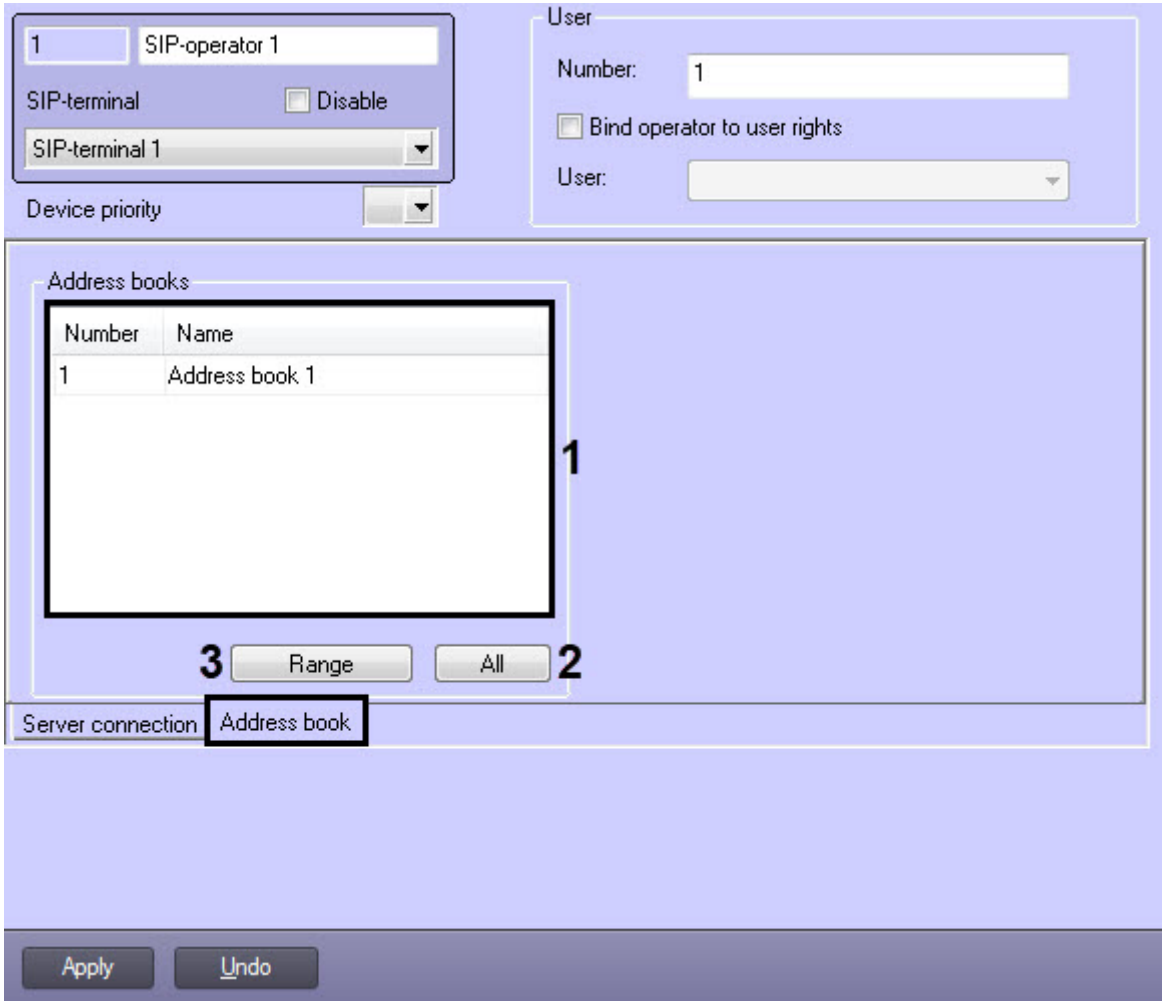


Table describes the setting parameters of the **Address book** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Address books**	Select the value in the column	Sets the list of address books, the numbers of which will be available for this SIP-operator	-	-	-
	Number	Select the value from the list	Selects the address book identifier	Identifiers of the **Address book** objects registered in the system	-	Depends on the number of the **Address book** objects in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
	Name	Select the value from the list	Selects the name of the address book in *Intellect*	Names of the **Address book** objects registered in the system	-	Depends on the number of the **Address book** objects in the system
2	**All**	Click the button	Adds all existing address books to the table	-	-	-
3	**Range**	Click the button	Opens the **Add address books** window to add multiple address books	-	-	-

26.1.5.8.40 The Settings panel of the Address book object

The settings panel of the **Address book** object is shown in the figure.

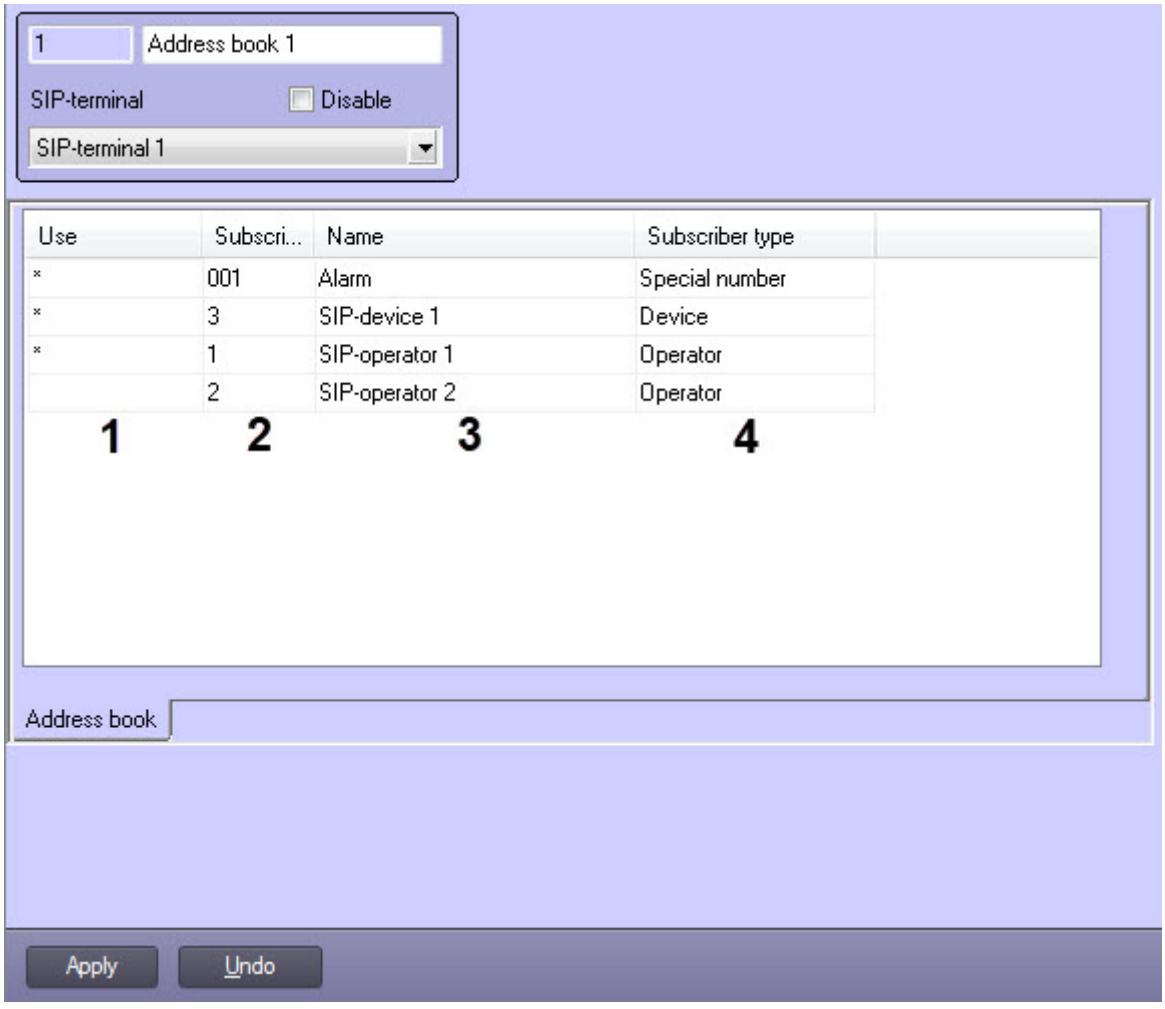


Table describes the setting parameters of the **Address book** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Use**	Set the checkbox	Sets a list of subscriber numbers that should be available in this address book	Boolean type	Clear	Set—the number is added to this address book Clear—the number isn't added to this address book
2	**Subscriber**	Automatically	Displays the subscriber number	-	-	-
3	**Name**	Automatically	Displays the name of the object in *Intellect*	-	-	-
4	**Subscriber type**	Automatically	Displays the type of subscriber: Operator, Device, Special number	-	-	-

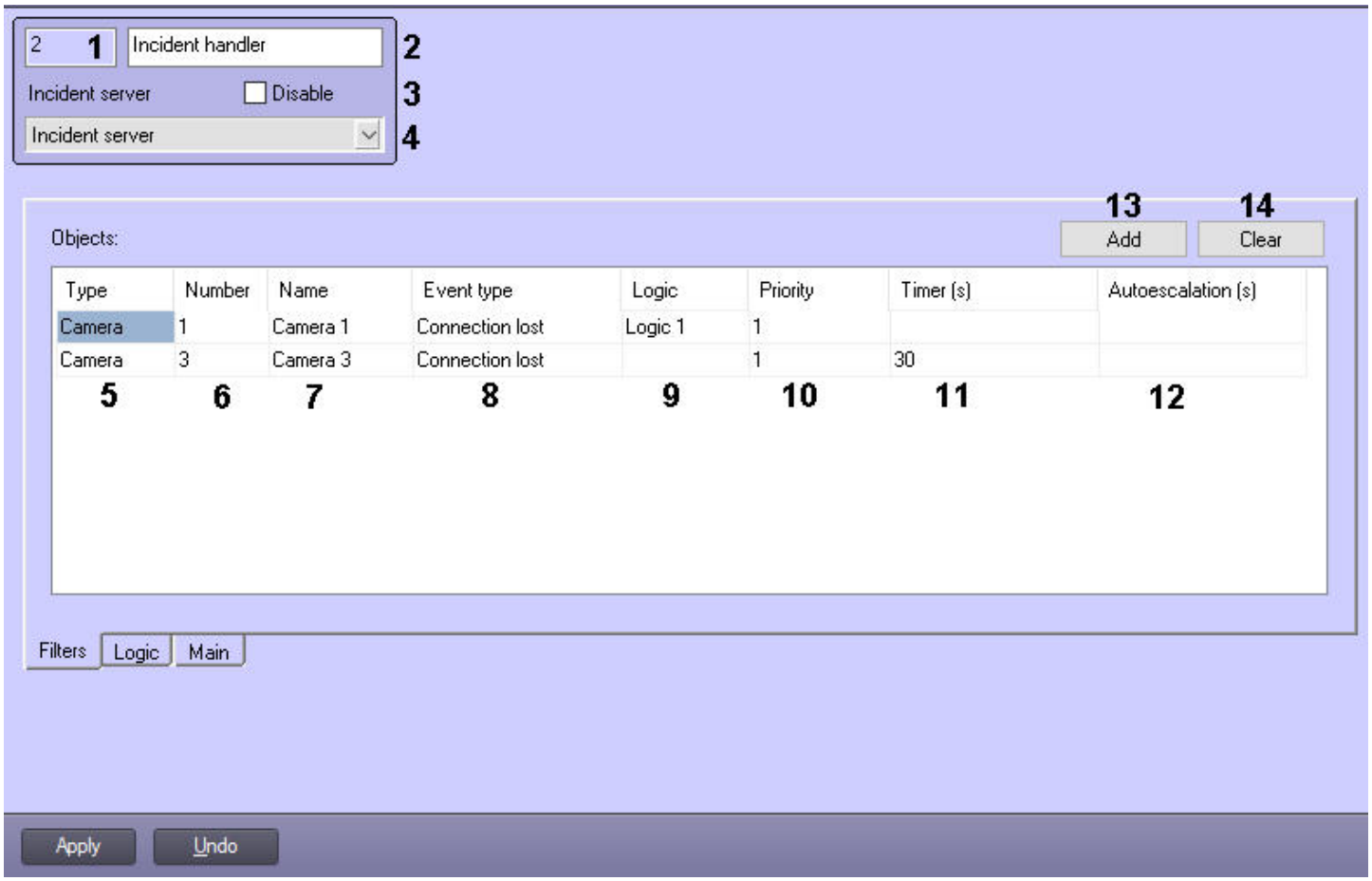
26.1.5.8.41 The Settings panel of the Incident handler object

On this page:

- Object general settings and the Filters tab
- The Logic tab
- The Main tab

The settings panel for the **Incident handler** object is shown in the figures. The description of the **Incident handler** setting parameters is given in the corresponding tables.

26.1.5.8.41.1 Object general settings and the Filters tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Incident handler** interface object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Incident handler** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Incident handler** object in the system	Latin, Cyrillic and service characters	Incident handler	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Incident handler** object in the system	Boolean type	Clear	Set—the **Incident handler** object is disabled and isn't used Clear—the **Incident handler** object is enabled and used
4	**Incident server**	Select the value from the list	Sets the **Incident server** parent object for the given **Incident handler** object	Names of the **Incident server** objects registered in the system	Name of the **Incident server** parent object	Depends on the number of the **Incident server** objects in the system

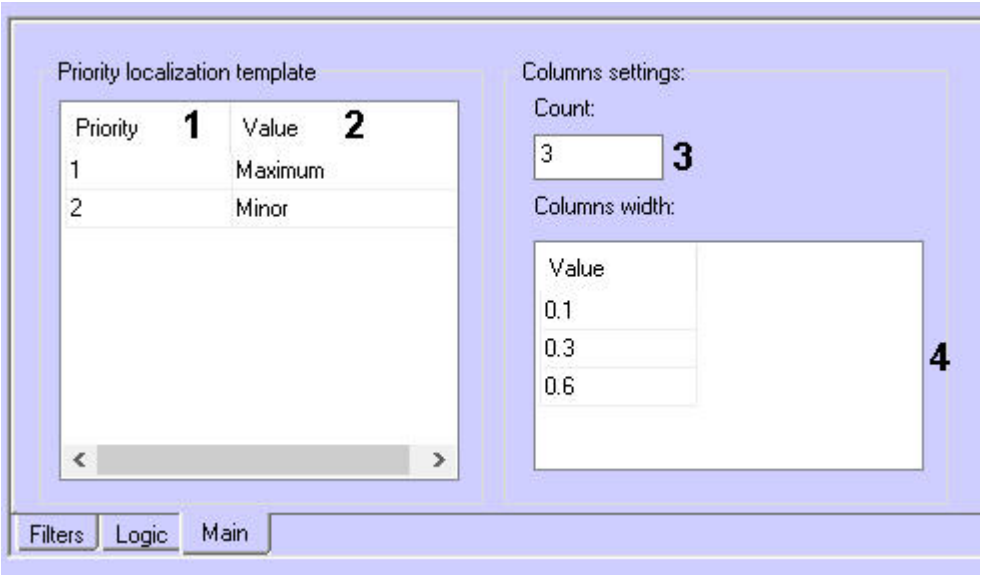
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Filters** tab						
5	**Type**	Select the value from the list	Sets the type of objects for which the events should be displayed in the **Incident manager** window	Available object types	-	Depends on the objects registered in the system. Only those object types are available for selection for which the "INFORMATION" or "ALARM" value is selected on the **Events** tab in the **Processing messages** column in the ddi.exe utility (see The Events tab)
6	**Number**	Select the value from the list	Sets the number of the object for which the events should be displayed in the **Incident manager** window	Sequence of numbers	-	Depends on the number of the objects of the specified type registered in the system
7	**Name**	Automatically	Sets the name of the object for which the events in the **Incident manager** window should be displayed	Names of the objects registered in the system	-	Depends on the objects registered in the system
8	**Event type**	Select the value from the list	Sets the events displayed in the **Incident manager** interface window	Events available to the selected object	-	Depends on the object type
9	**Logic**	Enter the value into the field	Sets the logic that will be used to handle the events of the corresponding object. The logic has to be specified. Otherwise, the selected events will not be displayed	Logic name	-	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 255
10	**Priority**	Select the value from the list	Priority level for events of the corresponding object	Priority level	0	Depends on the priority templates created on the **Main** tab
11	**Timer (s)**	Enter the value into the field	Sets the time in seconds from the moment the event occurred, after which the **TIME_IS_OVER** event is generated. The timer will also count down the specified time in the interface in the **Time (s)** column until it reaches zero	Time in seconds	-	>=0
12	**Autoescalation (s)**	Enter the value into the field	Sets the time in seconds from the moment the event occurs, after which the event will be automatically escalated. Autoescalation is performed within one **Incident manager** and works if the operator has the escalation rights	Time in seconds	-	>=0
13	**Add**	Click the button	Opens the window for selecting events as a group (see Displaying and handling events in bulk)			
14	**Clear**	Click the button	Clears the table with the selected objects and events			

26.1.5.8.41.2 The Logic tab

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Create copy**	Click the button	If you select a logic in the list of logics and click on the button to create a copy, a copy of the selected logic will be created. It will appear in the list of logics	-	-	-
2	**+**	Click the button	Creates a new logic	-	-	-
3	**-**	Click the button	Removes the logic selected in the logic list	-	-	-
4	List of logics	Select the value from the list	Selectes the logic which elements are displayed in the list on the right	List of the created logics	-	Depends on the number of the created logics
5	**Starting**	Set the checkbox	Selects the element that will be displayed first for the operator when processing the event. To select the starting element: 1. Select an element in the table. 2. Click the **Edit** button. 3. In the **Starting element** drop-down list, select **Yes**. 4. Click the **OK** button	Boolean type	Clear	Set—the element is the starting element in the logic Clear—the element isn't a starting element in logic Only one element in the logic can be the starting element
6	**Element ID**	Enter the value into the field	Element name	Latin, Cyrillic and service characters	-	From 0 to 255 characters
7	**Element type**	Select the value from the list	Selects the element type (see Configuring the elements)	Available element types	-	Image Button

						Comboboxes Comment Radio buttons Checkboxes
8	**Multitasking**	Select the value from the list	By default, when processing an event, you can move on to processing other events from any element of logic. Using the **Multitasking** setting, you can allow or deny the ability to switch to processing another event if the operator is on the selected element	Available multitasking values	-	**Deny**—when this element appears, the operator cannot switch to processing another event until the operator moves to the element with the **Allow** value or completes processing the event **Allow**—when this element appears, the operator can proceed to processing another event **Blank field**—the multitasking setting of the previous logic element is applied to the selected element
9	**Edit**	Click the button	Opens a window for editing the selected element (see Configuring the elements)	-	-	-

26.1.5.8.41.3 The Main tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Priority localization template** group						
1	**Priority**	Enter the value into the field	Priority level	Priority level	-	Numeric value, positive integer
2	**Value**	Enter the value into the field	Priority description. If the priority description is set, then it will be displayed in the **Incident**	Priority description	-	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 255

			manager, otherwise the priority level will be displayed			
The **Columns settings** group						
3	**Count**	Enter the value into the field	Sets the number of columns when displaying the event processing logic in the **Incident manager** interface	Sequence of numbers	4	0–100
4	**Columns width**	Enter the value into the field	Sets the width of the columns when displaying the event processing logic in the **Incident manager** interface	Pixels or fractions	150 pixels	Percentage values should be set in fractions of 1, for example, 0.25. If a value greater than 1 is specified, then it will be taken in pixels

26.1.5.9 The Interfaces tab

The **Interfaces** tab is used to create and configure the user interface of the video surveillance and audio monitoring system.

26.1.5.9.1 Interfaces tab components

The **Interface** tab displays a tree of the system objects, corresponding to the user interface components, and a settings panel used to configure the system object selected in the tree. The settings panels of the system objects used in the video surveillance and audio monitoring system are described in the following sections.

26.1.5.9.2 The Settings panel of the Display object

The **Display** object is used to register virtual displays in the system, which are used as a basis for interface components created in *Intellect.* The settings panel of the **Display** object is shown in the figure.

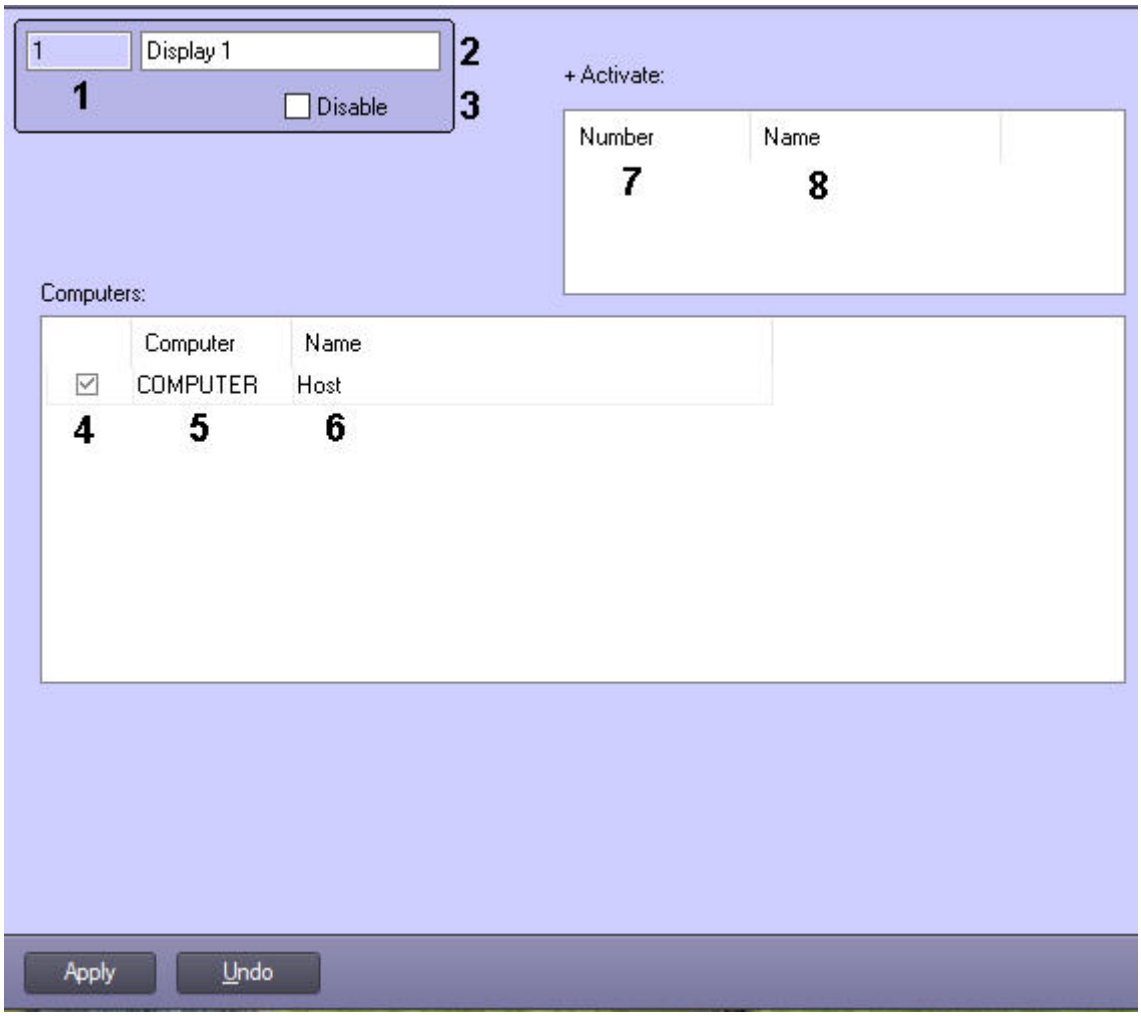


Table describes the setting parameters corresponding to the elements of the settings panel of the **Display** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Display** object in the digital video surveillance system with distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Display** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Display** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	Display	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Display** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Display** object is disabled and isn't used Clear—the **Display** object is enabled and used
The **Computers** group						

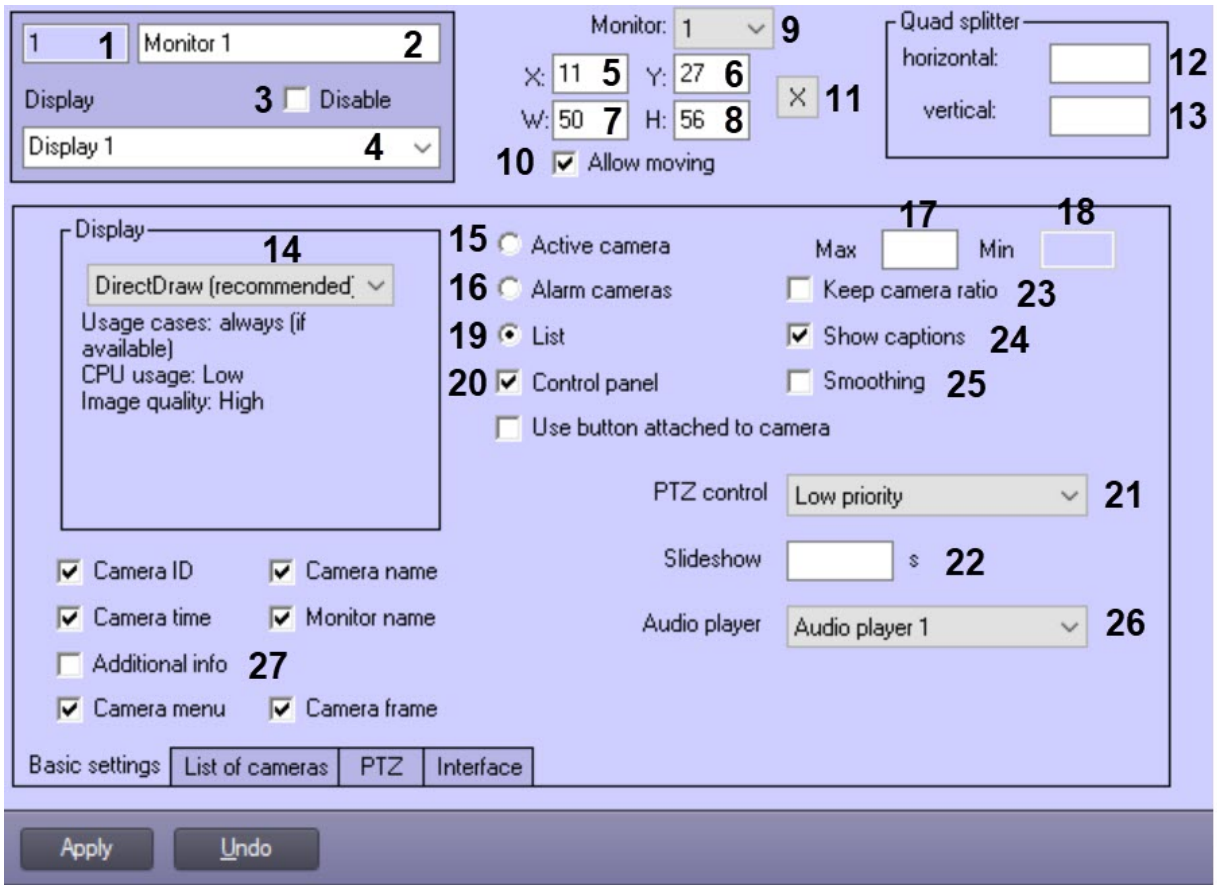
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	Select an element*	Set the checkbox	Contains a list of computers (Server, Remote Administrator's workstation, Remote workstation) connected to the given Server (Remote Administrator's workstation). The checkboxes corresponding to the computers determine whether or not the computers should display the **Monitor** objects created on the basis on the given **Display** object	Boolean type	Clear	Set—the selected computer will display the **Monitor** object created on the basis of the given **Display** object Clear—the selected computer will not display the **Monitor** object created on the basis of the given **Display** object
5	**Computer**	Automatically	Sets the computer name in the local network	Computer name in the local network	Computer name in the local network	Depends on the number of objects in the local network. A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
6	**Name**	Automatically	Sets the name to the computer in the digital video surveillance system with distributed architecture	Name of the **Computer** object registered in the system	Name of the **Computer** object registered in the system	Depends on the number of objects in the digital video surveillance system with distributed architecture A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
The **+Activate** group						
7	**Number**	Select the value from the list	Sets the number of the **Display**, the objects of which will be displayed on the configured **Display** at the same time with its objects	Identifiers of the **Display** type objects registered in the system	-	Depends on the number of the objects registered in the system
8	**Name**	Automatically	Name of the **Display**, the objects of which will be displayed on the configured **Display**. Filled out automatically after selecting the Number	Name of the **Display** object registered in the system	-	Depends on the number of the objects registered in the system

*Name of the element isn't displayed in the settings panel of the given object.

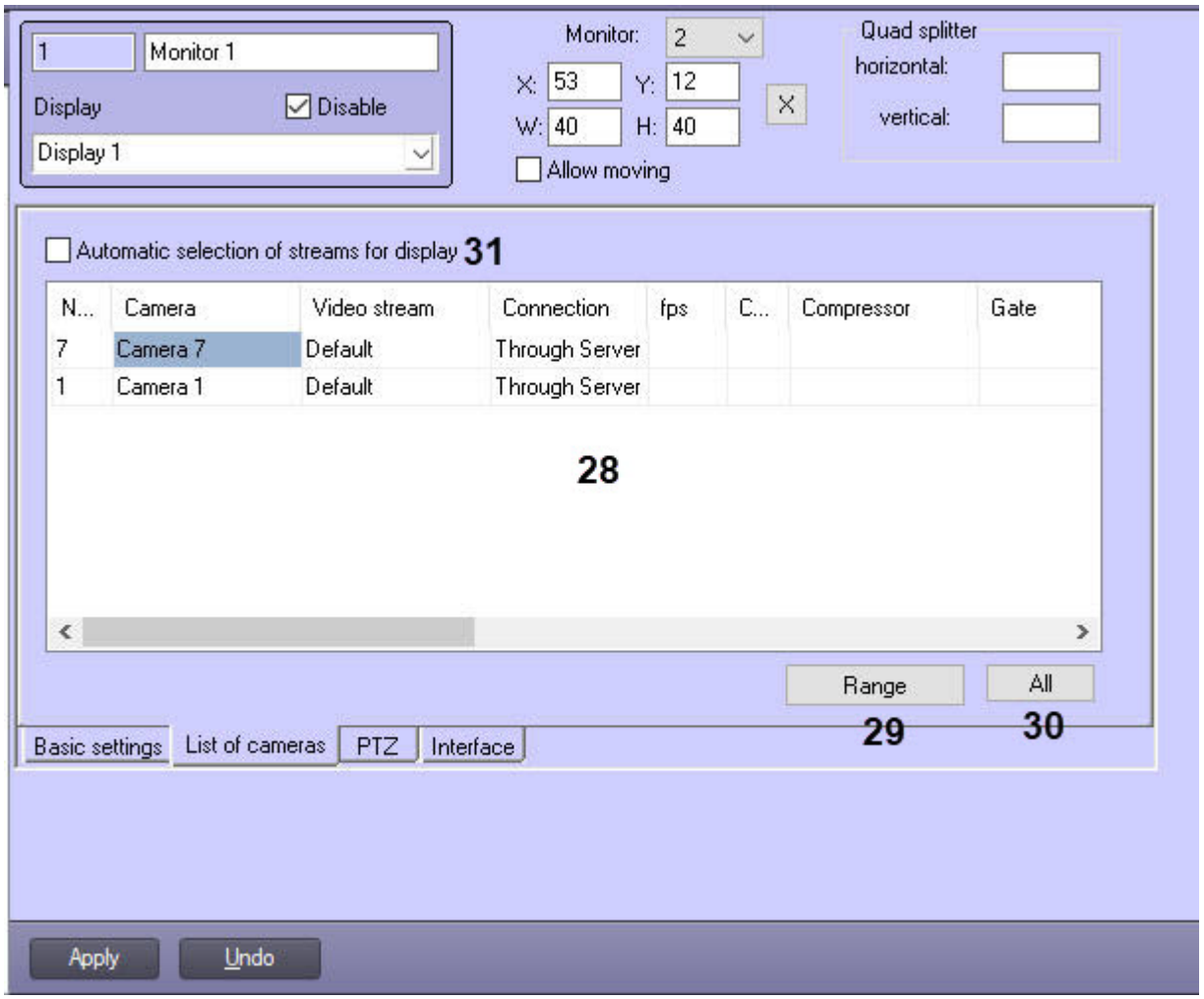
26.1.5.9.3 The Settings panel of the Monitor object

The settings panel of the **Monitor** object is shown in the figures.

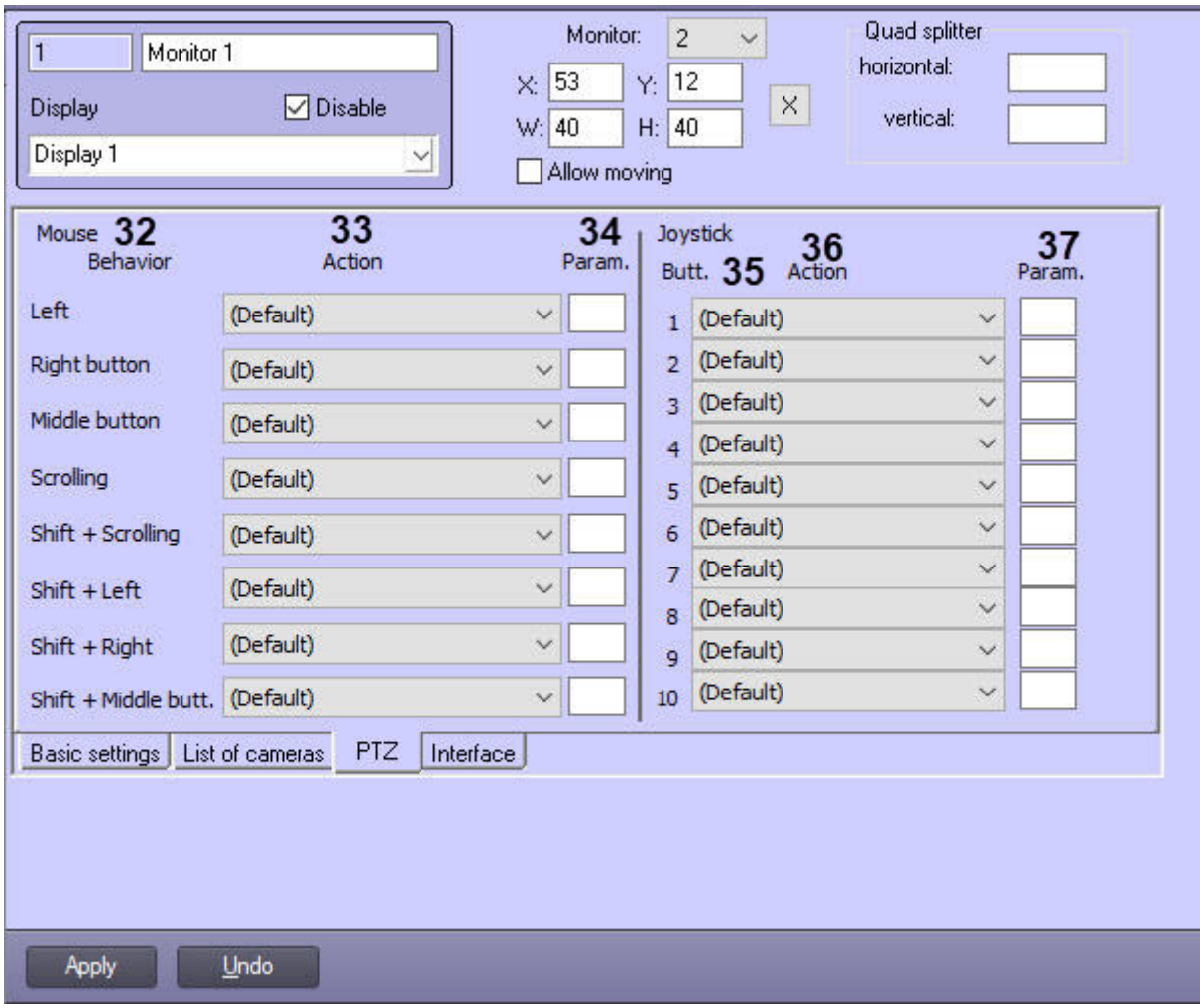
The **Basic settings** tab.



The **List of cameras** tab.


1
Monitor 1
Display
Disable
Display 1
Monitor:
2
X: 53
Y: 12
W: 40
H: 40
Allow moving
Quad splitter
horizontal:
vertical:
Automatic selection of streams for display
31
N...
Camera
Video stream
Connection
fps
C...
Compressor
Gate
7
Camera 7
Default
Through Server
1
Camera 1
Default
Through Server
28
Range
All
29
30
Basic settings
List of cameras
PTZ
Interface
Apply
Undo

The **PTZ** tab.



The **Interface** tab.

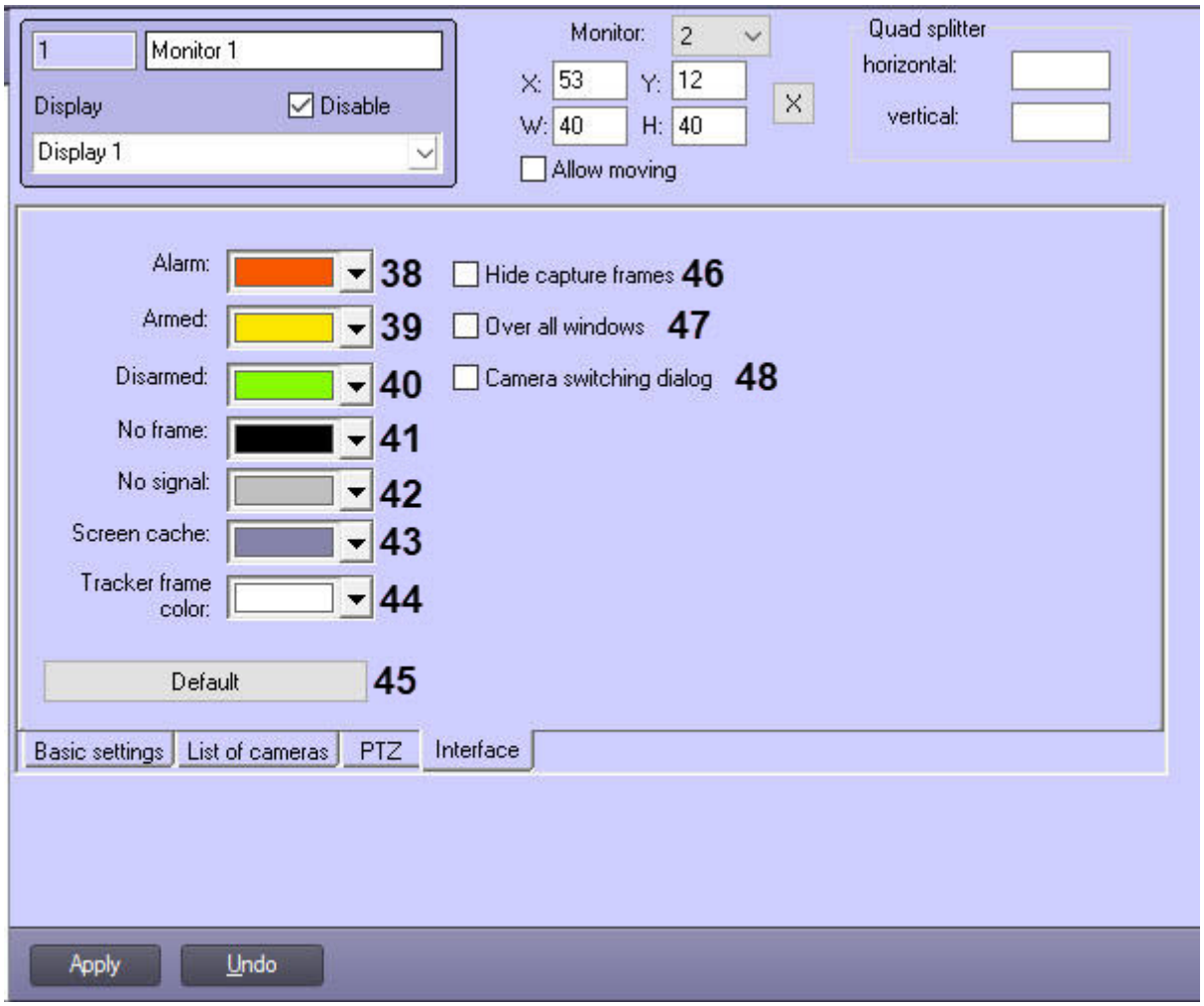
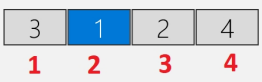


Table describes the setting parameters of the **Monitor** interface object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Monitor** interface object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Monitor** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Monitor** object in the system	Latin, Cyrillic and service characters	Monitor	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Monitor** object in the system	Boolean type	Clear	Set—the **Monitor** object is disabled and isn't used Clear—the **Monitor** object is enabled and used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Display**	Select the value from the list	Sets the **Display** parent object for the given **Monitor** object	Names of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system
The **Coordinates** group						
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Monitor** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed computer monitors
6	**Y**	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Monitor** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed computer monitors
7	**W**	Enter the value into the field	Sets the width of the **Monitor** interface window	% of the screen width	-	From 20 to 900 if control panel is enabled. Otherwise, from 0 to 900. This restriction can be disabled using the UnlimitMonitorSize registry key (see Registry keys reference guide)
8	**H**	Enter the value into the field	Sets the height of the **Monitor** object if the control panel is disabled	% of the screen width	-	From 0 to 900. This restriction can be disabled using the UnlimitMonitorSize registry key (see Registry keys reference guide)
9	**Monitor**	Select the value from the list	Sets the number of the physical monitor, the coordinates for which are set. The monitors are numbered in the order of their physical location from left to right, from top to bottom. The 1st monitor is the one in the upper left corner regardless of which monitor is set as main or what number the monitor has in OS. In the figure below, the monitor numbers in OS are given in gray while the numbers in *Intellect* are red.  ***Attention! It is recommended to set the same resolution for all monitors in the system. Different resolution is only allowed if all monitors are aligned along any border (for example, upper border)***	Sequence of numbers	1	From 1 to 16
10	**Allow moving**	Set the checkbox	Allows moving the the **Monitor** interface window manually, if the control panel is enabled	Boolean type	Clear	Set—the manual moving is allowed ClearSet—the manual moving isn't allowed

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
11	The X button	Click the button	Opens the window for specifying the position of the **Monitor** interface window	-	-	-
The **Quad splitter** group						
12	**horizontal**	Enter the value into the field	Sets the number of the surveillance windows that should be displayed horizontally on the **Monitor**. If value is not specified (the field is blank), then the default grid of the surveillance windows depending on the selected layout is displayed	Sequence of numbers	-	From 1 to 64
13	**vertical**	Enter the value into the field	Sets the number of the surveillance windows that should be displayed vertically on the **Monitor**. If value is not specified (the field is blank), then the default grid of the surveillance windows depending on the selected layout is displayed	Sequence of numbers	-	From 1 to 64
The **Basic settings** tab						
14	**Display**	Select the value from the list	Sets the mode for processing the video signals from the video cameras by the graphics card	Names of the display modes	DirectDraw (Recommended)	**Direct3D** is used when it is necessary to display the video from the fisheye cameras or the signal decoded using Intel QuickSync technology **DirectDraw (Recommended)** is used by default in all other cases **Programmed**—video signals are not processed by the graphics card
15	**Active camera**	Set the radio button	Sets the display mode for an active camera window only	Boolean type	Clear	Set—the **Active camera** mode is enabled and used Clear—the **Active camera** mode is disabled and isn't used
16	**Alarm cameras**	Set the radio button	Sets the display mode for alarm cameras windows	Boolean type	Clear	Set—the **Alarm cameras** mode is enabled and used Clear—the **Alarm cameras** mode is disabled and isn't used
17	**Max**	Enter the value into the field	Sets the maximum number of the video cameras windows that can be simultaneously displayed on the **Monitor** in the **Alarm cameras** and **List** modes. If the number of alarm cameras is greater than the maximum number, the **Monitor** will display the number of cameras specified in the **Max** field	An integer greater than zero (for example, 1, 2, 50)	-	Depends on the number of the cameras registered in the system. There are no restrictions on the number of cameras
18	**Min**	Enter the value into the field	Sets the minimum number of video cameras windows that can be displayed on the **Monitor** in the **Alarm camers** mode. If the number of the	An integer from zero and greater	-	Depends on the number of the cameras registered in the system. There are no restrictions on the number of cameras.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			alarm cameras is less than the minimum number, the **Monitor** will display fewer cameras than specified in the **Min** field. At the same time, the **Monitor** fold will remain consistent with the **Min** field	(for example, 1, 2, 50)		0—when there are no alarms, the camera windows aren't displayed in the **Monitor** window
19	**List**	Set the radio button	Set the display mode of the surveillance windows according to the selected layout	Boolean type	Set	Set—the **List** mode is enabled and used Clear—the **List** mode is disabled and isn't used
20	**Control panel**	Set the checkbox	Enables the display of the toolbar on the **Monitor** in the **List** mode	Boolean type	Clear	Set—the control panel is enabled and used Clear—the control panel is disabled and isn't used
21	**PTZ control**	Select the value from the list	Sets the priority to control the PTZ devices using the **Monitor** object	Names of the PTZ devices control priorities	Low priority	**Forbidden**—the option of the PTZ control using the **Monitor** object is disabled **Low priority**—low priority of control **Normal priority**—medium priority of control **High priority**—high priority of control
22	**Slideshow**	Enter the value into the field	Sets the period of the automatic slideshow of the camera windows when the control panel is enabled	Period in seconds (s)	Blank field	**Blank field** or **0**—the camera windows are scrolled every 3 seconds **An integer from 1 to 600**—the camera windows are scrolled at the specified interval
23	**Keep camera ratio**	Set the checkbox	Sets the ratio of the width and height of the video image in the surveillance windows on the **Video surveillance monitor**	Boolean type	Clear	Set—the ratio of the width and height of the video image corresponds to the ratio of the camera Clear—video image fits the entire area of the **Surveillance window**, while the ratio may be affected
24	**Show captions**	Set the checkbox	Shows the captions for the cameras of the **Monitor** interface window. In large distributed systems it is recommended to disable captions on those monitors where captions are not planned to be shown	Boolean type	Set	Set—the **Captions** submenu is available in the context menu of the **Monitor** interface window Clear—the **Captions** submenu is unavailable in the context menu of the **Monitor** interface window
25	**Smoothing**	Set the checkbox	It is used when it is required to display video with greater resolution on which the ladder effect appears when displaying in the small window. *Note. When this feature is enabled, the CPU load of the computer where the display is performed increases. It is recommended to use only to display video from analog cameras or low-resolution video*	Boolean type	Clear	Set—smoothing is applied Clear—smoothing isn't applied

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
26	**Audio player**	Select the value from the list	Sets the **Audio player** object used to playback the audio signals and export video recordings with audio from the **Monitor** interface	Names of the **Audio player** objects registered in the system	-	Depends on the number of the **Audio players** registered in the system
27	Group of checkboxes used to display the elements of the **Surveillance windows**	Set the checkboxes	Allows enabling and disabling the display of various elements of the Surveillance window such as number, name, time, menu, camera frame and additional info on the camera, as well as the name of **Video surveillance monitor**	Boolean type	All checkboxes are set except **Additional info**	Set—the corresponding element is displayed in the Surveillance windows of all cameras added to the Video surveillance monitor Clear—the corresponding element isn't displayed in the Surveillance windows on the Video surveillance monitor
The **List of cameras** tab						
28	**Number**	Select the value from the list	Sets the number of the video camera to display on the **Monitor**	Sequence of numbers	-	Depends on the number of the video cameras registered in the system
	Camera	Select the value from the list	Sets the name of the video camera to display on the **Monitor**	Name of the cameras registered in the system	-	Depends on the number of the video cameras registered in the system
	Video stream	Select the value from the list	Sets the number of the video stream displayed from the video camera when connected directly. If connected via the Server, this setting doesn't affect anything	Numbers of the video streams	Default	1, 2, 3, 4—video streams numbers **Default**—default video stream
	Connection	Select the value from the list	Sets the way of receiving video image from the camera	Ways of receiving video	Through Server	**Direct**—the video stream is received directly from the camera **Through Server**—the video stream is received from the Server, to which the camera is connected
	fps	Select the value from the list	Set the FPS for transmitting the video signal to the Client Monitor	Sequence of numbers	-	1, 2, 3, 4, 6, 8, 12, 16, 20, 25, 30
	Compression	Select the value from the list	Set the compression level for transmitting the video signal to the Client Monitor. The given value leads to extra consumption of Server resources	Sequence of numbers	-	In the order of increasing the compression level 0, 1, 2, 3, 4, 5 0—the video signal is not compressed 5—maximum compression of the video signal
	Compressor	Select the value from the list	Sets the algorithm for the video stream compression which is used for the video signal recompression when displaying on the **Monitor.** If you set	List of available algorithms	-	MJPEG, Motion Wavelet 3.5, MPEG4

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			the compressor, you should also set the value in the **Compression** list			
	Gate	Select the value from the list	Sets the **Videogate** object via which the live and archive video from the selected camera should be transmitted to the **Monitor**	Names of the **Videogate** objects registered in the system	-	Depends on the number of the **Videogate** objects registered in the system
	Backup archive	Select the value from the list	Sets the **Backup archive** object from which the video archive from the selected camera should be transmitted to the **Monitor**	Names of the **Backup archive** objects registered in the system	-	Depends on the number of the **Backup archive** objects registered in the system
	Edge storage	Select the value from the list	Sets the **Edge storage** object from which the video archive should be transmitted to the **Monitor** via the selected camera	Names of the **Edge storage** objects registered in the system	-	Depends on the number of the **Edge storage** objects registered in the system
	Gateway for Backup archive	Select the value from the list	Sets the **Videogate** object via which the video archive of the **Backup archive** object should be transmitted to the **Monitor**	Names of the **Videogate** objects registered in the system	-	Depends on the number of the **Videogate** objects registered in the system
	VMDA metadata storage	Select the value from the list	Sets the **VMDA metadata storage** object used for the forensic search in the archive of the corresponding camera	Names of the **VMDA metadata storage** objects registered in the system	-	Depends on the number of the **VMDA metadata storage** objects registered in the system
	Type of display	Select the value from the list	Sets the type of conversion performed in the **Surveillance window** on the **Video surveillance monitor**	Supported conversion types	PTZ	**PTZ**—virtual telemetry **Panorama**—panoramic view
	Macro1	Select the value from the list	Sets the first macro to be displayed in the function menu of the camera in the **Surveillance window**	Names of the **Macro** objects registered in the system	-	Depends on the number of the **Macro** objects registered in the system
	Macro2	Select the value from the list	Sets the second macro to be displayed in the function menu of the camera in the **Surveillance window**	Names of the **Macro** objects registered	-	Depends on the number of the **Macro** objects registered in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
				in the system		
	Guid	Automatically	Displays the unique identifier of the camera in the system	Sequence of numbers, Latin and service characters	-	A line containing a sequence of any characters (letters, digits, service characters) enclosed in {curly brackets}
29	**Range**	Click the button	Access to complex selection and editing of cameras parameters to display on the **Monitor**	-	-	-
30	**All**	Click the button	Selects all cameras registered in the system to display on the **Monitor**	-	-	-
31	**Automatic selection of streams for display**	Set the checkbox	Enables the function of automatic selection of video stream for display on the **Monitor**. Affects cameras for which the **On default** video stream is selected—see item 28	Boolean type	Clear	Set—video stream for display is selected depending on the size of the video image on the **Monitor** and the required frame frequency Clear—video stream is selected depending on the **Video stream** and **Connection** settings and on the settings of the Server and video camera from which the stream is required
The **PTZ** tab						
32	**Mouse Behavior**	-	The list of available actions with a mouse	-	-	-
33	**Action**	Select the value from the list	Sets the reaction performed when executing the corresponding action with a mouse	Reaction list of the **PTZ device** object	(Default)	Reaction list of the **PTZ device** object
34	**Param.**	Enter the value into the field	Sets the value of the reaction parameter if it's required	Depends on the selected action	-	Depends on the selected reaction. For the reactions connected with the presets, it is a preset number. For other reactions, it is speed, if the selected reaction allows speed specifying as a parameter. If the parameter isn't specified, the speed value from the settings of the **PTZ device** object that is connected with the **Camera** seleected on the **Monitor**, is used
35	**Joystick Butt.**	-	List of joystick buttons	-	-	-
36	**Action**	Select the value from the list	Sets the reaction which should be performed when clicking the joystick button	List of reaction of the **PTZ device** object	(Default)	List of reaction of the **PTZ device** object

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
37	**Param.**	Enter the value into the field	Sets the value of the reaction parameter if it is required	Depends on the selected action	-	Depends on the selected reaction. For the reactions connected with the presets, it is a preset number. For other reactions, it is speed, if the selected reaction allows speed specifying as a parameter. If the parameter isn't specified, the speed value from the settings of the **PTZ device** object that is connected with the **Camera** seleected on the **Monitor**, is used
The **Interface** tab						
38	**Alarm**	Select the value from the list	Sets the frame color of the **Surveillance window** in the alarm state	RGB colors	Red	RGB color palette
39	**Armed**	Select the value from the list	Sets the frame color of the **Surveillance window** when the camera is armed	RGB colors	Yellow	RGB color palette
40	**Disarmed**	Select the value from the list	Sets the frame color of the **Surveillance window** when the camera is disarmed	RGB colors	Green	RGB color palette
41	**No frame**	Select the value from the list	Sets the frame color of the **Surveillance window** when there is no frame in it	RGB colors	Black	RGB color palette
42	**No signal**	Select the value from the list	Sets the frame color of the **Surveillance window** when there is no signal from the camera	RGB colors	Grey	RGB color palette
43	**Screen cache**	Select the value from the list	Sets the **Surveillance window** background color that is displayed when the video from the camera does not cover completely the **Surveillance window**, for example, when the camera proportions are maintained	RGB colors	Purple	RGB color palette
44	**Tracker frame color**	Select the value from the list	Sets the frame color to highlight the tracking objects on the video image	RGB colors	White	RGB color palette
45	**Default**	Click the button	Sets the default frame colors of the **Surveillance window**	-	-	-
46	**Hide capture frames**	Set the checkbox	Hides the frames displayed by the *Face detection* module when a person's face is detected on the video image	Boolean type	Clear	Set—the Face detection frames aren't displayed Clear—the Face detection frames are displayed
47	**Over all windows**	Set the checkbox	Enables the display of the **Video surveillance monitor** on top of all windows	Boolean type	Clear	Set—the **Video surveillance monitor** is displayed on top of all windows Clear—the **Video surveillance monitor** is displayed in the default mode

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
48	**Camera switching dialog**	Set the checkbox	Enables a special dialog for selecting a camera in the **Surveillance window**	Boolean type	Clear	Set—a special dialog is used for camera selection Clear—the camera is selected in the function menu of the **Surveillance window**

26.1.5.9.4 The Settings panel of the Audio player object

The settings panel of the **Audio player** object is shown in the figure.

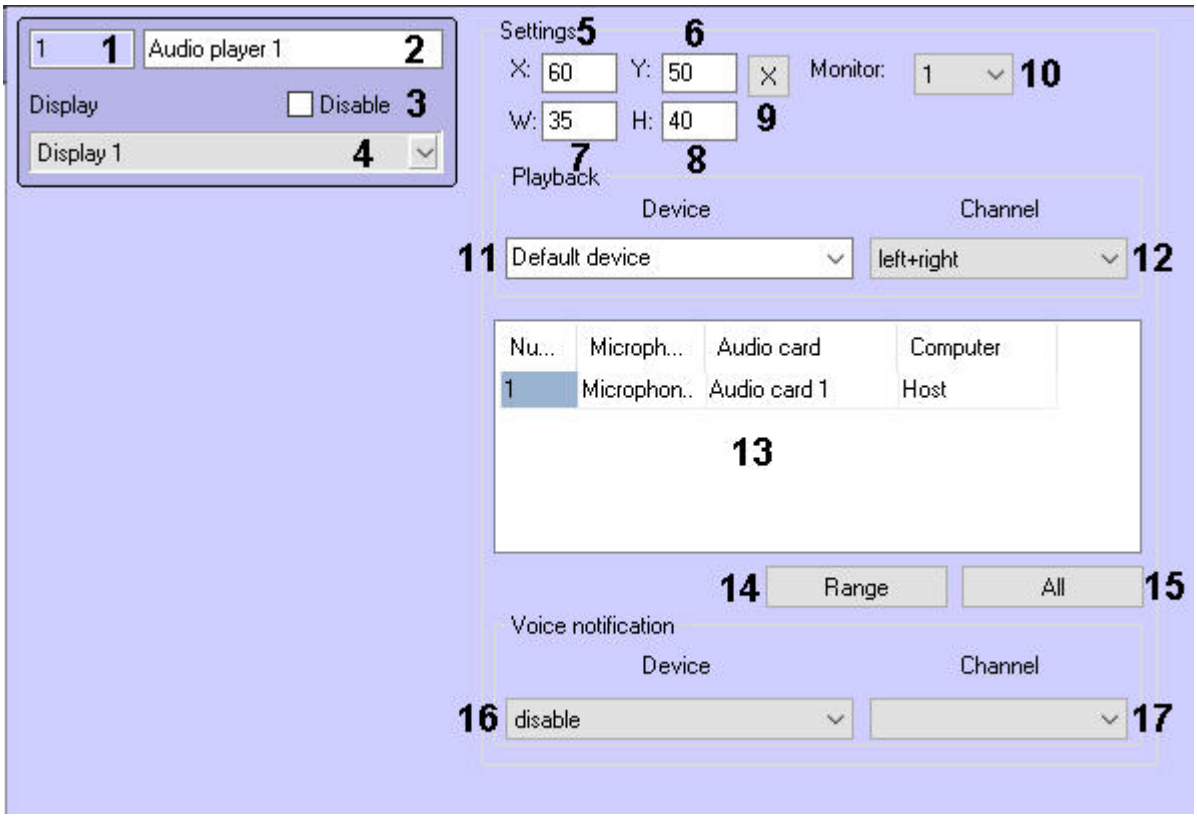


Table describes the setting parameters corresponding to the elements of the settings panel of the **Audio player** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Audio player** object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Audio player** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **Audio player** object in the system	Latin, Cyrillic and service characters	Audio player	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Audio player** object in the system	Boolean type	Clear	Set—the **Audio player** object is disabled and isn't used Clear—the **Audio player** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object for the given **Audio player** object	Names of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system
The **Settings** group						
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Audio player** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
6	**Y**	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Audio player** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
7	**W**	Enter the value into the field	Sets the width of the **Audio player** interface window	% of the screen width	-	From 35 to M*100, where M is the number of the installed monitors
8	**H**	Enter the value into the field	Sets the height of the **Audio player** interface window	% of the screen height	-	From 40 to M*100, where M is the number of the installed monitors
9	The X button	Click the button	Opens a window to set the position of the **Audio player** window	-	-	-
10	**Monitor**	Select the value from the list	Sets the number of the physical monitor, the coordinates for which are set. The monitors are numbered in the order of their physical location from left to right, from top to bottom. The 1st monitor is the one in the upper left corner regardless of which monitor is set as main or what number the monitor has in OS	Sequence of numbers	1	From 1 to 16
The **Playback** group						
11	**Device**	Select the value from the list	Sets the audio device to which the audio signals should be transmited for playback. This setting is available only if the **Display** with this **Audio Player** is assigned to one computer in the distributed system (see Assigning the displays to the operator workstations). If the **Display** is assigned to multiple computers, this setting cannot be changed and only the **Default device** can be used	Names of audio devices registered in the system	Default device	Depends on the number of the audio devices in the system. Standard sound card is the **Default device**
12	**Channel**	Select the value from the list	Sets the channel for the audio signals playback.	Left+right, left,right	Left+right	**Left+right**—audio signal is transmitted to left and right channels of audio device

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			This setting is available only if the **Display** with this **Audio Player** is assigned to one computer in the distributed system (see Assigning the displays to the operator workstations). If the **Display** is assigned to multiple computers, this setting cannot be changed			**Left**—audio signal is transmitted to the left channel of the audio device **Right**—audio signal is transmitted to the right channel of the audio device
The microphones table						
13	**Name**	Select the value from the list	Sets the microphone, the audio signals from which should be recorded and/or played back	Names of the **Microphone** objects registered in the system	-	Depends on number of the **Microphone** objects in the system
14	**Range**	Click the button	Opens the window for bulk addition of microphones	-	-	-
15	**All**	Click the button	Adds all microphones created in the hardware tree to the list	-	-	-
The **Voice notification** group						
16	**Device**	Select the value from the list	Sets the voice notification device when an alarm is registered by video cameras	Names of the voice notification devices registered in the system	disable	Depends on the voice notification devices registered in the system. Standard sound card is the **Default device**
17	**Channel**	Select the value from the list	Sets the channel of the voice notification when an alarm is registered by video cameras	Left+right, left, right	-	**Left+right**—audio signal is transmitted to the left and right channels of the voice notification device **Left**—audio signal is transmitted to the left channel of the voice notification device **Right**—audio signal is transmitted to the right channel of the voice notification device

26.1.5.9.5 The Settings panel of the Telemetry control panel object

The **Telemetry control panel** object is used to register and configure the **Universal PTZ control panel** interface object in *Intellect.* The **Universal PTZ control panel** interface object is used to control the PTZ devices.

The settings panel of the **Telemetry control panel** object is shown in the figure.

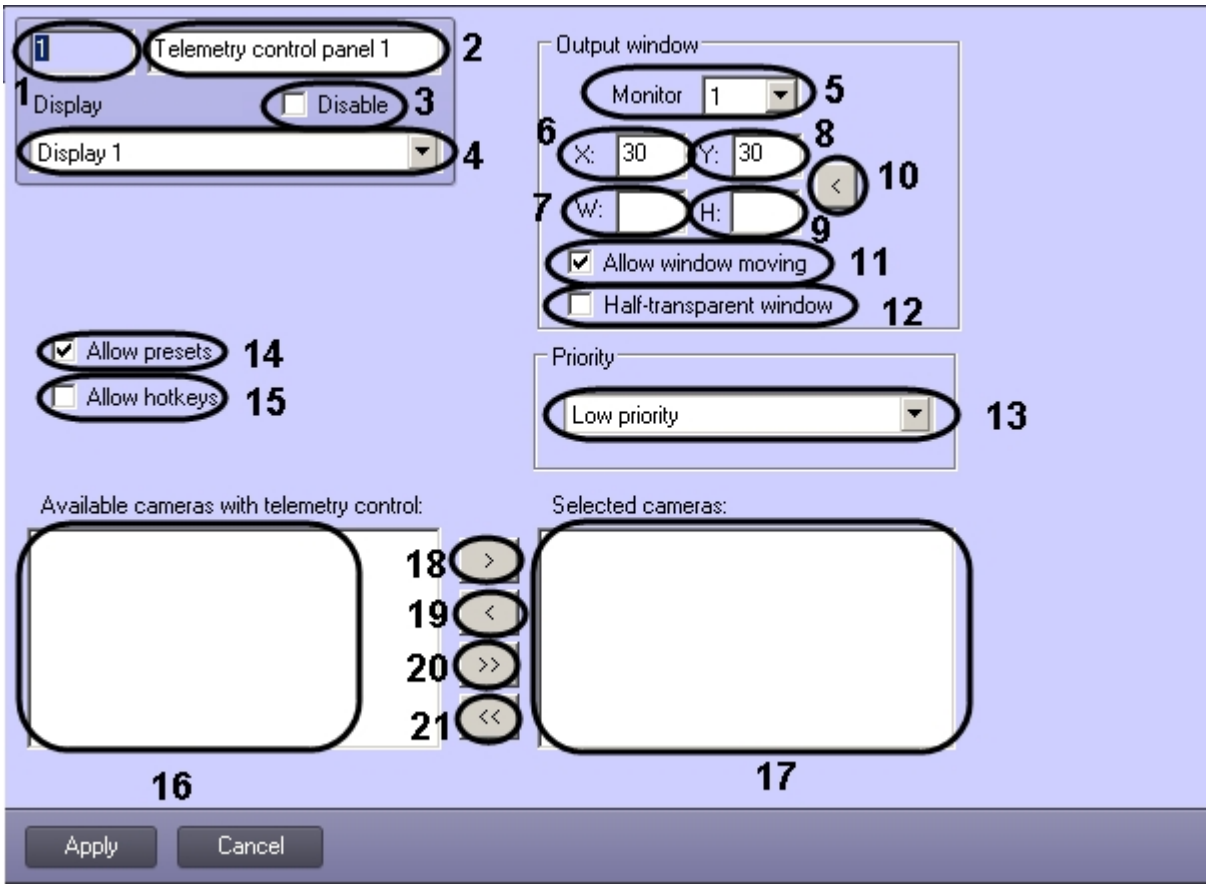


Table describes the setting parameters corresponding to the elements of the settings panel of the **Telemetry control panel** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Telemetry control panel** object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Telemetry control panel** objects in the system
2	Name*	Enter the value into the field	Sets the name of the **Telemetry control panel** object in the system	Latin, Cyrillic and service characters	Telemetry control panel	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Telemetry control panel** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Telemetry control panel** object is disabled and isn't used Clear—the **Telemetry control panel** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object in the digital system with distributed architecture to which	Names of the **Display** objects registered in the system	Name of the **Display** parent object.	Depends on the number of the **Display** objects in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			the given **Telemetry control panel** object belongs			
The **Output window** group						
5	**Monitor**	Select the value from the list	Sets the number of the monitor for which the coordinates are set	Number of the monitor in OS	1	1-16
6	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Telemetry control panel** on the screen	% of the screen width	30	From 0 to M*100, where M is the number of the installed monitors
7	**W**	Enter the value into the field	Sets the width of the **Telemetry control panel** interface window	% of the screen width	-	From 18 to M*100, where M is the number of the installed monitors
8	**Y**	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Telemetry control panel** on the screen	% of the screen height	30	From 0 to M*100, where M is the number of the installed monitors
9	**H**	Enter the value into the field	Sets the height of the **Telemetry control panel** interface window	% of the screen height	-	From 34 to M*100, where M is the number of the installed monitors
10	Current coordinates*	Click the button	Sets the current coordinates of the **Telemetry control panel** in the X, Y, W and H fields	-	-	-
11	**Allow window moving**	Set the checkbox	Allows moving the **Telemetry control panel** using the mouse	Boolean type	Set	Set—allow moving the **Telemetry control panel** Clear—disable moving the **Telemetry control panel**
12	**Half-transparent window**	Set the checkbox	Displays the half-transparent **Telemetry control panel**	Boolean type	Set	Set—display the half-transparent **Telemetry control panel** Clear—do not display the half-transparent **Telemetry control panel**
13	**Priority**	Select the value from the list	Sets the priority of the PTZ devices control	Names of the priorities to control the PTZ devices	Low priority	**Forbidden**—control of the PTZ device using the **Telemetry control panel** is forbidden **Low priority**—control of the PTZ device using the **Telemetry control panel** is performed after it controls the devices with Normal or High priority

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Normal priority—control of the PTZ device using the **Telemetry control panel** is performed after it controls devices with High priority **High priority**—control of the PTZ device using the **Telemetry control panel** is performed in the first place
14	**Allow presets**	Set the checkbox	Allows saving the position of the PTZ device in the presets	Boolean type	Set	Set—allow saving the position of the PTZ device in the presets Clear—disable saving the position of the PTZ device in the presets
15	**Allow hotkeys**	Set the checkbox	Enables the PTZ device control using the keyboard	Boolean type	Clear	Set—keyboard can be used to control the PTZ device Clear—keyboard hotkeys cannot be used to control the PTZ device
16	**Available cameras with telemetry control**	Automatically	Displays the video cameras with the PTZ devices	Names of the **Camera** objects registered in the system	List of all **Camera** objects registered in the system	Depends on the number of the PTZ devices in the digital system with distributed architecture
17	**Selected cameras**	Select by clicking the arrow keys	Sets the video cameras with the PTZ devices that can be controlled using the **Telemetry control panel**	-	-	Depends on the number of the PTZ devices in the digital system with distributed architecture
18	One to the right*	Click the button	Moves the selected PTZ device from the **Available cameras with telemetry contro**l list to the **Selected cameras** list	-	-	-
19	One to the left*	Click the button	Moves the selected PTZ device from the **Selected cameras** list to the **Available cameras with telemetry control** list	-	-	-
20	All to the right*	Click the button	Moves all PTZ devices from the **Available cameras with telemetry control** list to the **Selected cameras** list	-	-	-
21	All to the left*	Click the button	Moves all PTZ devices from the **Selected cameras** list to the **Available cameras**	-	-	-

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
			with telemetry control list			

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.9.6 The Settings panel of the Backup archive panel object

The **Backup archive panel** object is used to register and configure the **Backup archive panel** interface object in *Intellect,* which allows the Operator to configure video data archiving.

The settings panel of the **Backup archive panel** object is shown in the figure.

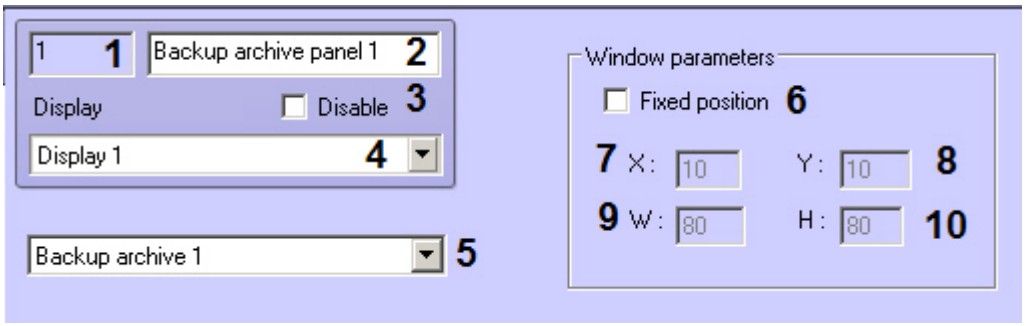


Table describes the setting parameters corresponding to the elements of the settings panel of the **Backup archive panel** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Backup archive panel**	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Backup archive panel** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Backup archive panel** object	Latin, Cyrillic and service characters	Backup archive panel	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state of the **Backup archive panel** object	Boolean type	Clear	Set—the **Backup archive panel** object is disabled and isn't used Clear—the **Backup archive panel** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object of the digital system with distributed architecture, to which the given **Backup archive panel** object belongs	Name of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the digital video surveillance system with distributed architecture
5	Backup archive*	Select the value from the list	Sets a **Backup archive**, which the Operator will control using the **Backup archive panel** interface object	Name of the **Backup archive** objects registered in the system	Backup archive 1	Depends on the number of the **Backup archive** objects in the digital video surveillance system with distributed architecture

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
6	**Fixed position**	Set the checkbox	Allows moving the **Backup archive panel** on the screen using the mouse	Boolean type	Clear	Set—the **Backup archive panel** cannot be moved Clear—the **Backup archive panel** can be moved
7	**X**	Enter the value into the field (Automatically, if the **Fixed position** checkbox is set)	Sets the X coordinate in the horizontal axis for the upper left corner of the **Backup archive panel** on the screen	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
8	**Y**	Enter the value into the field (Automatically, if the **Fixed position** checkbox is set)	Sets the Y coordinate in the vertical axis for the upper left corner of the **Backup archive panel** on the screen	% of the screen height	Not defined	From 0 to M*100, where M is the number of the installed monitors
9	**W**	Enter the value into the field (Automatically, if the **Fixed position** checkbox is set)	Sets the width of the **Backup archive panel**	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
10	**H**	Enter the value into the field (Automatically, if the **Fixed position** checkbox is set)	Sets the height of the **Backup archive panel**	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.9.7 The Settings panel of the Map object

The **Map** object is used to register and configure the **Map** interface object in *Intellect*, which allows creating and positioning the icons of the installed devices on the map of the protected area and using the icons to operate the devices.

The settings panel of the **Map** object is shown in the figure:

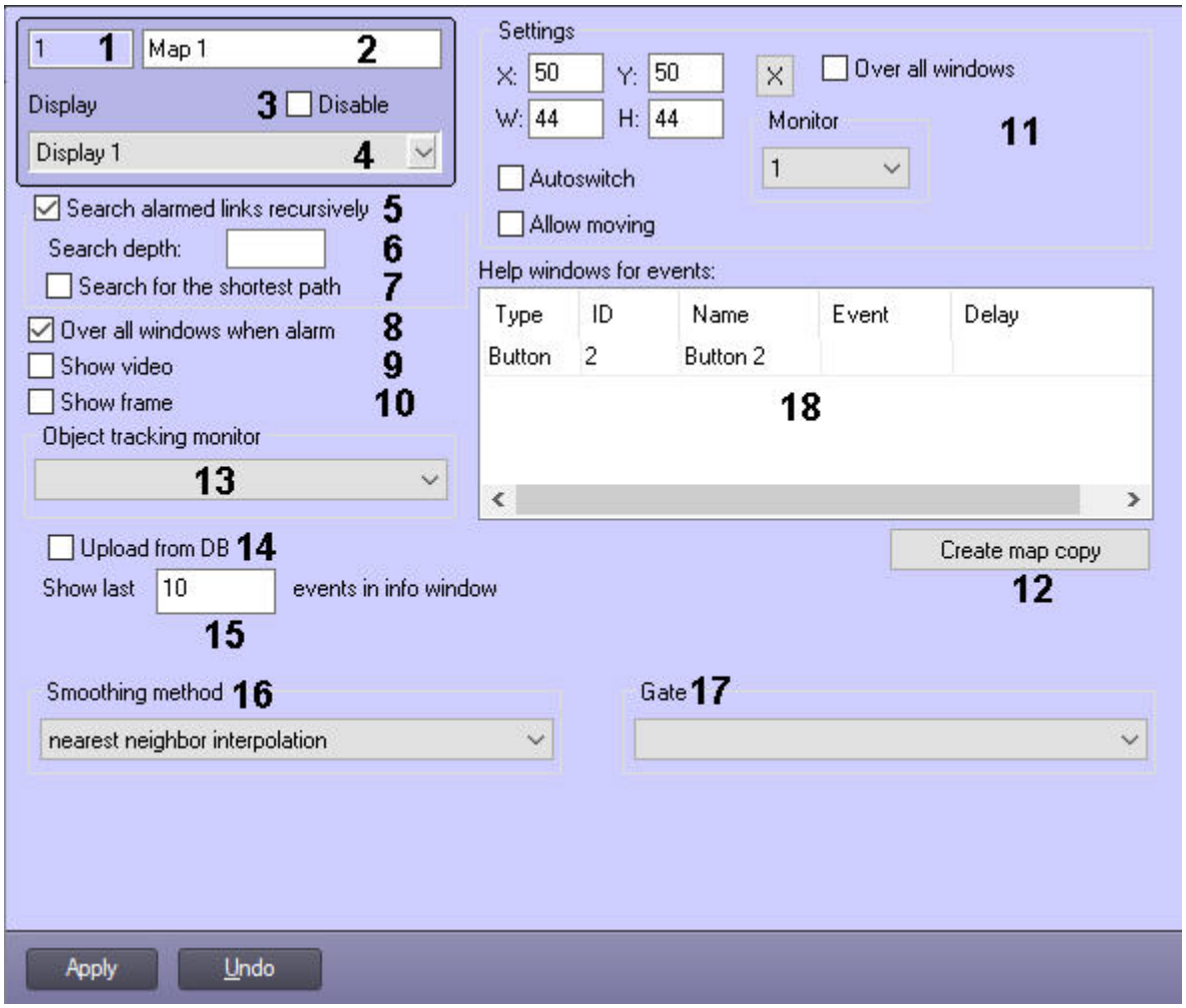


Table describes the setting parameters corresponding to the elements of the settings panel of the **Map** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **Map** object in the digital video surveillance system with distributed architecture	Sequence of numbers	-	From 1 and above. Depends on the number of the **Map** objects in the digital video surveillance system with distributed architecture
2	Name	Enter the value into the field	Sets the name of the **Map** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	Map	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the status of the **Map** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Map** object is disabled and isn't used Clear—the **Map** object is enabled and used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Display**	Select the value from the list	Sets the **Display** parent object of the digital system with distributed architecture to which the given **Map** object belongs	Name of the **Display** objects registered in the system	Name of the **Display** parent object.	Depends on the number of the **Display** objects in the digital video surveillance system with distributed architecture
5	**Search alarmed links recursively**	Set the checkbox	Sets if recursive search for the objects on the layers is possible. The recursive search is a search, where the transition from one layer, containing an object, to another layer, containing an icon, is performed by successive jumps to the the neighboring layers, using sequential links	Boolean type	Clear	Set—a recursive search is enabled Clear—a recursive search is disabled
6	**Search depth**	Enter the value into the field	Sets the search depth for alarms across map layers if the Map is multi-layered. This parameter determines how many layers will indicate the alarm. The value can only be entered if the **Search alarmed links recursively** checkbox is set.	Sequence of numbers	Clear	**Empty field**—search across layers is not limited; **0**—related layers are not taken into account during search, that is, in case of alarm, only the layer on which the alarm occurred will blink; **>0**—indicates the number of layers through which the search will be performed. For example, the Map has 6 interconnected layers and the alarm appeared on the 3rd layer. If the key value=1, the alarm will blink on layer 3, as well as on layers 2 and 4
7	**Search for the shortest path**	Set the checkbox	Enables the search for the shortest path to the alarmed layer. If there are several paths from the active layer to the alarmed layer, then the shortest path is automatically found and selected when the **Alarm** signal is received (only one icon, that is **Link to layer**, will blink in the active layer, indicating the shortest path). Works together with the **Search alarmed links recursively** option only	Boolean type	Clear	Set—search for the shortest path is enabled Clear—search for the shortest path is disabled
8	**Over all windows when alarm**	Set the checkbox	Sets if the window of the **Map** interface object can be displayed over all active applications in case the **Alarm** signal is received from any object of the **Map** interface object	Boolean type	Clear	Set—the window of the **Map** interface object is displayed over all active applications in case the **Alarm** signal is received from any object of the **Map** interface object Clear—the window of the **Map** interface object isn't displayed over all active applications in case the **Alarm** signal is received from any object of the **Map** interface object
9	**Show video**	Set the checkbox	Enables the function of live and archive video request from the map for cameras and objects linked with cameras	Boolean type	Clear	Set—the functions to request live and archive video are available in the menu of the **Camera** objects and objects linked with cameras

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the functions to request live and archive video are not available in the menu of the **Camera** objects and objects linked with cameras
10	**Show frame**	Set the checkbox	Enables the function of frame request from the map for cameras and objects linked with cameras	Boolean type	Clear	Set—the function to request archive frame is available in the menu of the **Camera** objects and objects linked with cameras Clear—the function to request archive frame is not available in the menu of the **Camera** objects and objects linked with cameras
The **Settings** group						
11	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Map** interface object on the screen	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Map** interface object on the screen	% of the screen height	Not defined	From 0 to M*100, where M is the number of the installed monitors
	W	Enter the value into the field	Sets the width of the **Map** interface object window	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the **Map** interface object window	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
	Autoswitch	Set the checkbox	Sets autoswitch to the **Alarm** layer in the **Map** interface object	Boolean type	Clear	Set—when **Alarm** is received from an object, the system will switch to the layer where the object is located Clear—when **Alarm** is received from an object, the system won't switch to the layer where the object is located
	The **×** button	Click the button	Opens a window to set the map position using a test window	-	-	-
	Over all windows	Set the checkbox	Allows displaying the **Map** window on top of all windows	Boolean type	Clear	Set—the **Map** is displayed on top of all windows Clear—the **Map** is displayed in standard mode

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
	Monitor	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	1–9
	Allow moving	Set the checkbox	Allows moving the **Map** interface window manually	Boolean type	Clear	Set—allow moving the **Map** interface window manually Clear—disable moving the **Map** interface window manually
Outside groups						
12	**Create map copy**	Click the button	Creates another **Map** object with all parameters identical to the given object	-	-	-
13	**Object tracking monitor**	Select the value from the list	Selects the object tracking monitor. For details, see Using absolute telemetry	Names of the available **Monitor** objects	-	Depends on the number of the **Monitor** objects created in the system
14	**Upload from DB**	Set the checkbox	Enables uploading events from database to show on the **Map**	Boolean type	Clear	Set—the events are uploaded from the database on *Intellect* start, so the events before and after *Intellect* start are displayed on the **Map** Clear—only the events occurred after *Intellect* start are displayed on the **Map**
15	**Show last ____ events in info window**	Enter the value into the field	Sets the number of events of the selected object to be displayed in the info window on the **Map**	Sequence of numbers	10	From 1 to 99
16	**Smoothing method**	Select the value from the list	Sets the **Map** smoothing method when scaling *Note. Smoothing minimizes ladder-like diagonal edges of the image and gives the impression of softer borders and higher resolution*	Names of the smoothing methods	-	low quality high quality bilinear interpolation bicubic interpolation nearest neighbor method high quality bilinear interpolation high quality bicubic interpolation
17	**Gate**	Select the value from the list	Sets the **Videogate** through which the video will be displayed on the **Map**	Names of the **Videogate** objects registered in the system	-	Depends on the number of the **Videogate** objects in the digital video surveillance system with distributed architecture
The **Help windows for events** table						

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
18	**Type**	Select the value from the list	Sets the type of an object. When an event is received from this object, a pop-up tip with the name of the event is displayed	Types of objects registered in the system	-	Depends on the number of the objects registered in the system
	id	Select the value from the list	Sets the object identifier. When an event is received from this object, a pop-up tip with the name of the event is displayed	Identifiers of the objects of the selected type registered in the system	-	Depends on the number of the objects registered in the system
	Name	Automatically	Sets the name of an object. When an event is received from this object, a pop-up tip with the name of the event is displayed	Names of the objects of the selected type registered in the system	-	Depends on the number of the objects registered in the system
	Event	Select the value from the list	Sets the name of an event. When this event is received, a pop-up tip is displayed	Events of the objects of the selected type	-	Depends on the object type
	Delay	Enter the value into the field	Sets the time period in seconds for the pop-up tip to be displayed after the event is received	Integer	-	>=0

26.1.5.9.8 The Settings panel of the Layer object

The **Layer** object is used to create and configure the layers of the map of the protected facilities in *Intellect.*

The settings panel of the **Layer** object is shown in the figure.

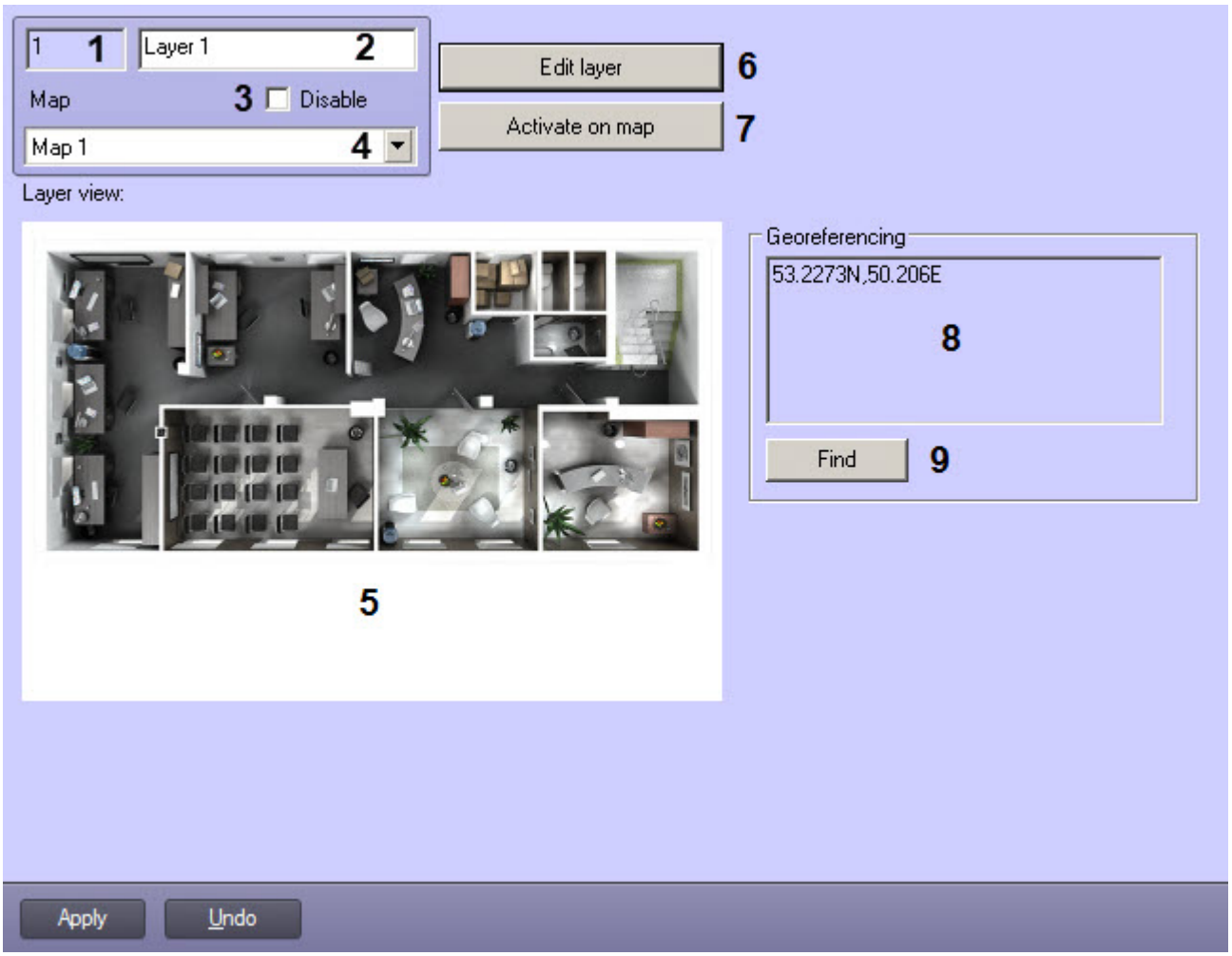


Table describes the setting parameters corresponding to the elements of the settings panel of the **Layer** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Layer** object in the digital video surveillance system with distributed architecture	Sequence of numbers	-	From 1 and above. Depends on the number of the **Layer** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Layer** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	Layer	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Layer** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Layer** object is disabled and isn't used Clear—the **Layer** object is enabled and used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Map**	Select the value from the list	Sets the **Map** parent object of the digital system with distributed architecture, to which the given **Layer** object belongs	Names of the **Map** objects registered in the system	Name of the **Map** parent object	Depends on the number of the **Map** objects in the digital video surveillance system with distributed architecture
5	Schematic view of the layer	-	Displayes the layout of the protected territory	-	-	-
6	**Edit layer**	Click the button	Opens the panel, which allows adding/removing and configuring the icons of the installed devices on the schematic view of the protected territory	-	-	-
7	**Activate on map**	Click the button	Displays on the given layer on top of all layers on the **Map** interface object	-	-	-
8	**Georeferencing**	Using the *Map editor* utility	Displays the coordinates set using the *Map editor* utility —see Configuring map binding to coordinate grid	Coordinates	-	Latitude and longitude coordinates accurate to the 4th digit, with point as decimal separator. Value example: 53.2273N,50.206E
9	**Find**	Click the button	Displays a Google map at the coordinates specified in the **Georeferencing** field	-	-	-

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.9.9 The Settings panel of the Event viewer object

On the page:

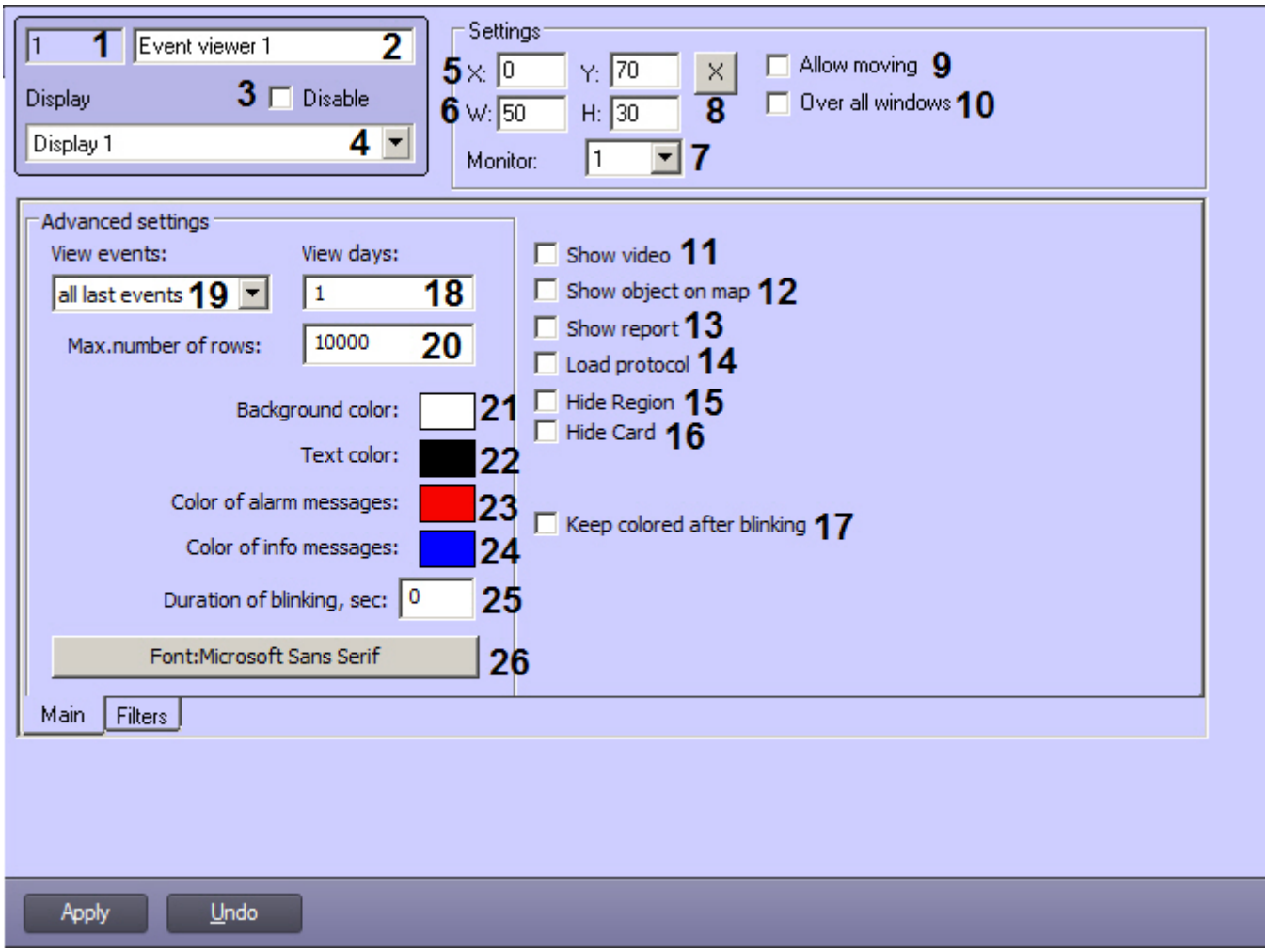
- The Main tab
- The Filters tab

The **Event viewer** object is used to register and configure an interface object in *Intellect.* The interface object is used to display text information about the specified events initialized by the digital video surveillance system with distributed architecture.

The settings panel of the **Event viewer** object is shown in the figures.

Tables below describe the setting parameters corresponding to the elements of the settings panel of the **Event viewer** object.

26.1.5.9.9.1 The **Main** tab



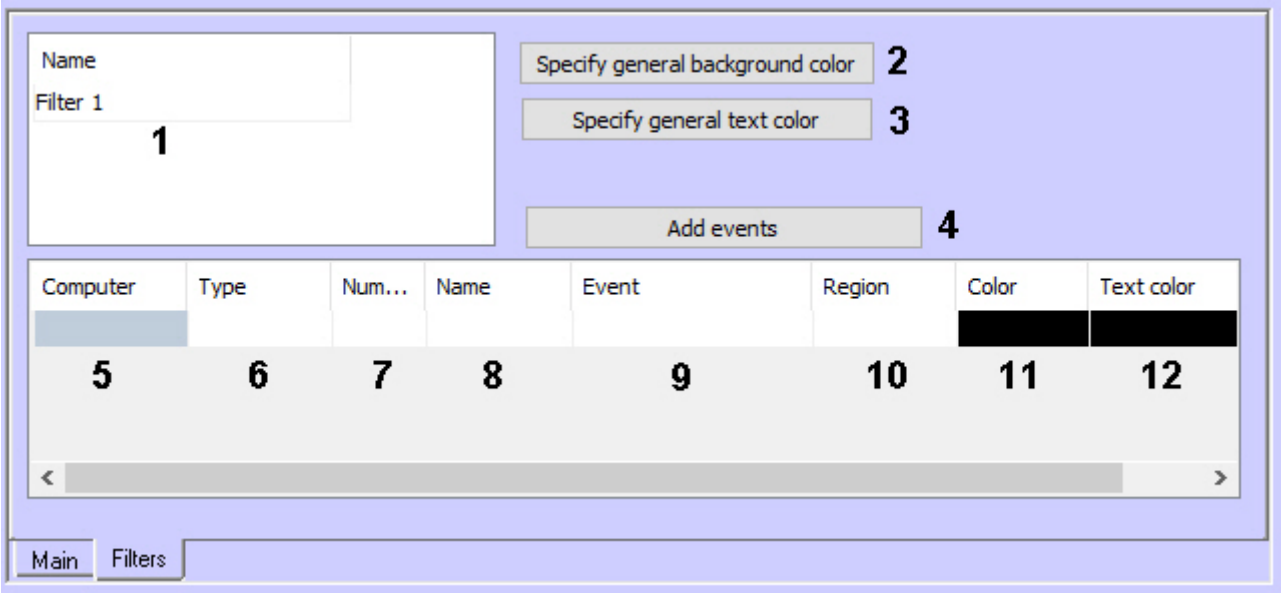
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Event viewer** object in the digital video surveillance system with distributed architecture	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Event Viewer** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Event viewer** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	Event viewer	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Event viewer** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Event viewer** object is disabled and isn't used Clear—the **Event viewer** object is enabled and used

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Display**	Select the value from the list	Sets the **Display** parent object of the digital system with distributed architecture, to which the given **Event viewer** object belongs	Names of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the digital video surveillance system with distributed architecture
The **Settings** group						
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the window of the **Event viewer** interface object on the screen	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the window of the **Event viewer** interface object on the screen	% of the screen height	Not defined	From 0 to M*100, where M is the number of the installed monitors
6	**W**	Enter the value into the field	Sets the width of the window of the **Event viewer** interface object	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the window of the **Event viewer** interface object	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
7	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	1–16
8	**The × button**	Click the button	Opens the window to set the **Event viewer** window size and position using the mouse	-	-	-
9	**Allow moving**	Set the checkbox	Allows the Operator to change the position of the **Event viewer** window using the mouse	Boolean type	Clear	Set—the Operator can change the position of the **Event viewer** window Clear—the Operator cannot change the position of the **Event viewer** window
10	**Over all windows**	Set the checkbox	Allows displaying the **Event viewer** window on top of all windows	Boolean type	Clear	Set—the **Event viewer** window is displayed on top of all windows Clear—the **Event viewer** window is displayed in the standard mode
11	**Show video**	Set the checkbox	Allows the Operator to view the events archive initialized by the **Event viewer** as **Record to disk** using the **Event viewer** window	Boolean type	Clear	Set—the Operator can view the events archive using the **Event viewer** window Clear—the Operator cannot view the events archive using the **Event viewer** window
12	**Show object on map**	Set the checkbox	Allows the Operator to view the objects, displayed in the **Event viewer** window, on the map	Boolean type	Clear	Set—the Operator can view the objects, displayed in the **Event viewer** window, on the map

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the Operator cannot view the objects, displayed in the **Event viewer** window, on the map
13	**Show report**	Set the checkbox	Allows the Operator to create a printed form of the report and print the information about all events registered by the **Event viewer** over a specified period of time	Boolean type	Clear	Set—the Operator can creating a printed form of the report and print the information about all events registered by the **Event viewer** over a specified period of time Clear—the Operator cannot creat a printed form of the report and print the information about all events registered by the **Event viewer** over a specified period of time
14	**Load protocol**	Set the checkbox	Determines if the latest 1000 events registered by the **Event viewer** with the latest system start, should be downloaded with the start of *Intellect*	Boolean type	Clear	Set—the latest 1000 events registered by the **Event viewer** with the latest system start, are downloaded with the start of *Intellect* Clear—the latest 1000 events registered by the **Event viewer** with the latest system start, aren't downloaded with the start of *Intellect*
15	**Hide Region**	Set the checkbox	Hides the **Region** column in the **Event viewer** window	Boolean type	Clear	Set—the **Region** column isn't displayed Clear—the **Region** column is displayed
16	**Hide Card**	Set the checkbox	Hides the **Card** column in the **Event viewer** window. See also Card number displaying in the Event viewer window for access events	Boolean type	Clear	Set—the **Card** column isn't displayed Clear—the **Card** column is displayed
17	**Keep colored after blinking**	Set the checkbox	Sets the highlighting of the alarm messages by the selected color after the blinking stops	Boolean type	Clear	Set—the alarm messages are highlighted by the selected color after the blinking stops Clear—the alarm message isn't highlighted by the selected color after the blinking stops. It is highlighted by the color specified in the filter
The **Advanced settings** group						
18	**View days**	Enter the value into the field	Sets the period over which the events should be displayed in the **Event viewer** window, if there are more than 10,000 events (or other value set for the **Max.number of rows** parameter). If there are less events, then all events are displayed regardless of the value of this parameter	Days	1	More than 1
19	**View events**	Select the value from the list	Sets the events that should be displayed in the **Event viewer** window	-	all events	**all events**—all events are displayed in the **Event viewer** window **last event**—one last event is displayed in the **Event viewer** window

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						all last events—all last events for all selected objects are displayed
20	**Max.number of rows**	Enter the value into the field	Sets the maximum number of events to display in the **Event viewer**	Sequence of numbers	10000	1–50000
21	**Background color**	Select the value from the list or on the **Select color** panel	Sets the background color in the **Event viewer** window	RGB, CMY or HSL	White	Corresponds to the standard range of the selected color system
22	**Text color**	Select the value from the list or on the **Select color** panel	Sets the text color in the **Event viewer** window	RGB, CMY or HSL	Black	Corresponds to the standard range of the selected color system
23	**Color of alarm messages**	Select the value from the list or on the **Select color** panel	Sets the color of the alarm message lines in the **Event viewer** window. To apply the setting, the **Duration of blinking, sec** parameter should be other than 0	RGB, CMY or HSL	Red	Corresponds to the standard range of the selected color system
24	**Color of info messages**	Select the value from the list or on the **Select color** panel	Sets the color of the information message lines in the **Event viewer** window. To apply the setting, the **Duration of blinking, sec** parameter should be other than 0	RGB, CMY or HSL	Blue	Corresponds to the standard range of the selected color system
25	**Duration of blinking, sec**	Enter the value into the field	Sets the duration of the alarm message blinking in the **Event viewer** window	seconds	Not defined	More than 0
26	**Font:**<current font>	Click the button	Sets the font of the nformation messages in the **Event viewer** window	Standard Windows **Font** dialog window	Depends on OS settings	-

26.1.5.9.9.2 The **Filters** tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Name**	Enter the value into the field	Sets the filter name in the **Event viewer** window	Latin, Cyrillic and service characters	Filter 1, Filter 2, etc.	Depends on the number of the created filters
2	**Specify general background color**	Click the button	Opens the window to select the message background color in the default filter	-	-	-
3	**Specify general text color**	Click the button	Opens the window to select the message text color in the default filter	-	-	-
4	**Add events**	Click the button	Opens the window for bulk adding the events from an object of the selected type	-	-	-
5	**Computer**	Select the value from the list	Sets the **Computer** object on the basis of which the objects included in the filter should be created	Names of the **Computer** objects registered in the system	Not defined	Depends on the number the **Computer** objects in the distributed video surveillance system
6	**Type**	Select the value from the list	Sets the types of a device that should be displayed in the **Event viewer**. ***Note.*** *If the field is blank, the* ***Event viewer*** *window displays all events of all objects in the system*	Types of objects registered in the system.	Not defined	Depends on the number of the device types created in the digital video surveillance system with distributed architecture
7	**Number**	Select the value from the list	Sets the identification number of the device. ***Note.*** *If the field is blank, the* ***Event viewer*** *window displays all events of all objects of the selected type*	Sequence of numbers	Not defined	Depends on the number of the created devices of the selected type in the digital video surveillance system with distributed architecture

8	**Name**	Automatically	Displays the name of the device selected in the previous item	Name of the objects of the selected type registered in the system	Name of specified system object	Depends on the number of the devices of the selected type in the digital video surveillance system with distributed architecture
9	**Event**	Select the value from the list	Sets the event received from the selected devices and that should be logged into the **Event viewer**. ***Note.*** *If the field is blank, the* ***Event viewer*** *window displays all events received from the specified devices*	Names of the event types for the selected type of devices	Not defined	Depends on the type of an object
10	**Region**	Select the value from the list	Sets the region. The events from the devices located in this region will be displayed in the **Event viewer**	Name of the region registered in the system.	Not defined	Depends on the number of the **Region** structure elements created in the digital video surveillance system with distributed architecture
11	**Color**	Select the value from the list	Sets the messages highlighting color in the **Event viewer** window	RGB, CMY or HSL	White	Corresponds to the standard range of the selected color system
12	**Text color**	Select the value from the list	Sets the messages text color in the **Event viewer** window	RGB, CMY or HSL	Black	Corresponds to the standard range of the selected color system

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.9.10 The Settings panel of the Operator protocol object

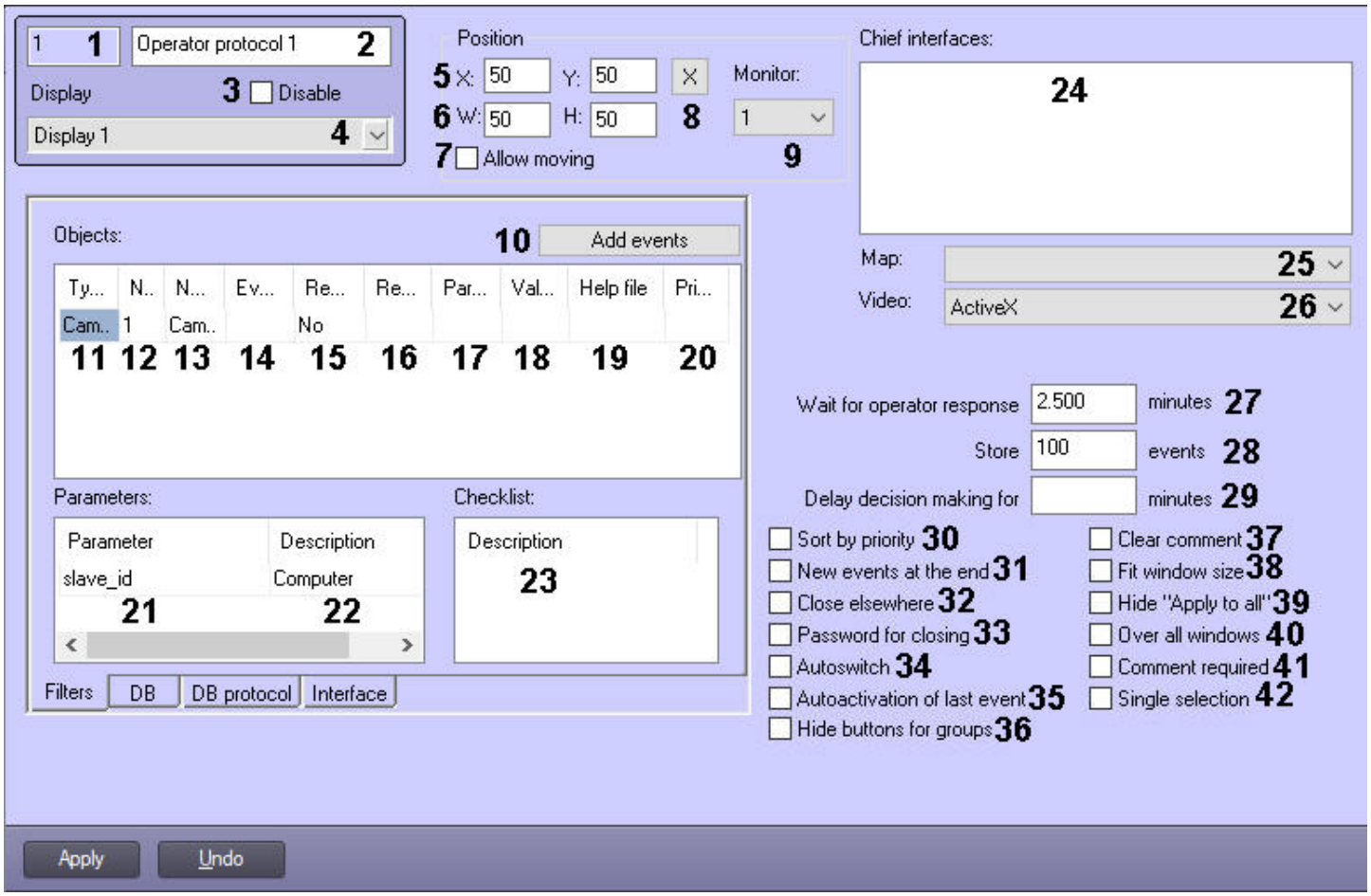
On the page:

- The Filters tab
- The DB tab
- The DB protocol tab
- The Interface tab

The settings panel of the **Operator protocol** object is shown in the figures.

Tables below describe the setting parameters corresponding to the elements of the settings panel of the **Operator protocol**.

26.1.5.9.10.1 The **Filters** tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Operator protocol** object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Operator protocol** objects in the system
2	Name*	Enter the value into the field	Sets the name of the **Operator protocol** object in the system	Latin, Cyrillic and service characters	Operator protocol	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the status (enabled or disabled) of the **Operator protocol** object in the system	Boolean type	Clear	Set—the **Operator protocol** object is disabled and isn't used Clear—the **Operator protocol** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object for the given **Operator protocol** object	Name of the **Display** objects registered in the system.	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Operator protocol** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Operator protocol** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
6	**W**	Enter the value into the field	Sets the width of the **Operator protocol** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the **Operator protocol** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
7	**Allow moving**	Set the checkbox	Allows moving the **Operator protocol** interface window manually	Boolean type	Clear	Set—allow moving the **Operator protocol** interface window manually Clear—disable moving the **Operator protocol** interface window manually
8	The **×** button	Click the button	Opens a test window to set the position of the **Operator protocol** interface window	-	-	-
9	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	From 1 to 16
10	**Add events**	Click the button	Opens the window for bulk adding the events from an object of the selected type	-	-	-
The **Filters** tab						
11	**Type**	Select the value from the list	Sets the type of objects, the events from which should be displayed in the **Operator protocol** window	Available object types	-	Depends on the objects registered in the system. Only the objects for which the INFORMATION or ALARM value is selected in the **Messages processing** column on the **Events** tab in the ddi.exe utility are available for selection (see The Events tab)
12	**Number**	Select the value from the list	Sets the number of an object, which events should be displayed in the **Operator protocol** window	Sequence of numbers	-	Depends on the number of the objects of the specified type registered in the system
13	**Name**	Automatically	Sets the name of an object, which events should be displayed in the **Operator protocol** window	Names of the objects registered in the system	-	Depends on the objects registered in the system
14	**Event type**	Select the value from the list	Sets the events displayed in the **Operator protocol** interface window	Events available for	-	Depends on the object type

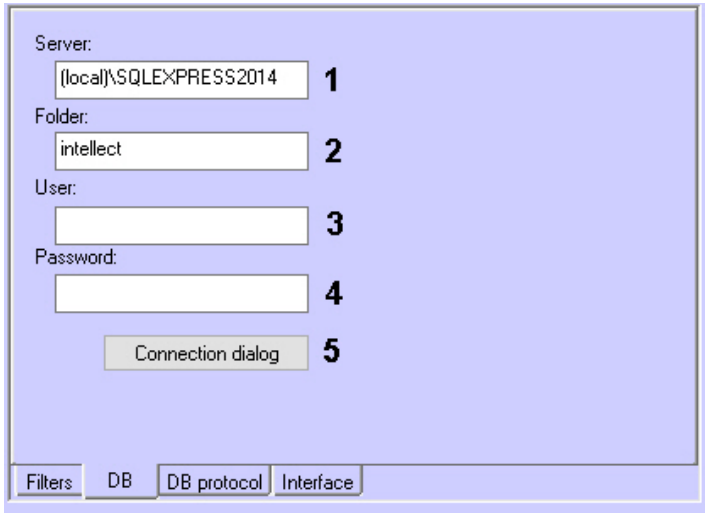
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
				the selected object		
15	**Request password**	Select the value from the list	Defines the necessity of password to process the event	Boolean type	-	Set—password confirmation is required to process the event Clear—password confirmation isn't required to process the event
16	**Region**	Select the value from the list	Sets the **Region** object corresponding to the monitored object	List of the **Region** objects created in the system	-	Depends on the number of the **Region** objects created in the system
17	**Parameter**	Enter the value into the field	Sets the parameter of the monitored object	Depends on the event type	-	Depends on the event type
18	**Value**	Enter the value into the field	Sets the parameter value of the monitored object	Depends on the event type	-	Depends on the event type
19	**Help file**	Enter the value into the field	Sets the full path to the text file in pdf, doc, docx, txt or other format which contains the help guide about the event processing	File address in the file system	-	Depends on the file system limitations
20	**Priority**	Select the value from the list	Sets the event priority for sorting by importance	Sequence of numbers	-	1–10 The lower the value, the higher the priority
The **Parameters** table						
21	**Parameter**	Enter the value into the field	Sets the name of the parameter, the value of which should be displayed in the **Operator protocol** interface window	Latin, Cyrillic and service characters	-	Depends on the parameters sent by the event
22	**Description**	Enter the value into the field	Enter a short description of the specified parameter	Latin, Cyrillic and service characters	-	0–255 characters
The **Checklist** table						
23	**Description**	Enter the value into the field	Sets the description of the action that the operator must perform before assigning a status to the event	Latin, Cyrillic and service characters	-	0–255 characters
Not in the group						
24	**Chief interfaces**	Set the checkbox	Sets the **Operator protocol** object, to which the events should be sent after the time specified in the **Wait for operator response for** field	List of the available **Operator protocol**	-	Depends on the number of the **Operator protocol** objects created in the system

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
				objects in the system		
25	**Map**	Select the value from the list	Sets the **Map** interface object used to display the monitored object	List of the available **Map** objects in the system	-	Depends on the number of the **Map** objects created in the system
26	**Video**	Select the value from the list	Sets the method of the archive and live video display on the event in the **Operator protocol**	Available display methods	ActiveX	**ActiveX**—archive will open in a separate window **Monitor**—archive will open on the selected Video surveillance monitor
27	**Wait for operator response ____ minutes**	Enter the value into the field	Sets the time after which the event will be assigned the **Non-processed event** type or the event will be escalated	Min	2.5	0–10000 Fractional values can be specified; integer and fractional parts are point-separated. For example, to set 2 minutes 30 seconds time period, enter 2.5
28	**Store ____ events**	Enter the value into the field	Enter the maximum number of events that can be displayed simultaneously in the list of the current events	Sequence of numbers	100	Any integer starting from 0
29	**Delay decision making for ____ minutes**	Enter the value into the field	Sets the time for which the operator can delay the event processing	Min	-	0–600 The value is not specified or 0—the operator can not delay the event processing Greater than 0—the parameter sets the time for which the operator can delay the event processing Fractional values can be specified; integer and fractional parts are point-separated. For example, to set 2 minutes 30 seconds time period, enter 2.5
30	**Sort by priority**	Set the checkbox	Enables the sorting of events by priority. The descending sorting is performed in this order: Escalated, Alarm, Information and Standard (the last three event parameters can be set in the DDI file—see The Events tab)	Boolean type	Clear	Set—sorting by priority is enabled Clear—sorting by time the events are received is enabled
31	**New events at the end**	Set the checkbox	Places new events at the end of the current events list	Boolean type	Clear	Set—new event is placed at the end of the list Clear—new event is placed at the beginning of the list
32	**Close elsewhere**	Set the checkbox	Decides whether to delete the event from other **Operator protocols** when it is processed in one of the **Operator protocols**	Boolean type	Clear	Set—when the event is processed in one of the **Operator protocol**, it is deleted from other **Operator protocols** Clear—when the event is processed in one of the **Operator protocol**, it stays unprocessed in other **Operator protocols**

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
33	**Password for closing**	Set the checkbox	Sets the necessity to enter the password to process the event	Boolean type	Clear	Set—the event processing must be confirmed with a password Clear—password is not required for event processing
34	**Autoswitch**	Set the checkbox	Enables autoswitch to the **Current events** tab in the **Operator protocol** window when a new event occurs	Boolean type	Clear	Set—autoswitch is enabled Clear—auto switch is disabled
35	**Autoactivation of last event**	Set the checkbox	Enables the automatic activation of the cell of the event received last	Boolean type	Clear	Set—the cell of the event received last is automatically activated Clear—when the new event is received, the cell selected by the Operator remains active
36	**Hide buttons for groups**	Set the checkbox	Hides the event processing buttons when a group of events is selected	Boolean type	Clear	Set—the event processing buttons are displayed when a group of events is selected Clear—the event processing buttons are hidden when a group of events is selected
37	**Clear comment**	Set the checkbox	Clears the comment field after the event has beed processed by the Operator	Boolean type	Clear	Set—the comment field is automatically cleared after the event has been processed by the Operator Clear—the comment text remains in the comment field after the event has been processed by the Operator
38	**Fit window size**	Set the checkbox	Enables the automatic resizing of the cell to fit the entire **Operator protocol** window	Boolean type	Clear	Set—the cell size is set equal to the size of the **Operator protocol** window area, that is not occupied by the event control panel Clear—the cell size is set according to the content size
39	**Hide "Apply to all"**	Set the checkbox	Disables the **Apply to all** button	Boolean type	Clear	Set—the **Apply to all** button is hidden in the **Operator protocol** window, and the Operator cannot process all events at once Clear—the **Apply to all** button is available in the **Operator protocol** window
40	**Over all windows**	Set the checkbox	Enables the **Operator protocol** to be displayed on top of all windows	Boolean type	Clear	Set—the **Operator protocol** window is displayed on top of all windows Clear—the **Operator protocol** window is displayed in the standard mode
41	**Comment required**	Set the checkbox	Prevents event processing without entering a comment	Boolean type	Clear	Set—the buttons for classifying the events (**Alarm situation**, **Suspicious situation**, **False alarm**) do not appear until the **Comment** field is filled Clear—the Operator can classify (process) the event without entering a comment

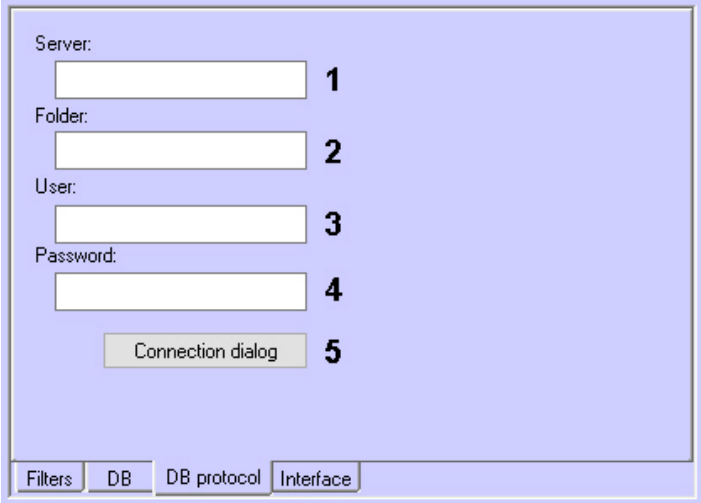
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
42	**Single selection**	Set the checkbox	Prevents the Operator from selecting multiple events using the Shift and Ctrl keys	Boolean type	Clear	Set—the Operator cannot select multiple events using the Shift and Ctrl keys Clear—the Operator can select multiple events using the Shift and Ctrl keys

26.1.5.9.10.2 The **DB** tab



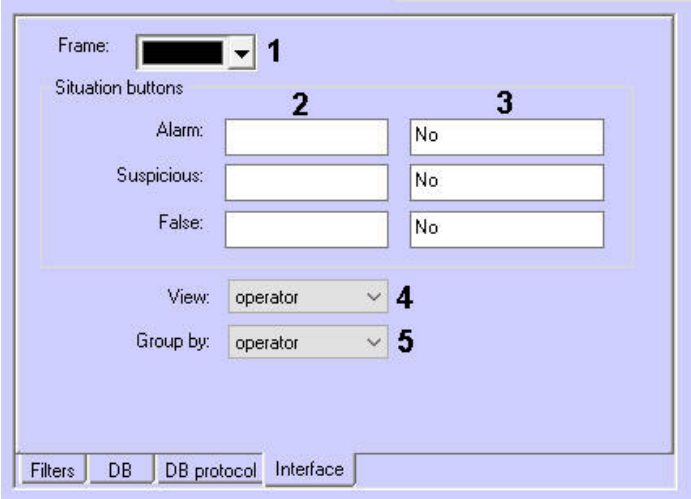
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Server**	Enter the value into the field	Sets the name of the database Server, in which the required database is stored	Latin, Cyrillic and service characters	Name of the Server used by the system	-
2	**Folder**	Enter the value into the field	Sets the name of the database, in which the events are stored	Latin, Cyrillic and service characters	Name of the main database used by the system	-
3	**User**	Enter the value into the field	Sets the username for authorization in the database Server	Latin, Cyrillic and service characters	-	-
4	**Password**	Enter the value into the field	Sets the password for authorization in the database Server	Latin, Cyrillic and service characters	-	-
5	**Connection dialog**	Click the button	Opens the dialog box of the database Server connection	-	-	-

26.1.5.9.10.3 The **DB protocol** tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Server**	Enter the value into the field	Sets the name of the database Server, in which the required **Event Viewer** database is stored (if extracted to a separate DB)	Latin, Cyrillic and service characters	Name of the Server used by the **Event Viewer** database (if extracted to a separate DB)	-
2	**Folder**	Enter the value into the field	Sets the name of the **Event Viewer** database (if extracted to a separate DB), in which the events are stored	Latin, Cyrillic and service characters	Name of the **Event Viewer** database (if extracted to a separate DB) used by the system	-
3	**User**	Enter the value into the field	Sets the username for authorization in the **Event Viewer** database Server (if extracted to a separate DB)	Latin, Cyrillic and service characters	-	-
4	**Password**	Enter the value into the field	Sets the password for authorization in the **Event Viewer** database Server (if extracted to a separate DB)	Latin, Cyrillic and service characters	-	-
5	**Connection dialog**	Click the button	Opens the dialog box of **Event Viewer** database Server connection (if extracted to a separate DB)	-	-	-

26.1.5.9.10.4 The **Interface** tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Frame**	Select the value from the list	Sets the frame color of the active cell	Color palette	Black	RGB color
2	Name*	Enter the value into the field	Sets the names for the alarm assessing buttons	Latin, Cyrillic and service characters	-	0–255 characters
3	Keyboard shortcut*	Press the key combination	Sets the key shortcuts for the events assessment	Keyboard combinations	-	You can combine the Ctrl, Alt and Shift keys with any other keys on the keyboard. For example, the Ctrl+Shift+Alt+A or the Ctrl+A shortcuts are allowed, but the D+A or D+Ins shortcuts are not allowed, etc.
4	**View**	Select the value from the list	Sets the option of displaying events on the **Current events** tab	Available display options	operator	**operator**—the Operator can choose a full or a simple view. **full**—the events are displayed as cells with screenshots **simple**—the events are displayed as lines without screenshots
5	**Group by**	Select the value from the list	Sets the option of grouping events on the **Current events** tab	Available grouping options	operator	**operator**—the Operator can choose the grouping options **default**—event grouping is disabled **object**—the events are grouped by object **event**—the events are grouped by event types **region**—the events are grouped by regions

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.9.11 The Settings panel of the External window object

The **External window** object is used to display the dialog window of various applications in the specified screen area. The applications can be either AxxonSoft applications or third-party applications.

The settings panel of the **External window** object is shown in the figure.

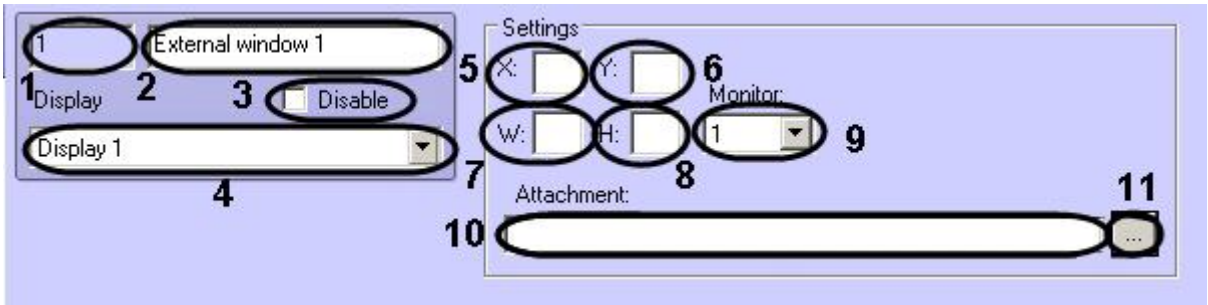


Table describes the setting parameters corresponding to the elements of the settings panel of the **External window** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **External window** object	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **External window** objects
2	Name*	Enter the value into the field	Sets the name of the **External window** object	Latin, Cyrillic and service characters	External window	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **External window** object	Boolean type	Clear	Set—the **External window** object is disabled and isn't used Clear—the **External window** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object, to which the given **External window** object belongs	Name of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects
The **Settings** group						
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the window of the **External window** interface object on the screen	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
6	**Y**	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the window of the **External window** interface object on the screen	% of the screen height	Not defined	From 0 to M*100, where M is the number of the installed monitors
7	**W**	Enter the value into the field	Sets the width of the window of the **External window** interface object	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
8	**H**	Enter the value into the field	Sets the height of the window of the **External window** interface object	% of the screen width	Not defined	From 0 to M*100, where M is the number of the installed monitors
9	**Monitor**	Select the value from the list	Sets the number of monitor which is used to display the window of the third-party application	Number of monitors	1	1–16
10	**Attachment**	Enter the value into the field	Sets the path to the application, which should be launched. ***Note.*** *All windows of the application will be opened simultaneously if the application contains several windows*	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 250
11	The **...** button	Click the button	Displays the standard Windows open dialog box to specify the path to the application that you want to run	-	-	-

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.9.12 The Settings panel of the Scene object

The settings panel of the **Scene** interface object is shown in the figure.

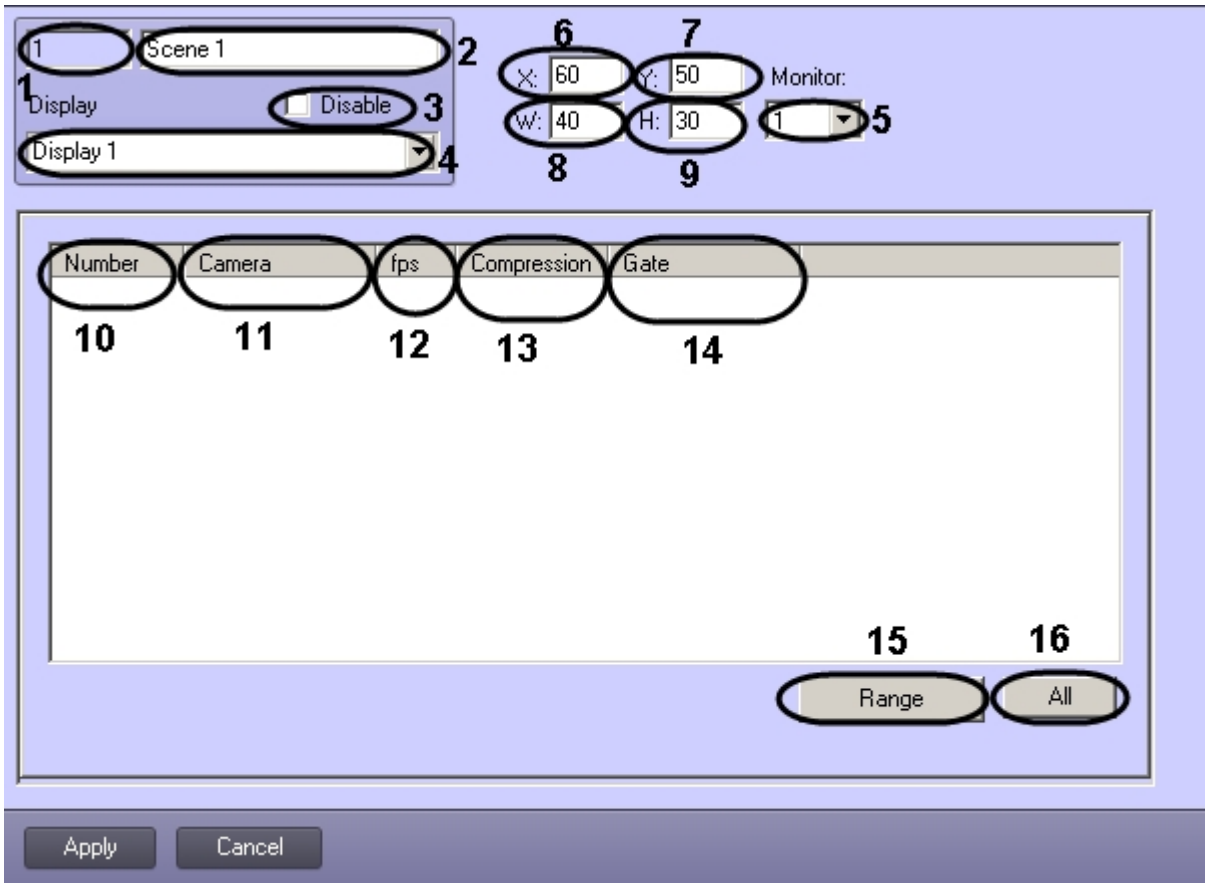


Table describes the elements of the settings panel of the **Scene** object.

26.1.5.9.13 The settings panel of the HTML Interface object

The **HTML Interface** object is used to display the content of web-pages and other files in the *Intellect* interface window.

The settings panel of the **HTML Interface** object is shown in the figure.

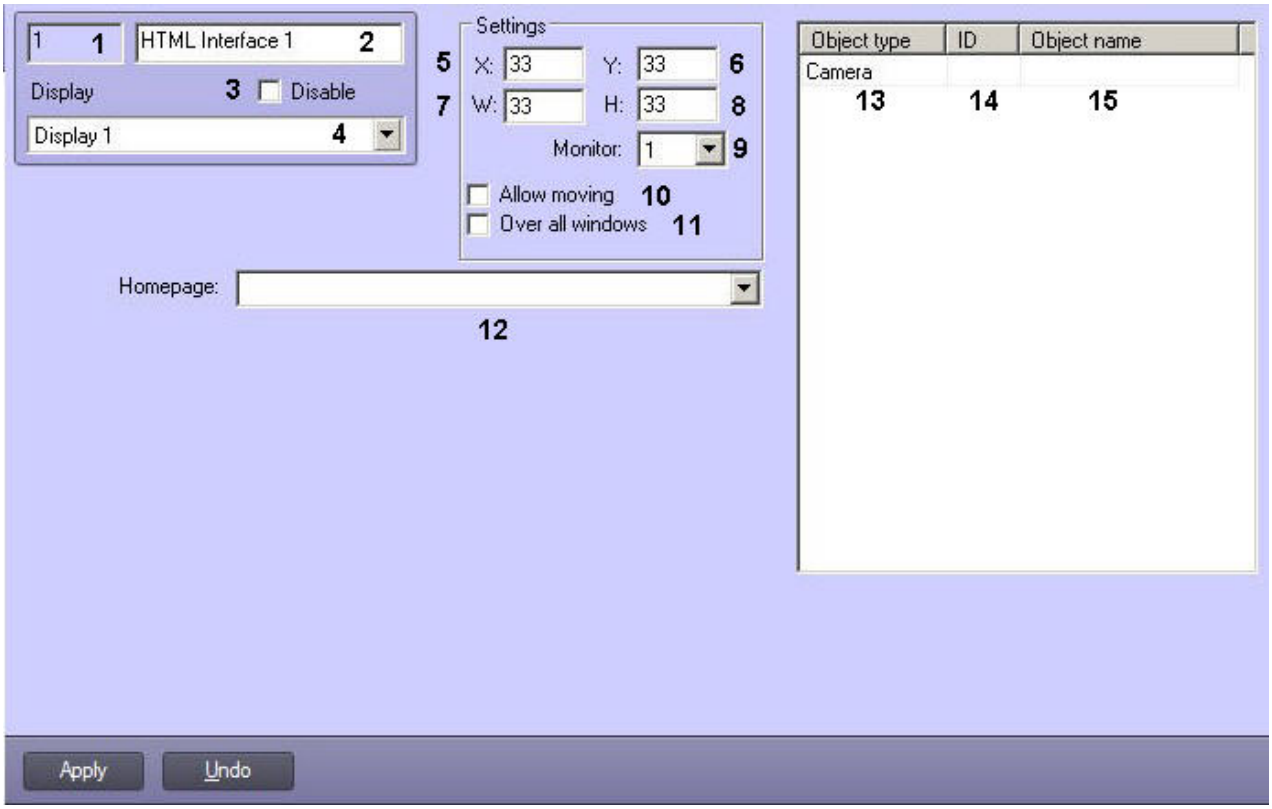


Table describes the setting parameters corresponding to the elements of the settings panel of the **HTML Interface** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **HTML Interface** interface object in the system	Sequence of numbers	-	Depends on the number of the **HTML Interface** objects in the system
2	Name	Enter the value into the field	Sets the name of the **HTML Interface** object in the system	Latin, Cyrillic and service characters	HTML Interface	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **HTML Interface** object in the system	Boolean type	Clear	Set—the **HTML Interface** object is disabled and isn't used Clear—the **HTML Interface** object is enabled used
4	**Display**	Select the value from the list	Sets the **Display** parent object for the given **HTML Interface** object	Names of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system

The **Settings** group						
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **HTML Interface** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed computer monitors
6	**Y**	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **HTML Interface** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed computer monitors
7	**W**	Enter the value into the field	Sets the width of the **HTML Interface** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed computer monitors
8	**H**	Enter the value into the field	Sets the height of the **HTML Interface** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed computer monitors
9	**Monitor**	Select the value from the list	Sets the number of the monitor that should display the interface object	Sequence of numbers	1	Depends on the number of the connected computer monitors
10	**Allow moving**	Set the checkbox	Allows moving the **HTML Interface** interface object using the mouse	Boolean type	Clear	Set—it is possible to move the **HTML Interface** interface object using the mouse Clear—it is not possible to move the **HTML Interface** interface object using the mouse
11	**Over all windows**	Set the checkbox	Allows displaying the **HTML Interface** interface window on top of all windows	Boolean type	Clear	Set—the **HTML Interface** window is displayed on top of all windows Clear—the **HTML Interface** window is displayed in the standard mode
12	**Homepage**	Select the value from the list	Sets the homepage that should be displayed in the **HTML Interface** interface window	Name of the **HTML page** objects registered in the system	-	Depends on the number of the **HTML page** objects in the system
13	**Object type**	Select the value from the list	Sets the type of object, the state of which should be monitored using the HTML interface	Types of objects created in the system	-	Depends on the objects created in the system
14	**ID**	Select the value from the list	Sets the ID of the object, the state of which should be monitored using the HTML interface	Sequence of numbers	-	Depends on the objects created in the system
15	**Object name**	Automatically	Displays the name of the object, the state of which should be monitored using the HTML interface	Name of the object of the selected type with the specified ID	-	Depends on the objects created in the system

26.1.5.9.14 The settings panel of the HTML page object

The **HTML page** object is used to configure the web pages displayed in the **HTML Interface** interface window.

The settings panel of the **HTML page** object is shown in the figure.

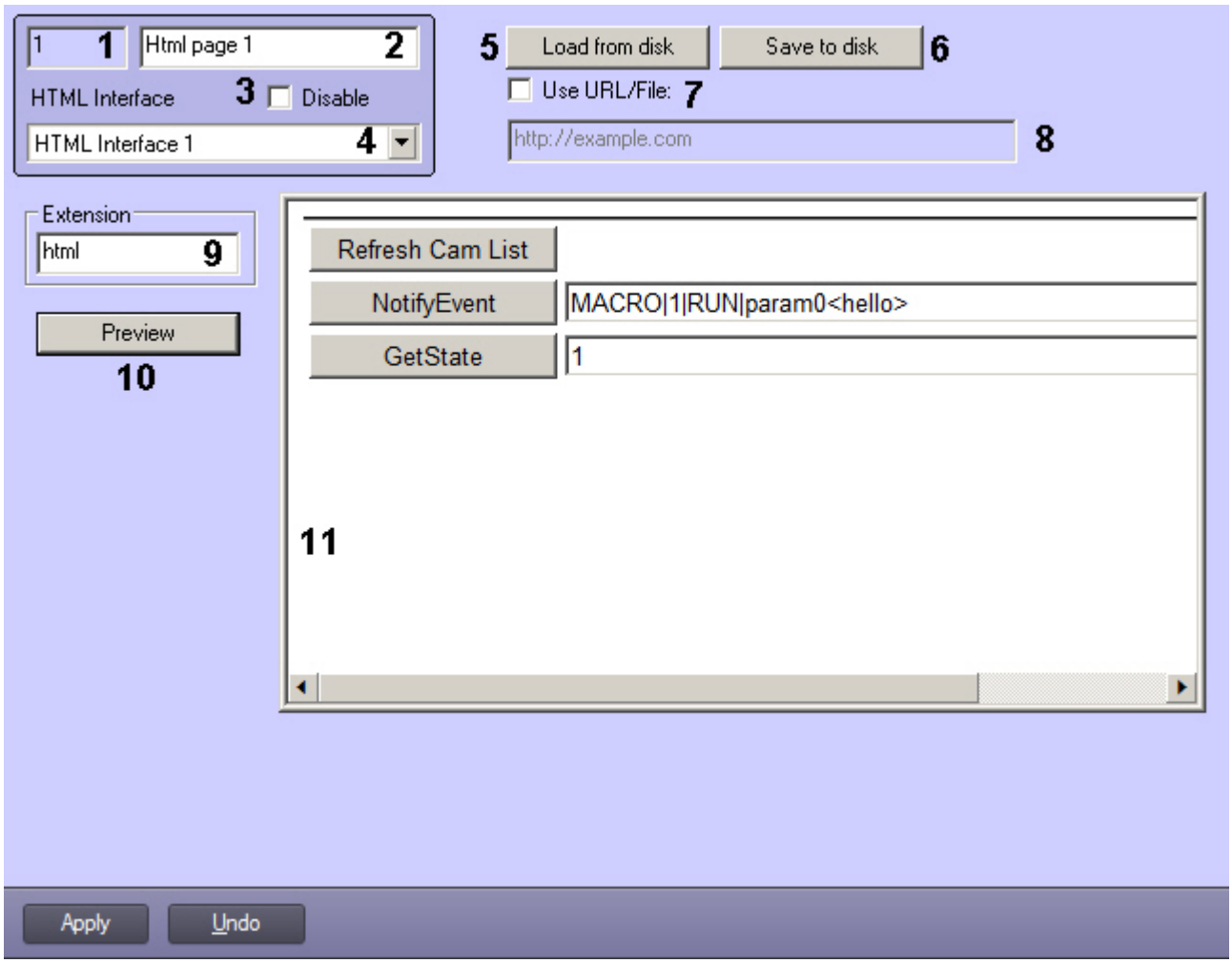


Table describes the setting parameters corresponding to the elements of the settings panel of the **HTML page** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **HTML page** interface object in the system	Sequence of numbers	-	Depends on the number of the **HTML page** objects in the system
2	**Name**	Enter the value into the field	Sets the name of the **HTML page** object in the system	Latin, Cyrillic and service characters	HTML page	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **HTML page** object in the system	Boolean type	Clear	Set—the **HTML page** object is disabled and isn't used Clear—the **HTML page** object is enabled and used

4	**HTML Interface**	Select the value from the list	Sets the **HTML Interface** parent object for the given **HTML page** object	Name of the **HTML Interface** objects registered in the system	Name of the **HTML Interface** parent object	Depends on the number of the **HTML Interface** objects in the system
5	**Load from disk**	Click the button	Opens the standard open file dialog box to load a file of a web page or some other file type from disk	-	-	-
6	**Save to disk**	Click the button	Opens the standard open file dialog box to save a file of a web-page or some other file type to disk	-	-	-
7	**Use URL/ File**	Set the checkbox	Enables or disables downloading a web page or other file type by URL	Boolean type	Clear	Set—the specified URL is opened when addressing to the HTML page Clear—the saved file of the HTML page is opened when addressing to the HTML page (see Link to the HTML page object)
8	**Use URL/ File**	Enter the value into the field	The field is used to specify the link to the web page or a file that will open when addressing to the configured HTML page	Link in the URL format	-	Number of characters is not limited
9	**Extension**	Automatically	Displays the extension of the opened file	Extensions of files supported by the Internet Explorer browser	html	From 0 to 16 characters
10	**Preview**	Click the button	Displays the selected web page or a file in the preview window	-	-	-
11	Preview window	Automatically	Preview of a web page or a file	-	Not displayed	-

26.1.5.9.15 The Settings panel of the Display manager object

The settings panel of the **Display manager** object is shown in the figure.

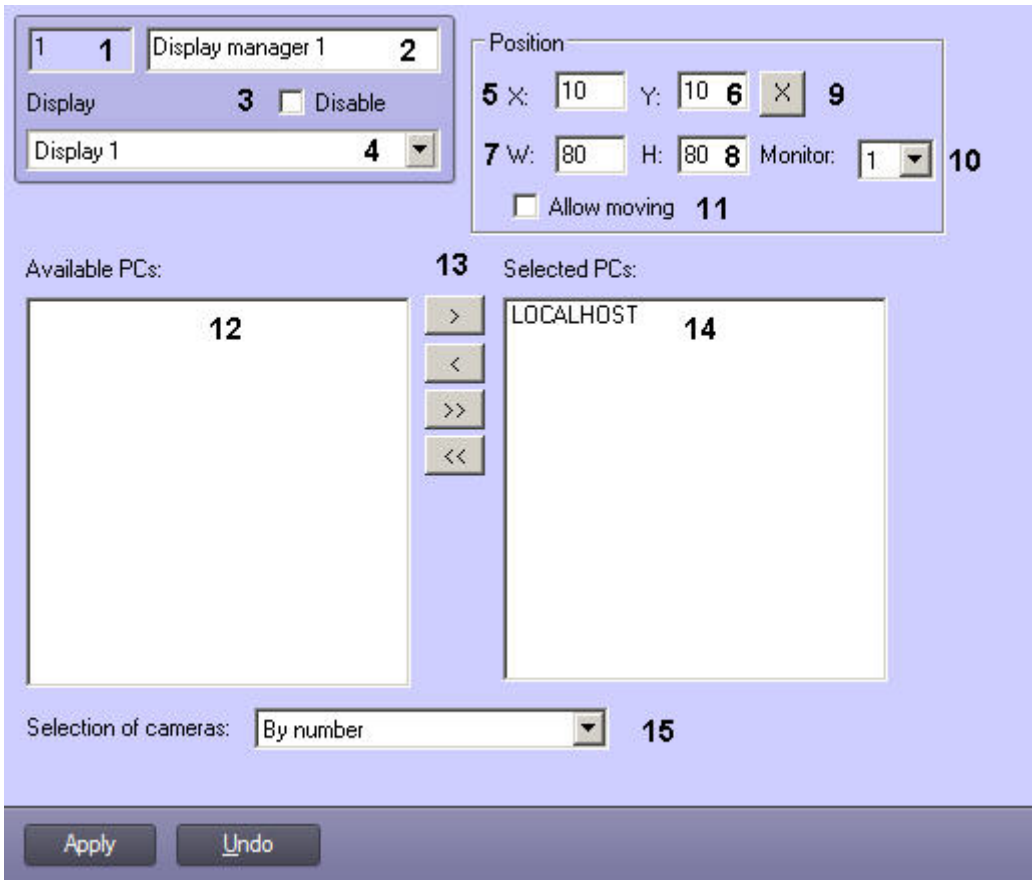


Table describes the setting parameters of the **Display manager** interface object.

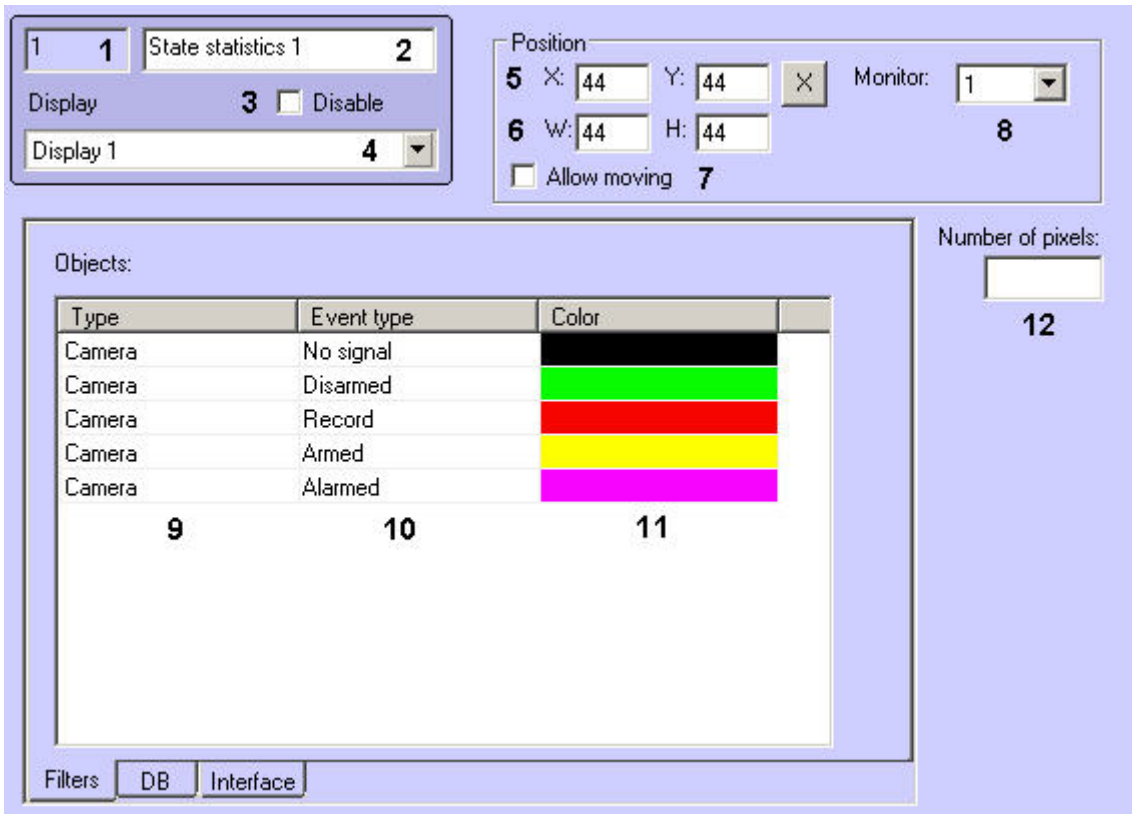
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **Display manager** interface object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Display manager** objects in the system
2	Name	Enter the value into the field	Sets the name of the **Display manager** object in the system	Latin, Cyrillic and service characters	Display manager	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Display manager** object in the system	Boolean type	Clear	Set—the **Display manager** object is disabled and isn't used Clear—the **Display manager** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object, to which the given **Display manager** object belongs	Name of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system

5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Display manager** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
6	**Y**	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Display manager** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
7	**W**	Enter the value into the field	Sets the width of the **Display manager** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
8	**H**	Enter the value into the field	Sets the height of the **Display manager** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
9	The **×** button	Click the button	Opens the window for automatic setting of the X, Y, W and H parameters	-	-	-
10	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	From 1 to 16
11	**Allow moving**	Set the checkbox	Allows moving the **Display manager** interface window manually	Boolean type	Clear	Set—allow moving the **Display manager** interface window manually Clear—disable moving the **Display manager** interface window manually
12	**Available PCs**	The **>**, **<**, **>>**, **<<** buttons	Contains a list of the **Computer** objects that haven't been selected to be managed via the **Display manager**	Names of the **Computer** objects registered in the system	Depends on the number of the **Computer** objects registered in the system	Depends on the number of the **Computer** objects registered in the system
13	The **>**, **<**, **>>**, **<<** buttons	Click the button	Move the computers from the **Available PCs** list to the **Selected PCs** list and back	-	-	-
14	**Selected PCs**	The **>**, **<**, **>>**, **<<** buttons	Contains a list of the **Computer** objects that are selected to be managed via the **Display manager**	Names of the **Computer** objects registered in the system	-	Depends on the number of the **Computer** objects registered in the system
15	**Selection of cameras**	Select the value from the list	Sets the cameras sorting method in the **Display manager** interface	Available sorting methods	By number	By number By name

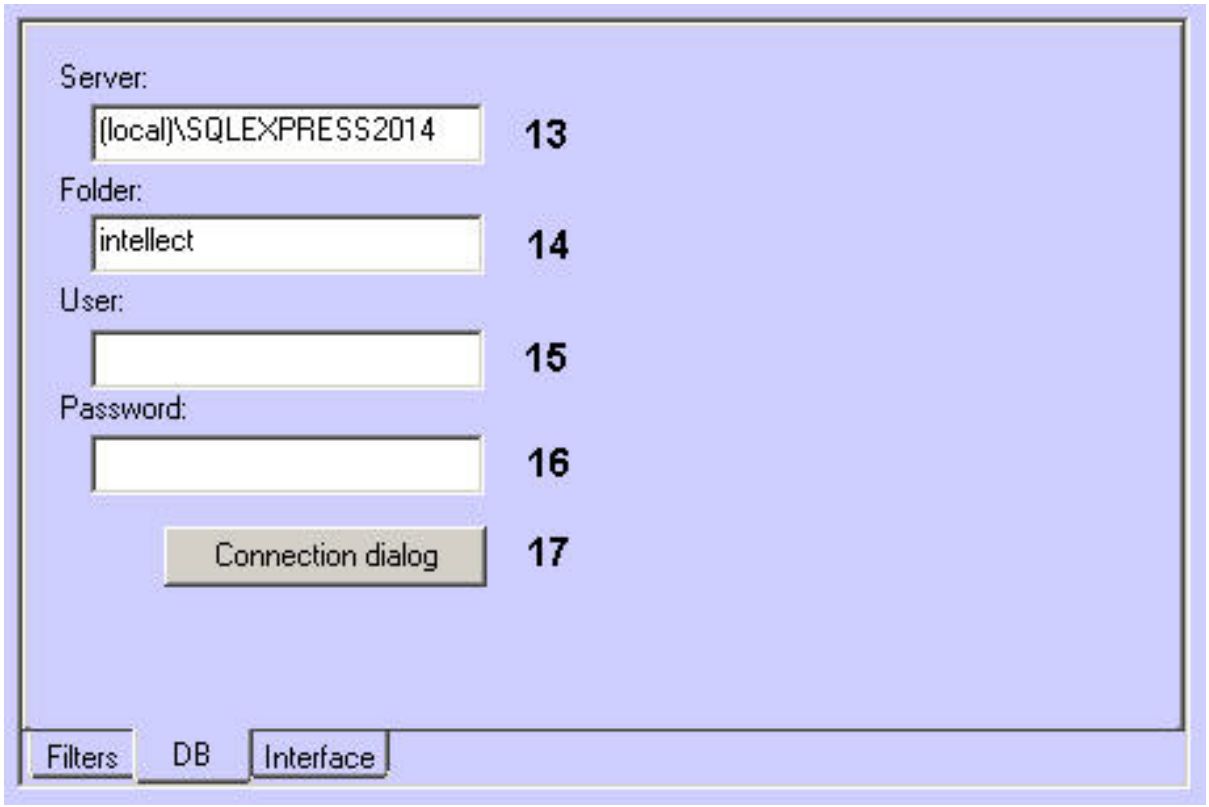
26.1.5.9.16 The Settings panel of the State statistics object

The settings panel of the **State statistics** object is shown in the figures.

The **Filters** tab.



The **DB** tab.



The **Interface** tab.

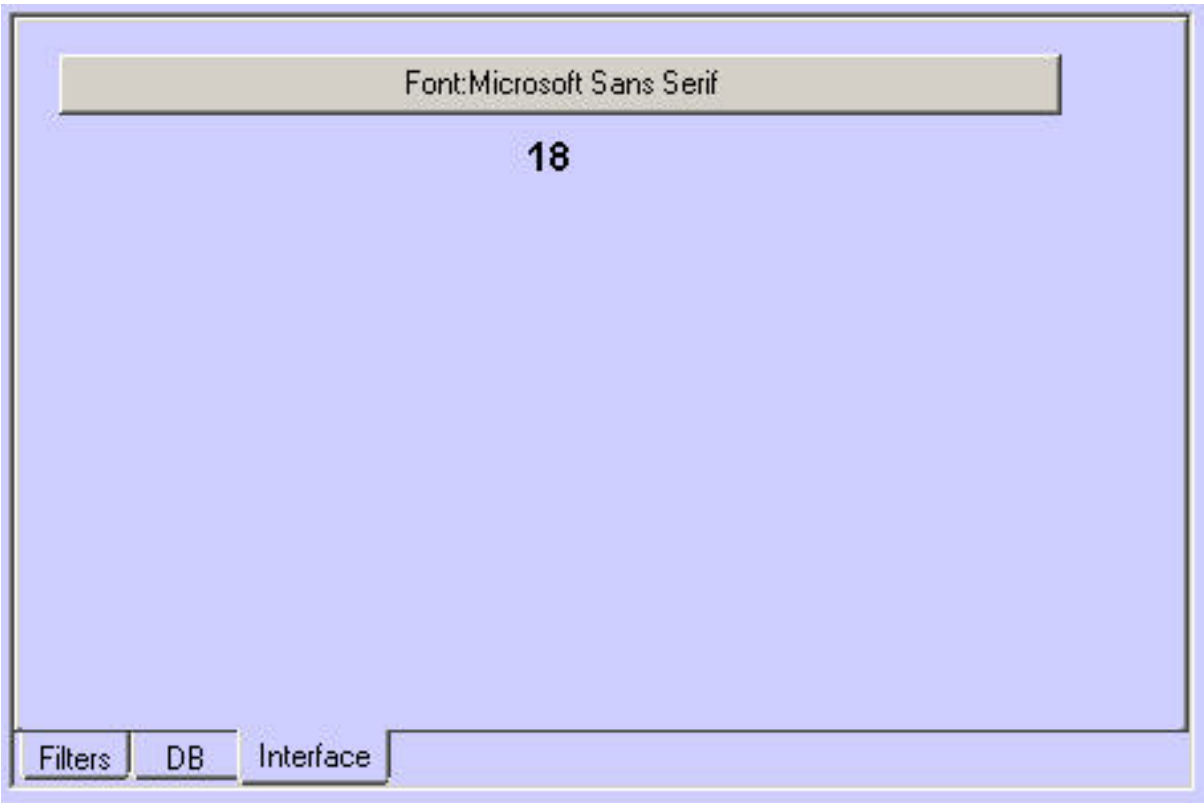


Table describes the setting parameters of the **State statistics** interface object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Filters** tab						
1	Identification number	Automatically	Displays the identification number of the **State statistics** interface object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **State statistics** objects in the system
2	Name	Enter the value into the field	Sets the name of the **State statistics** object in the system	Latin, Cyrillic and service characters	State statistics	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the chechbox	Sets the state (enabled or disabled) of the **State statistics** object in the system	Boolean type	Clear	Set—the **State statistics** object is disabled and isn't used Clear—the **State statistics** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object, to which the given **State statistics** object belongs	Name of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system

5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **State statistics** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **State statistics** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
6	**W**	Enter the value into the field	Sets the width of the **State statistics** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the **State statistics** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
7	**Allow moving**	Set the checkbox	Allows moving the **State statistics** interface window manually	Boolean type	Clear	Set—allow moving the **State statistics** interface window manually Clear—disable moving the **State statistics** interface window manually
8	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	From 1 to 16
9	**Type**	Select the value from the list	Sets the type of the objects, which events should be displayed in the **State statistics** window.	Available object types	-	Depends on the objects registered in the system. You can select only those object types, which have the "INFORMATION" or "ALARM" value selected in the **Processing messages** column on the **Events** tab of the ddi.exe utility (see The Events tab)
10	**Event type**	Select the value from the list	Sets the events that should be displayed in the **State statistics** window	Events available for the selected object	-	Depends on the object type
11	**Color**	Select the value from the list	Sets the color of the state displayed in the table and on the graph in the **State statistics** interface window	Color palette	Black	RGB color
12	**Number of pixels**	Enter the value into the field	Sets the number of pixels to be displayed on the state graph	Sequence of numbers	0	>=0
The **DB** tab						
13	**Server**	Enter the value into the field	Sets the name of the database Server, where the required database is stored	Latin, Cyrillic and service characters	Name of the server used by the system	-
14	**Folder**	Enter the value into the field	Sets the name of the database, where the events should be stored	Latin, Cyrillic and service characters	Name of the main database used by the system	-

15	**User**	Enter the value into the field	Sets the username to authorize on the database Server	Latin, Cyrillic and service characters	-	-
16	**Password**	Enter the value into the field	Sets the password to authorize on the database Server	Latin, Cyrillic and service characters	-	-
17	**Connection dialog**	Click the button	Opens the dialog box to connect the database Server	-	-	-
The **Interface** tab						
18	**Font**	Click the button	Opens the dialog box for selecting the text font for the table and the graph (except for the legend) in the **State statistics** window	-	-	-

26.1.5.9.17 The Settings panel of the Charts object

The settings panel of the **Charts** object is shown in the figure.

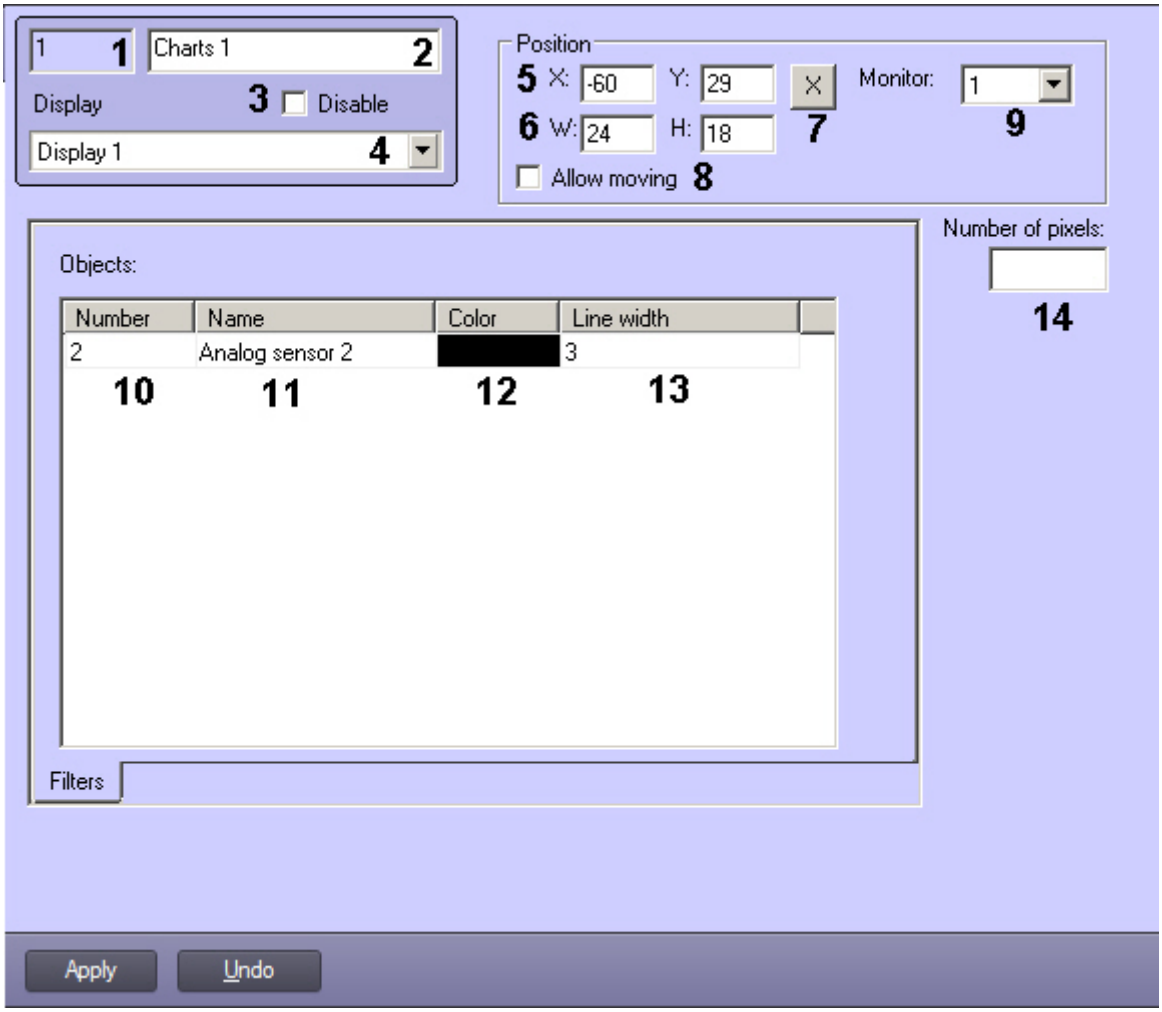


Table describes the setting parameters of the **Charts** interface object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Filters** tab						
1	Identification number	Automatically	Displays the identification number of the **Charts** interface object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Charts** objects in the system
2	Name	Enter the value into the field	Sets the name of the **Charts** object in the system	Latin, Cyrillic and service characters	**Charts**	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the chechbox	Displays the state (enabled or disabled) of the **Charts** object in the system	Boolean type	Clear	Set—the **Charts** object is disabled and isn't used Clear—the **Charts** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object, to which the given **Charts** object belongs	Name of the **Display** objects registered in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Charts** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Charts** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
6	**W**	Enter the value into the field	Sets the width of the **Charts** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the **Charts** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
7	The **×** button	Click the button	Opens a test window set the position of the **Charts** window	-	-	-
8	**Allow moving**	Set the checkbox	Allows moving the **Charts** interface window manually	Boolean type	Clear	Set—allow moving the **Charts** interface window manually Clear—disable moving the **Charts** interface window manually
9	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	From 1 to 16

10	**Number**	Select the value from the list	Sets the identifier of the **Analog sensor** object, the data from which should be displayed in the chart	Sequence of numbers	-	Depends on the **Analog sensor** objects in the system
11	**Name**	Select the value from the list	Sets the name of the **Analog sensor** object, the data from which should be displayed in the chart	Names of the **Analog sensor** objects	-	Depends on the **Analog sensor** objects in the system
12	**Color**	Select the value from the list	Sets the display color of the corresponding analog sensor on the chart in the **Charts** interface window	Color palette	Black	RGB color
13	**Line width**	Enter the value into the field	Sets the width of the line in the chart	Sequence of numbers	5	>0
14	**Number of pixels**	Enter the value into the field	Sets the number of pixels to be displayed in the chart	Sequence of numbers	0	>=0

26.1.5.9.18 The Settings panel of the SIP-panel object

The settings panel of the **SIP-panel** object is shown in the figures below.

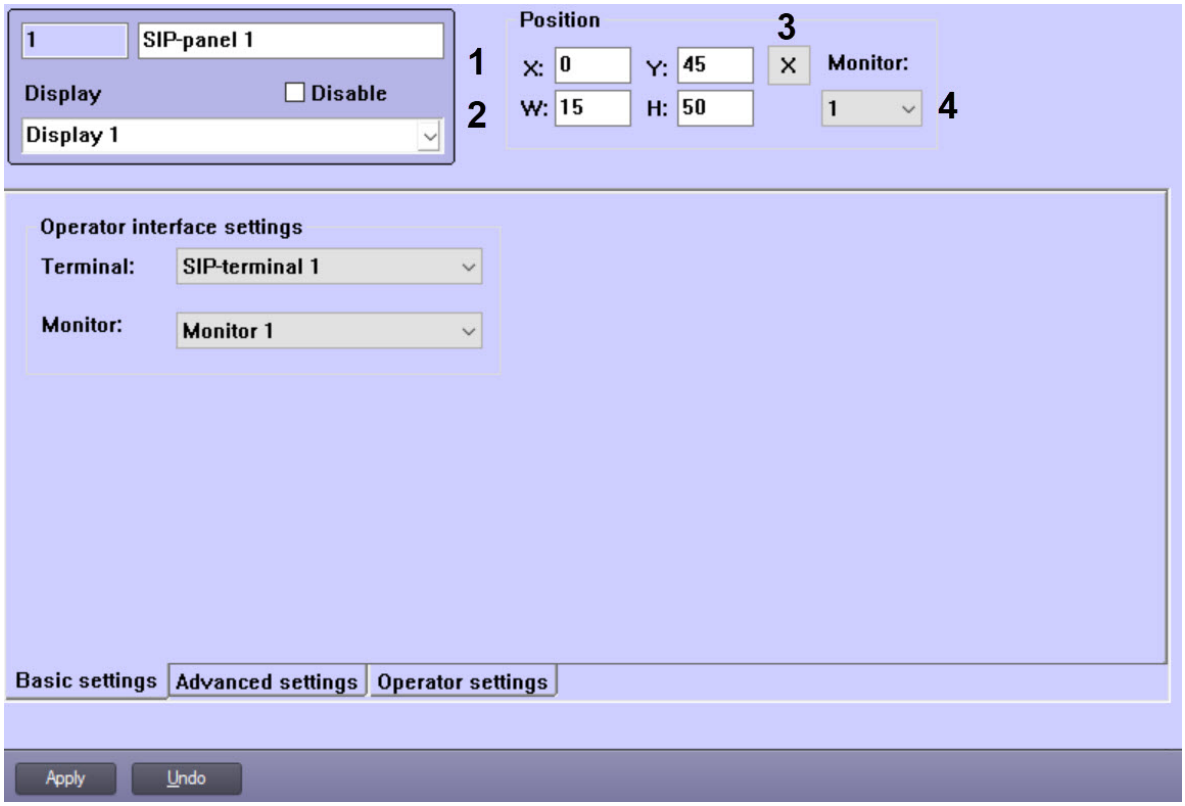


Table describes the setting parameters of the **SIP-panel** interface object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Position** group						

1	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **SIP-panel** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **SIP-panel** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
2	**W**	Enter the value into the field	Sets the width of the **SIP-panel** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the **SIP-panel** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
3	The **×** button	Click the button	Opens a test window for changing the coordinates of the **SIP-panel** interface window	-	-	-
4	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	From 1 to 16

The **Basic settings** tab.

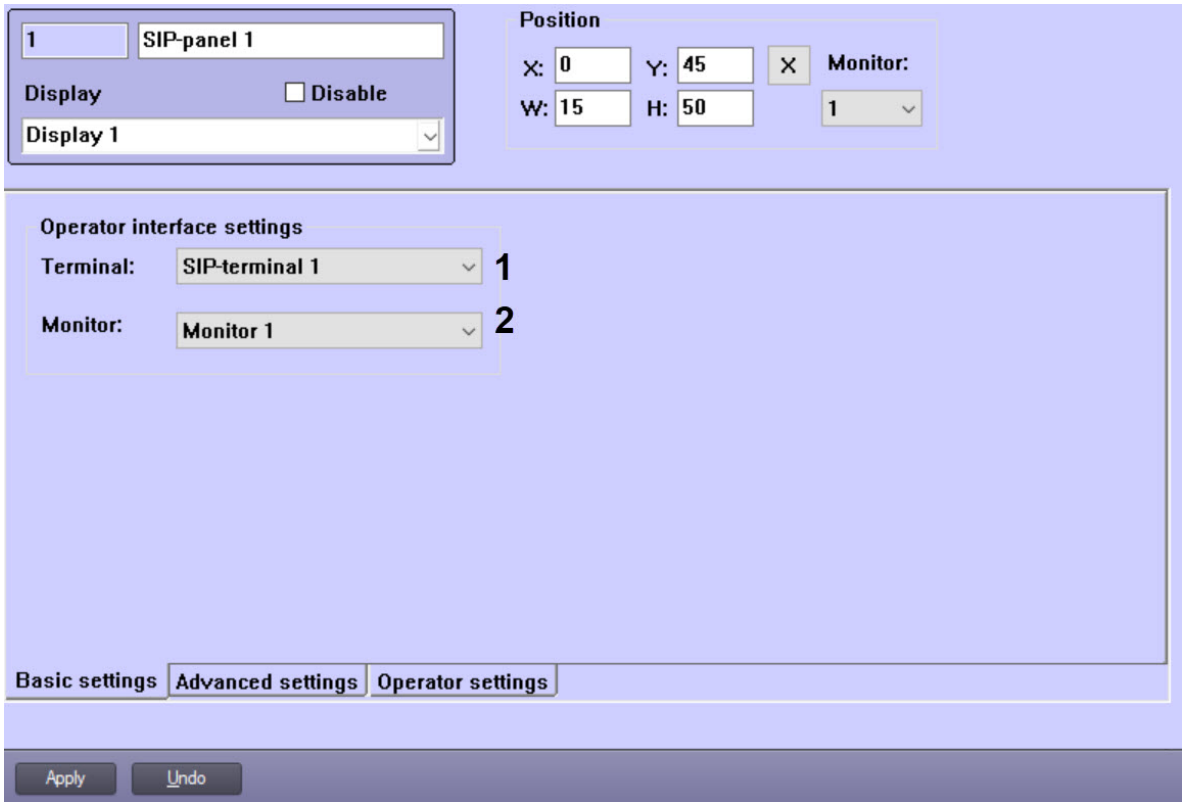


Table describes the parameters of the **Basic settings** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range

1	**Terminal**	Select the value from the list	Sets the **SIP-terminal** object, which SIP-devices use the **SIP-panel**	Name of the **SIP-panel** objects registered in the system	-	Depends on the number of the **SIP-terminal** objects in the system
2	**Monitor**	Select the value from the list	Sets the the **Monitor** object corresponding to the **Video surveillance monitor** to which the video cameras associated with the corresponding SIP-devices are added	Name of the **Monitor** objects registered in the system	-	Depends on the number of the **Monitor** objects in the system

The **Advanced settings** tab.

Table describes the parameters of the **Advanced settings** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Interface behavior** group						
1	**Display only when calling**	Set the checkbox	Displays the **SIP-panel** only when calling	Boolean type	Clear	Set—the **SIP-panel** is only displayed when calling Clear—the **SIP-panel** is always displayed
2	**New calls to the end**	Set the checkbox	Enables adding new calls to the end of the list	Boolean type	Clear	Set—new calls are added to the end of the list Clear—new calls are added to the top of the list

3	**Disable keypress sound**	Set the checkbox	Disables keypress sound on the **SIP-panel**	Boolean type	Clear	Set—keypress sound disabled Clear—keypress sound is enabled
4	**Maximize screen on call**	Set the checkbox	Enables automatic display switching on call	Boolean type	Clear	Set—when a call is made to the **SIP-terminal** that corresponds to the **SIP-panel**, the screen to which the **SIP-panel** is added is displayed automatically Clear—when a call is made to the **SIP-terminal** that corresponds to the **SIP-panel**, the screen is not displayed automatically
5	**Calls to unknown users**	Set the checkbox	Enables the option to call unknown users *Note. Unknown user is a number that is present in the **SIP-terminal**, but not in the address book of the current SIP-operator*	Boolean type	Set	Set—calls to unknown users are allowed Clear—calls to unknown users are not allowed
6	**Switch to incoming**	Set the checkbox	Automatically switches to the tab of the **SIP-panel** with the incoming calls, which occurs with incoming calls or call on hold	Boolean type	Set	Set—automatic switch to the tab with incoming calls is enabled Clear—automatic switch to the tab with incoming calls is disabled
The **Interface elements** group						
7	**Dial pad**	Set the checkbox	Displays the dial pad in the interface	Boolean type	Set	Set—the dial pad is displayed Clear—the dial pad is hidden
	Caption	Set the checkbox	Displays the tab names in the interface. When disabled, only the **Call** tab will be displayed without displaying the name	Boolean type	Set	Set—the tab names are displayed Clear—only the **Call** tab is displayed without displaying the name
	Archive	Set the checkbox	Displays the **Archive** tab in the interface	Boolean type	Set	Set—the **Archive** tab is displayed Clear—the **Archive** tab is hidden
	Call control buttons	Set the checkbox	Displays the buttons at the bottom of the panel to control a call	Boolean type	Set	Set—call control buttons are displayed Clear—call control buttons are hidden

The **Operator settings** tab.

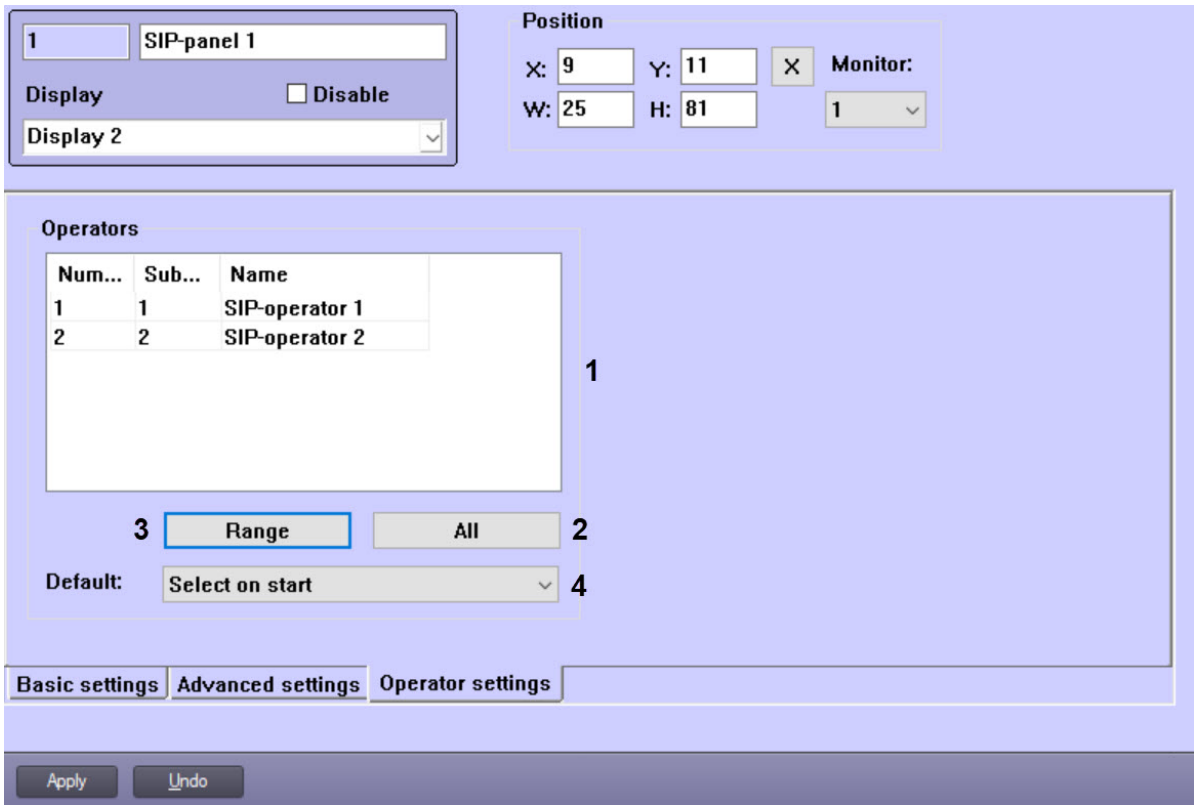


Table describes the parameters of the **Operator settings** tab.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	The **Operators** table	Select the value in the column	Sets the list of the **SIP-operators** who can work with this **SIP-panel**	-	-	-
	Number	Select the value from the list	Selects a **SIP-operator** identifier	Identifiers of the **SIP-operator** objects registered in the system	-	Depends on the number of the **SIP-operator** objects in the system
	Subscriber	Select the value from the list	Selects a **SIP-operator** number	Numbers of the **SIP-operator** objects registered in the system	-	Depends on the number of the **SIP-operator** objects in the system
	Name	Select the value from the list	Selects a **SIP-operator** name in *Intellect*	Names of the **SIP-operator** objects registered in the system	-	Depends on the number of the **SIP-operator** objects in the system
2	**All**	Click the button	Adds all existing **SIP-operators** to the table	-	-	-
3	**Range**	Click the button	Opens the **Add operators** window to add multiple **SIP-operators**	-	-	-

4	**Default**	Select the value from the list	Sets the default **SIP-operator**	-	**Select on start**	**Select on start**—when you first start the **SIP-panel**, it is necessary to select the appropriate **SIP-operator** in the authorization window. Next time you will be logged in under the previously selected **SIP-operator** **User rights**—you will log into the **SIP-panel** as the **SIP-operator** that is linked to the *Intellect* user rights. You should also be logged into *Intellect* with the corresponding user rights **SIP-operator from the list**—logging into the **SIP-panel** will be made at once as the selected **SIP-operator**. Depends on the number of the **SIP-operator** objects in the system

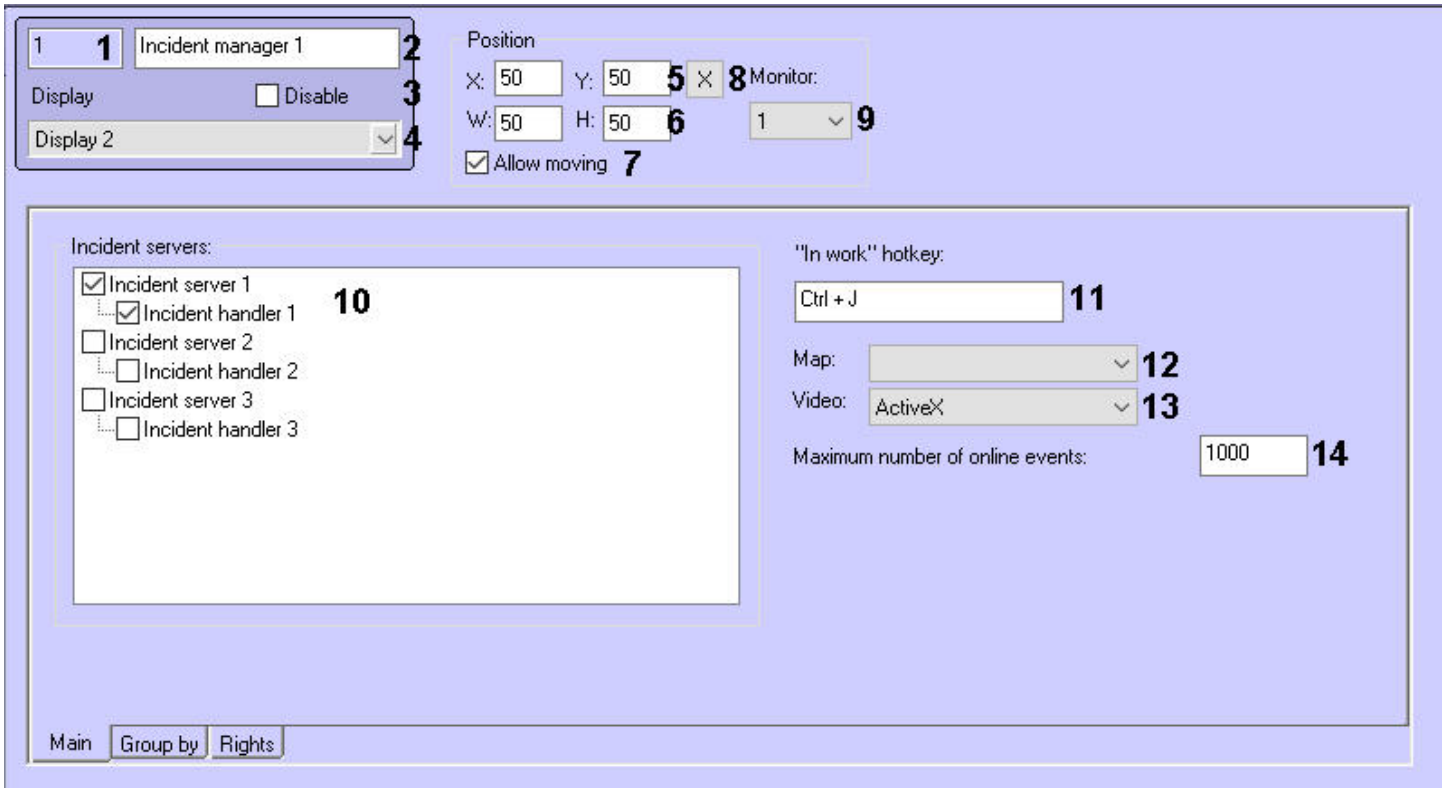
26.1.5.9.19 The Settings panel of the Incident manager object

On this page:

- General object settings and the Main tab
- The Group by tab
- The Rights tab

The settings panel for the **Incident manager** interface object is shown in the figures. The description of the **Incident manager** setting parameters is given in the corresponding tables.

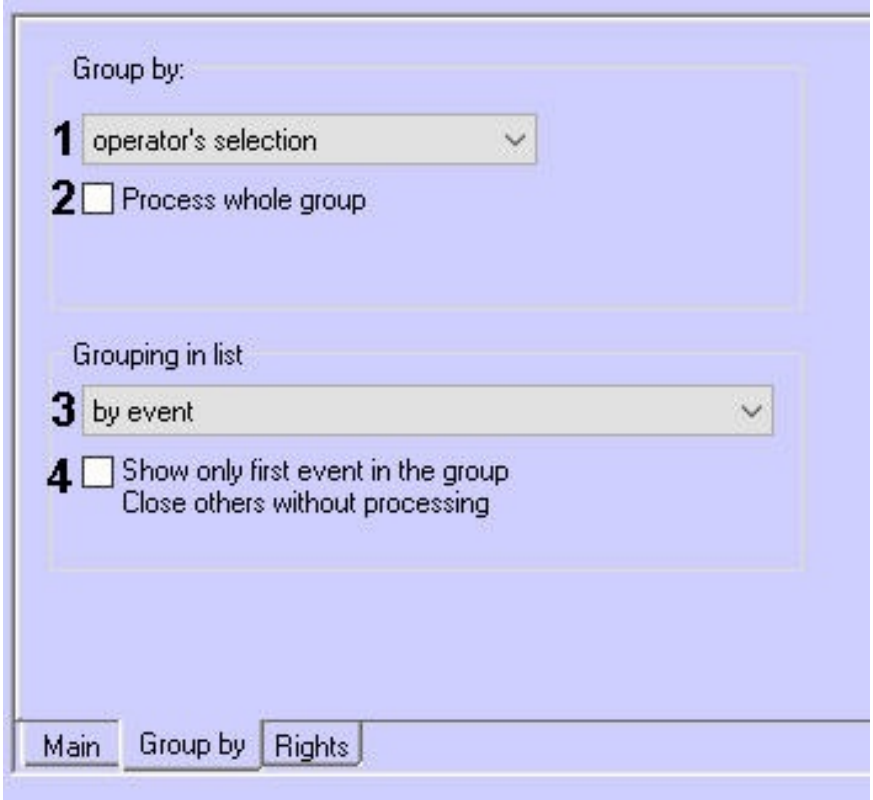
26.1.5.9.19.1 General object settings and the Main tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **Incident manager** interface object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Incident manager** objects in the system
2	Name	Enter the value into the field	Sets the name of the **Incident manager** object in the system	Latin, Cyrillic and service characters	Incident manager	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Incident manager** object in the system	Boolean type	Clear	Set—the **Incident manager** object is disabled and isn't used Clear—the **Incident manager** object is enabled and used
4	**Display**	Select the value from the list	Sets the **Display** parent object for this **Incident manager** object	Names of the **Display** objects created in the system	Name of the **Display** parent object	Depends on the number of the **Display** objects in the system
5	**X**	Enter the value into the field	Sets the X coordinate in the horizontal axis for the upper left corner of the **Incident manager** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	Y	Enter the value into the field	Sets the Y coordinate in the vertical axis for the upper left corner of the **Incident manager** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
6	**W**	Enter the value into the field	Sets the width of the **Incident manager** interface window	% of the screen width	-	From 0 to M*100, where M is the number of the installed monitors
	H	Enter the value into the field	Sets the height of the **Incident manager** interface window	% of the screen height	-	From 0 to M*100, where M is the number of the installed monitors
7	**Allow moving**	Set the checkbox	Allows moving the **Incident manager** interface window manually	Boolean type	Clear	Set—allow moving the **Incident manager** window manually Clear—disable moving the **Incident manager** interface window manually
8	The × button	Click the button	Opens a test window set the position of the **Incident manager** window	-	-	-
9	**Monitor**	Select the value from the list	Sets the number of the monitor in the system for which the coordinates are specified	Numbers of the monitors in OS	1	From 1 to 16

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Main** tab						
10	**Incident servers**	Set the checkbox	Sets the **Incident server** and **Incident handler** objects, the events and processing logic from which will be displayed in the interface	Boolean type	Clear	Set—use the selected **Incident server** or **Incident handler** objects Clear—do not use the selected **Incident server** or **Incident handler** objects
11	**"In work" hotkey**	Enter the value into the field	Sets a hotkey, using which the operator can start processing the event. To set the hotkey, place the mouse cursor in the field and press the required key or key combination on the keyboard	Keyboard keys	-	All possible keyboard keys and key combinations using Ctrl, Shift and Alt
12	**Map**	Select the value from the list	Sets the **Map** object, which will be linked with the **Incident manager**. In the **Incident manager**, the operator can highlight the object on the map from which the event was received	List of **Map** objects available in the system	-	Depends on the number of the **Map** objects created in the system
13	**Video**	Select the value from the list	Sets the video display mode for archive and live video on event in the **Incident manager**	Available display modes	**ActiveX**	**ActiveX**—archive will open in a separate window **Monitor**—archive will open on the selected **Video surveillance monitor**
14	**Maximum number of online events**	Enter the value into the field	Sets the maximum number of events that can be simultaneously displayed in the interface	Sequence of numbers	10	10-5000

26.1.5.9.19.2 The Group by tab



№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Group by**	Select the value from the list	Sets the method of grouping events in the **Incident manager**	Available grouping methods	operator's selection	**operator's selection**—the operator can choose the grouping method in the **Incident manager** interface **disabled**—the event grouping is disabled **region**—the events are grouped by region **event**—the events are grouped by event type **object**—the events are grouped by object
2	**Process whole group**	Set the checkbox	Sets two options: 1. Blocking of group events for processing by other operators in case one operator took the event from the group into processing. In this case, the events of the group remain available for processing only by this operator	Boolean type	Clear	Set—events of the filtered group are blocked for other operators if one operator has already started processing an event from the group. When one event from a group is escalated, the whole group is escalated Clear—events of the filtered group are not blocked if the operator has already started processing an event from the group. When one event is escalated, the whole group is not escalated

			2. When one event of the selected group is escalated, all events of this group will be escalated too			
3	**Grouping in list**	Select the value from the list	Sets the method of grouping events in the event list	Available grouping methods	no grouping	**no grouping**—all events will be displayed in the event display window without grouping. If filtering is set, then all events of the selected filter will be displayed **by event**—the events will be grouped by object type/object ID/ event type/logic ID
4	**Show only first event in the group. Close others without processing**	Set the checkbox	Sets the event display options within a group	Boolean type	Clear	Set—only the first event from the group is displayed, the rest of the events are closed without processing after the first event is processed Clear—all events of the group are displayed

26.1.5.9.19.3 The Rights tab

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**Number**	Select the value from the list	The number of the user for who the rights should be set	Positive integers	-	Depends on the number of the users registered in the system
2	**Name**	Select the value from the list	The name of the user (usually first or last name) for who the rights should be set. Filled in automatically when selecting a user number	Names of the registered users	-	Depends on the users registered in the system
3	**Take in work**	Set the checkbox	Sets the right for the corresponding user to take events into processing	Boolean type	Clear	Set—the user can take events into processing

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
						Clear—the user cannot take events into processing
4	**Close**	Set the checkbox	Sets the right for the corresponding user to close the event without processing	Boolean type	Clear	Set—the user can close an event without processing Clear—the user cannot close an event without processing
5	**Suspend**	Set the checkbox	Sets the right for the corresponding user to suspend the event processing	Boolean type	Clear	Set—the user can suspend the event processing Clear—the user cannot suspend the event processing
6	**Track handling**	Set the checkbox	Sets the right for the corresponding user to see the event handling steps taken by other users	Boolean type	Clear	Set—the user sees the event handling steps taken by other users Clear—the user does not see the event handling steps taken by other users
7	**Take any**	Set the checkbox	Sets the right for the corresponding user to take into processing the events with any status	Boolean type	Clear	Set—the user can take into proccesing the event with any status Clear—the user cannot take into proccesing the event with any status
8	**Escalate**	Set the checkbox	Sets the right for the corresponding user to escalate the events (give them to other users for processing)	Boolean type	Clear	Set—the user can escalate the event Clear—the user cannot escalate the event
9	**Work with escalated**	Set the checkbox	Sets the right for the corresponding user to process the escalated events	Boolean type	Clear	Set—the user can take into processing the escalated events Clear—the user cannot take into processing the escalated events

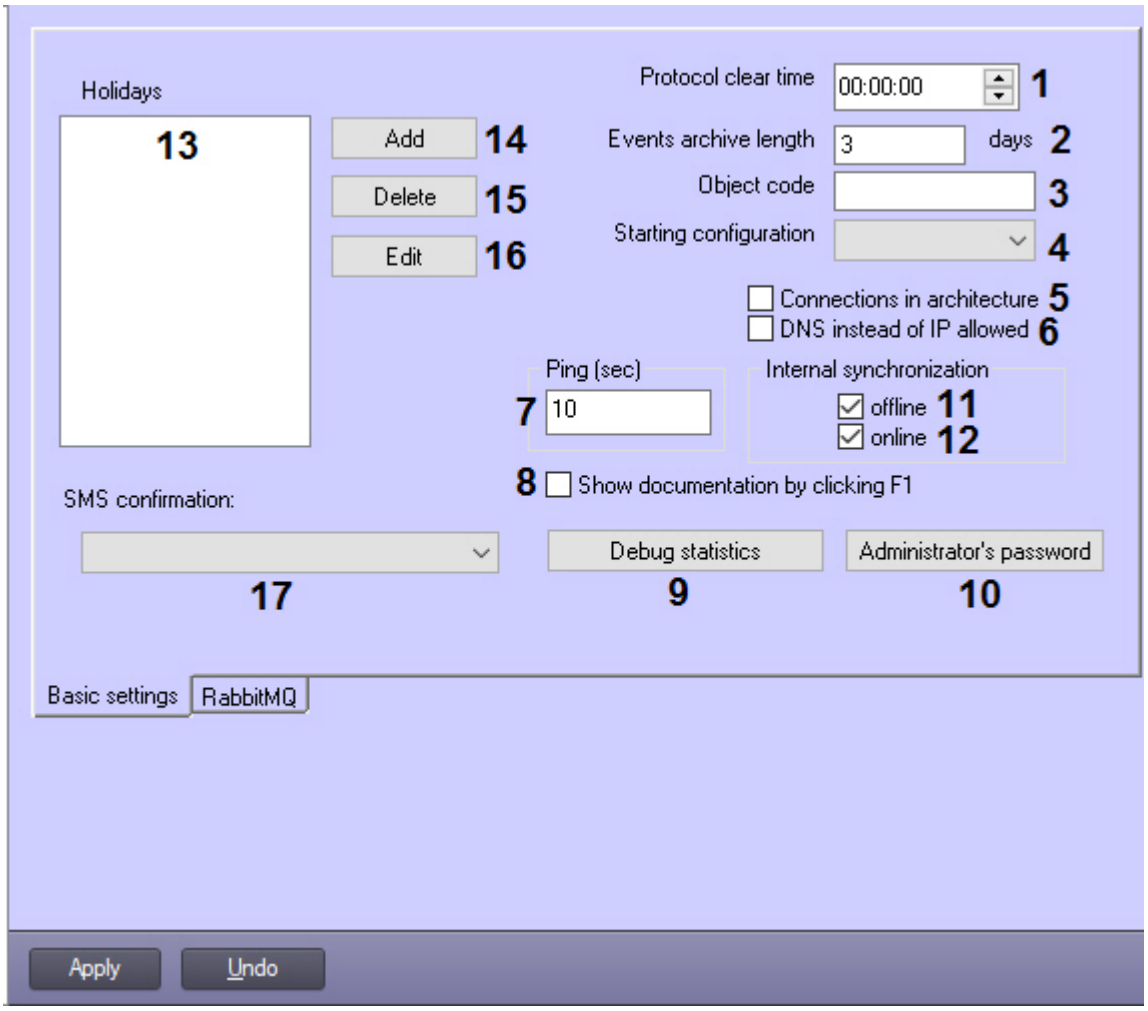
26.1.5.10 The Programming tab

26.1.5.10.1 The Settings panel of the Security zone object

The **Security zone** object is used for the general configuration of *Intellect*.

The settings panel of the **Security zone** object is shown in the figures.

The **Basic settings** tab.



The **RabbitMQ** tab.

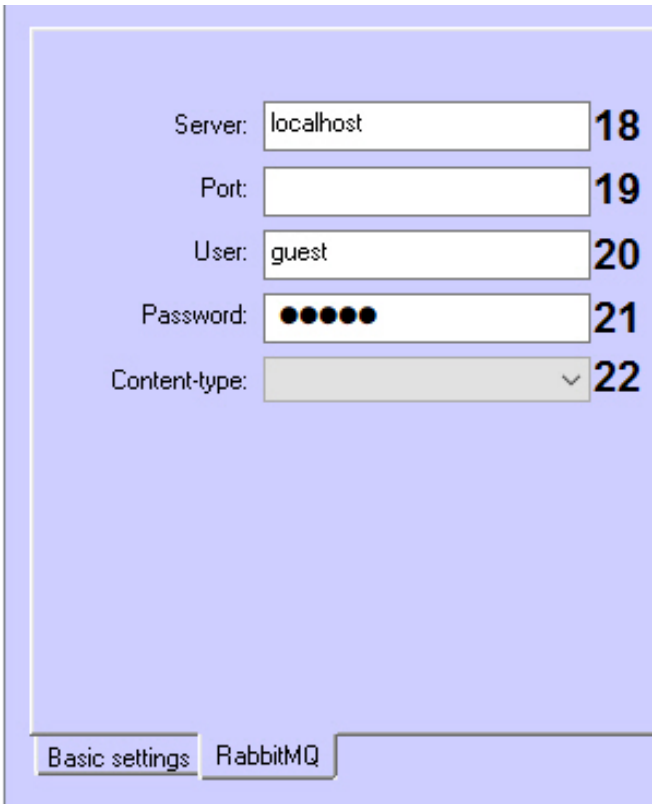


Table describes the setting parameters corresponding to the elements of the settings panel of the **Security zone** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
The **Settings** group						
1	**Protocol clear time**	Enter the value into the field using the **up** and **down** buttons	Sets the time of the day at which to start cleaning up the **Event Viewer** database according to the **Events archive length** parameter	HH:MM:SS	Current system time at the moment of the object setting panel opening	00:00:00 to 23:59:59
2	**Events archive length____days**	Enter the value into the field	Sets the number of days to store information about the events registered by *Intellect* and recorded into both the **Event Viewer** and the **Incident server**. This parameter affects all computers in a distributed system	Days	3	Not less than 0
3	**Object code**	Enter the value into the field	Sets the number of the access control card, which is automatically displayed in the settings panel of the **User** object, when the object is created in the **Object code** field	Sequence of numbers	Not defined	More than 1

4	**Starting configuration**	Select the value from the list	Sets the macro, which will be automatically launched at *Intellect* start	Names of the **Macro** objects registered in the system	Not defined	Depends on the number of the **Macro** objects created in the digital video surveillance system with distributed architecture
5	**Connections in architecture**	Set the checkbox	Sets the computers with which the created **Computer** object should exchange the data about the system configuration parameters: with all computers in the digital video surveillance system with distributed architecture or only with the **Computer** object on the basis of which the given object was created	Boolean type	Clear	Set—when creating a new computer, the **Connection** checkboxes in the **Architecture** tab are set for all computers in the architecture Clear—when creating a new computer, the **Connection** checkbox in the **Architecture** tab is set only for the computer on which this new object is created
6	**DNS instead of IP allowed**	Set the checkbox	Sets the address of the Server/Remote Administrator's workstation/Remote Client in the **Architecture** tab as DNS name, not only IP address	Boolean type	Clear	Set—when configuring the interaction of the computers in the distributed system, DNS name (instead of IP address) of the Server/ Remote Administrator's workstation/Remote Client can be specified in the **Architecture** tab Clear—when configuring the interaction of the computers in the distributed system, IP address of the Server/ Remote Administrator's workstation/Remote Client should be specified in the **Architecture** tab
7	**Ping (sec)**	Enter the value into the field	Sets the check period for the computer connection to the Server	Sequence of numbers	10	>=1
8	**Show documentation by clicking F1**	Set the checkbox	Enables opening documentation in the pdf format by pressing F1, when *Intellect* is started. Administrator's Guide is opened on the Server and the Remote Administrator's workstation; Operator's Guide is opened on the Remote Client	Boolean type	Clear	Set—the documentation is displayed by pressing F1 Clear—the feature of displaying the documentation by pressing F1 is disabled
9	**Debug statistics**	Click the button	Opens the window with the events queue statistics	-	-	-
10	**Administrator's password**	Click the button	Open a dialog box for setting the Administrator's password	-	-	-

The **Internal synchronization** group						
11	**offline**	Set the checkbox	Enables the offline synchronization of the events	Boolean type	Set	Set—the offline synchronization is enabled. When the computer is reconnected, it gets all the events for the period when there was no connection Clear—the offline synchronization is disabled. When the computer is reconnected, it does not get the events for the period when there was no connection
12	**online**	Set the checkbox	Enables the online synchronization of the events	Boolean type	Set	Set—the online synchronization is enabled. The events are sent right after they occur according to the configuration parameters of the computer interaction in the distributed system Clear—the online synchronization is disabled. The events are not sent
The **Holidays** group						
13	Date*	-	List of calendar days which will be defined as holidays in *Intellect*	Date	Not defined	Date format: DD-MM-YY
14	**Add**	Click the button	Opens the **Calendar** dialog box to set the date of a new holiday	-	-	-
15	**Delete**	Click the button	Deletes the selected holiday date from the **Date** list	-	-	-
16	**Edit**	Click the button	Opens the **Calendar** dialog box to change the date of the selected holiday in the list	-	-	-
SMS confirmation						
17	**SMS confirmation**	Enter the value into the field	Sets the **Short Message** object for two-factor authentication—see Configuring two-factor authentication	Names of the **Short Message** objects registered in the system	Not defined	Depends on the number of the **Short Message** objects created in the system
The **RabbitMQ** tab						
18	**Server**	Enter the value into the field	Sets the RabbitMQ host address	Latin characters, digits and service characters	localhost	Host IP address or name

19	**Port**	Enter the value into the field	Sets the RabbitMQ host port	Latin characters, digits and service characters	Not defined	0–65535 If the port is 0 or not specified, RabbitMQ won't run
20	**User**	Enter the value into the field	Sets the RabbitMQ host user name	Latin characters, digits and service characters	guest	Depends on the registered RabbitMQ users
21	**Password**	Enter the value into the field	Sets the RabbitMQ host user password	Latin characters, digits and service characters	guest	Depends on the registered RabbitMQ users
22	**Content-type**	Select the value from the list	Sets the type of the sent/received content	Supported types of content	plain/text	**application/json**—a message in JSON format is sent **plain/text**—*Intellect* event is sent in the following format: "TYPE|ID|EVENT"

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.10.2 The Settings panel of the Macro object

The **Macro** object is used to support the automatic execution of a pre-defined sequence of commands upon occurrence of certain events, registered by *Intellect.*

The settings panel of the **Macro** object is shown in the figure.

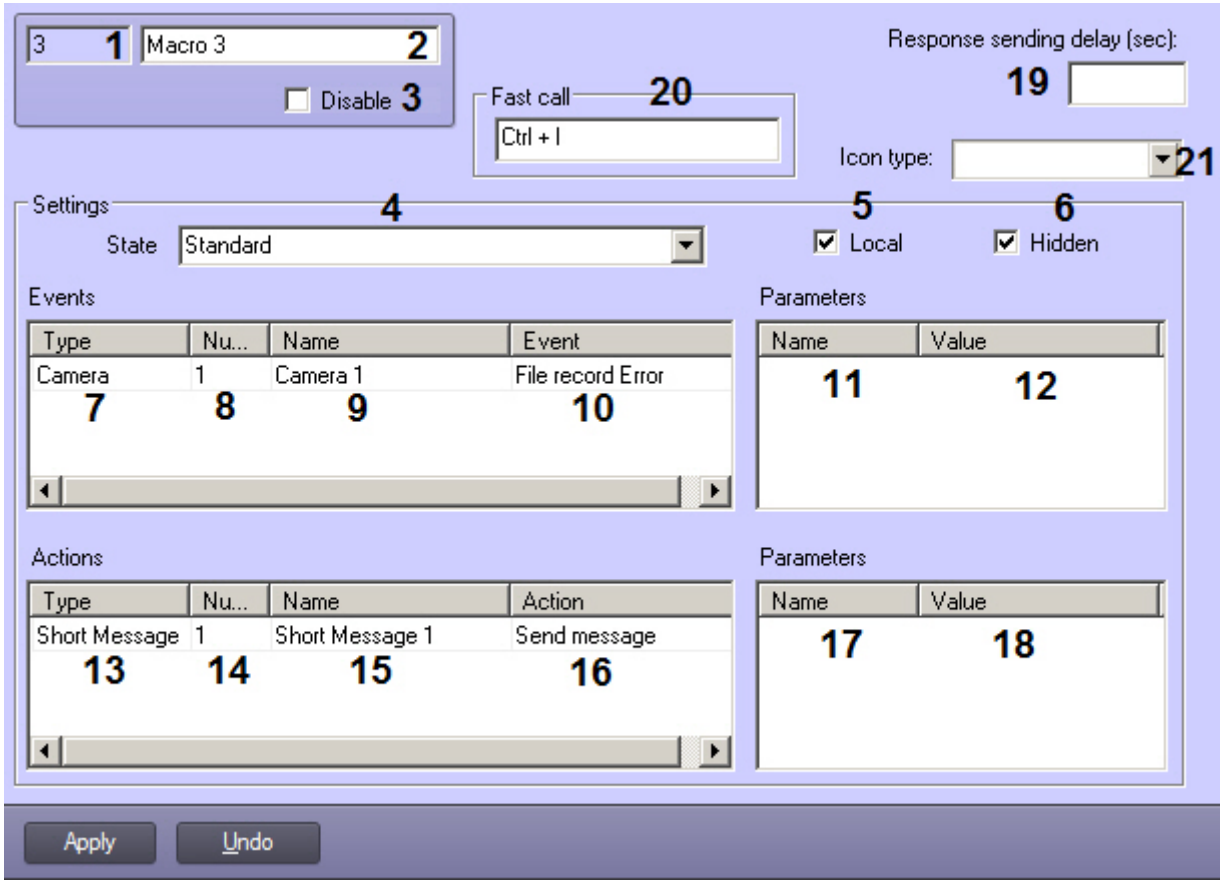


Table describes the setting parameters corresponding to the elements of the settings panel of the **Macro** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Macro** object in the digital video surveillance system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Macro** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the **Macro** object name.	Latin, Cyrillic and service characters	Macro	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Macro** object	Boolean type	Clear	Set—the **Macro** object is disabled and isn't used Clear—the **Macro** object is enabled and used
The **Settings** group						
4	**State**	Enter the value into the field	Sets the message displayed in the information board of the main menu of *Intellect,* when the given macro is running	Latin, Cyrillic and service characters	Not defined	**Standard**—no message will be displayed in the information board of the main menu of *Intellect.* A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 60
5	**Local**	Set the checkbox	Sets the computers, which will execute the given macro (all computers of the digital video surveillance system with distributed architecture or only the given computer). *Note. This checkbox does not apply to hide and show reactions of any Display. Regardless of the checkbox, when called from the Server/ RAW, the reactions are executed on the Server/RAW and all connected Clients; when called on the Client, the reactions are executed only on the Client*	Boolean type	Clear	Set—the macro will be executed only on the given computer Clear—the given macro will be executed on all computers of the digital video surveillance system with distributed architecture
6	**Hidden**	Set the checkbox	Determines, whether or not the name of this macro will be displayed in the main control panel of *Intellect* to be started manually	Boolean type	Clear	Set— the name of the macro will not be displayed in the main control panel of *Intellect* Clear—the name of the macro will be displayed in the main control panel of *Intellect*

The **Events** subgroup						
7	**Type**	Select the value from the list	Sets the type of objects in the digital video surveillance system with distributed architecture, in which the event registration triggers a macro	Types of objects registered in the system	-	Depends on the total number of the types of objects created in the digital video surveillance system with distributed architecture
8	**Number**	Select the value from the list	Sets the identification number of the object in the digital video surveillance system with distributed architecture, in which the event registration triggers a macro	Sequence of numbers	-	Depends on the total number of the objects of the specified type created in the digital video surveillance system with distributed architecture
9	**Name**	Automatically	Displays the name of the selected object in the digital video surveillance system with distributed architecture	Names of the objects of the specified type registered in the system	-	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 60
10	**Event**	Select the value from the list	Sets the event that triggers a macro for the specified object	Names of the events available for the given type of objects	-	List of events is created individually for each type of object
The **Parameters** subgroup ***Note.*** *The given subgroup is not active for all types of objects*						
11	**Name**	Automatically	Sets the name of the additional parameter for the selected type of object in the **Events** subgroup	Latin and service characters, digits	Not defined	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 60
12	**Value**	Enter the value into the field	Sets the value for the parameter in the **Name** column	Latin and service characters, digits	Empty field	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters—from 1 to 250
The **Action** subgroup						
13	**Type**	Select the value from the list	Sets the type of objects in the digital video surveillance system with distributed architecture, to which the command is forwarded, when the conditions set in the **Events** subgroup to trigger a macro are met	Names of the types of objects registered in the system	-	Depends on the total number of the types of objects created in the digital video surveillance system with distributed architecture
14	**Number**	Select the value from the list	Sets the identification number of the object in the digital video surveillance system with distributed architecture, to which the	Sequence of numbers	-	Depends on the total number of the objects of the specified type in the digital video surveillance

			command is forwarded, when the conditions set in the **Events** subgroup to trigger a macro are met			system with distributed architecture. If the field is left blank, the reaction will be performed for all objects of the selected type. If you enter the **#** symbol in the field, the identifier of the object from which the event was received will be substituted into the reaction. The object types in the **Events** and **Actions** tables may differ. When the macro is run manually from the main control panel, the # symbol is treated as if the field was blank, i.e. the macro is executed for all objects of the selected type. Example of using the # symbol: disarm the camera if the “Detach” event was received from it
15	**Name**	Automatically	Displays the name of the selected object in the digital video surveillance system with distributed architecture	Names of the objects of the selected type registered in the system	-	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters— from 1 to 60
16	**Action**	Select the value from the list	Sets the action, which the given device performs, when the conditions to trigger the given macro are met	Names of the actions, available in the system for the objects of the specified type	-	List of events is created individually for each type of object
The **Parameters** subgroup ***Note.*** *The given subgroup is not active for all types of objects*						
17	**Name**	Automatically	Sets the name of the additional parameter for the selected type of object in the **Actions** subgroup	Latin and service characters, digits	Not defined	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters— from 1 to 60
18	**Value**	Enter the value into the field	Sets the value for the parameter in the **Name** column	Latin and service characters, digits	-	A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. Number of characters— from 1 to 250
Outside the groups						
19	**Response sending delay (sec)**	Enter the value into the field	Sets the time period (in seconds) that must pass after the events specified in the **Events** column occur and before executing the	Sequence of numbers	-	>0

			reactions specified in the **Actions** column. ***Note.*** *If the events reoccur before the specified time period expires, the reaction execution wait period will be prolonged, i.e. reactions will be executed only once when events do not reoccur over the specified period*			
20	**Fast call**	Left-click in the field and press the required key combination	Sets a keyboard shortcut for a macro. ***Note.*** *If the same combination of keys is set for several macros, when pressing a key combination, all of these macros will run*	Key combinations	-	Individual keys of the main or numeric keyboard, as well as these keys in combination with Shift, Ctrl and Alt
21	**Icon type**	Select the value from the list	Sets a set of icons for displaying a macro on the map. By default, an empty value is set for all macros which corresponds to the "Macro 1" icon. ***Note.*** *Changing the icon type will take effect after restarting the map interface. To restart the interface, restart Intellect or log in once again under the corresponding Operator account*	Available icon types on the map	-	Macro 1–Macro 7, empty value

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.10.3 The Settings panel of the Program object

The **Program** object is used to create specialized programs in the embedded programming environment of *Intellect.*

The settings panel of the **Program** object is shown in the figure.

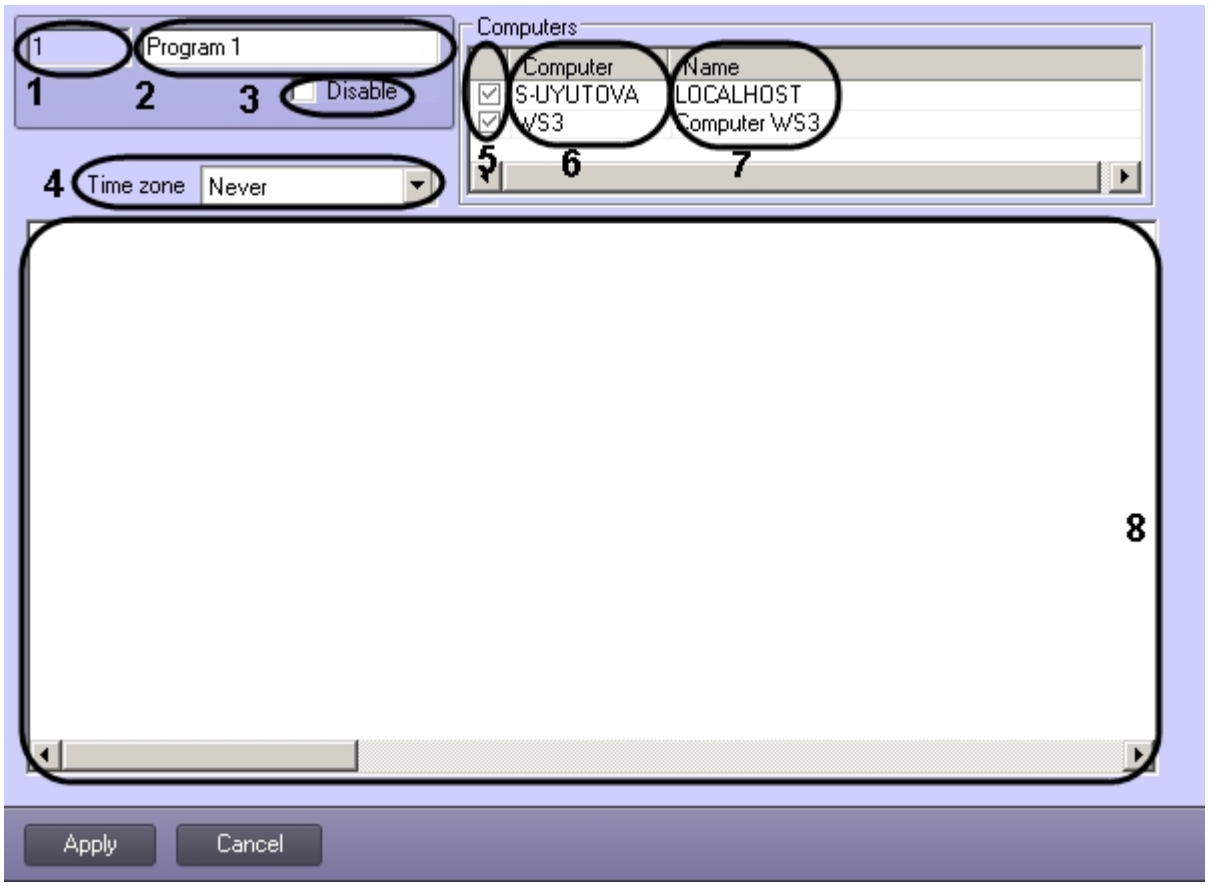


Table describes the setting parameters corresponding to the elements of the settings panel of the **Program** object.

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.10.4 The Settings panel of the Time schedule object

In *Intellect,* the **Time schedule** object determines the time parameters for any actions, which should be initiated at certain time.

The settings panel of the **Time schedule** object is shown in the figure.

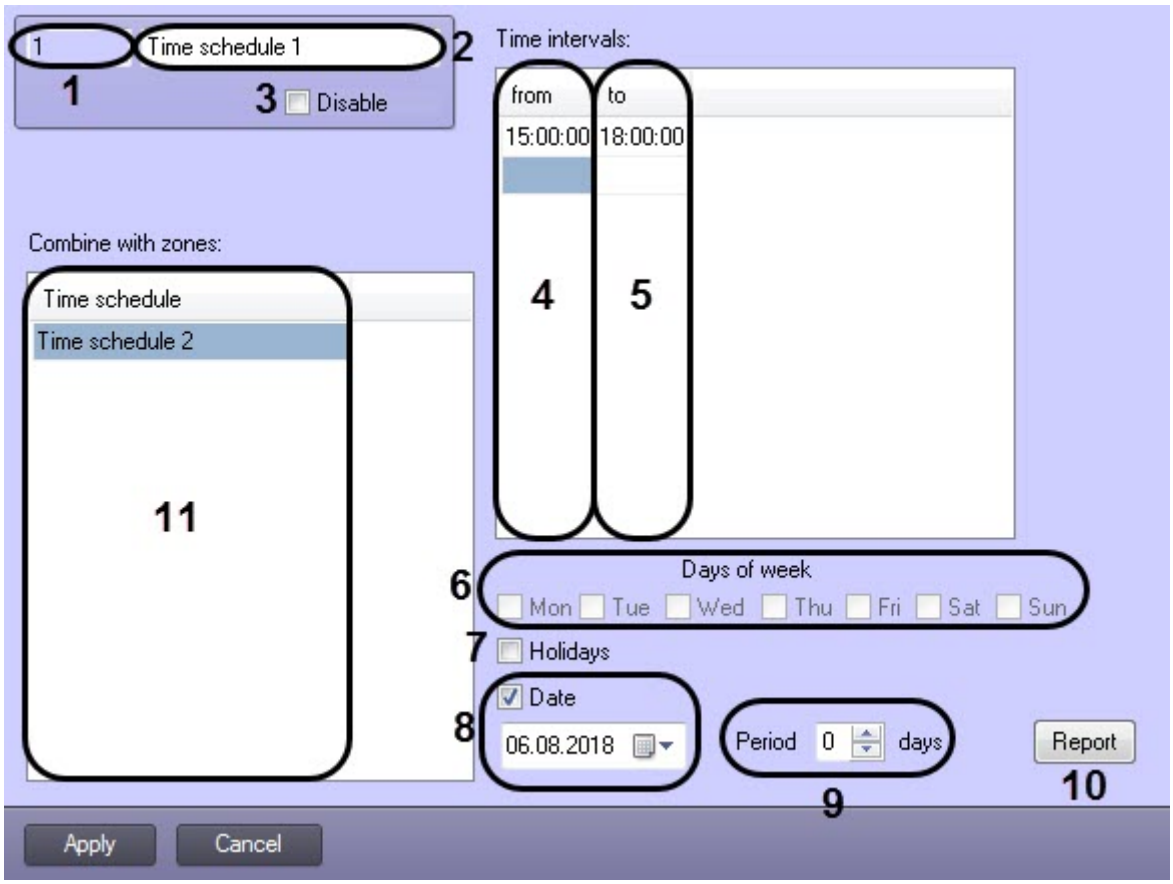


Table describes the setting parameters corresponding to the elements of the settings panel of the **Time schedule** object.

26.1.5.10.5 The Settings panel of the Script object

The **Script** object is used to create specialized programs in the JScript language.

The settings panel of the **Script** object is shown in the figure.

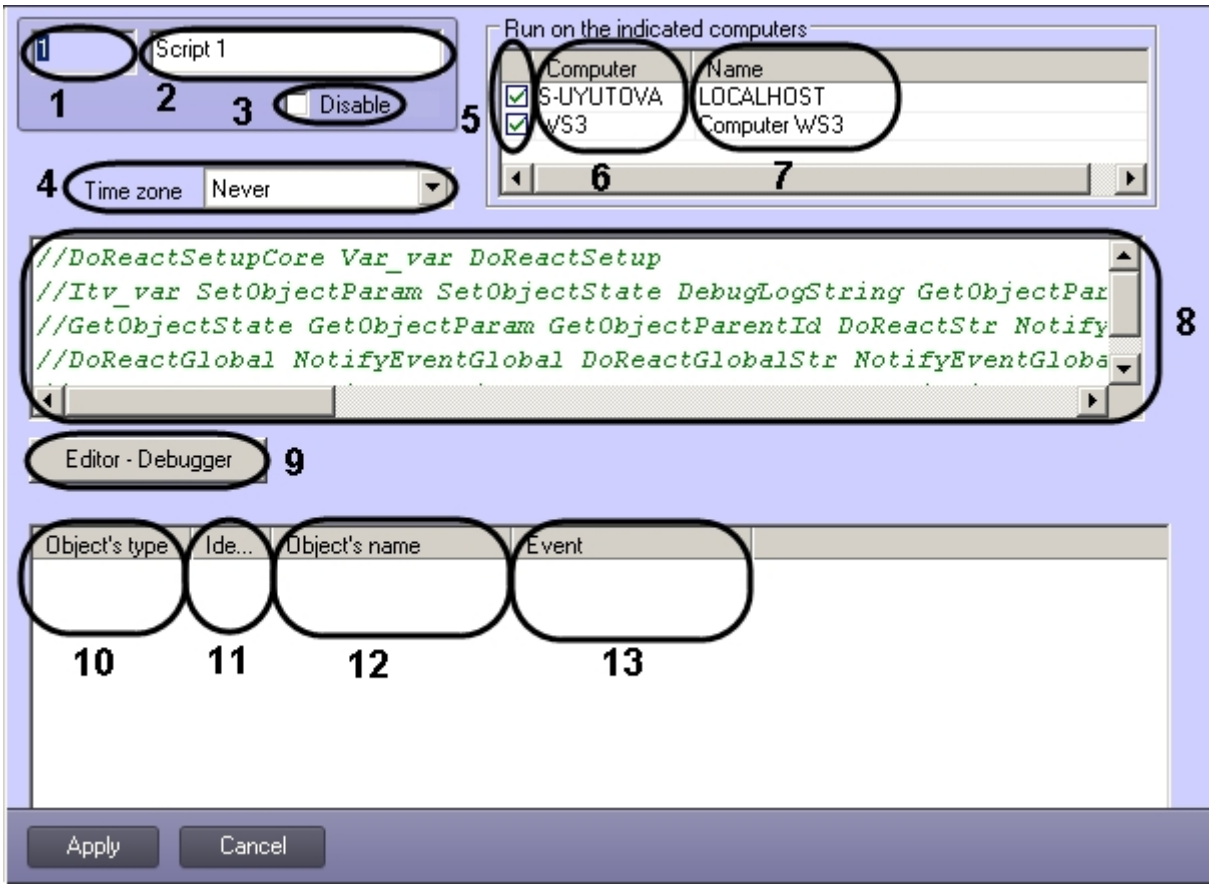


Table describes the setting parameters corresponding to the elements of the settings panel of the **Script** object.

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.10.6 The Settings panel of the Region object

The **Region** object is used to create the zones, which break down the protected areas into structural elements. The **Region** objects allow:

1. grouping the hardware based on the attributes of a certain region;
2. executing certain operations simultaneously with all objects of the same type belonging to the same region.

The settings panel of the **Region** object is shown in the figure.

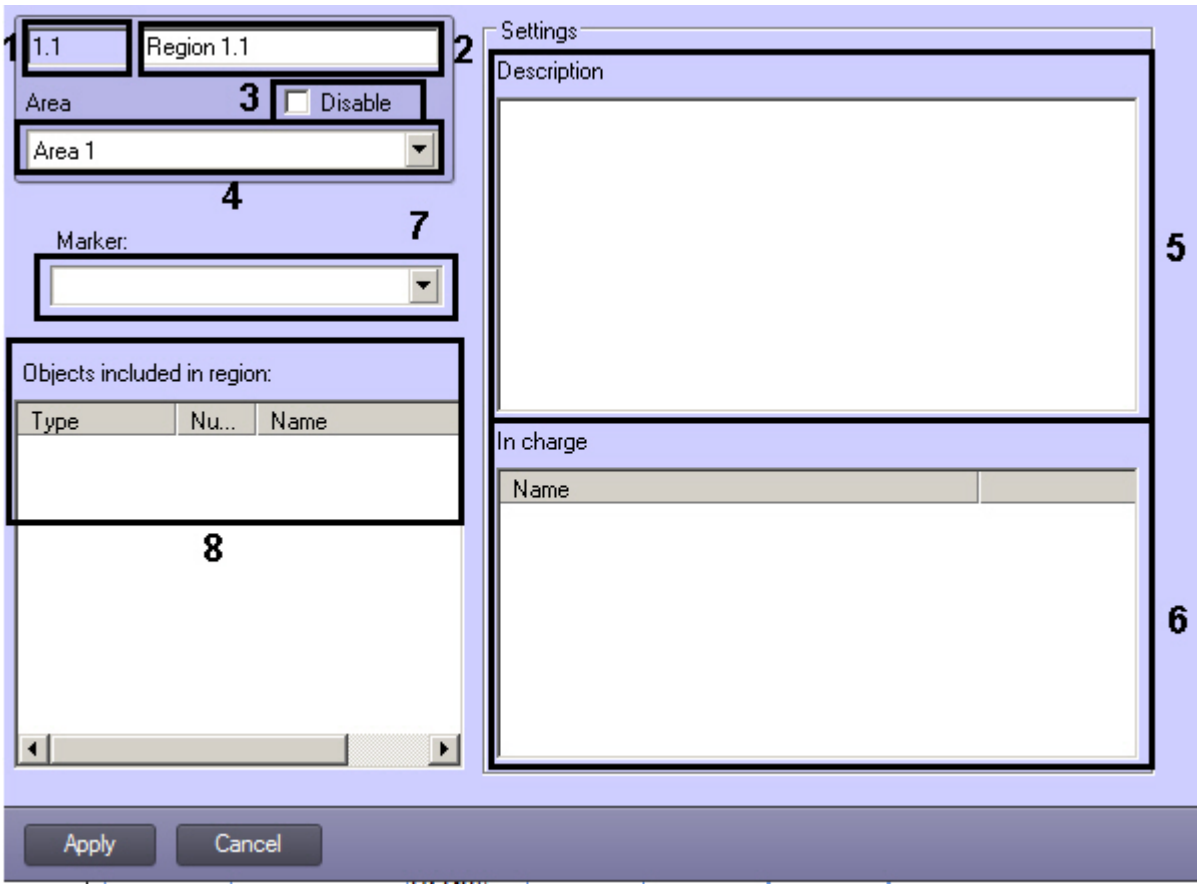


Table describes the setting parameters corresponding to the elements of the settings panel of the **Region** object.

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.10.7 The Settings panel of the Rule of states transition object

The settings panel of the **Rule of states transition** object is shown in the figure.

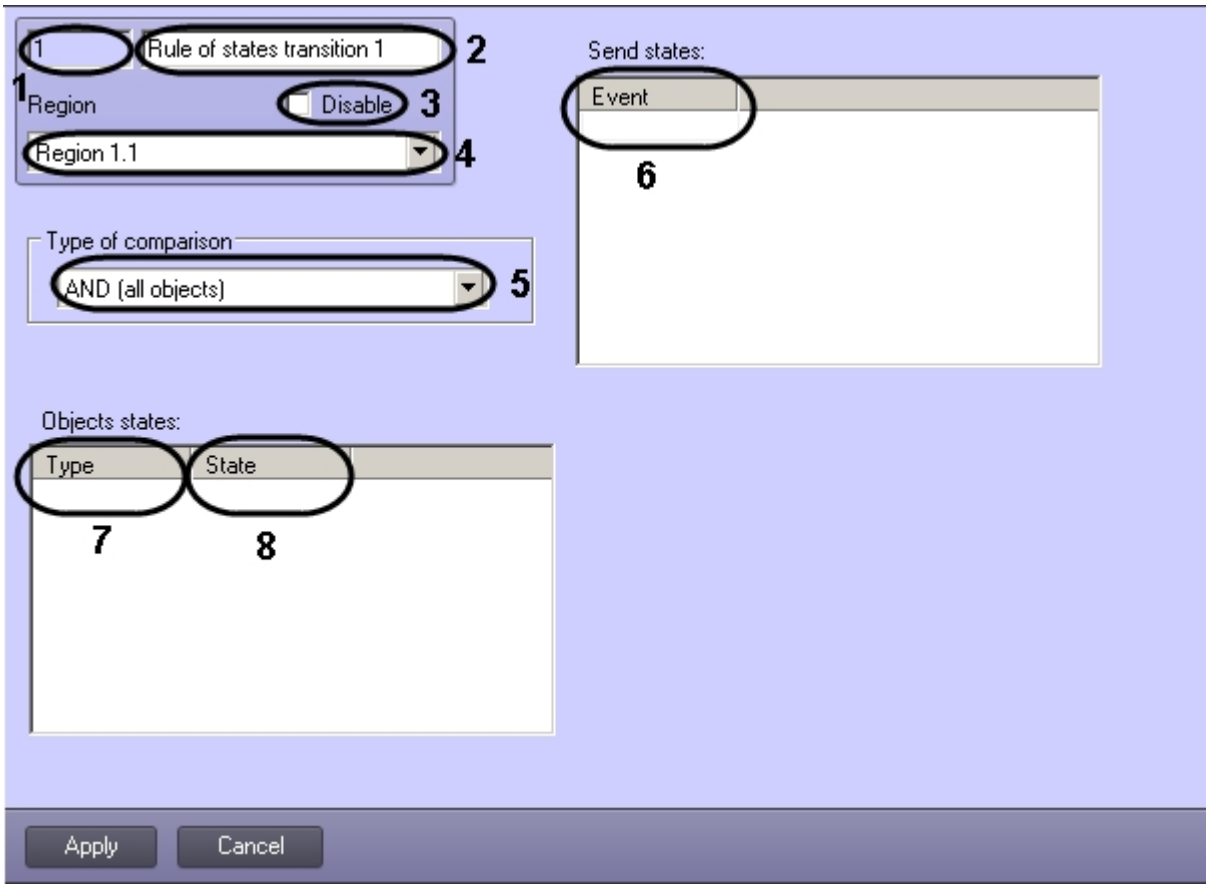


Table describes the setting parameters of the **Rule of states transition** object.

26.1.5.10.8 The Settings panel of the Macro event object

The **Macro event** object is used for creating events in case of occurrence of the events chain in the specified time period.

The settings panel of the **Macro event** object is shown in the figure.

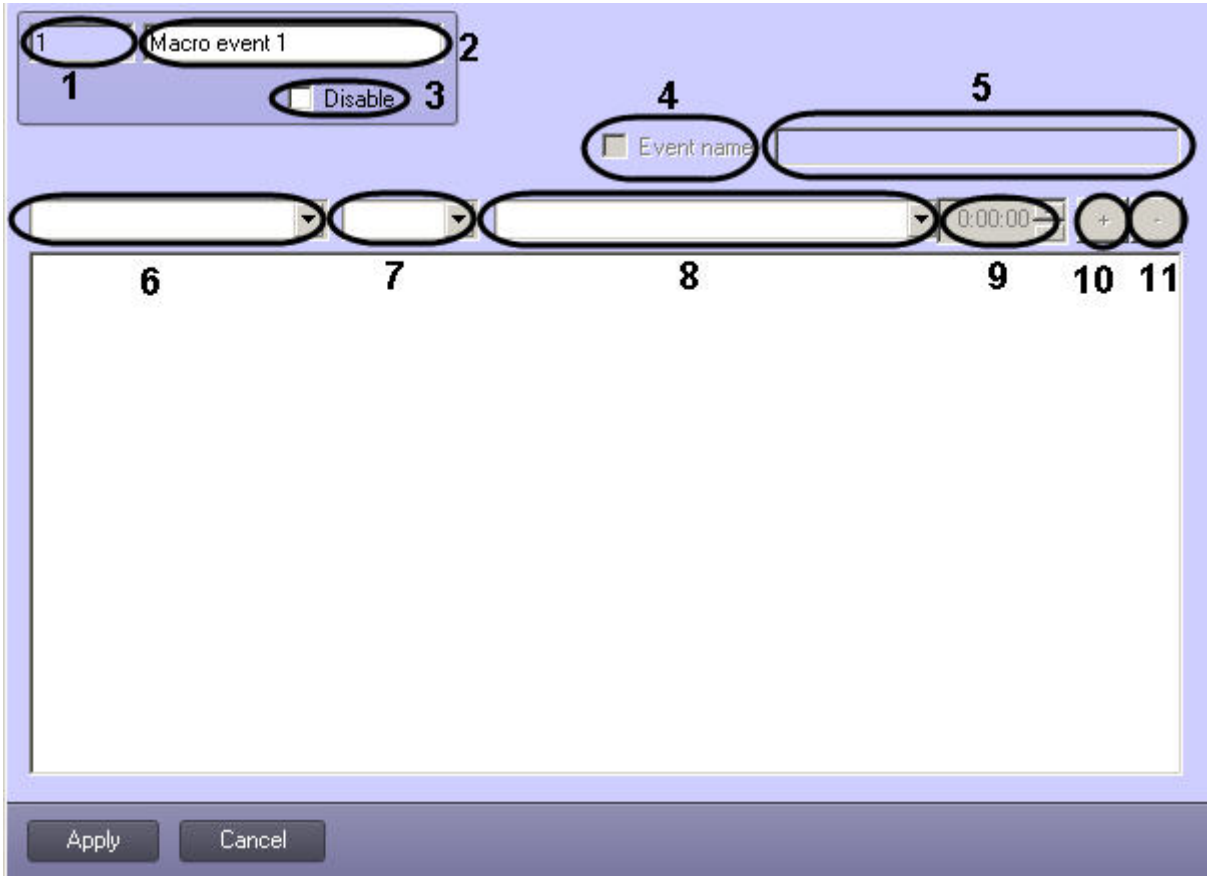


Table describes the setting parameters corresponding to the elements of the settings panel of the **Macro event** object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Macro event** object	Sequence of numbers	-	Depends on the number of the **Macro event** objects in the digital video surveillance system with distributed architecture
2	Name*	Enter the value into the field	Sets the name of the **Macro event** object	Latin, Cyrillic and service characters	Macro event	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Macro event** object in the digital video surveillance system with distributed architecture	Boolean type	Clear	Set—the **Macro event** object is disabled and isn't used Clear—the **Macro event** object is enabled and used
4	**Event name**	Set the checkbox	The checkbox determines whether the macro event is generated when the events chain occurs or when the event timeout expires	Boolean type	Clear	Set—event is generated Clear—event isn't generated

5	**Event name**	Enter the value into the field	Sets the name of the macro event which is transmitted in the param0 parameter	Latin, Cyrillic and service characters		A line containing a sequence of any characters (letters, digits, service characters), case-insensitive. No more than 120 characters
6	Object type*	Select the value from the list	Sets the type of objects, the events from which should be monitored	Object types created in the system	-	Depends on the objects created in the system
7	Number*	Select the value from the list	Sets the number of the object of the selected type, the event from which should be monitored	Identifiers of the objects of the selected type registered in the system	-	Depends on the number of the objects of the selected type
8	Event type*	Select the value from the list	Sets the event type of the selected object which should be monitored	List of events available for the object of the selected type	-	Depends on the selected object type
9	Timeout*	Enter the value into the field	Sets the timeout of the waiting for the event of the selected type to occur	HH:MM:SS	-	Time in the HH:MM:SS format
10	**+** button	Click the button	Adds an event to the chain	-	-	-
11	**-** button	Click the button	Removes an event from the chain with all events that are lower in the chain	-	-	-

*Name of the element isn't displayed in the settings panel of the given object.

26.1.5.11 The Users tab

26.1.5.11.1 The Users tab components

The **Users** tab has the following elements:

1. The tree of departments and users in them. The settings panel of the **User** and **Department** objects contain the parameters used when configuring *ACFA Intellect.* That is why only the main settings of these objects are described in this document.
2. The list of user rights.

26.1.5.11.2 The Settings panel of the Department object

The settings panel of the **Department** object is shown in the figure.

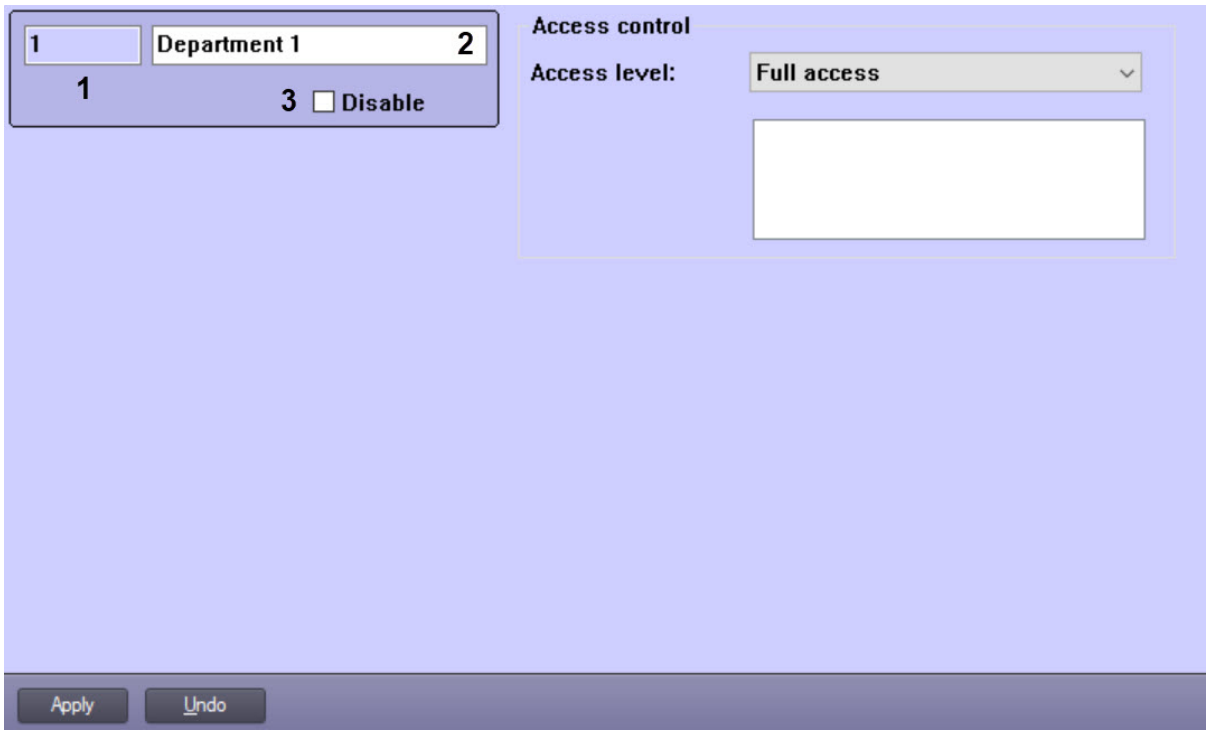


Table describes the setting parameters of the **Department** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **Department** system object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **Department** objects in the system
2	Name	Enter the value into the field	Sets the name of the **Department** object in the system	Latin, Cyrillic and service characters	Department	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **Department** object in the system	Boolean type	Clear	Set—the **Department** object is disabled and isn't used Clear—the **Department** object is enabled and used

26.1.5.11.3 The Settings panel of the User object

The settings panel of the **User** object is shown in the figure.

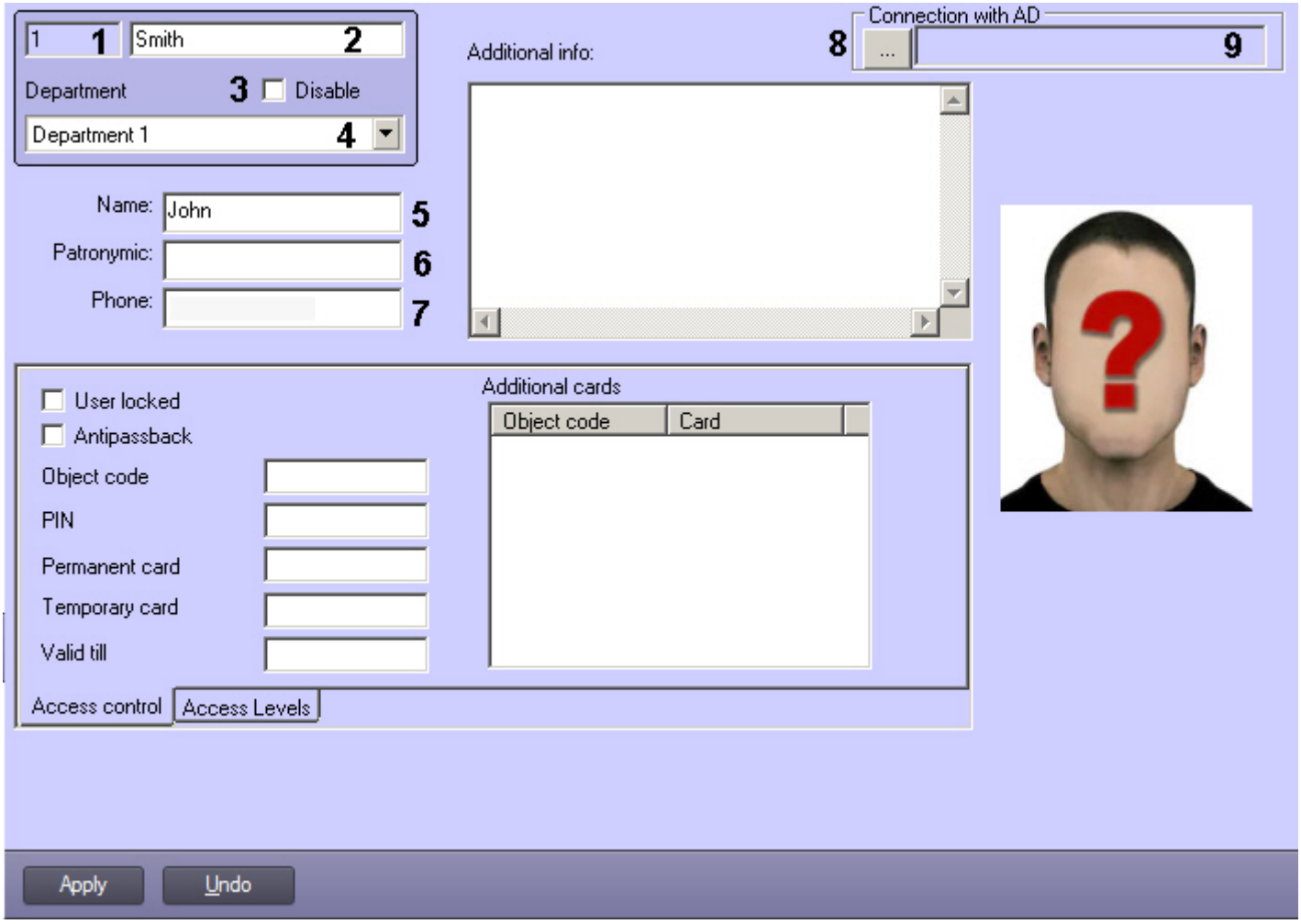


Table describes the setting parameters of the **User** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number	Automatically	Displays the identification number of the **User** system object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **User** objects in the system
2	Name	Enter the value into the field	Sets the name of the **User** object in the system (usually the user's last name)	Latin, Cyrillic and service characters	**User**	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60. Do not enter **rs** in this field when registering Operator accounts, as this value is used as a default username in *Intellect Web Report System*
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **User** object in the system	Boolean type	Clear	Set—the **User** object is disabled and isn't used Clear—the **User** object is enabled and used

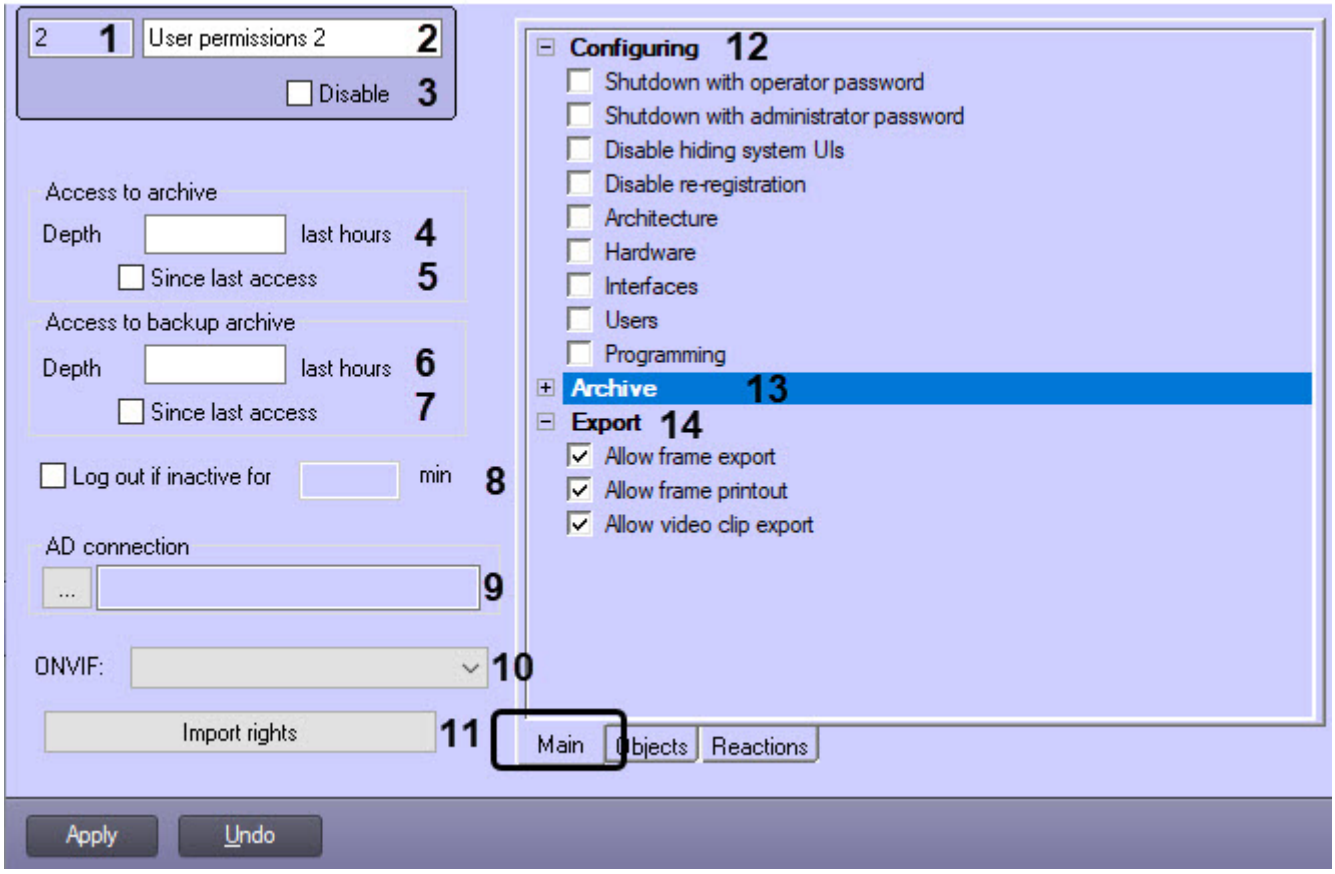
№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
4	**Department**	Select the value from the list	Sets the **Department** parent object for the given **User** object	Names of the **Department** objects registered in the system	Name of the **Department** parent object	Depends on the number of the **Department** objects in the system
5	**Name**	Enter the value into the field	Sets the user's name	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters
6	**Patronymic**	Enter the value into the field	Sets the user's patronymic	Latin, Cyrillic and service characters	-	A line containing a sequence of any characters
7	**Phone**	Enter the value into the field	Sets the user's phone number for the two-factor authentication	Phone number	-	+ [country code][city code] [subscriber number] For example, +11234567890
8	**Connection with AD**	Click the button	Opens a window to configure the connection between the *Intellect* and the Windows Active Directory users	-	-	-
9	**Connection with AD**	Automatically	Displays the Active Directory user identifier connected with the *Intellect* user	Latin and service characters	-	Depends on the Active Directory identifier values

The settings of the **User** object are used to configure the access control system. It is usually changed using the *Access Manager* module in the *ACFA Intellect* subsystem (see Access Manager Module Settings and Operation Guide). In the *Access Manager* module you can also add the photo displayed on the **User** object settings panel.

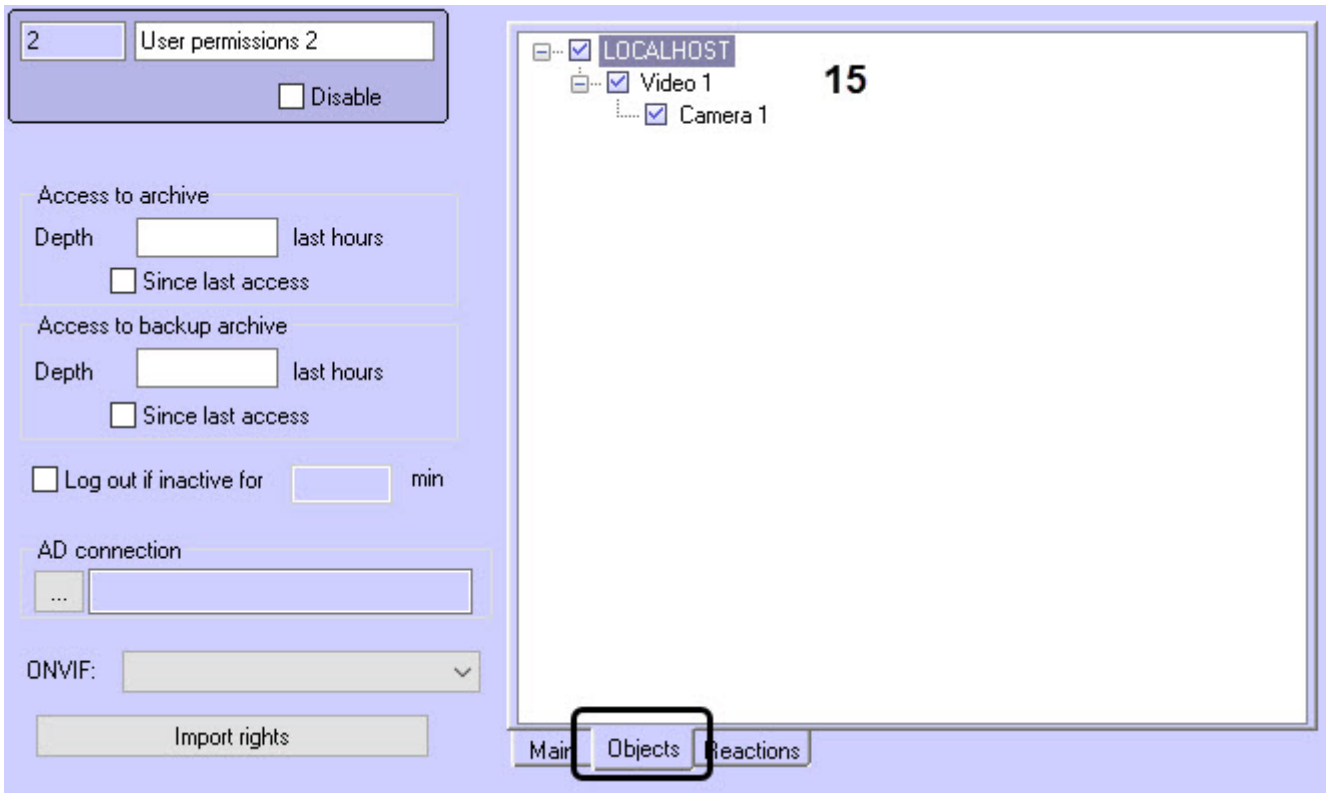
You can also add or change the user's photo using the *Face recognition and search* module that is a part of *Face Intellect* (for details on how to configure and work with this module, see *Face Intellect* documentation in the AxxonSoft documentation repository).

26.1.5.11.4 The Settings panel of the User permissions object

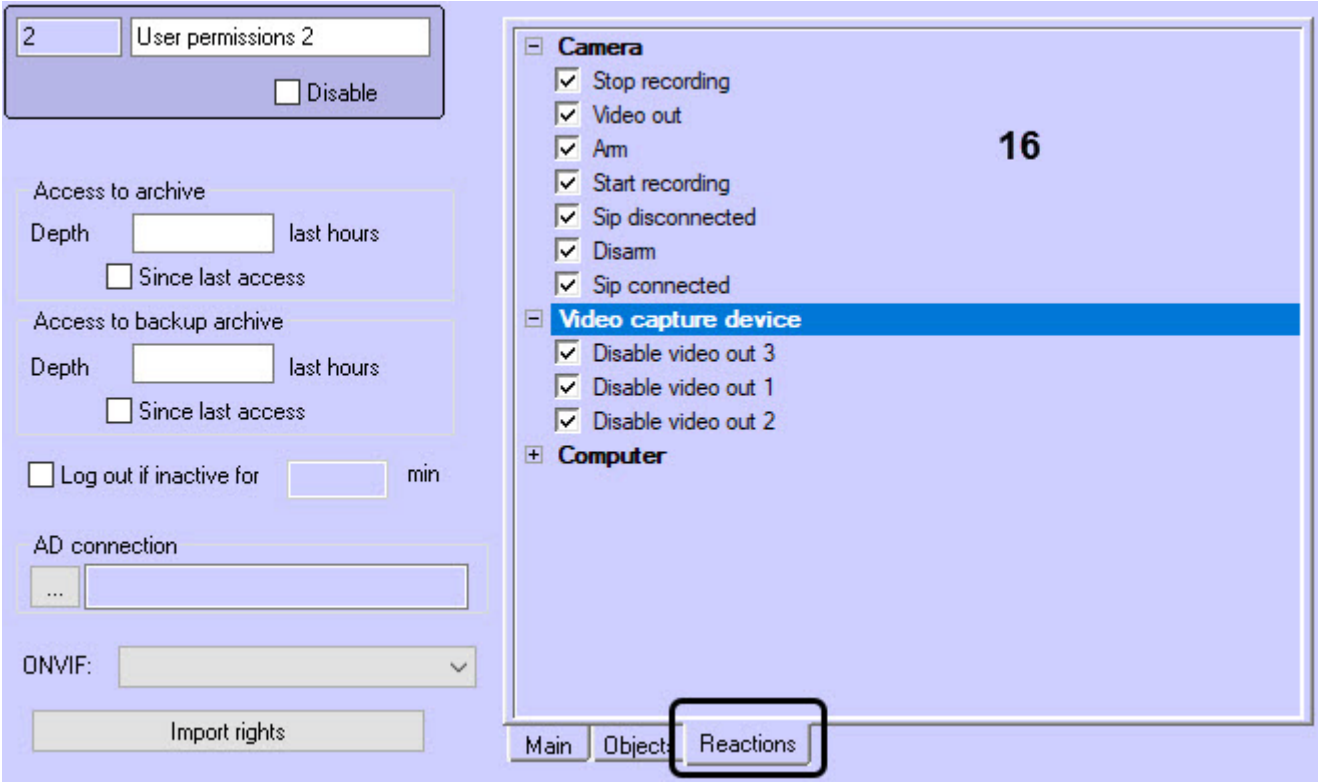
The settings panel of the **User permissions** object is shown in the figures.



The **Main** tab.



The **Objects** tab.



The **Reactions** tab.

Table describes the setting parameters of the **User permissions** system object.

№	Parameter	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **User permissions** object in the system	Numbers, letters, periods, hyphen, dash and underscore	-	Depends on the number of the **User permissions** objects in the system
2	Name*	Enter the value into the field	Sets the name of the **User permissions** object in the system	Latin, Cyrillic and service characters	User permissions	A line containing a sequence of any characters (letters, digits, service characters except > and < characters), case-insensitive. Number of characters—from 1 to 60
3	**Disable**	Set the checkbox	Sets the state (enabled or disabled) of the **User permissions** object in the system	Boolean type	Clear	Set—the **User permissions** object is disabled and isn't used Clear—the **User permissions** object is enabled and used
The **Access to archive** group						
4	**Depth __ last hours**	Enter the value into the field	Sets the number of the last hours of the video archive that can be viewed	Non-negative integer	-	>=0 The 0 value means that you are not allowed to view the archive

5	**Since last access**	Set the checkbox	Sets the time to determine the archive depth	Boolean type	Clear	Set—the number of hours available for viewing are counted from the moment the user logged in Clear—the number of hours available for viewing are counted from the current moment
The **Access to backup archive** group						
6	**Depth __ last hours**	Enter the value into the field	Sets the number of the last hours of the backup archive that can be viewed	Non-negative integer	-	>=0 The 0 value means that you are not allowed to view the backup archive
7	**Since last access**	Set the checkbox	Sets the time to determine the backup archive depth	Boolean type	Clear	Set—the number of hours available for viewing are counted from the moment the user logged in Clear—the number of hours available for viewing are counted from the current moment
Outside the group						
8	**Log out if inactive for __ minutes**	Set the checkbox, enter the value into the field	Sets the time period (in minutes) when the Operator is inactive. At the end of this period the session has be terminated	Boolean type, integer	Clear	Set—when the Operator is inactive for the specified time period, session is automatically terminated. To continue operation, log in the system specifying the username and password Clear—session is not automatically terminated when the Operator is inactive
9	**AD connection**	Click the button	Opens a dialog window to configure the connection between user permissions and Windows Active Directory groups	-	-	-
10	**ONVIF**	Select the value from the list	Matches the *Intellect* user permissions with ONVIF permissions according to the specification	Supported types of permissions	-	Administrator Operator User
11	**Import permissions**	Click the button	Imports the settings of the user permissions from other **User permissions** objects	-	-	-
The **Main** tab						
The **Configuring** group						
12	**Shutdown with operator password**	Set the checkbox	Allows shutting down *Intellect* using the password of the currently authorized Operator	Boolean type	Clear	Set—Operator with these permissions is allowed to shut down *Intellect* Clear—Operator with these permissions is not allowed to shut down *Intellect*
	Shutdown with administrator password	Set the checkbox	Allows shutting down *Intellect* using the password of the Administrator	Boolean type	Clear	Set—*Intellect* shuts down only when the Administrator password is used

						Clear—*Intellect* can shut down in other ways
	Disable hiding system UIs	Set the checkbox	Allows hiding interface windows in *Intellect*	Boolean type	Clear	Set—interface windows cannot be hidden Clear—interface windows can be hidden
	Disable re-registration	Set the checkbox	Allows changing the user in *Intellect*	Boolean type	Clear	Set—user cannot be changed Clear—user can be changed
	The group of **Tabs*** checkboxes	Set the checkbox	Specifies the tabs of the **System settings** dialog window that can be accessed when the user gets the corresponding permissions	Boolean type	All checkboxes are clear	The following values are available for each tab: Set—Operator is allowed to manage the objects in the tab Clear—Operator cannot access the tab
The **Archive** group						
13	**Allow removing video archive files**	Set the checkbox	Determines whether video archive files can be removed from the **Video surveillance monitor** interface	Boolean type	Clear	Set—the **Remove video from the feature menu** item is available in the Monitor Clear—removing video from the **Video surveillance monitor** interface is not available
	Allow protecting files from overwriting	Set the checkbox	Allows protecting the files from being overwritten	Boolean type	Clear	Set—Operator added to these permissions can protect the archive records from loop recording Clear—Operator cannot protect the archive records from loop recording
	Allow removing file protection	Set the checkbox	Sets the possibility to remove protection from the files that are protected from being overwritten	Boolean type	Clear	Set—Operator added to these permissions can remove file protection Clear—Operator cannot remove file protection
	Allow viewing hidden archive	Set the checkbox	Allows viewing the hidden archive	Boolean type	Clear	Set—Operator added to these permissions can view the hidden archive Clear—Operator cannot view the hidden archive
	Allow checking "hidden" archive	Set the checkbox	Allows hiding the archive	Boolean type	Clear	Set—Operator added to these permissions can hide the archive Clear—Operator cannot hide the archive
	Allow unchecking "hidden" archive	Set the checkbox	Allows unhiding the archive	Boolean type	Clear	Set—Operator added to these permissions can unhide the archive Clear—Operator cannot unhide the archive
	Allow hiding screen before	Set the checkbox	Allows hiding the screen before and after inverted mask	Boolean type	Clear	Set—Operator added to these permissions can hide the screen before and after inverted mask

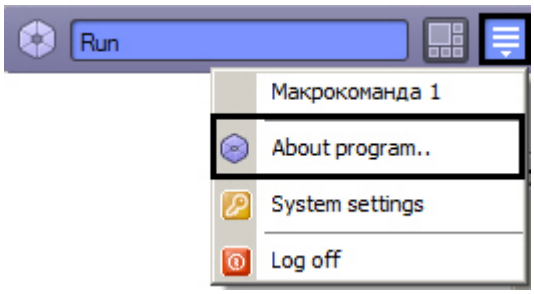
	and after inverted mask					Clear—Operator cannot hide the screen before and after inverted mask
	Allow showing live video after creating inverted mask	Set the checkbox	Allows viewing live video before and after inverted mask	Boolean type	Clear	Set—Operator added to these permissions can view live video before and after inverted mask Clear—Operator cannot view live video before and after inverted mask
	Allow VMDA filters use	Set the checkbox	Allows saving and loading archive search templates when working with **Video surveillance monitor**	Boolean type	Clear	Set—Operator with the appropriate permissions will have access to the **Save the template** and **Load the template** buttons in the **Video surveillance monitor** Clear—the **Save the template** and **Load the template** buttons in the **Video surveillance monitor** will be hidden for the Operator
The **Export** group						
14	**Allow frame export**	Set the checkbox	Allows exporting the archive frames	Boolean type	Set	Set—Operator added to these permissions can export video archive frames Clear—Operator cannot export video archive frames
	Allow frame printout	Set the checkbox	Allows printing archive frames	Boolean type	Set	Set—Operator added to these permissions can print video archive frames Clear—Operator cannot print video archive frames
	Allow video clip export	Set the checkbox	Allows exporting video archive records	Boolean type	Set	Set—Operator added to these permissions can export video records Clear—Operator cannot export video records
The **Objects** tab						
15	The list of system objects*	Set the checkboxes	Displays the objects created in the system and allows setting the administration and monitoring permissions	-	-	see Limiting access to the system objects administration, control and viewing functions
The **Reactions** tab						
16	The list of system object reactions*	Set the checkboxes	Sets the list of reactions that Operator can run	Boolean type	Set	Set—Operator can run the reaction Clear—Operator cannot run the reaction

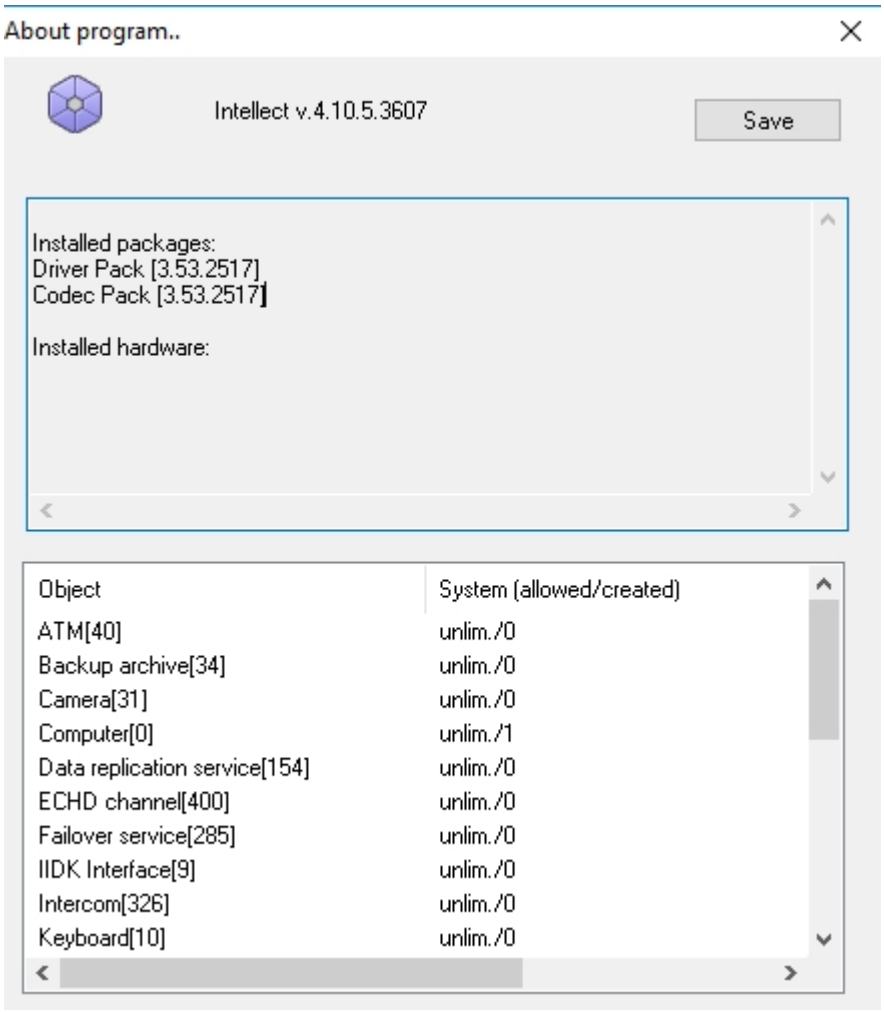
* Name of the object isn't displayed on the settings panel.

26.1.6 Information about program

The information about the program includes *Intellect* version, installed packages (vertical solutions, Drivers Pack, Codec Pack, etc.) and hardware and restrictions to object count set by the license key.

Click the **Execute** button on the Main control panel, then select **About program...** to open this window.





Note

It is possible to hide the **Save** button from the **About program...** window. To do this, change the **Shell** key value to any other one that does not contain the "**explorer**" string (see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).

26.2 Appendix 2. Relevant information on using Windows operating system

26.2.1 Working with Windows OS registry

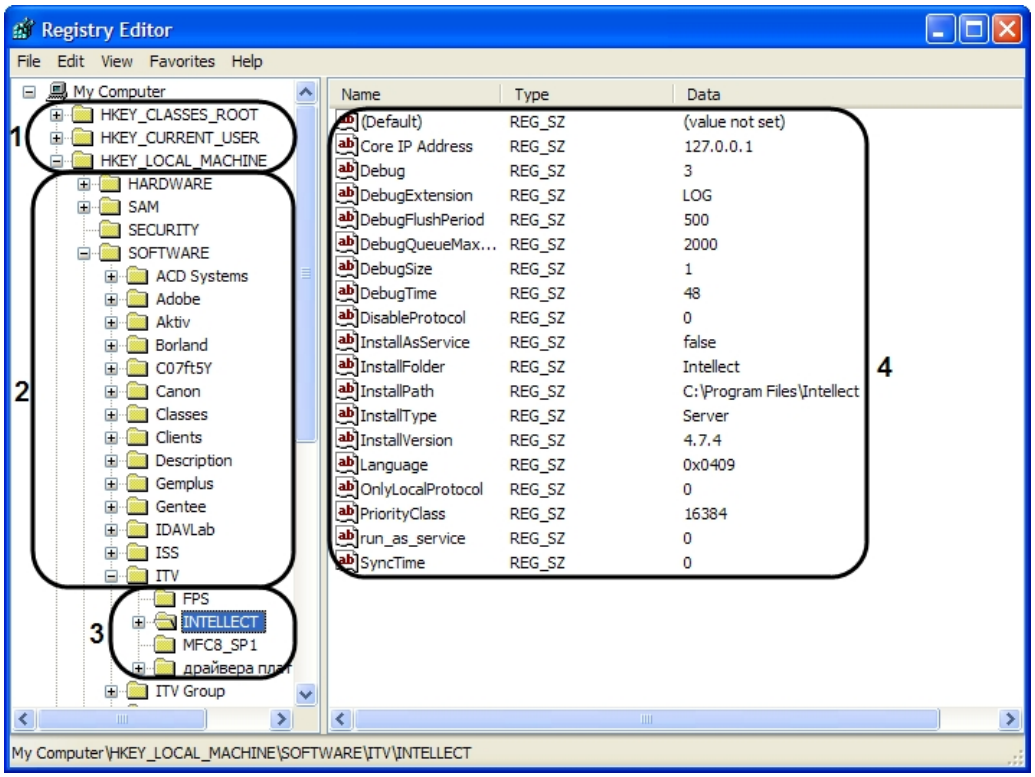
26.2.1.1 General information about Windows OS registry

Windows system registry is a database containing the settings of the operating system (hardware, software, users). When system parameters of the operating system are changed, the system registry is updated.

You can edit the registry using the regedit.exe utility included in the standard set of service programs in Windows. The information about the OS settings is stored in two hidden files in the Windows directory: system.dat and user.dat. The registry is a hierarchical structure, the branches of which constitute the keys that contain parameters and subkeys. The registry has six main branches described in the table.

Branch name	**Description**
HKEY_CLASSES_ROOT	Contains the information about the software configuration, including the ties of the file types to certain applications, drag-and-drop parameters, printer parameters and COM
HKEY_CURRENT_USER	Contains user system configuration settings. This section is created and populated with information from the HKEY_USERS section upon user login
HKEY_LOCAL_MACHINE	Contains the parameters of the computer, drivers and other hardware. The information in this section is common to all users of the computer
HKEY_USERS	Contains the information about all users who have accounts on this computer. Contains two types of parameters: common to all users and specific to each user
HKEY_CURRENT_CONFIG	Contains the information about the current hardware configuration
HKEY_DYN_DATA	Indicates the part of the HKEY_LOCAL_MACHINE section that is needed for Plug & Play devices. This section changes when you add or remove devices from the system

The branches, keys and subkeys are visually similar to the structure of the user folders, allowing nested branches. The figure shows the main elements of the registry.



1. Branch.
2. Key.
3. Subkey.
4. Parameter.

A parameter has three characteristics: name, data type and value. A key can have only one parameter with no name, which serves as a default value for the key. It is recommended to give the parameter of the registry key a meaningful name, indicating its purpose.

Windows has a set of registry data types. The most commonly used types are described in the table.

Data type	**Description**	**Purpose**
REG_DWORD	A parameter of this type takes 4 bytes and is displayed in hexadecimal and decimal format	Many service or driver parameters are of this type. Example: 0x00000240(576) — decimal value of the parameter is given in parenthesis
REG_BINARY	Binary data in an arbitrary form. Maximum length of the parameter of this type is 16 bytes	Most information on hardware components is stored as binary data and displayed in the registry editor in the hexadecimal format, for example "01 00 00 00"
REG_SZ	A string ending with a null character	Example: "C:\Windows"
REG_MULTI_SZ	Multiline text. An array of strings ending with a null. An array ends with two null characters	This type usually has lists and other records in an easy-to-read format. The records are separated by spaces, commas, or other characters
REG_EXPAND_SZ	Data string of variable length ending with a null character	This type contains undisclosed links to environment variables
REG_FULL_RESOURCE _DESCRIPTOR	A sequence of nested arrays	This type is used for storing the list of device resources or drivers

Note

The settings in the Tweaki utility affect the values of the registry keys — see Tweaki.exe utility for advanced setup of the Intellect software system.

Registry keys reference guide

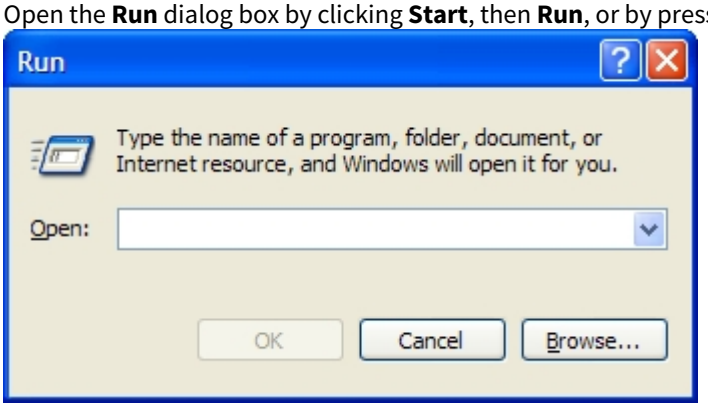
26.2.1.2 Using the registry editor

26.2.1.2.1 Starting and shutting-down the editor

Several programs allow editing the system registry. The regedit.exe utility is included in the standard set of Windows service programs.

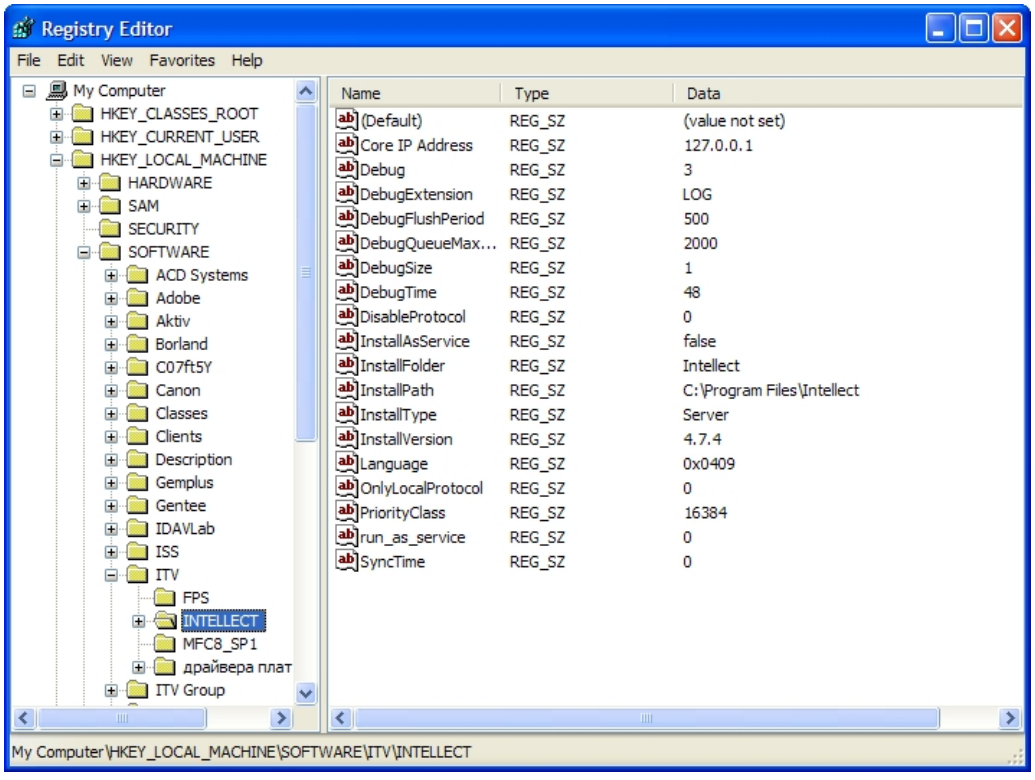
To start the editor, do the following:

1. Open the **Run** dialog box by clicking **Start**, then **Run**, or by pressing WIN+R keys on the keyboard.

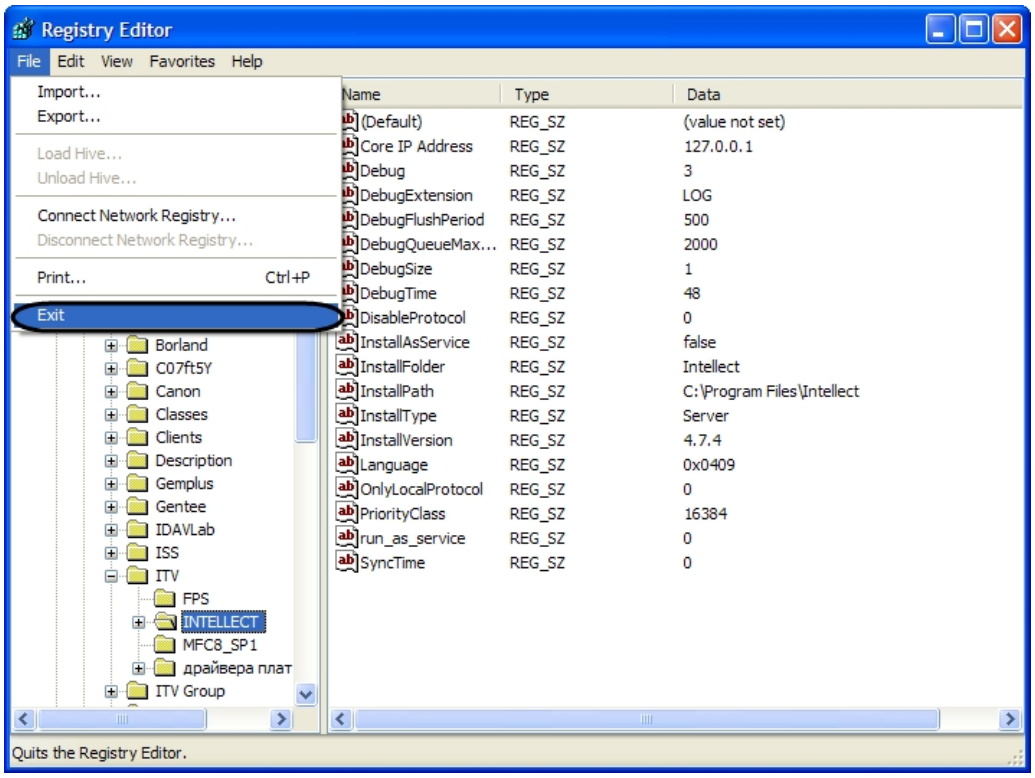


2. Enter “regedit” in the **Open** field of the dialog box.
3. **Click OK.**

The registry editor window will open.

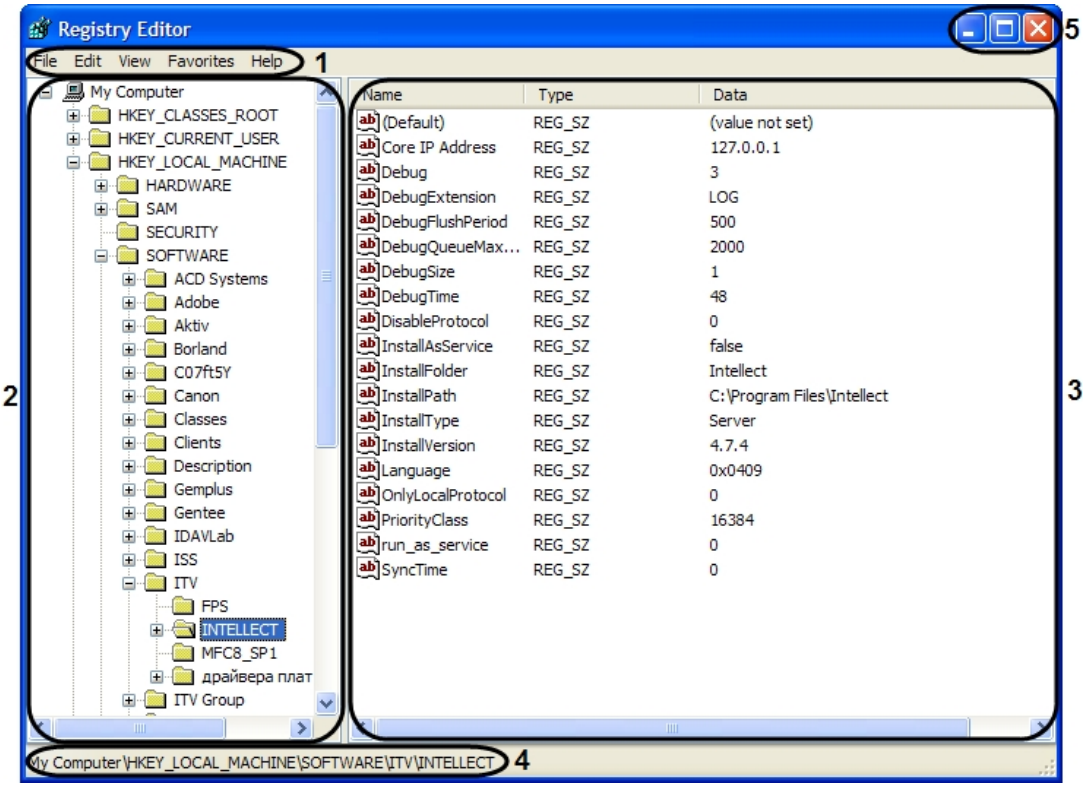


To close the registry editor, click the button, or select **Exit** from File menu.



26.2.1.2.2 Interface elements of the registry editor

Figure shows the elements of the registry editor window.



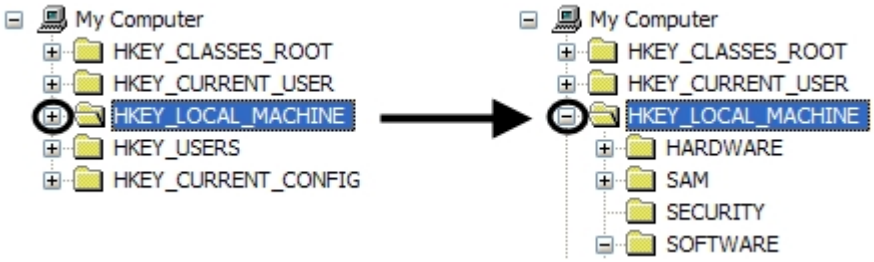
1. Main menu. Contains the commands and settings.
2. Registry tree. Displays the structure of the registry.
3. Parameters table. Displays the parameters of the selected key.

4. Information line. Displays the pathname of the selected object.
5. Control buttons (left to right): Minimize, Restore, Close.

26.2.1.2.3 Navigating the registry tree

The registry structure is shown on the left of the window in a tree similar to the folders tree in Explorer. The tree contains six main branches, each of which contains keys, subkeys and parameters shown in the right panel of the window.

To enter a lower level folder (key), click the plus icon next to the parent folder.

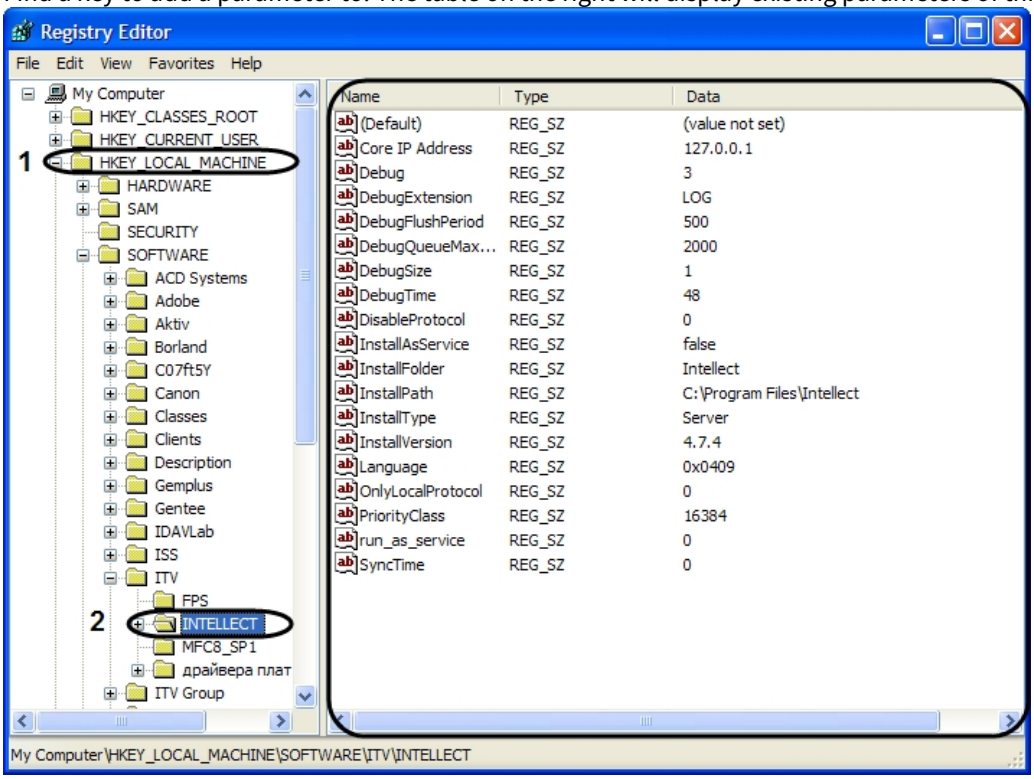


To contract the branch, click the minus icon next to it.

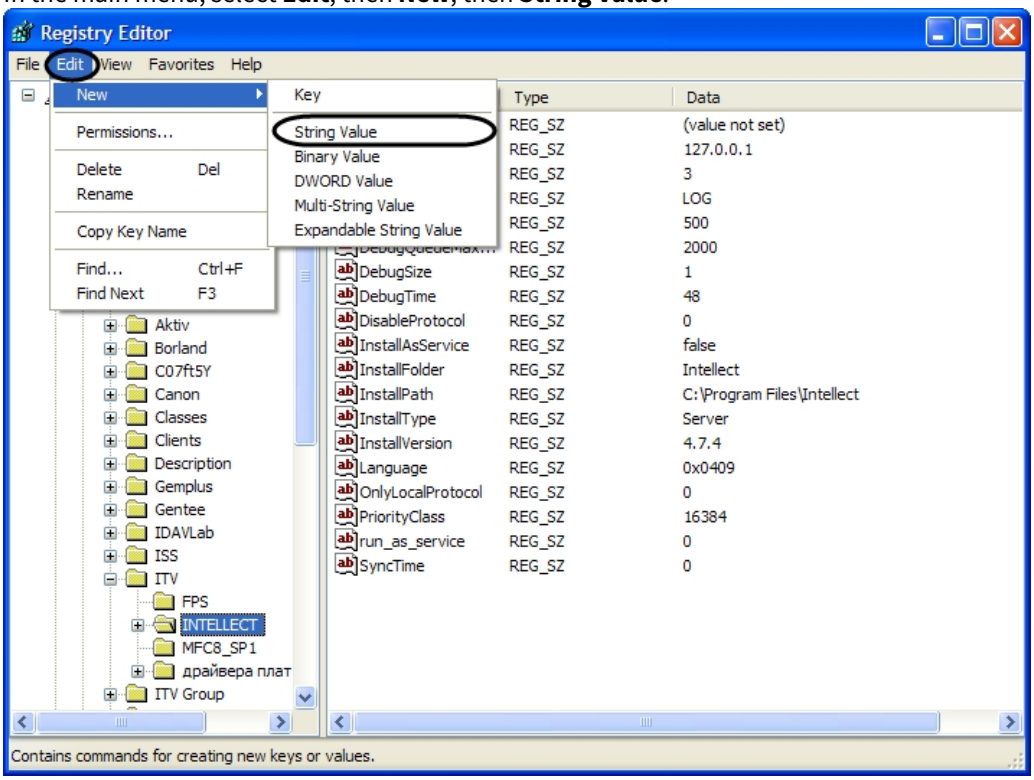
26.2.1.3 Adding string parameters to the registry

To add a string parameter to a key, do the following:

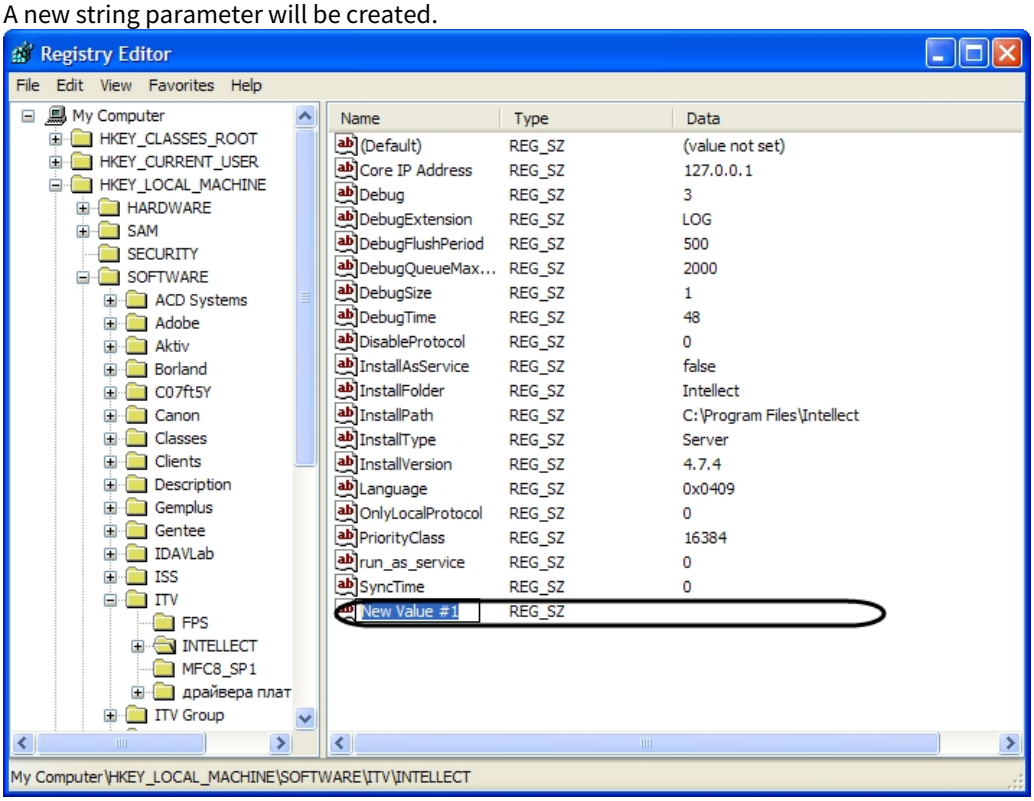
1. Select the required branch and click the plus icon. All folders (keys) inside this branch will be displayed.
2. Find a key to add a parameter to. The table on the right will display existing parameters of this key.



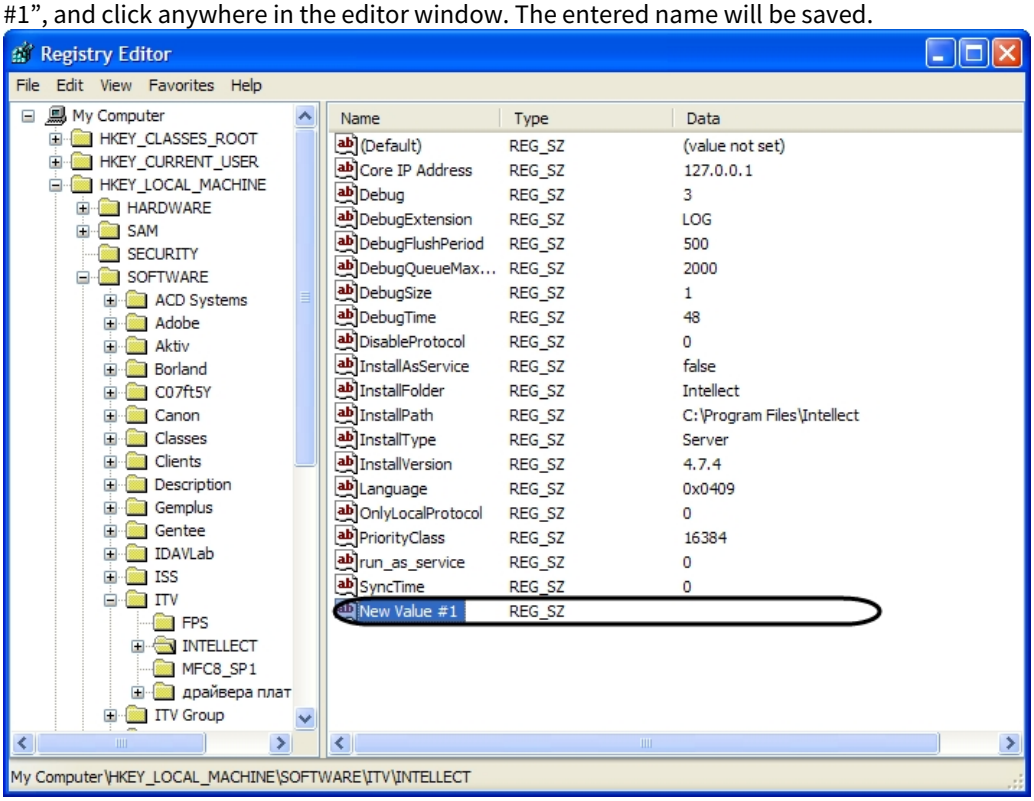
3. In the main menu, select **Edit**, then **New**, then **String Value**.



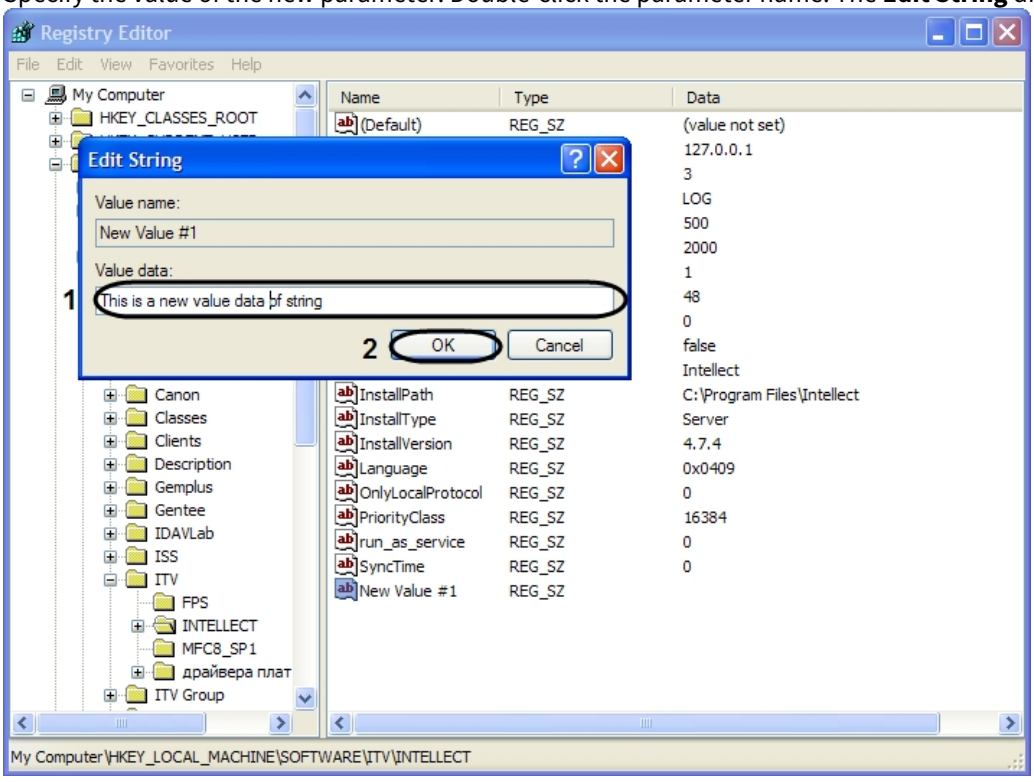
4. A new string parameter will be created.



5. Assign a name to the new parameter. Enter the name in the highlighted name field, which by default reads “New Value #1”, and click anywhere in the editor window. The entered name will be saved.

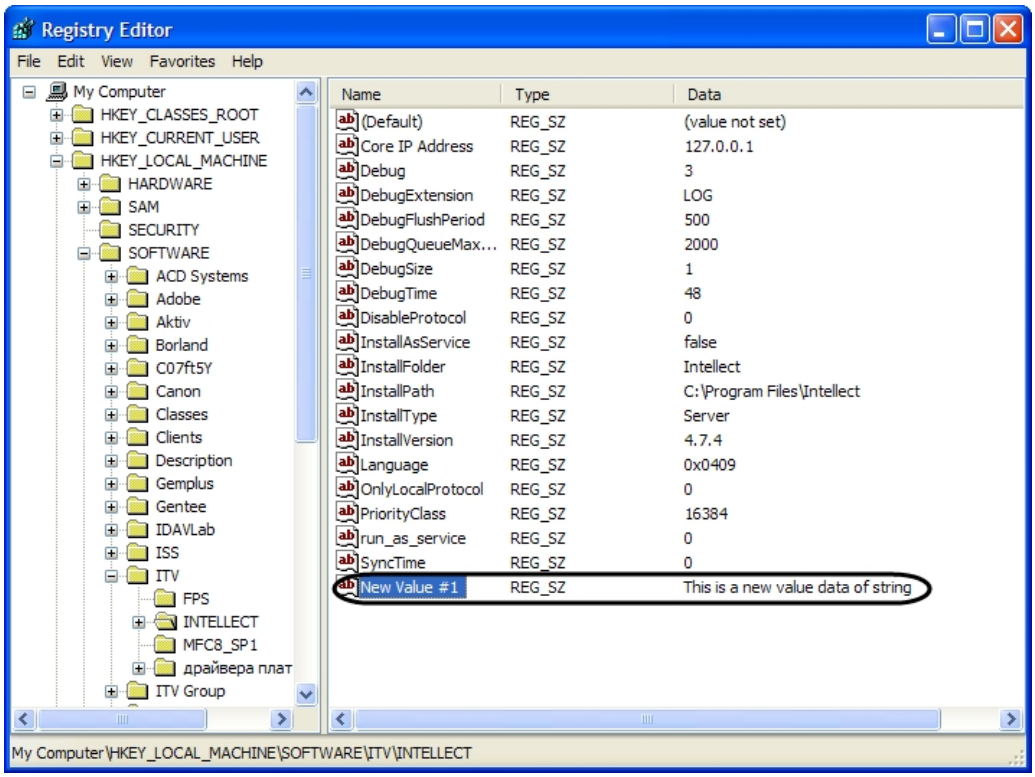


6. Specify the value of the new parameter. Double-click the parameter name. The **Edit String** dialog box will open.



Enter the value into the **Value Data** field (1) and click **OK** (2).

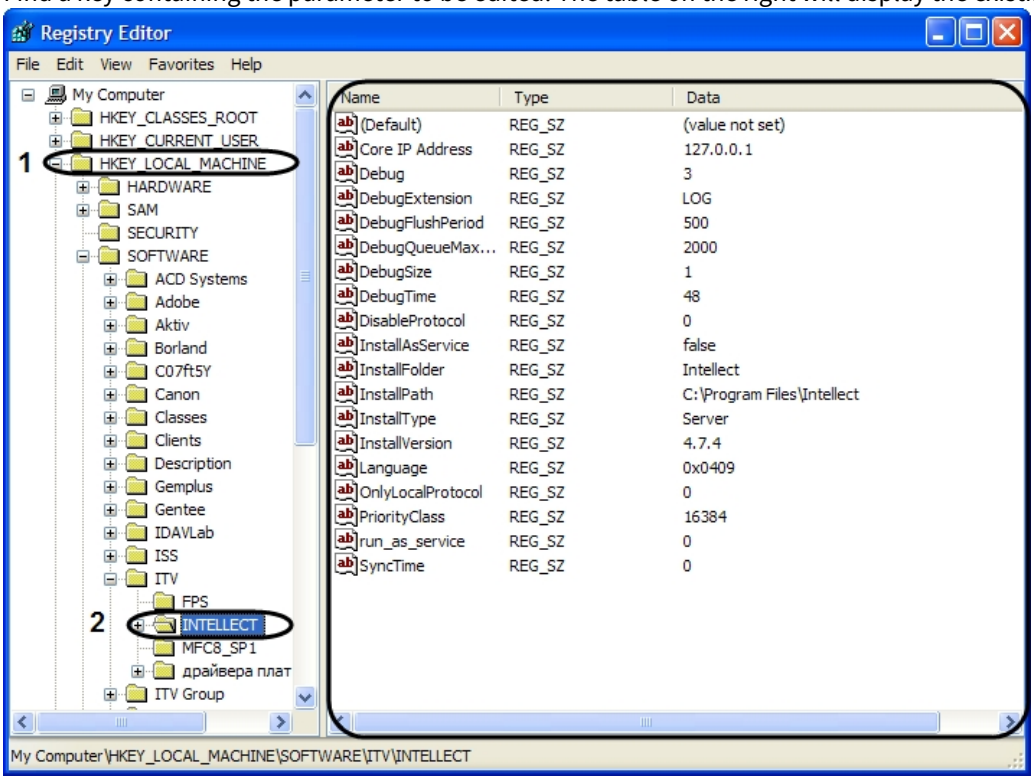
A string parameter with a specified value will be created. To edit the value, repeat step 5.



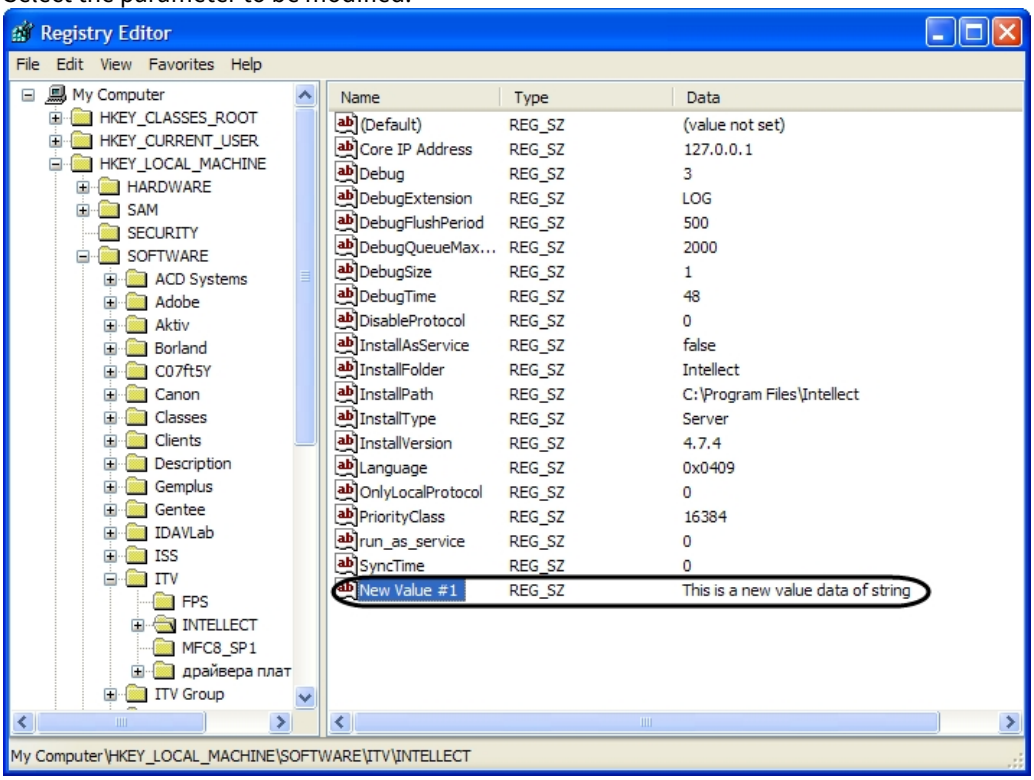
26.2.1.4 Modifying the value of string parameters in Windows OS registry

To modify the value of a string parameter, do the following:

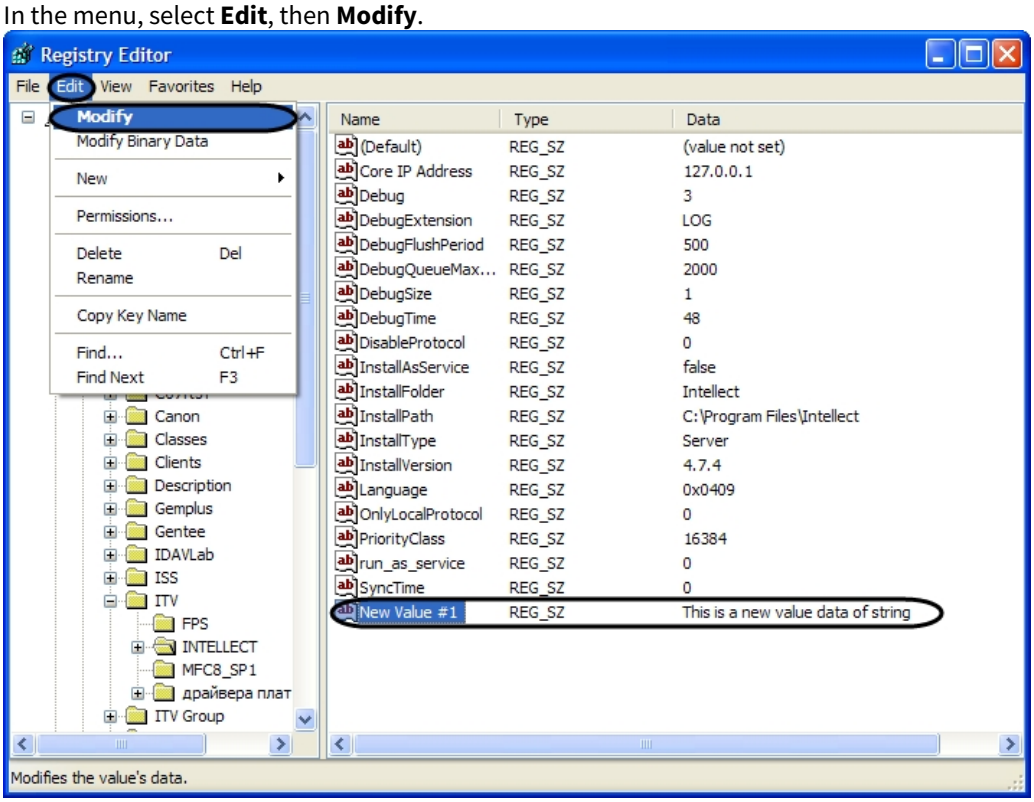
1. Select the required branch and click the plus icon. All folders (keys) inside this branch will be displayed.
2. Find a key containing the parameter to be edited. The table on the right will display the existing parameters of this key.



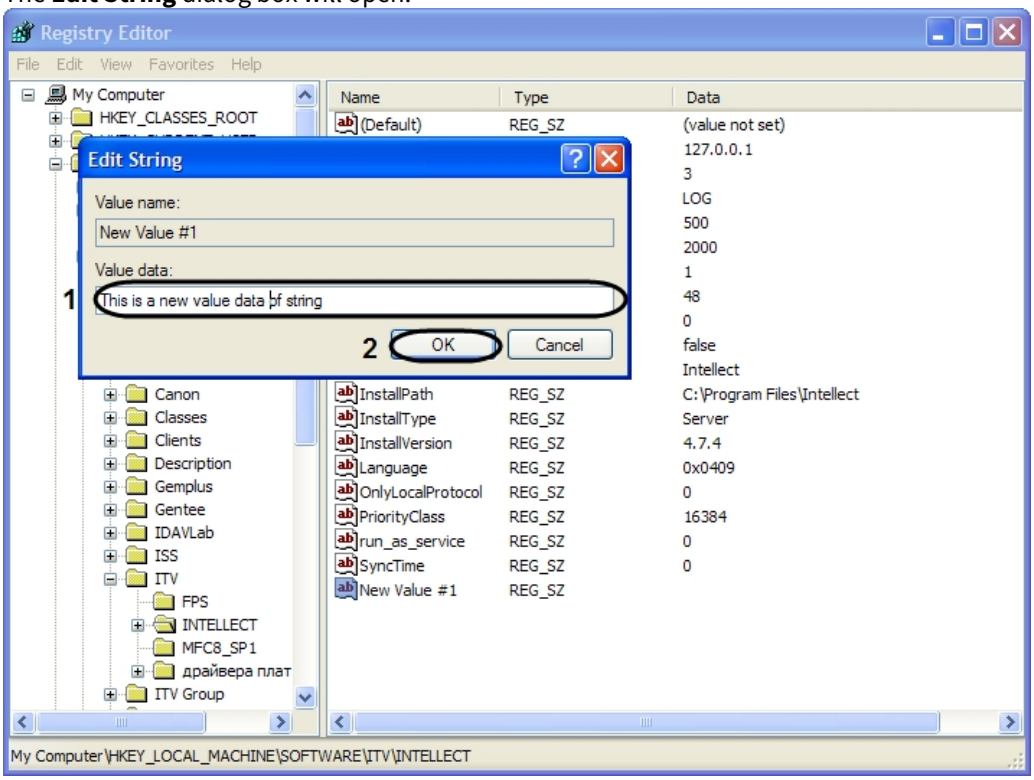
3. Select the parameter to be modified.



4. In the menu, select **Edit**, then **Modify**.

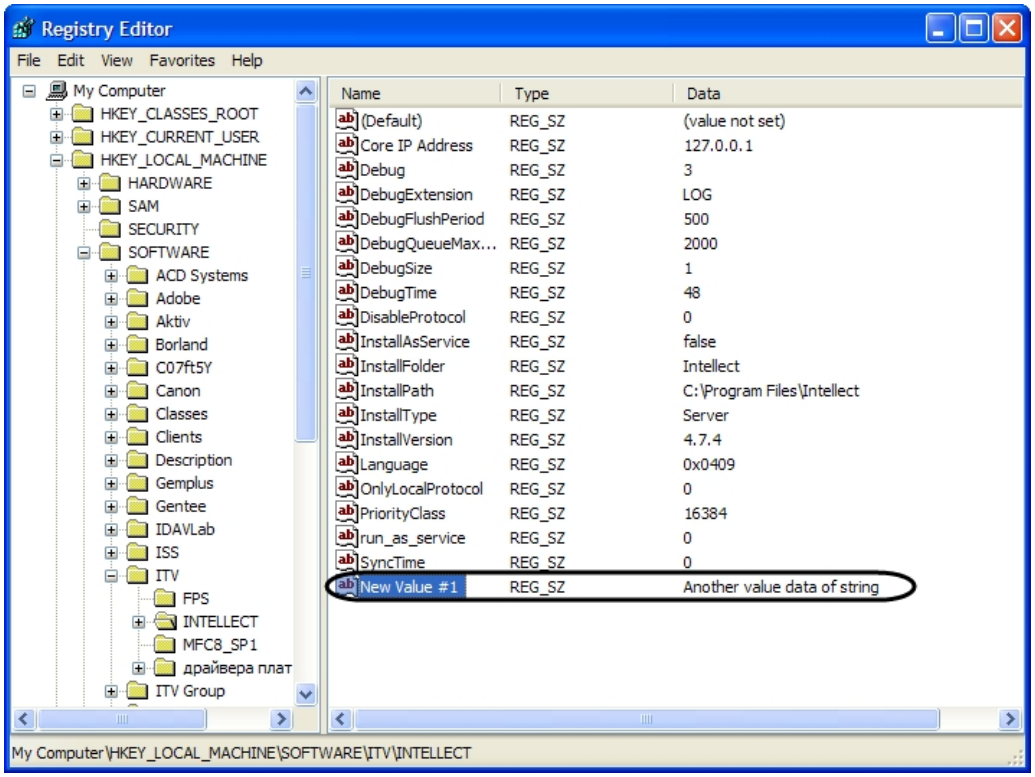


The **Edit String** dialog box will open.



5. Modify the value of the parameter. Delete the old value and enter a new one into the **Value Data** field (1). Click **OK** (2).

The value of the parameter will be changed.

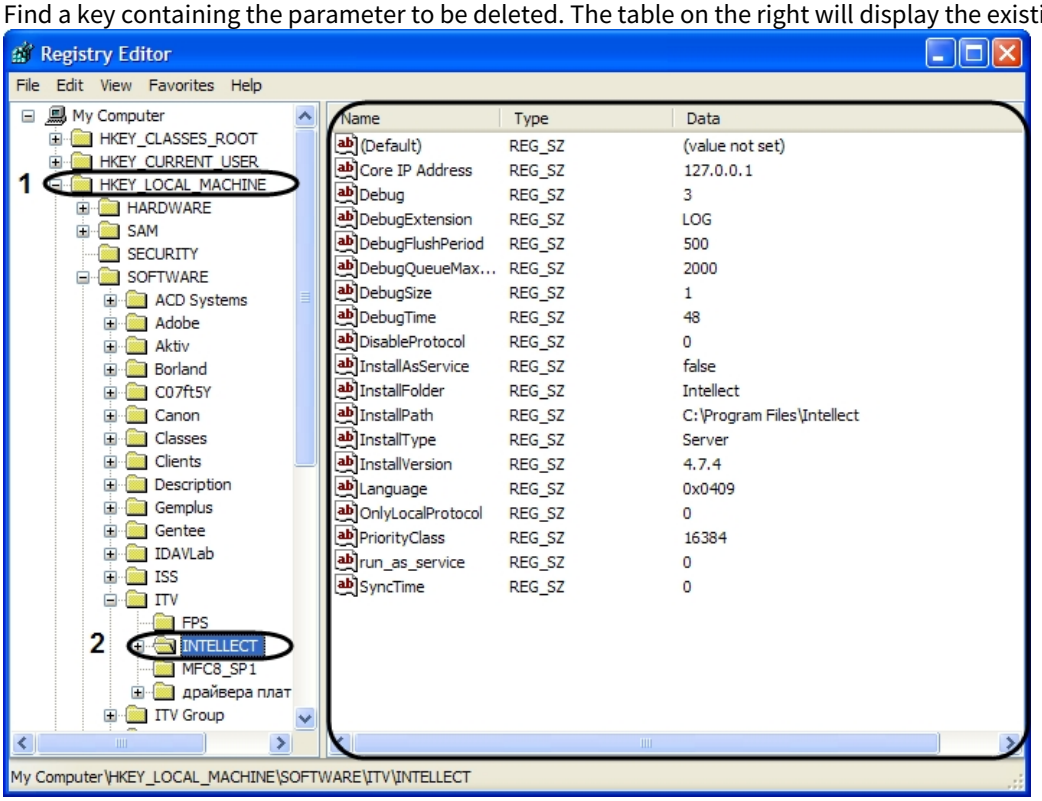


26.2.1.5 Deleting parameters from the Windows OS registry

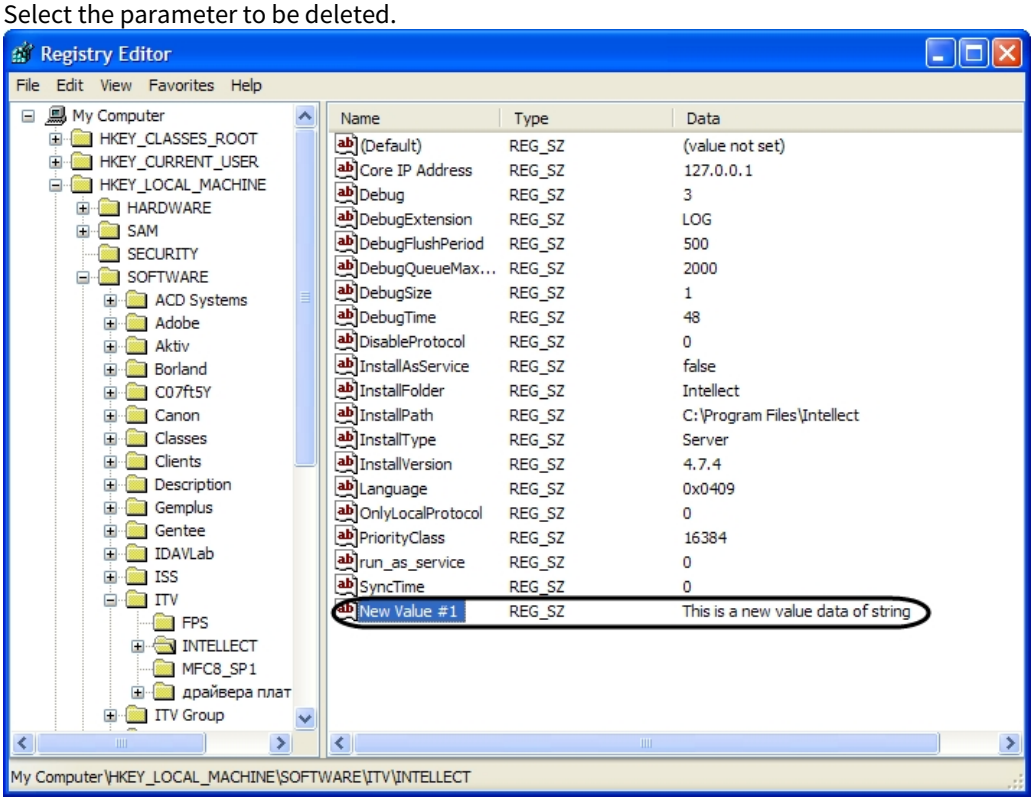
To delete a string parameter from the registry, do the following:

1. Select the required branch and click the plus icon. All folders (keys) inside this branch will be displayed.

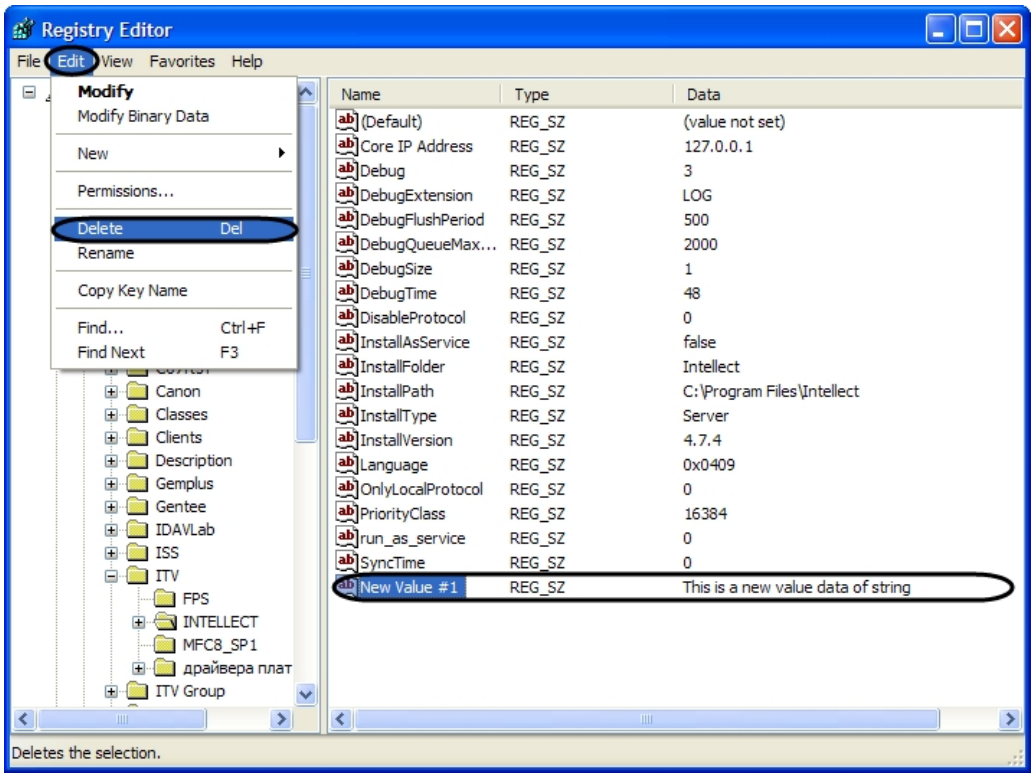
2. Find a key containing the parameter to be deleted. The table on the right will display the existing parameters of this key.



3. Select the parameter to be deleted.



4. In the menu, select **Edit**, then **Delete**.



The string parameter will be deleted from the registry.

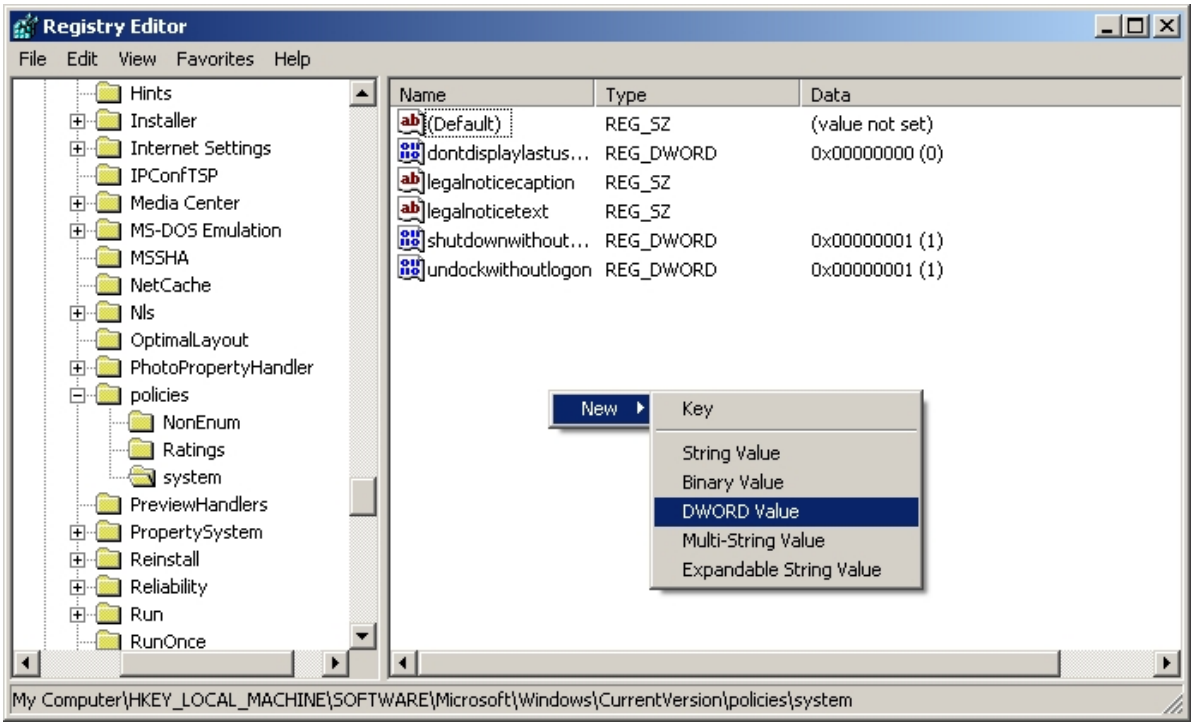
> **Note.**
>
> The **Edit** menu can also be opened as a context menu by right-clicking the required parameter.

26.2.1.6 Configuring network drives visibility when UAC is enabled in Windows OS

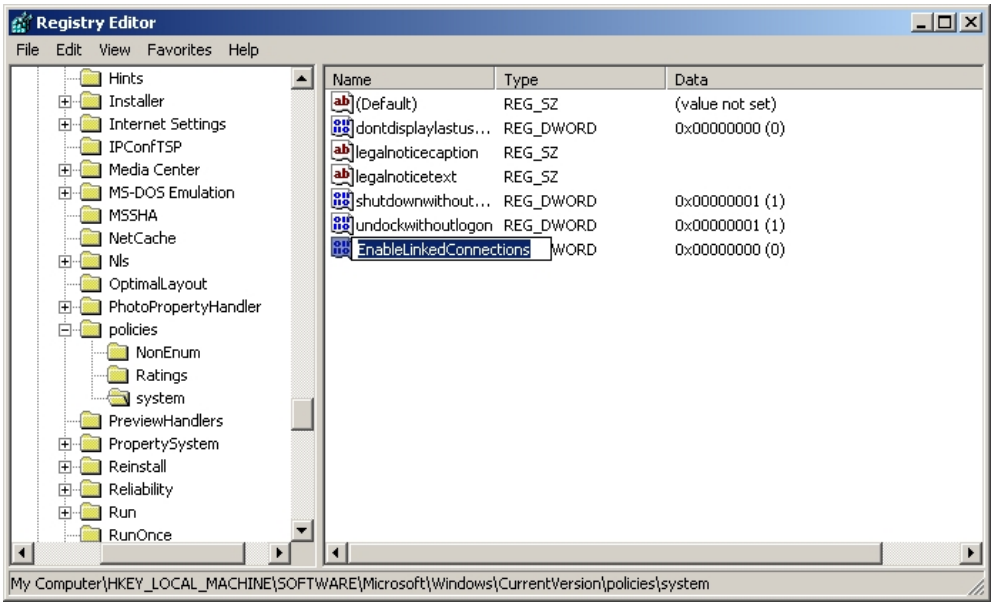
To configure archive storing to network drives when UAC is enabled in *Intellect,* create the EnableLinkedConnections key in the registry. For this do the following::

1. Open subsection of HKEY_LOCAL_MACHINE \ SOFTWARE \Microsoft \Windows \CurrentVersion \Policies \System registry.

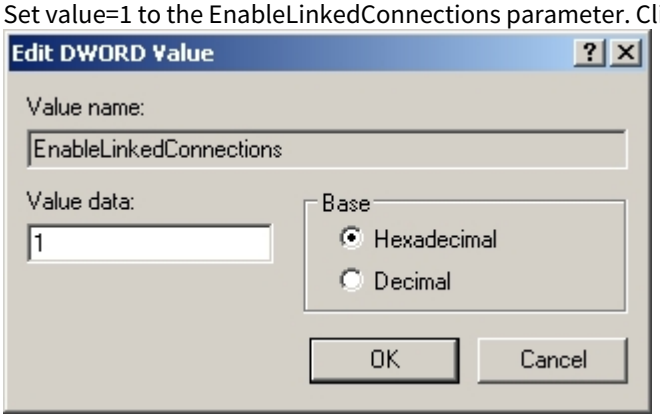
2. Create a new DWORD value.



3. Set EnableLinkedConnections name to the new value and click Enter.



4. Set value=1 to the EnableLinkedConnections parameter. Click the **OK** button.



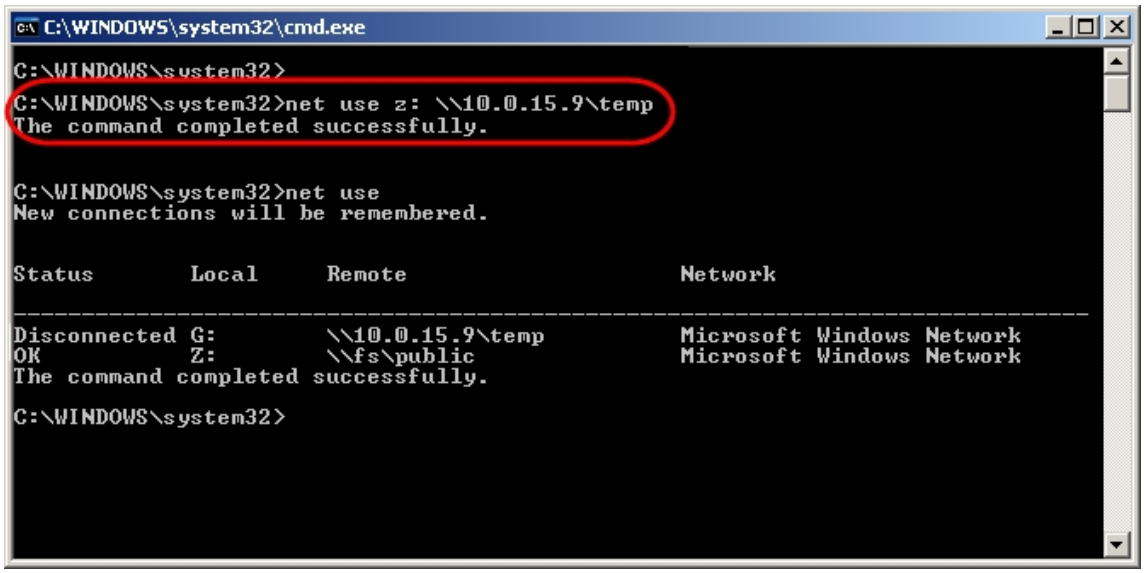
5. Exit the registry editor and restart your computer.

The EnableLinkedConnections registry key is created.

26.2.2 Connecting network disks in Windows Vista and Windows 7 OS

In some cases network disks are not displayed in *Intellect* software settings in Windows Vista and Windows 7 OS when UAC is on. In order for the network disks to appear in *Intellect* settings, connect them in Windows OS as the administrator or as the user on whose behalf the video module will be launched, as follows:

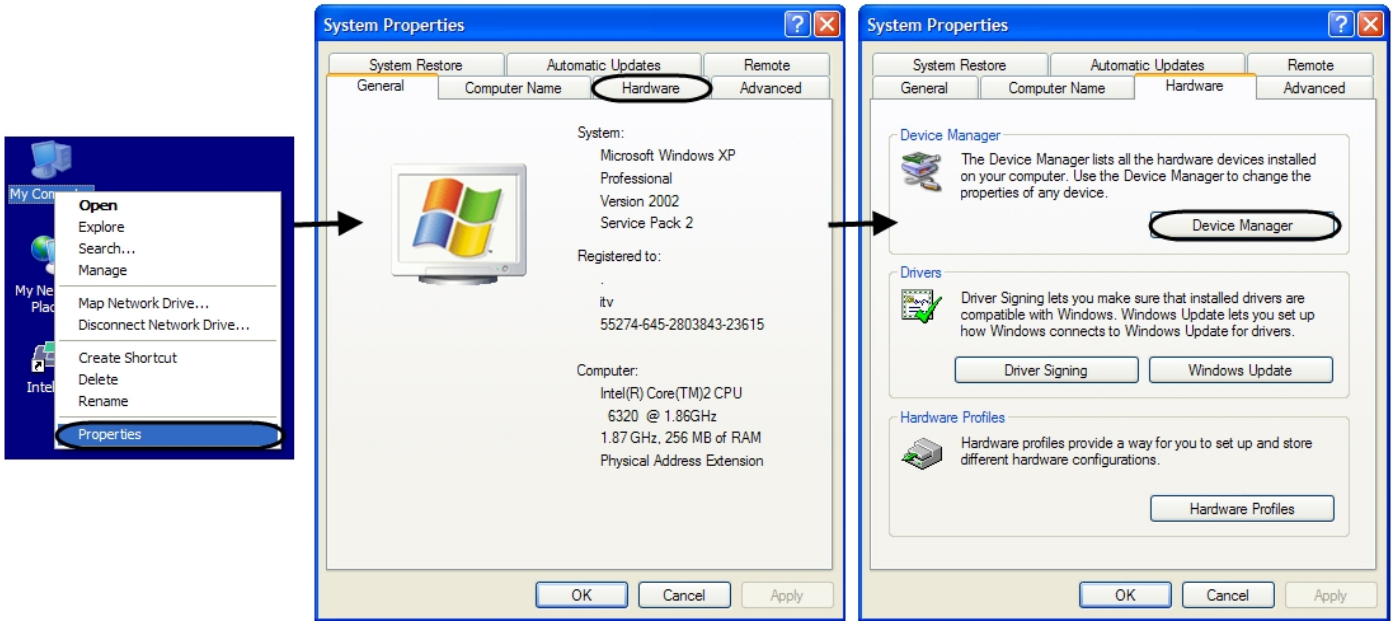
1. Call a command prompt. Select **Run** in **Start** menu and enter «cmd» in entry field and click **OK**.
2. Enter «net use Z: \\Address\Folder» in the command prompt; **Z** is letter of Roman alphabet that will represent net disk in the system, **Address** is IP-address of net disk, **Folder** is a name of folder.



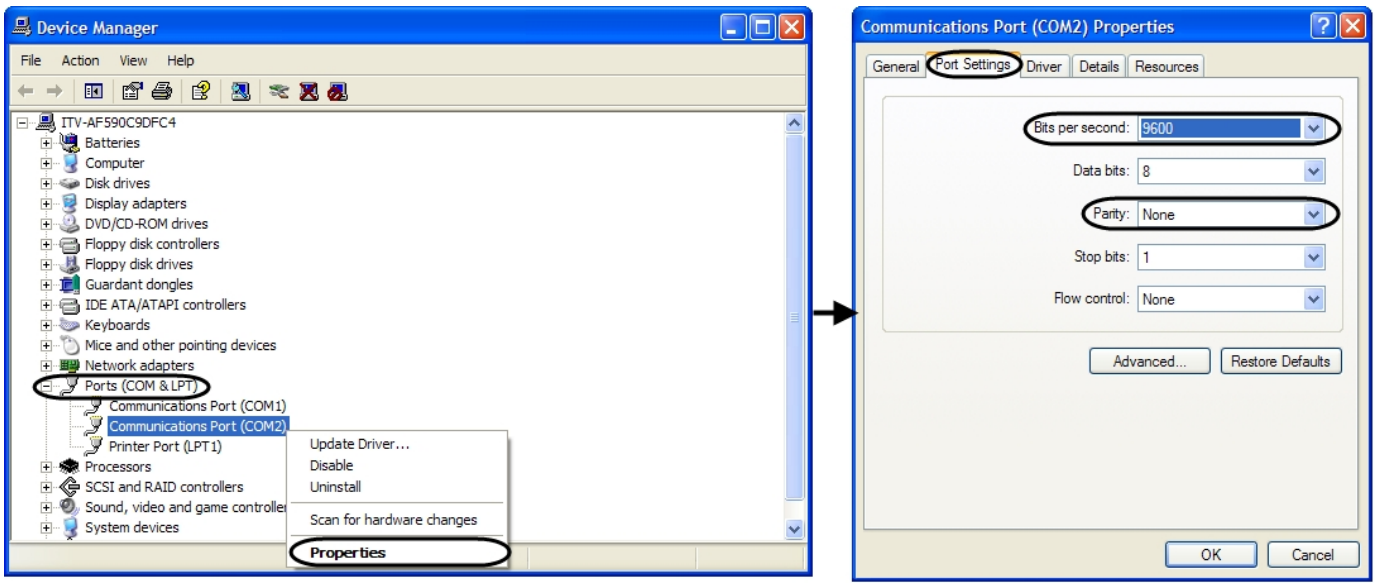
Net disk appears in *Intellect* settings after beeing connected.

26.2.3 Setting up serial (COM) ports in Windows

To view and edit the settings of COM ports, start the **Device Manager**. Right-click the **My Computer** icon on the **Desktop** and select **Properties** in the drop-down menu. The **System Properties** window will open. Open the **Hardware** tab and click the **Device Manager** button.



The **Device Manager** window will open. Expand the **Ports (COM & LPT)** branch and select the COM port to which the device to be set up is connected. Then, right-click the required COM port in the tree to open the drop-down menu and select **Properties**. The settings of the port will open in a dialog window. Go to the **Port Settings** tab to view and edit the **Bits per Second** and the **Parity** parameters.



26.2.4 Working with Windows OS services for operating Intellect™ installed as a Service

26.2.4.1 General information on Intellect operation as a Service

26.2.4.1.1 Starting the Service

Intellect, installed as a Service, is started before user authorization in Windows OS and before Windows applications are launched (including the Explorer application which is used for starting such applications as Windows OS and various other applications installed on the Server). The **Intellect Core Server** service performs the start. The **Intellect Core Server** service is created when *Intellect* is installed as a Service. By default, the intellect.exe executable module is used to start *Intellect.*

Note

When you work with *Intellect* installed as a Service, you can shut down *Intellect* normally, while the service remains running, and *Intellect* can be restarted.

Note

If intellect64.exe must be started when the **Intellect Core Server** service starts, you need to change the value of the core_module_name registry key (see Registry keys reference guide) and restart the service.

26.2.4.1.2 Users

When installing *Intellect* as a Service in Windows, the IntellectUsers user group will be created, and the user who performed the installation will be added to this group. To add other users to the IntellectUser group, use Windows OS means. The users in the IntellectUsers group have the rights to configure *Intellect* installed as a Service and access its interfaces. When it is necessary to provide the access to *Intellect* interfaces for a large number of users, it may be convenient to use the Active Directory (AD) service —see Configuring Intellect as a Service to work with Active Directory (AD).

Note

To start *Intellect* as a different user, you must either assign administrator rights to this user, or increase the rights, as described in OS settings for correct operation of Remote Admin Workstation or Server.

Note

For more information about user groups and working with them, see Microsoft Help website http://windows.microsoft.com.

When a user from the IntellectUsers group logs in, *Intellect* restarts as this user. If you don't want to start *Intellect* as this user (in other words, *Intellect* must remain running as the SYSTEM user), disable the restart using the Tweaki.exe utility—see The Settings panel of the Windows section.

Note

If *Intellect* is running as some user (not as SYSTEM), if you change the user to any other user without logging out the first user, *Intellect* won't restart. It will remain running as the first user.

26.2.4.1.3 Access to the database

If *Intellect* is installed as a Service, and the database connection is performed using Windows credentials, then to work as any user different from the user who installed *Intellect,* it is necessary that this user have the corresponding SQL server permissions.

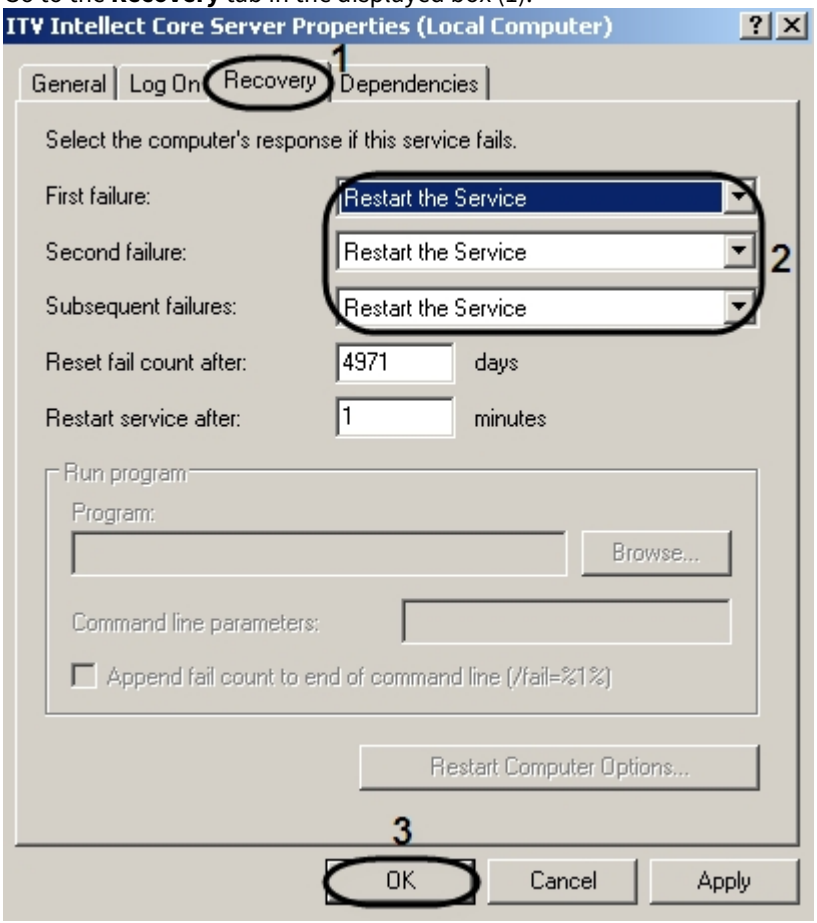
Installation of Intellect as a Server/Remote Administrator's workstation

26.2.4.2 Configuring the restart of the Intellect Core Server service

If the Intellect Core Server service is to be restarted, do the following:

1. Go to the Windows Control Panel in the **Start** menu.
2. Select **Administrative Tools -> Services**. The list of services registered in the system is displayed.
3. Select the **Properties** item in the context menu of the Intellect Core Server service.
4. The context menu is called with the right click on the name of the service.

5. Go to the **Recovery** tab in the displayed box (1).



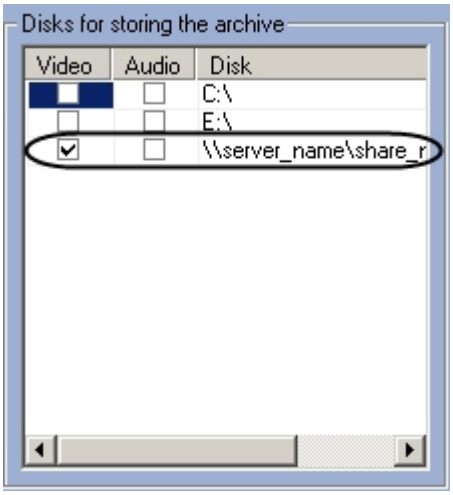
6. In the corresponding drop-down lists select the actions to be performed in case of the first, second and subsequent system failures (2).
7. To save the changes, click the **OK** button (3).

The restart of the Intellect Core Server service is now configured.

26.2.4.3 Using network disks of INTELLECT™ installed as a Service

If it is necessary to use network disks for working with archive in Intellect™ that is installed as a Service you should add them by setting UNC path, the following way:

1. Go to the last line in the list of disks and click the "↓" key.



2. Set a path to the network disk in appeared line in the **Disk** column. UNC path is set in "\\server_name\share_name" format where the "server_name" is the name of file server and the "share_name" is the network name of public folder.

3. Set the check box for created disk in the **Video** column.

> **Note.**
>
> If network disk is added not by setting the UNC path, then recording on it is unavailable in **Intellect is installed as a Service** mode.

> **Attention!**
>
> If INTELLECT™ is installed as a Service on Windows XP OS, it is impossible to record on network disks.

Recording on network disks in INTELLECT™ installed as as a Service is performed only in case when INTELLECT™ is started under some user (not under SYSTEM) and the user is logged in the system. When the user who belongs to the IntellectUsers group logs in the system, INTELLECT™ is restarted automatically on behalf of this user. Both network disks and UNC path are available for recording. If the user logs off the system, INTELLECT™ will restart under system account and all network disks are unavailable.

26.2.4.4 Starting Intellect as a Service

If *Intellect* was not installed as a Service, and you want to make it such, do one of the following:

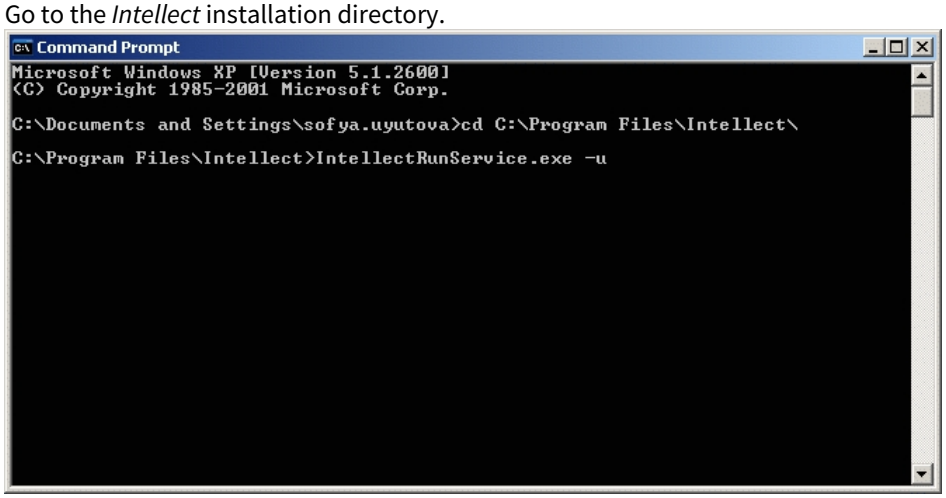
1. Reinstall *Intellect* and set the **Install Intellect as a service** checkbox (see Installing and removing Intellect).
2. Use the command line. In this case, do the following:
   a. Run the Windows cmd.exe command line in one of the following ways:
      i. Under the administrator account with disabled UAC.
      ii. Under the administrator account or user account with enabled UAC as administrator.
   b. Go to the *Intellect* installation directory.
   c. Run the "IntellectRunService.exe -i" command in the Windows command line. As a result, the **ITV Intellect Core Server** service will be registered in the system.
   d. Run the service manually in Windows **Task Manager** on the **Services** tab.

As a result, *Intellect* will be installed as a Service, the **ITV Intellect Core Server** service will be in the "Running" status.

26.2.4.5 Disabling Intellect as a Service startup

There are two ways to disable the startup of *Intellect* as a Service:

1. By restarting *Intellect*:
   a. Remove *Intellect* (see Removing INTELLECT™ software section).
   b. Install *Intellect* without setting the Server checkbox (see Installing INTELLECT™ software section).
2. By using the command prompt:
   a. Run the Windows cmd.exe command prompt:
      i. Under the administrator account with disabled UAC.
      ii. As administrator under the administrator account or user account with enabled UAC.
   b. Go to the *Intellect* installation directory.



c. Run IntellectRunService.exe –u command with the Windows command prompt.

Intellect as a Service startup is now disabled.

26.2.4.6 Configuring INTELLECT™ as a Service to work with Active Directory (AD)

In order to run *Intellect* that was installed as a Service using the users from an Active Directory (AD) domain without adding them to the local IntellectUsers group, it is necessary to specify the user group name in the **IntellectUserGroup** key of the Windows registry (for details, see Registry keys reference guide. For details on working with the registry, see Working with Windows OS registry).

This configuration may be useful for arranging the access to the *Intellect* as a Sevice interfaces for a large number of users. In this case, it will not be necessary to register all the required users in the local IntellectUsers group on each Server.

It is also necessary for this user group to have access and permission to inherit the subdirectories rights to the following directories:

1. Root directory on disk;
2. Windows registry branches:
   - For (x32): HKEY_LOCAL_MACHINE\SOFTWARE\ITV\
   - For (x64): HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ITV\

After you log in to Windows within an AD domain using the AD user account, this setting will allow you to provide the *Intellect* interface without adding a user to the IntellectUsers group. It does not require any additional user configurations to grant the access rights to the necessary Windows branches, the folder with the installed *Intellect*, the Video archive folders, or other service folders according to the access rights assigned to the user in *Intellect*.

> **Note**
>
> Please note that only one user at a time can operate *Intellect* running as a Service. Log out before logging in with other user's credentials. If a user just locks the display without logout before logging in with new credentials, *Intellect* interfaces are not available to such new user.

26.2.4.7 Updating Intellect installed as a Service

If *Intellect* as a Service was started manually after its installation (see Enabling Intellect as a Service startup), do the following to update it:

1. Change the **INSTALL_AS_SERVICE** registry key by setting the value to **1**. It is necessary to start the **ITV Intellect Core Server** service after the update.
2. Update according to the manual: Updating Intellect.

If *Intellect* was initially installed as a Service (i.e. the **Install Intellect as a service** checkbox was set when installing *Intellect),* you don’t need to change the registry key, you can go straight to updating according to the manual.

As a result, *Intellect* will be updated and continue to operate as a Service.

26.2.5 The list of TCP ports used in INTELLECT™

On the page:

- Intellect base
- ATM-Intellect and Monitoring
- Auto-Intellect
- Detector Pack

- POS-Intellect
- ACFA subsystem

The list of TCP ports used in INTELLECT™ is given in the table. The ports can be changed using the ChangePort registry key (see Registry keys reference guide for details).

MS SQL Server also uses TCP port 1433 and UDP port 1434 (by default) for database synchronization.

Note

MS SQL can use dynamical ports to synchronize databases.
To specify which ports are in use go to the **Start -> All programs -> Microsoft SQL Server Express 2014** -> **Configuration Tools** -> **SQL Server Configuration Manager** -> **SQL Server Network Configuration** -> **Protocol for SQLEXPRESS** -> **TCP/IP** -> **IP Adresses** menu and check which type and number of port are specified in the **IPAII** parameter.
Configure using of fix ports according to the manual on the http://technet.microsoft.com/en-gb/library/ms177440.aspx Microsoft web-site if using the dynamical ports is unacceptable.

Ports 8085 and 8087 are used to connect clients to Web Server 2.0 module.

Note.

This data is necessary for setting security system and firewall on the Server. The **Corresponding module to which connection is made** parameter is set for client-server modules. If there is the "-" sign in this column, this means connection to the INTELLECT.EXE kernel.

Intellect base

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
ARCHPANEL.RUN	Backup archive panel	22118	-
ATM	ATM	21090	-
AUDIO.RUN	Microphone	21008	-
AUDIO.RUN	Microphone	20903	VIDEO.RUN
AUDIO.RUN	Microphone	20904	VIDEO.RUN
AUDIO.RUN	Backup audio archive	20911	-
AUDIO.RUN	Audio playback card	20910 and 24008	-
CAM_TITLE.RUN	Captioner	21077	-
CAM_TITLE.RUN	Captioner	20900	VIDEO.RUN
CONFCHEKUTIL.RUN	Configuration check	22220	-

DIALOG.RUN	Operator query panel	21058	-
DRS.RUN	Data replication service	22175	-
EVENT_COUNTER.RUN	Event counter	22153	-
EVENT_VIEWER.RUN	Event viewer	21055	-
IIDK_TEST.EXE	IIDK interface	21030	-
INC_MANAGER.RUN	Incident Manager	22401	-
INC_SERVER.RUN	Incident Server	22432, 22439, 22440	-
JAVA.EXE	Web-server 2.0	22212	-
KEYB.RUN	Keyboard	21005	-
LDAPIMPORT.RUN	LDAP service	22252	-
LIVEPLAYER.RUN	Live sound switch	22199	-
MAP.RUN	Map	21051	-
MC_CLIENT.RUN	Intercom Control Monitor	22179	-
MESSAGE.RUN	Alarm Message Window	21056	-
MMS.RUN	Mail Message Service	21031	-
OPERATORPROTOCOL.RUN	Operator protocol	22215	-
PLAYER.RUN	Audio player	20910	AUDIO.RUN
PLAYER.RUN	Audio player	21060	-
SLAVE.EXE	Computer	21111	-
SMS.RUN	Short Message Service	21035	-
STREAMINGSERVER.RUN	rtsp Server	22228	-
TELEMETRY.RUN	Telemetry Controller	21010	-
TELEMETRY_PANEL.RUN	Telemetry control panel	22101	-
TITLEVIEWER.RUN	Search by captions	20978	CAM_TITLE.run

TITLEVIEWER.RUN	Search by captions	22112	-
VIDEO.RUN	-	20900	-
VIDEO.RUN	Video Capture Device	21050	-
VIDEO.RUN	Video stream archiever	20901	-
VIDEO.RUN	Video stream gate	20902	-
VMDADB.RUN	VMDA metadata storage	22219	-
VMS.RUN	Voice Message Service	21032	-
VNS.RUN	Voice notification service	21004	-
WEBSERVER.RUN	Web-server	21034	-
WINDOW.RUN	External window	21053	-
OPCIE.RUN	HTML Interface	22141	-
Manitou.run	Manitou software	22302	-
QueuesManager.run	Queues Manager	22322	-
display_manager.run	Display Manager	22323	-
SipPanel.run	SIP panel	22331	-
StreamTerminal.run	SIP terminal	22332, 22537	-
BacNetInt.run	BacNet	22350	-
ADataCenter.Web.exe	Intellect Data Webservice	5000	-

ATM-Intellect and Monitoring

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
VIDEOSRV.EXE	IIDK interface	21030	-
VIDEOSRV.EXE	VideoServer	20900	VIDEO.RUN
VIDEOSRV_C.RUN	ATM-Intellect Pro	22001	-
VIDEOSRV_E.RUN	Search in archive	22003	-

VIDEOSRV_M.RUN	Monitoring	22222	-
VIDEOSRV_R.RUN	Monitoring reports	22223	-
VIDEOSRV_S.RUN	ATM-Intellect Workstation	22002	-
VIDEOSRV.EXE	ATM-Intellect Pro	7777	VIDEOSRV.EXE
EVENTATM.EXE (Integration with ATM through XFS)	-	8888	VIDEOSRV.EXE
TELLMEDLL.DLL (Integration with ATM through the SKS software)	-	8888	VIDEOSRV.EXE
VMON_ITV.DLL (Integration with ATM through the “Gold Crown” software)	-	8888	VIDEOSRV.EXE
STATEUPS.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
BATDISCH.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
POWEROFF.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
POWERON.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
VPIPECLIENT.EXE (Internet FPSU operation)	-	7777	VIDEOSRV.EXE
VPIPECLIENT.EXE (Internet FPSU operation)	-	8555	VPIPESERVER.EXE
VIDEOSRV.EXE	ATM-Intellect Pro	7777	VPIPESERVER.EXE
VIDEOSRV.EXE	ATM-Intellect Workstation	7777	VIDEOSRV.EXE
VIDEOSRV.EXE	ATM-Intellect Workstation	7777	CPDVAlarmServer.exe
CentralNetServer.exe	CSC	7755	VIDEOSRV.EXE
VIDEOSRV.EXE	Agent of Control	7777	VIDEOSRV.EXE
forward.run	Data gateway	22327	-

Note.

If *CSC (Central Server of Control)* is in use, then between *CSC* communication server and *Server of Control* the 20 and 21 TCP ports are used to provide FTP operation.

Auto-Intellect

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
DT_SERVER.RUN	Traffic Detector	22151	-
DT_SERVER.RUN	Traffic Detector	20900	VIDEO.RUN
DT_SERVER.RUN	Traffic Detector	22152	-
DT_SERVER.RUN	Traffic Detector	20988	-
DT_VIEWER.RUN	Traffic Monitor	22152	-
ITV_VEHICLE_DETECTOR.RUN	Vehicle Detector	22182	-
LPRDB.RUN	External Plates DB	22100	-
RADAR.RUN	Speed traps server	22157	-
ROSSI_FLOW.RUN	Potok recognition server	22119	-
TRAFFIC_PROCESSOR.RUN	Vehicle Processor	22181	-
URMLPR.RUN	LPR channel	22137	-
URMLPR.RUN	LPR channel	20900	VIDEO.RUN
URMLPR.RUN	LPR channel	10001	-
VEHICLE_TRACER.RUN	Vehicle Tracer	22187	-
VEHICLE_TRACER.RUN	Vehicle Tracer	20986	-
DETECTOR_EXT.RUN	Traffic Light Detection	20993	-

Detector Pack

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made

DETECTOR_EXT.RUN	Fluid level detection	20993	-

Face-Intellect

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
FACE_MONITOR.RUN	Face Monitor	21919	-
FACE_RECOGNITION_PROXY.RUN	Face Search Server	22207	-
FACE_RECOGNITION_WEB_PROXY.RUN	Web access to face search	22214	-
FIR_MONITOR.RUN	Recognized Faces Monitor	22135	-
FIR_MONITOR.RUN	Recognized Faces Monitor	20985	FIRSERVER.RUN
FIR_MONITOR.RUN	Recognized Faces Monitor	20900	VIDEO.RUN
FIRSERVER.RUN	Face Recognition Server	22136, 10000	-
WEBVIEWER.RUN	Web-interface viewing module	22216	-
FACE_CLIENT.RUN	Face recognition and search interface	22297, 20985	FIRSERVER.RUN via 20985

POS-Intellect

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
ALERTNURSES.RUN	Alert nurse	22196	-
POS.RUN	POS terminal	21012	-
POSAGGREGATOR.RUN	POS Replicator	22245	-
POSVIEWER.RUN	Receipt viewer	22111	-
POSVIEWER.RUN	Receipt viewer	20977	POS.RUN
McMixer.run	McMixer	22321	-

26.2.5.1 ACFA subsystem

Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
abc.run	ABC	22031	-
abc_cr.run	ABC control reader *	22235	-
agency_person.run	Visitor Management System	21057	-
aiu.run	"777 ROVALANT" system *	22145	-
aiu3.run	Rovalant 777 ISS *	22217	-
anson.run	Anson ACS *	22267	-
APDA.run	Tempo Reale ACS *	22188	-
apollosdk.run	ApolloSdk	22204	-
Bagulnik2.run	Bagulnik2 *	22195	-
biosmart.run	BioSmart	22236	-
bolid.run	"Bolid" (COM server)	21025	-
castle.run	Castle server	22183	-
castle_cr.run	CASTLE control reader *	22231	-
chrysantemum.run	PRHK *	22198	-
DB_Import.run	Data import	21022	-
Dunai2.run	Dunai 2 *	22255	-
dunai3.run	Dunai 3 *	22255	-
Elsys.run	Elsys *	22206	-
forsec.run	ForSec *	22166	-
forteza.run	Forteza	22237	-
Galaxy.run	Galaxy Dimension	22189	-

galaxy2.run	Honeywell ACS/SGPS	22239	-
gate_cr_z2.run	Z2 control reader *	21222	-
Hid.run	VertX / Edge ACS	22220	-
hunter.run	HUNTER PRO SFA	22256	-
intrepid.run	Intrepid Interface Module	22172	-
Intrepid2.run	Intrepid Grunt	22229	-
Intrepid3.run	Intrepid II System	22240	-
keyking.run	KeyKing ACS	22244	-
keywatcher.run	KeyWatcher ACS	22258	-
keywatcher_interface.run	KeyWatcher ACS Interface	22259	-
kodos.run	Kodos server *	22130	-
kodos_cr.run	KODOS control reader *	22155	-
kronverk.run	Kronverk *	22139	-
ksu_cr.run	KSU control reader *	22338	-
legos2.run	"Octagram" ACS/SFA *	22190	-
Magistrator.run	Magistrator *	22161	-
nac.run	"NAC" ACS *	21020	-
nc.run	HoneyWell N1000	21052	-
ncg9.run	Controller NCG-9	22266	-
net.run	"Net" system *	22185	-
nskat.run	SKAT ACS *	22248	-
opc_wrapper.run	OPC Wrapper	22263	-
Optex.run	Optex System	22232	-
orion.run	Bolid (SDK Orion) *	22173	-

paradox.run	Paradox SFA/ACS	22192	-
parsec_pr_x08.run	PR-x08 control reader *	22226	-
Paxton_NET2.run	ACS Paxton NET2	22233	-
pelco.run	PELCO	22234	-
perco.run	"Perco" ACS *	21019	-
PercoS20.run	Perco S20 controller *	22246	-
PhotoIdentification.run	Photo Identification	22163	-
pl.run	Polon Alfa System	22242	-
pnet3.run	ParsecNET 3 ACS/SFA *	22264	-
ravelin.run	Gate Parking ACS	22227	-
RifString.run	RifString system *	22197	-
Rosslare.run	Rosslare ACS *	22203	-
rovalant_a6_a16.run	"ROVALANT (A6, A16)" system *	22165	-
rubeg8_isb.run	Rubeg 8 ISS *	22256	-
rubezh.run	Rubeg SFA *	22261	-
rubicon.run	Rubicon SFA *	22209	-
rusguard.run	"RusGuard" ACS *	22250	-
salto.run	SALTO Server	22208	-
satel.run	"Satel"	21998	-
securiton.run	"Securiton" ACS *	22247	-
sintegral.run	Strelec-Integral SFA *	22257	-
sphinx.run	Sphinx server	22177	-
strelec.run	"Strelec" SFA *	22162	-
topol.run	Topol PSS *	22241	-

trombon.run	Trombone SFA	22224	-
tss2.run	"TSS" ACS/SFA *	22218	-
unipos.run	"UniPos" 7002	22184	-
nipos5xxx.run	UniPos ACFA 5100-5200	22211	-
vers_rs.run	VERS ACS*	22126	-
WorkTime.run	Work Time Accounting	22133	-
xabc.run	Fortecia ACS *	22260	-
zline.run	"ZLine" FSA *	22243	-
account_manager.run	Access Manager	22291	-
event_manager.run	Event Manager	22287	-
dsc.run	"DSC" FSA	22292	-
IntellectToNextBridge.run	ACFA Intellect - Axxon Next Bridge	22293	-
rubezh_global.run	"Rubezh Global" FSA *	22294	-
satel2.run	"Satel INTEGRA"	22296	-
Unicard.run	"Unicard" ACS	22298	-
zk.run	"ZK Teco" ACS	22299	-
glx2.run	"Galaxy Dimension v.2" FSA	22300	-
sintegral_web.run	"Strelec Integral Web Api" ACS *	22301	-
XTralis2WayProtocol.run	"ADPRO" PID	22303	-
Chomtech.run	"Chomtech" ACS	22304	-
Rbg08.run	"Rubezh-08" ACS *	22305	-
topol3.run	"Topol-3" PID *	22306	-
nedap_retail.run	"Nedap retail" FSA	22307	-

WinPak.run	"HoneyWell WinPak" ACFA	22308	-
fs80cr.run	BioSmart FS80 control reader	22309	-
evs_sk.run	"EVS" ACS *	22310	-
acfa_emulator.run	Virtual Access Server	22311	-
pvscr.run	PVS control reader	22312	-
bsveins.run	"Biosmart UniPass" ACS *	22313	-
RubezhGlobal.run	Third-party integration for R3 protocol of the Rubezh company. Not included to ACFA-Intellect.	22314	-
an.run	OPC Wrapper	22315	-
parsec_pr_p08.run	Parsec PR-P08 control reader	22318	-
suprema_cr.run	Suprema BioMini control reader	22319	-
UfdVolna.run	"Volna Alpha" PID *	22320	-
SCardDriver.run	PCSC Wrapper control reader	22324	-
NoderEe12.run	Noder EE12/EWE4" ACS	22325	-
LockerBox.run	"LockerBox" ACS *	22326	-
suprema_2.run	"Suprema 2" ACS	22328	-
NoderEw1.run	"Noder EW1" ACS	22329	-
hikvision.run	"HikVision" ACS	22330	-
suprema_realscan.run	Suprema Realscan control reader	22333	-
stalt.run	"Stalt-SV" ACS *	22334	-
percoS20v2.run	"PERCo-S-20" ACS *	22340	-
dingo.run	Dingo *	22346	-
snmpwrapper.run	SNMP Wrapper Parent object	22277	-
MorphoLite.run	MorphoAccess SIGMA Lite	22345	-

ratek.run	Ratek *	22352	-
gateipbase.run	Gate-IP-Base *	22351	-
elfar.run	EL-Far	22349	-
fp_sync.run	Face synchronization module	22357	-
vanderbilt_spc.run	Vanderbilt SPC	22355	-
alcoframe.run	Alcoframe	22365	-
virdi.run	Virdi Server	22371	-
modbuswrapper.run	Modbus Wrapper	22373	-
Stx1000.run	STX	22383	-
rakinda.run	Rakinda	22384	-
schindler.run	Schindler PORT	22386	-
texecom.run	Texecom panel	22369	-
textreader.run	Text reader	22372	-
pcscwrapper.run	Smart-card wrapper	22324	-
safekey.run	SafeKey Panel	22380	-
dahua.run	Dahua	22393	-
fft.run	FFT	22289	-
risco.run	RISCO	22399	-
onguard.run	OnGuard	22400	-
Symmetry.run	Symmetry	22404	-
Teltonika.run	Teltonika	22410	-
bosch.run	Bosch APE	22263	-
cerberus.run	Cerberus ECO controller	22268	-
CerberusPro.run	CerberusPro	22397	-

fibersensys.run	FiberSensys	22388	-
aritech.run	"Aritech FP2000" FSA	22275	-
telsap.run	"Telsap 2100" FSA	22272	-
Polon6000.run	"Polon6000" FSA	22347	-
NoderEw2.run	"Noder EW2/EWE2" ACS	22390	-
Esser.run	"ESSER by Honeywell" FSA	22396	-
nedap_aeos.run	Nedap AEOS	22317	-
Nitgen.run	NITGEN	22288	-
ansondb.run	AnsonDB	22270	-
rubezh_strazh.run	Rubezh Strazh *	22419	-
dozor.run	Dozor-1A *	22147	-
fsg.run	FSG	22286	-
suprema.run	Suprema Biometrical ACS	22276	-
senstar.run	Senstar	22418	-
velocity.run	Velocity	22274	-
abc_2.run	Controller ABC v2 *	22353	-
intellico.run	Intelliko *	22411	-
sdk_orion.run	SDK Orion *	22284	-
rusguard_2.run	Rusguard v2 *	22363	-
perco_cr.run	PERCO control reader *	21999	-
mion.run	M-ION *	22387	-
sphinx_oko.run	Sphinx Oko Base Unit *	22366	-
oko.run	Oko *	22359	-
lyrix.run	Lyrix *	22385	-
pui32.run	PUI 32 *	22290	-

UProxIP400.run	UProx IP-400 Server *	22392	-
keyguard.run	KeyGuard System *	22421	-
orlan.run	Orlan System *	22398	-
raskat.run	Raskat System *	22283	-
axrbc.run	Rubikon System *	22337	-
Start7.run	Start7 System *	22265	-
groza.run	Groza Detection Tool *	22412	-
alcoBarrier.run	AlcoBarrier *	22415	-
bosch_bis.run	Bosch BIS	22424	-

* These integrations are not included into the English version of ACFA subsystem and are given here for information only.

26.2.6 Configuring Windows Firewall

If the Intellect software works when the Windows firewall is enabled, then the firewall is to be configured in the following way:

1. Add all processes connected to the Intellect software working to the exceptions list (of allowed programs and components). At standard settings the firewall requires the permission to start the process at first attempt of the module launch.
   Attempt of the module launch is performed at creation the corresponding object in the hardware tree. It is needed to allow the access to the network when the request appears.
   If the access request is not displayed at the module launch attempt, add the needed processes to the allowed list manually.
2. While the *Intellect* software working in the distributed environment it is needed to add the SQLservr.exe and sqlbrowser.exe processes to the exceptions list (of allowed programs and components) on the Server with which the database synchronization is performed.

Note.

Detailed information on Windows Firewall configuration is presented in the Microsoft web-site: http://windows.microsoft.com/

26.2.7 Disable the Data execution prevention (DEP) function for Intellect software package

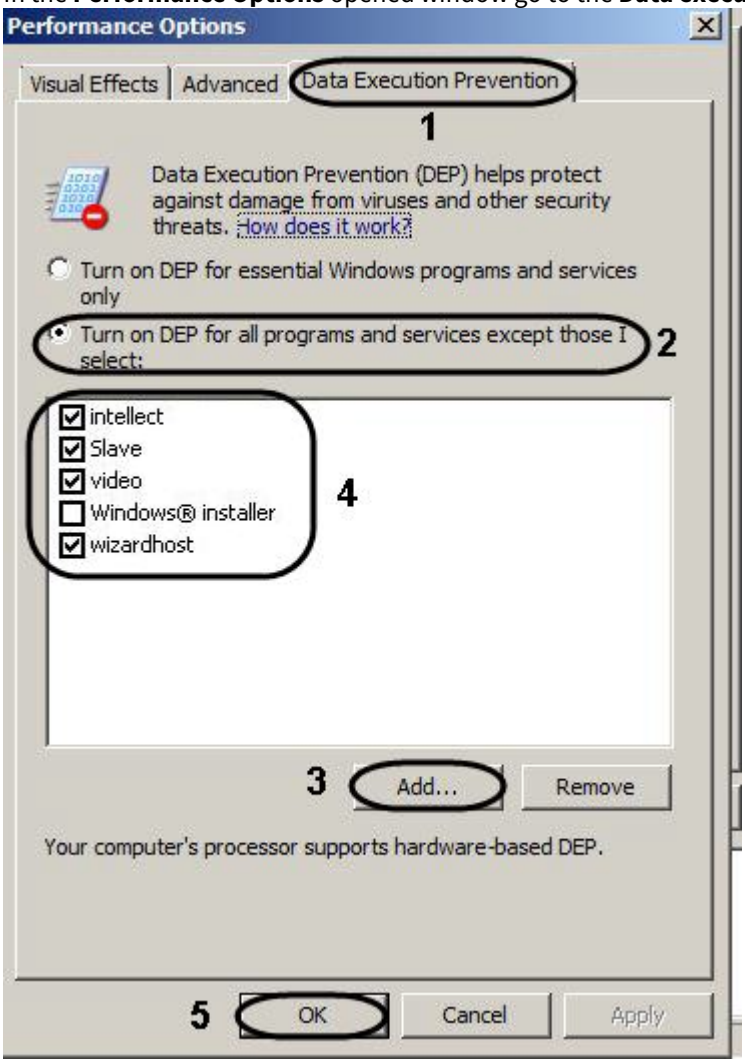
Attention!

Disabling Data Execution Prevention (DEP) should be made only on the recommendation of AxxonSoft technical support specialists.

To disable the DEP function for the Intellect software package, do the following:

1. Go to the **Start – Control panel – System** menu.
2. In the opened window go to the **Additional** tab and click the **Parameters** button in the **Performance** group.

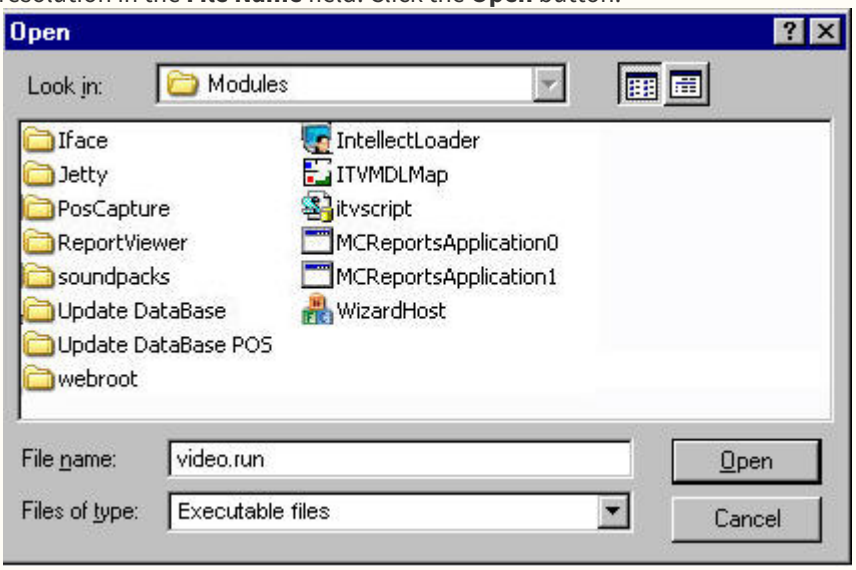
3. In the **Performance Options** opened window go to the **Data executing prevention** tab (1).



4. Set a switch in **Turn on DEP for all programs and services except those I select:** (2).
5. Click the **Add...** button and using the standard diolog of files opening specify the path to the intellect.exe executable file which is located in the Intellect installation directory.
6. **Intellect** item will appear in the programs list. Ensure that the checkbox is set opposite of this item (4).
7. Repeat 5-6 staps for Modules\video.run, slave.exe and Modules\wizardhost.exe files.

> ⚠ **Attention!**

To add the video.run file go to the Modules folder in the files opening dialog and enter the name of this file with resolution in the **File Name** field. Click the **Open** button.



8. Click the **OK** button in the **Performance Options** window(5).
9. Click the **OK** button in the **System** window.

Disabling of DEP for Intellect is completed.

Note.

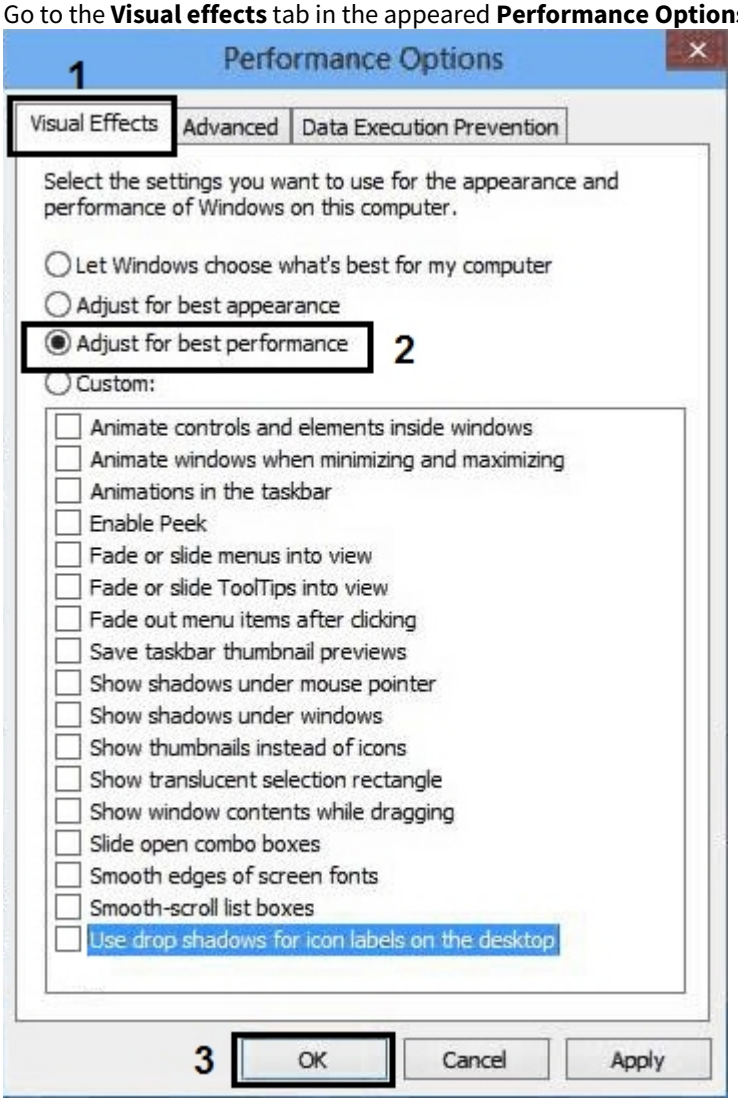
It is also possible the full DEP disabling on the computer. For full DEP disabling perform the **bcdedit.exe /set {current} nx AlwaysOff** command using the Windows command line from the <Windows>\system32 directory.

26.2.8 Configuring the best performance mode

On video Servers and Clients with installed *Intellect* Windows OS is to be set to the best performance mode:

1. Go to **Start – Control panel – System**.
2. In the appeared window go to the **Advanced** tab and click the **Settings** button in the **Performance** group.

3. Go to the **Visual effects** tab in the appeared **Performance Options** window (1).



4. Set the switch to **Adjust for best performance** position (2).
5. Click the **OK** button (3).

The best performance has been adjusted.

26.2.9 Features of ElasticSearch service operation

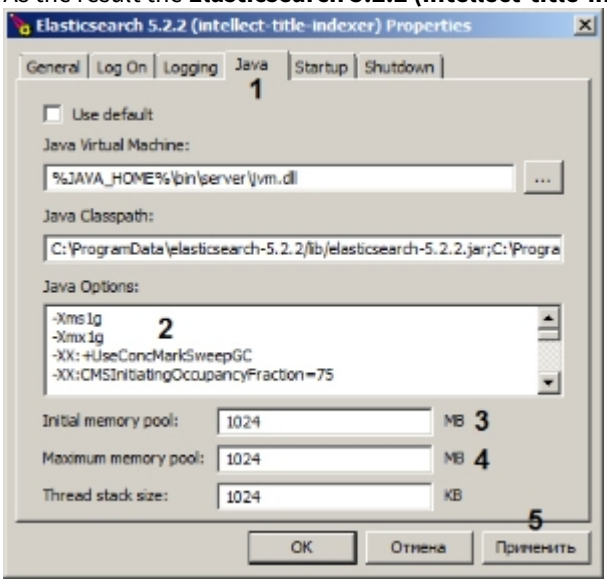
The ElasticSearch service is required for search by captions. It is included into the *Intellect* installation kit. If there is no need in search by captions, the service can be disabled at **Control panel - Administrative Tools - Services**. There is also SearchIndex parameter in the cam_title.run.config file to disable the use of the Elastic Search – see XML-file parameters reference guide.

26.2.9.1 Limiting RAM for Elasticsearch service

When installing *Intellect* in order to ensure the correct start of the Elasticsearch service, RAM allocated to this service is automatically limited on 32-bit systems.
If more RAM that Elasticsearch provides is required, do the following:

1. In the Windows command line go to the Elasticsearch installation directory, to the bin folder (by default, c:\ProgramData\elasticsearch-5.2.2\bin\).
2. Run the elasticsearch-service.bat batch file with "manager intellect-title-indexer" parameters:
   `elasticsearch-service.bat manager intellect-title-indexer`

3. As the result the **Elasticsearch 5.2.2 (intellect-title-indexer) Properties** window appears.



4. Go to the **Java** tab (1).
5. Reduce the value of the **Xms** (memory pool at the start of Java virtual machine) and **Xmx** (maximum memory pool for Java virtual machine) parameters (2). For instance, set them to 1 GB as follows:
   -Xms1g
   -Xmx1g
6. In the **Initial memory pool** field, specify the size (in megabytes) of the memory pool at the start of Java virtual machine (3).
7. In the **Maximum memory pool** field, specify the maximum memory pool size (in megabytes) for Java virtual machine (4).
8. Click the **Apply** button (5).

RAM for the Elasticsearch service is now limited.

26.2.9.2 Running titles database update for restoration of ElasticSearch

In some cases, ElasticSearch can stop working after continuous period of operation. If this happens, run titles database update in one of the following ways:

1. With the Cam_title_updater.exe utility to convert titles database.
2. With a macro and **Reindex** reaction of the **Captioner** object – see Creating and using macros.
3. With a script – see CAM_TITLE Captioner.

26.3 Appendix 3. INTELLECT™ software database management

26.3.1 INTELLECT™ software database functions

INTELLECT™ software database provides:

1. Data storage:
   a. data on registered system objects and their settings;
   b. departments and user accounts and rights;
   c. on registered system events;
   d. on changes in servers and Remote Admin Workstations configuration;
   e. on changes in registered system object specifications and their settings;
   f. data on network names and IP-addresses of distributed system servers, Remote Admin Workstations, Remote Clients and their interaction parameters;
2. Data replication from different servers and Remote Admin Workstations.

The main and the single default database of the INTELLECT™ software is the Configuration database. The Configuration database is used to realize all the above-listed functions.

INTELLECT™ software can be configured to store the registered system events not in the default Configuration database, but in the Events log database.

> **Note**
>
> To configure *Intellect* databases, use the idb.exe utility, which is described in the The idb.exe utility for converting databases, selecting database templates and making backup copies of databases section.

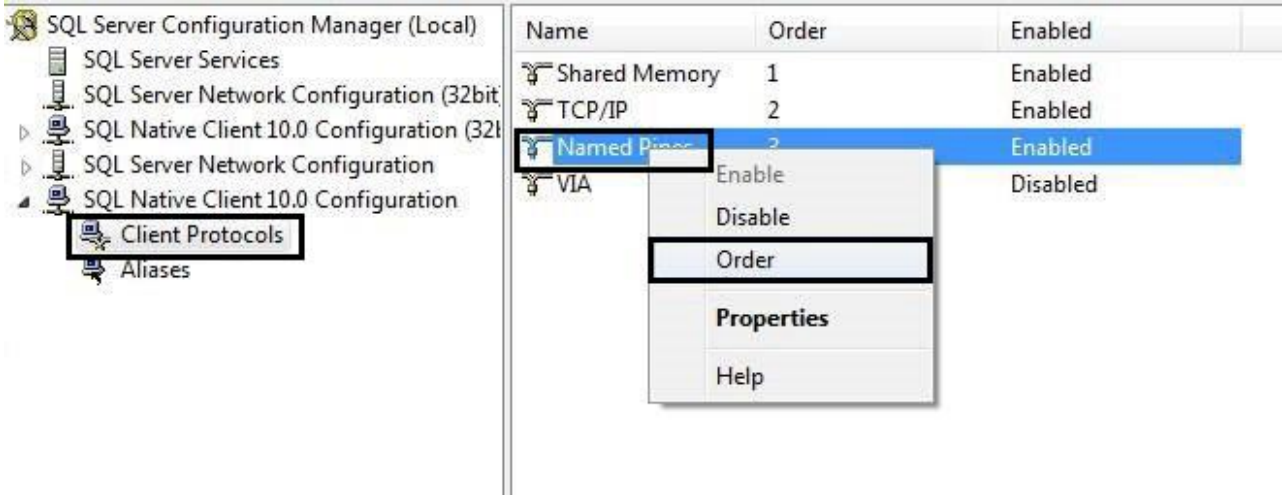
26.3.2 Guidelines on Intellect system database use

To provide the effective and steady performance of the *Intellect* system, take into account the recommendations on database use below:

1. Store the *Configuration* database on the MS SQL server. If the MS Access is used to store the database, it is strongly recommended to install the MS SQL server and to convert the database from MS Access to MS SQL format (see Converting the database from MS Access to MS SQL format).

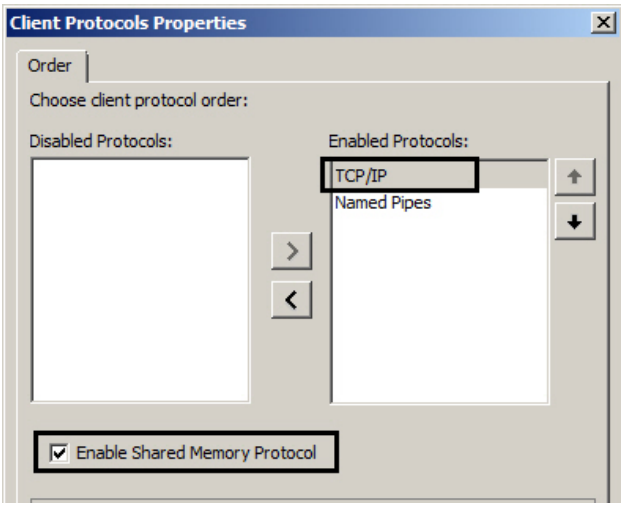
   > **Note**
   >
   > It is recommended to configure the automatic backup of Intellect database in MS SQL Server, for example, once a week (by default, the automatic backup is not configured).

2. The Servers and Remote Admin Workstation databases should be synced with the Administration server database.
3. If long-term centralized storage is necessary for registered system events, then it is recommended to apply *Intellect* software configuration on the Servers and the Remote Admin Workstations in order to store the events in the *Events log* database separately from the *Configuration* database (see Extracting event protocol into an individual database).
4. In case the Dynamic Host Configuration Protocol (DHCP) is used, make sure that the TCP/IP protocol priority for local databases is the highest. Otherwise, when the network cable is disconnected, the communication between the *Intellect* and its local database located on the same computer where *Intellect* is installed can be lost. To view and prioritize the network protocols, use the *SQL Server Configuration Manager* utility:
   a. Run the SQL Server Configuration Manager utility (**Start → Microsoft SQL Server Express 2014 → Configuration Tools**).
   b. In the left part of the utility's interface window, click the header of the **SQL Native Client Configuration** list, and then select the **Client Protocols** item in the drop-down list. In the right part of the window, right-click any protocol in the list and select the **Order** item in the context menu that appears.

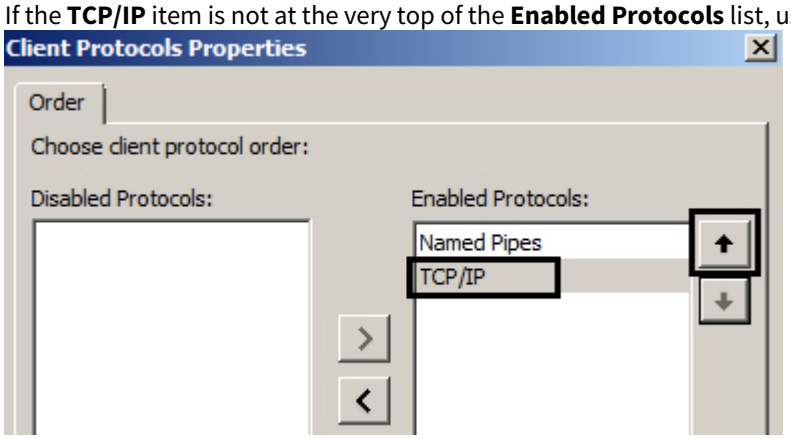


   c. In the **Client Protocols Properties** dialog box that appears, the list of client protocols for the local SQL databases in descending priority order is displayed in the **Enabled Protocols** field. Make sure that the **TCP/IP** item is located at the very top of the **Enabled Protocols** list. Also make sure that the **Enable Shared Memory Protocol** checkbox

is set.



d. If the **TCP/IP** item is not at the very top of the **Enabled Protocols** list, use the **Up** button to move it.



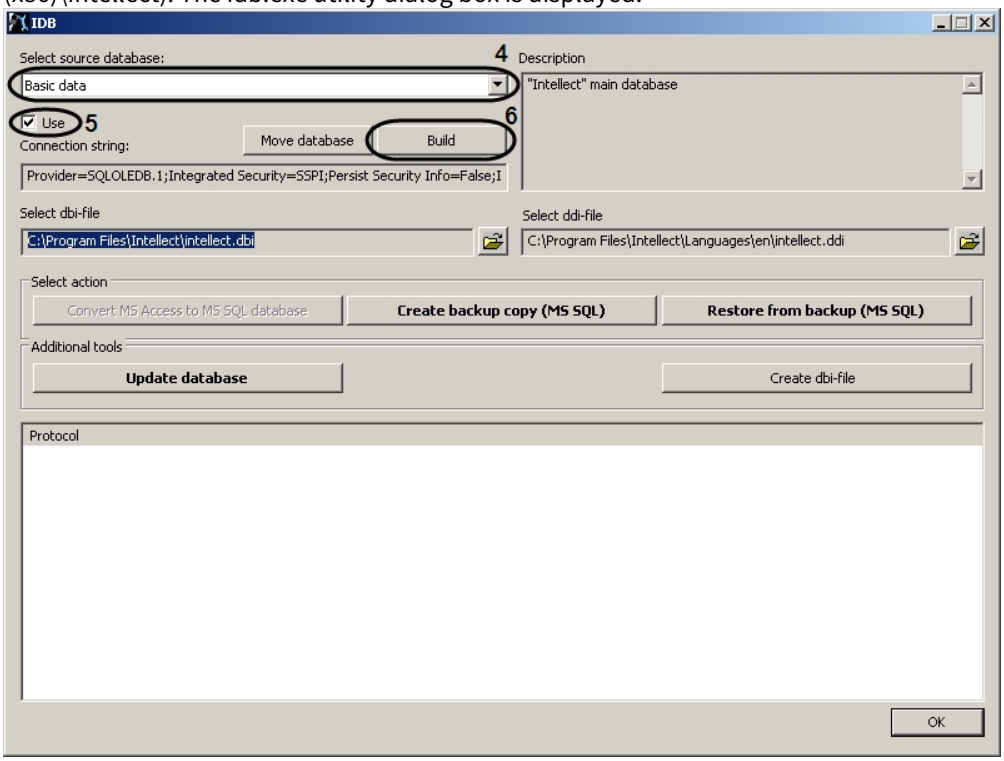
26.3.3 Converting the database from MS Access to MS SQL format

Intellect™ software version 4.10.0 is default configured to operate with the database MS SQL server format. MS Access format databases have been used in previous Intellect™ software versions. If the system needs configuration parameters, stored in MS Access format after INTELLECT™ software has been updated to version 4.10.0, it is strongly recommended to convert the database into MS SQL server format.

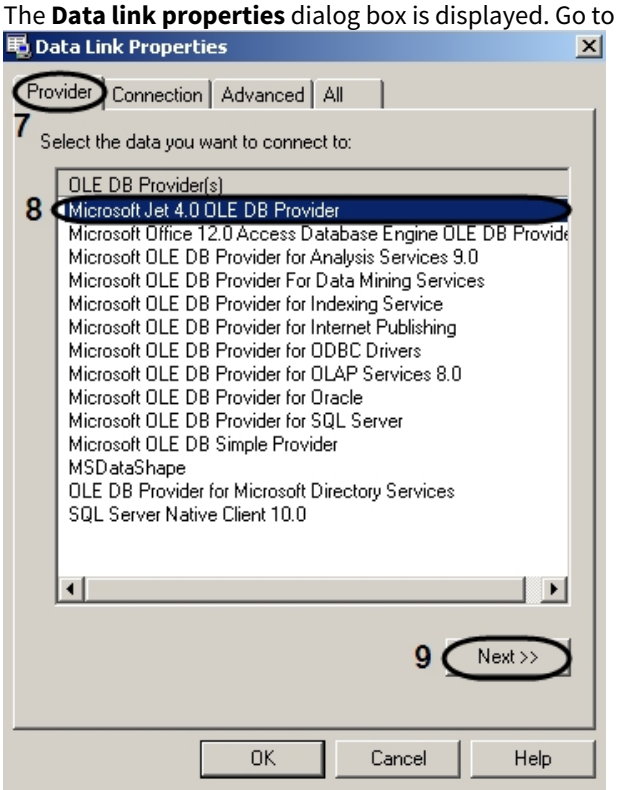
To convert the database from MS Access to MS SQL server format, follow the steps:

1. Set up MS SQL server software, if it has not been set up before.
2. Make sure that the MS SQL server software is on.

3. Launch the idb.exe utility in the root of the INTELLECT™ software installation directory (for example, C:\Program Files (x86)\Intellect). The idb.exe utility dialog box is displayed.

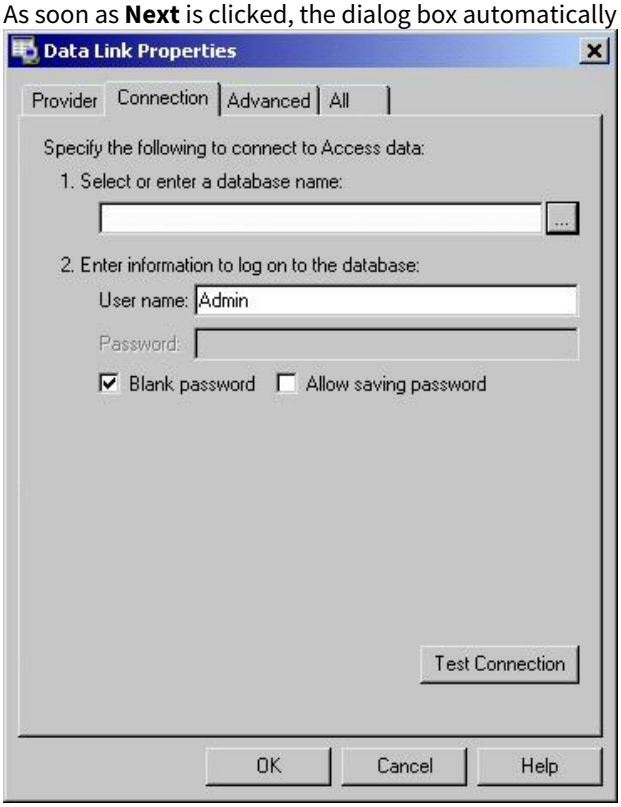


4. Choose the **Basic data** item from the **Select data source** list.
5. Check the **Use** checkbox, if not checked before.
6. Click **Build**.
7. The **Data link properties** dialog box is displayed. Go to the **Provider** tab in the **Data link** properties dialog box.

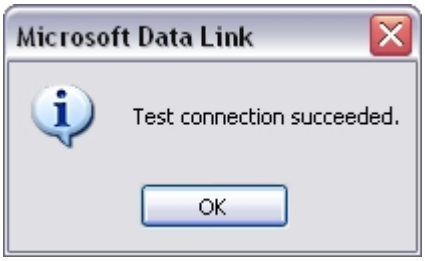


8. Select **Microsoft Jet 4.0 OLE DB** Provider from the **OLE DB Providers** list.
9. Click **Next**.

10. As soon as **Next** is clicked, the dialog box automatically takes you to **Connection** tab.

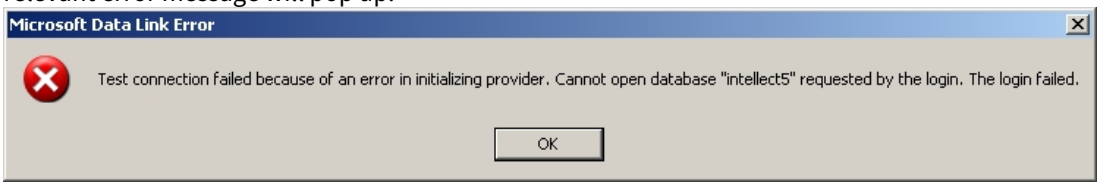


11. Type the complete path to the database file in the **1. Select or enter a database name** or select the necessary file from the file opening dialog box, which is displayed by the **...** button.
12. Enter the user name (login) for database access in the **User** field. If database access is not protected, leave the field empty.
13. If access to the database is protected, remove the default **Blank password** check and enter the database access password into the **Password** field.
14. Click **Test Connection**.
15. If MS Access database connection was completed, the **Test connection succeeded** message is displayed.



Click **OK** to close the window.

16. If the MS Access database name and/or authentication parameters of database connection were entered incorrectly, the relevant error message will pop up.



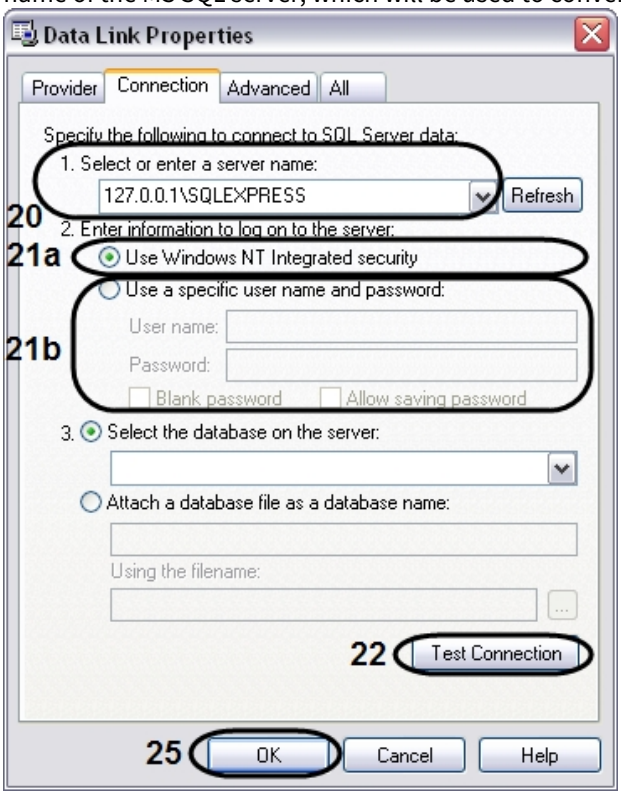
Click **OK** to close the window. Then enter the correct password and try the MS SQL server connection again.

17. Click **OK** in the **Data link properties** dialog box. The window closes.
18. Update the database structure. To do that click the **Convert MS Access to MS SQL** button in the idb.exe utility dialog box.

19. The **Select MS SQL server** message appears.

Click **OK** to close the window.

20. The **Data link properties** dialog box is displayed. In the **1.Select or enter a server name** select from the list or type the name of the MS SQL server, which will be used to convert the database.



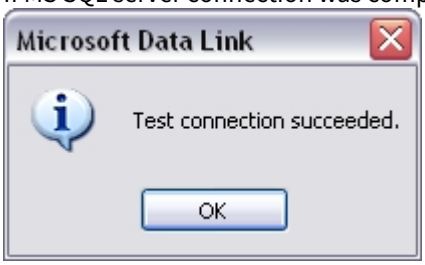
21. The **Enter information to log on to the server** box is checked to enter the type and authentication parameters of MS SQL server connection. MS SQL server authentication is performed through the user account, authorized in Windows OS, or the user name (login) and password, that protect the MS SQL server connection.
The method and parameters of authentication at the MS SQL server are set during MS SQL server installation.
Different settings need to be entered, with different authentication techniques for MS SQL server connection:
    a. If MS SQL server authentication is performed through the user account in Windows OS, switch to the **Windows NT account** box and check it.

> **Note.**
>
> If converting is performed via remote MS SQL server, it is necessary to log in computer with MS SQL server the user's current account from computer that performs the conversion.

    b. If MS SQL server authentication is performed through the user login and password, follow the sequence:
        i. switch to to the **Next user name and password** position.
        ii. in the **User** field: enter the user name (login) to connect MS SQL server.
        iii. if access to the MS SQL server is password protected, remove the default **Blank password** check and enter the database access password into the **Password** field.
        iv. Set the **Allow saving password** checkbox.
        v. Go to the **All** tab.
        vi. In the **Persist Security Info** field, set the **True** value. This is necessary to correctly save the user password.

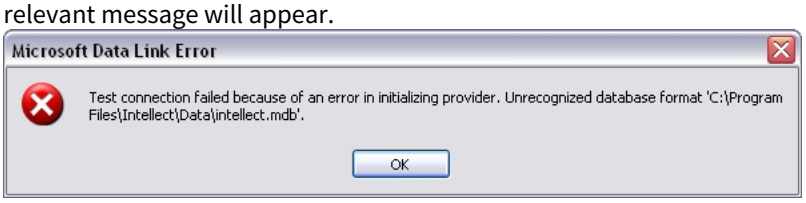
> **Note**
>
> Each time you change the server connection parameters, you must set the **Persist Security Info** field value to **True**.

22. Click **Test Connection**.
23. If MS SQL server connection was completed, the **Test connection succeeded** message is displayed.



Click **OK** to close the window.

24. If the MS SQL server name and/or authentication parameters of the MS SQL server connection were misentered, the relevant message will appear.



Click **OK** to close the window. Then enter the correct password and try MS SQL server connection again.

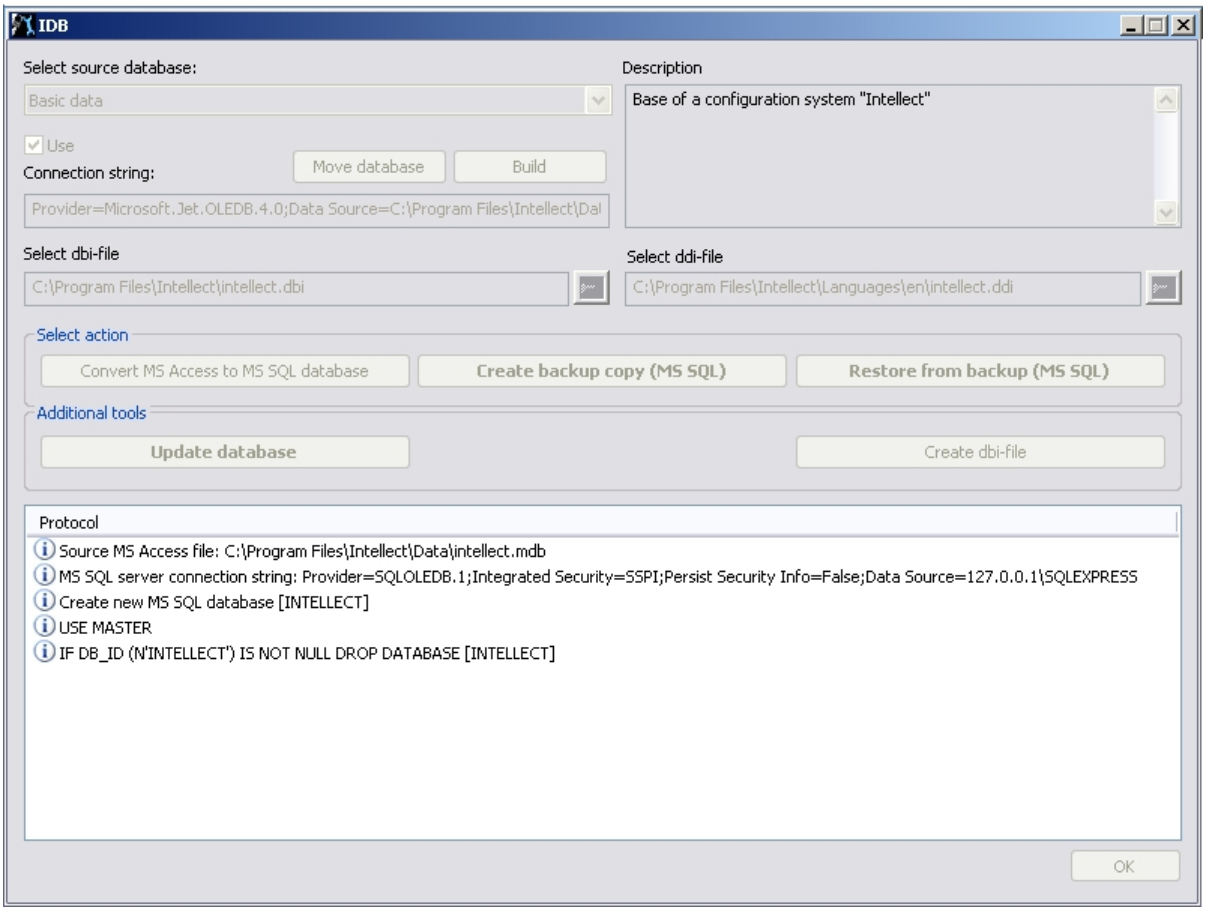
25. Click **OK** in the **Data link properties** dialog box.
26. The **Enter database name** message will appear.

Enter the name to be used for database storage on the MS SQL server in the top field. It is default recommended to use INTELLECT as the database name.

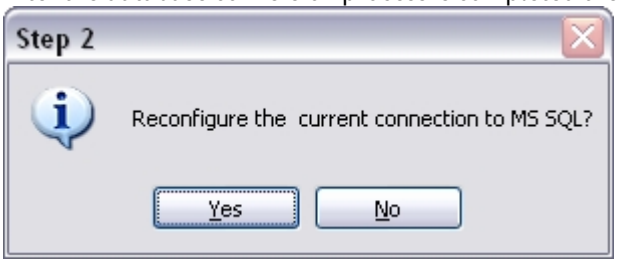
> **Note.**
>
> If the MS SQL server has a database with the same name, as has been entered in the **Enter the database name** field, it will be overwritten.

Confirm the entry of the database name by clicking **OK** and close the window.

27. Then the database conversion process starts from MS Access to the MS SQL server format, and the relevant steps appear in the **Protocol** table in the idb.exe utility dialog box.



28. After the database conversion process is completed the request message appears: "Reset current connection to MS SQL?".



Click the **Yes** button, if you want to set up INTELLECT™ software to operate with a MS SQL server format database, converted from MS Access format. Otherwise click **No**.
When the conversion process is successfully completed, the **Completed!** step appears in the **Protocol** table in the idb.exe utility window.

29. Click **OK** in the bottom right corner of the idb.exe utility window.

Converting the database from MS Access to MS SQL format is completed.

26.3.4 INTELLECT™ software database connection

When INTELLECT™ software is installed, it is configured to operate with the INTELLECT MS SQL server database.

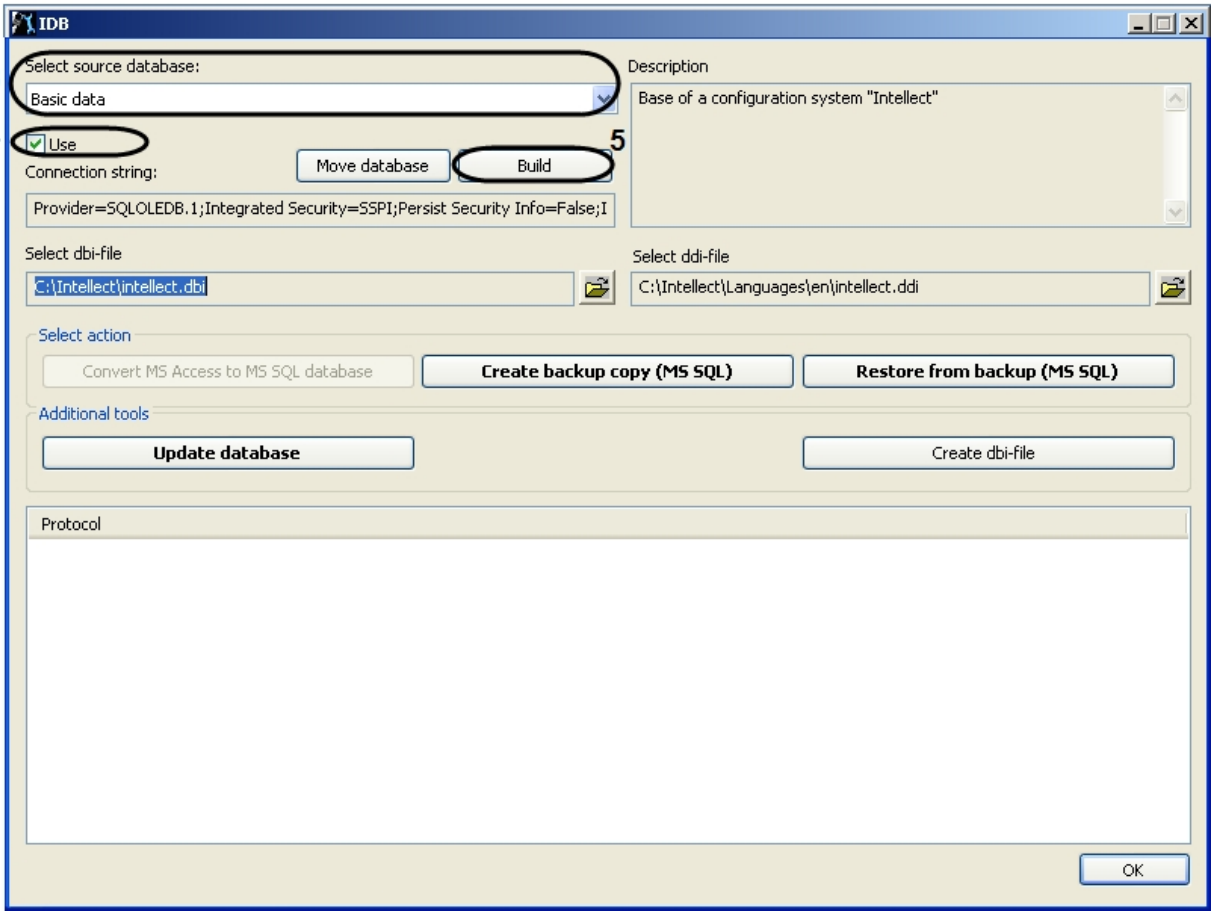
> **Note.**
>
> If the current database is stored in MS Access format, it needs to be converted to MS SQL format before INTELLECT™ software connection setup.

Note.

If Turkish Windows OS language pack and English localization of INTELLECT™ are in use, then connected database is to have the Latin1_General_100_CI_AS value of the **Collation** parameter.
In most cases, the default value of the parameter should be used. Ensure that you have the correct language settings in the operating system.

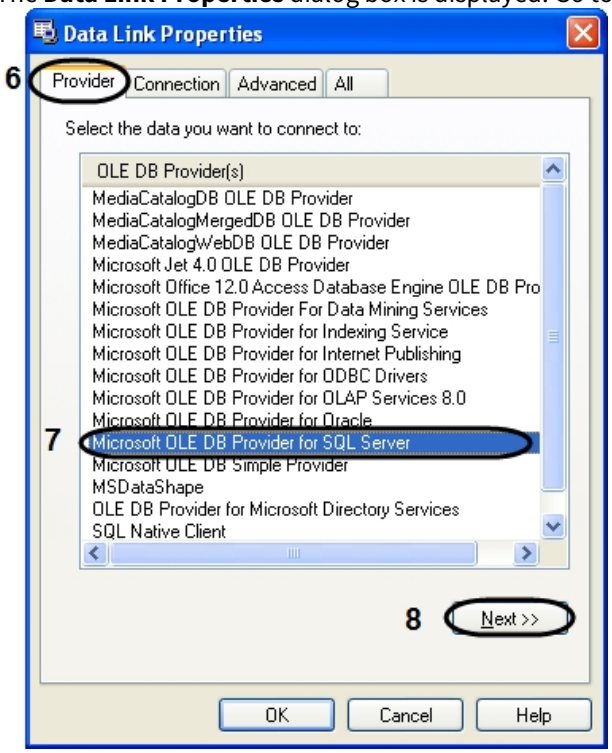
To connect the INTELLECT™ software Configuration database, do the following:

1. Make sure that MS SQL Server software operates.
2. Start the idb.exe utility in the root of the INTELLECT™ software installation directory (for example, C:\Program Files (x86) \Intellect). The idb.exe utility dialog box is displayed.

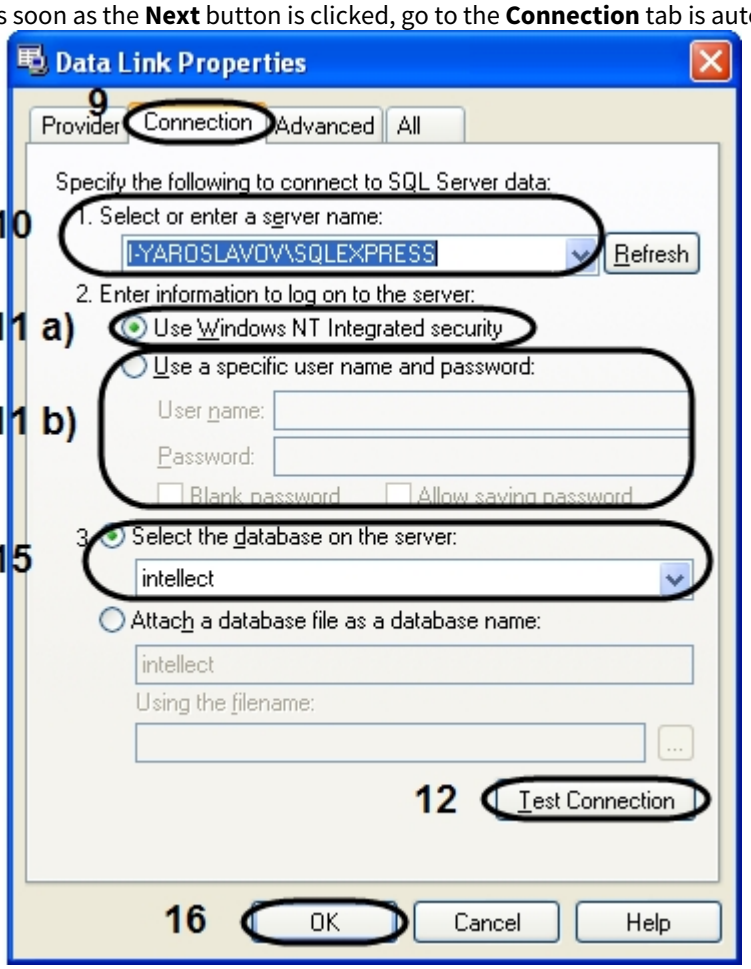


3. Choose the **Basic data** item in the **Select source database** list.
4. Set the **Use** checkbox, if not set before.
5. Click the **Build** button.

6. The **Data Link Properties** dialog box is displayed. Go to the **Provider** tab in the **Data Link Properties** dialog box.



7. Select **Microsoft OLE DB Provider for SQL Server** in the **OLE DB Provider(s)** list.
8. Click the **Next** button.
9. As soon as the **Next** button is clicked, go to the **Connection** tab is automatically performed.



10. In the **1.Select or enter a server name** line select in the list or type-in the name of MS SQL server which is used to store the database to be connected

> **Note.**
>
> In case of dynamic host configuration protocol (DHCP) use for the local database, set «127.0.0.1» IP address (without using computer names and "local" value) in the **1.Select or enter a server name**. Set «127.0.0.1» value when the static IP address is use. Otherwise there is disconnection of INTELLECT™ software with its local database when network cable is disconnected.
> If INTELLECT™ is connected to remote database configuration at IP address (e.g., 192.168.0.68\SQLEXPRESS), you cannot change and save INTELLECT™ software settings when there is a network connection break. If event protocol is extracted into an individual database, use any functioning way to specify a server name.

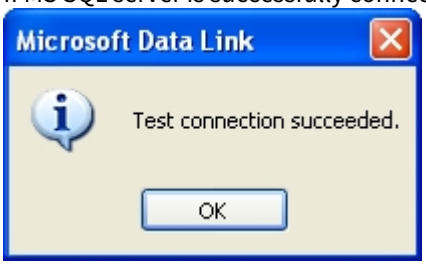
11. The **2.Enter information to log on to the server** group is used to specify the type and authentication parameters of the MS SQL server connection. MS SQL server authentication is performed through the user account, authorized in Windows OS, or by user name (login) and password that protect the MS SQL server connection.
The method and parameters of authentication at the MS SQL server are set during MS SQL server installation.
Different parameters are to be specified with different authentication techniques for MS SQL server connection:
    a. If MS SQL server authentication is performed through the user Windows OS account, switch to the **Use Windows NT Integrated security** position.

> **Note.**
>
> If converting is performed via the remote SQL server, the computer with MS SQL server installed must show the current user account. And the user is logged on under this account at the computer that performs the database connection.

    b. If MS SQL server authentication is performed through the user login and password, do the following:
        i. Switch to the **Use a specific user name and password**;
        ii. Specify the user name (login) to connect to the MS SQL server in the **User name** field.
        iii. If access to the MS SQL server is protected with a password, set the **Blank password** checkbox unchecked and specify the database access password in the **Password** field.
        iv. Set the **Allow saving password** checkbox.
        v. Go to the **All** tab.
        vi. In the **Persist Security Info** field, set the **True** value. This is necessary to correctly save the user password.

> **Note**
>
> Each time you change the server connection parameters, you must set the **Persist Security Info** field value to **True**.

12. Click the **Test Connection** button.
13. If MS SQL server is successfully connected, then the **Test connection succeeded** message is displayed.

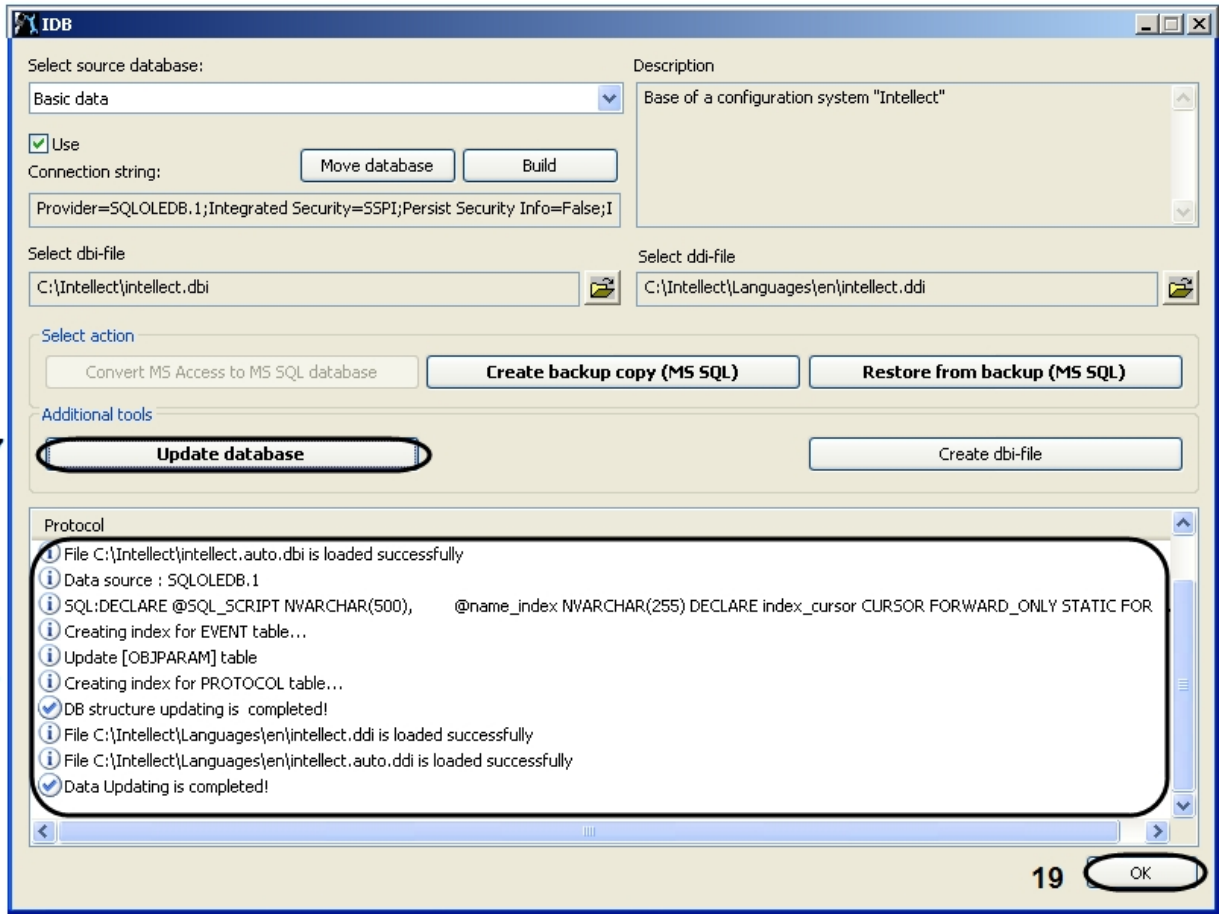


Click the **OK** to close the box.
14. If the MS SQL server name and/or authentication parameters of the MS SQL server connection were erroneous, the error message will appear.

Click the **OK** button to close the box. Then specify the correct password and try the MS SQL server connection again.

15. Select the name of the database to be connected in the **Select the database on the server** list.
16. Click the **OK** button in the **Data Link Properties** dialog box. The box closes.
17. It is strongly recommended to update the database structure after this. For this click the **Update database** button in the idb.exe utility dialog box. If DB is not updated on this step, the update is automatically performed at *Intellect* start-up; however, it might be difficult to track errors in this case.

> **Important!**
>
> If the Event Viewer is in the individual database (see Extracting event protocol into an individual database), then the Event Viewer database structure will be updated when updating the main database structure. So it is recommended to check connection to the Event Viewer database before updating the main database structure in order to prevent any errors.



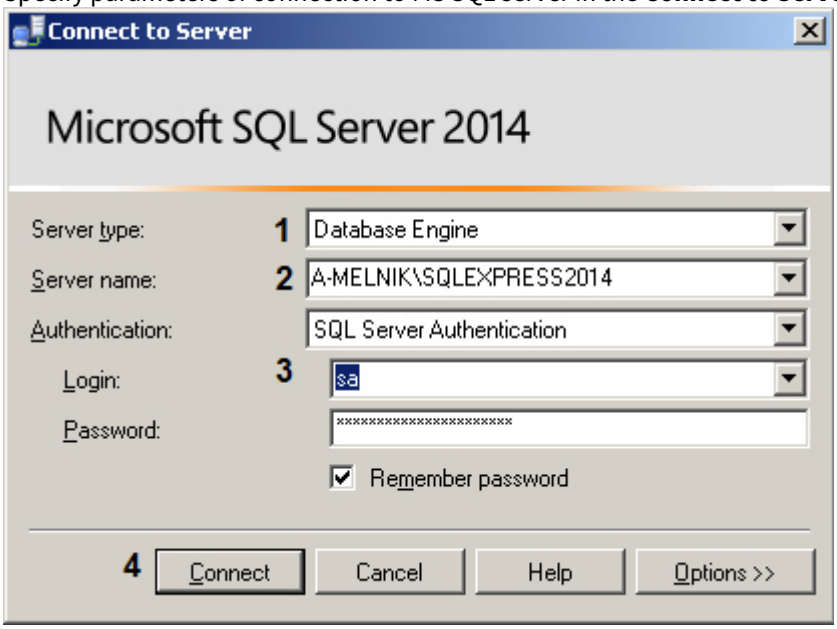
18. As a result the database structure update process starts, and the corresponding messages appear in the **Protocol** table. When the conversion process is successfully completed, the **Data Updating is completed!** message appears in the **Protocol** table of the idb.exe utility.
19. Click the **OK** in the bottom right corner of the idb.exe utility.

INTELLECT™ software database is now connected.

26.3.5 Viewing the Intellect database

To view the database stored on MS SQL server, do the following:

1. Download (from Microsoft website) and install *SQL Server Management Studio 2014* (see Microsoft documentation).
2. Start SQL Server Management Studio utility. Click **Start -> All Programs -> Microsoft SQL Server 2014 -> SQL Server Management Studio**.
3. Specify parameters of connection to MS SQL server in the **Connect to Server** window.

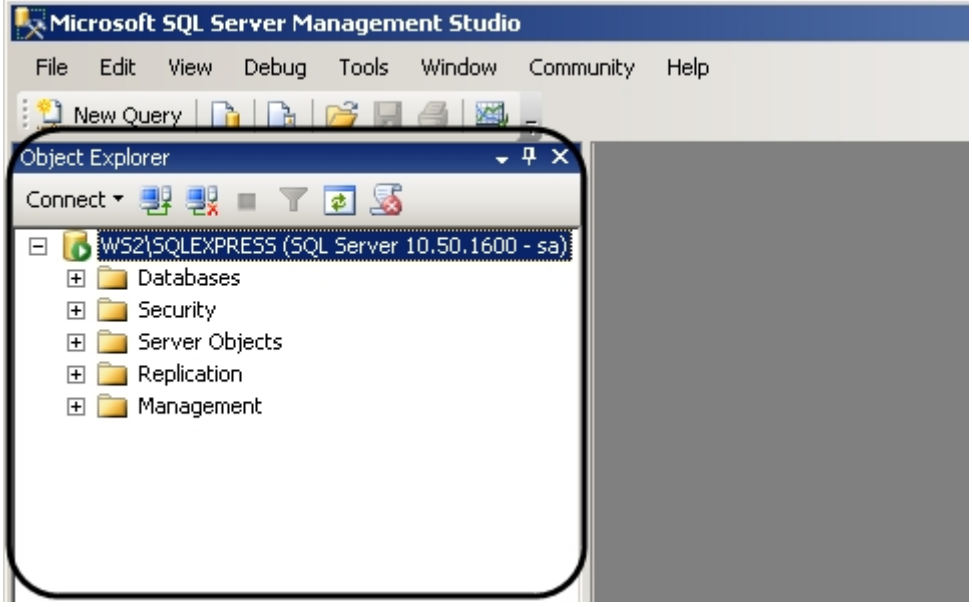


   a. Select the **Database Engine** type in the **Server type** list (**1**).
   b. Select the name of MS SQL server to which it is necessary to connect in the **Server name** list (**2**).
   c. Select authentication type used for connection to MS SQL server in the **Authentication** list (**3**).

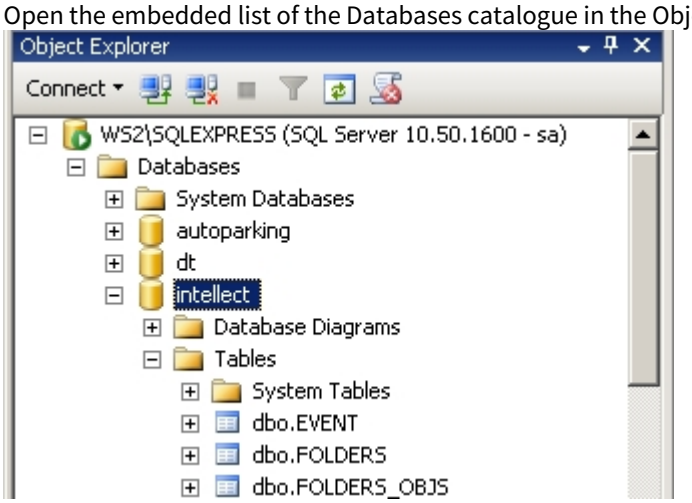
> **Note**
>
> The type of authentication that was selected while creating MS SQL server is specified.

> **Note**
>
> If SQL Server Authentication type is used, then select the user in the **Login** list and type-in the required password in the **Password** field (3).

4. Click **Connect** to connect to MS SQL server. If the connection is successful, then the **Object Explorer** window is displayed.

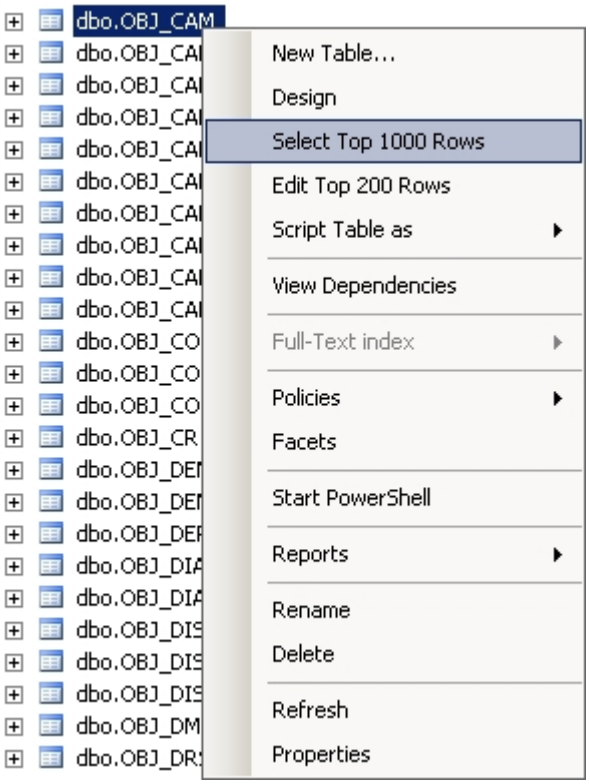


5. Open the embedded list of the Databases catalogue in the Object Explorer box and go to the required database.



6. Select the table for viewing in the **Tables** catalogue.

7. Select **Select Top 1000** Rows item in the context menu of the table.



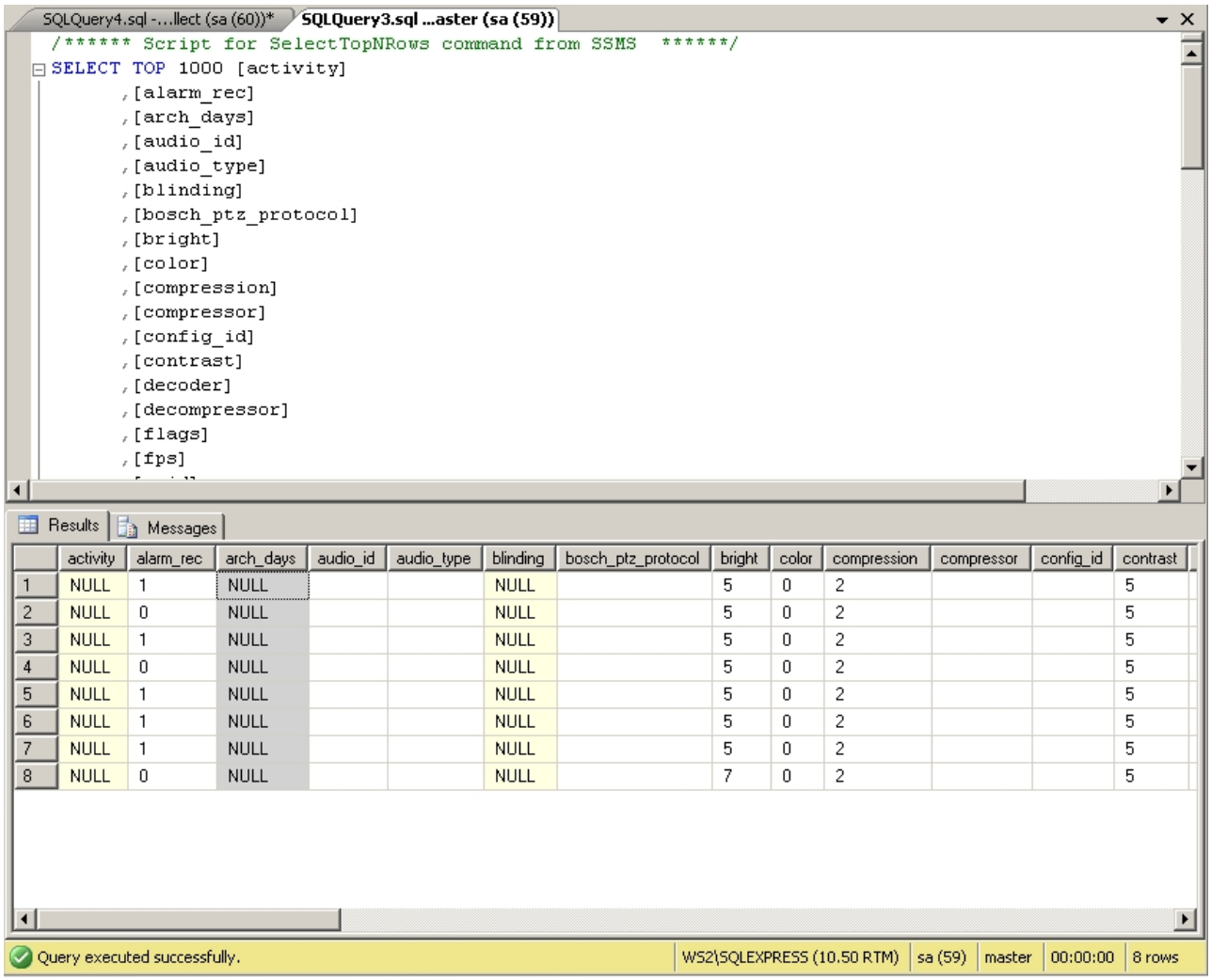
As a result the box with SQL Query on top of it and the table data selected by the query will be displayed.

Note

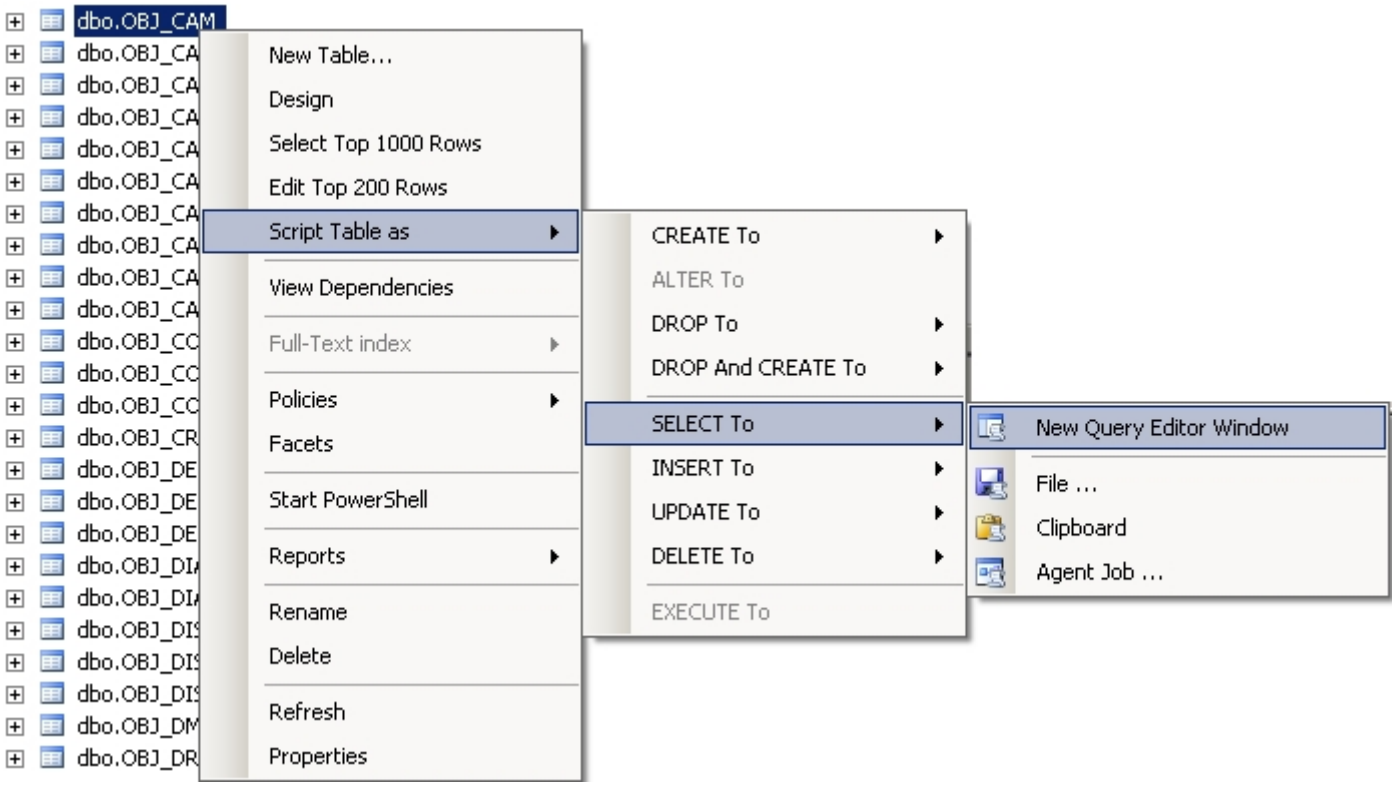
Using **Select Top 1000 Rows** command one can query the latest rows stored into the table. Not more than 1000 rows respond to a query.

Note

One can change the quantity of rows and set of fields requested in the table by editing SQL Query. To start modified SQL Query click Execute on the toolbar.



If one need to create his own query, then select **Script Table as -> SELECT To -> New Query Editor Window** in the context menu and type in SQL Query in the box.

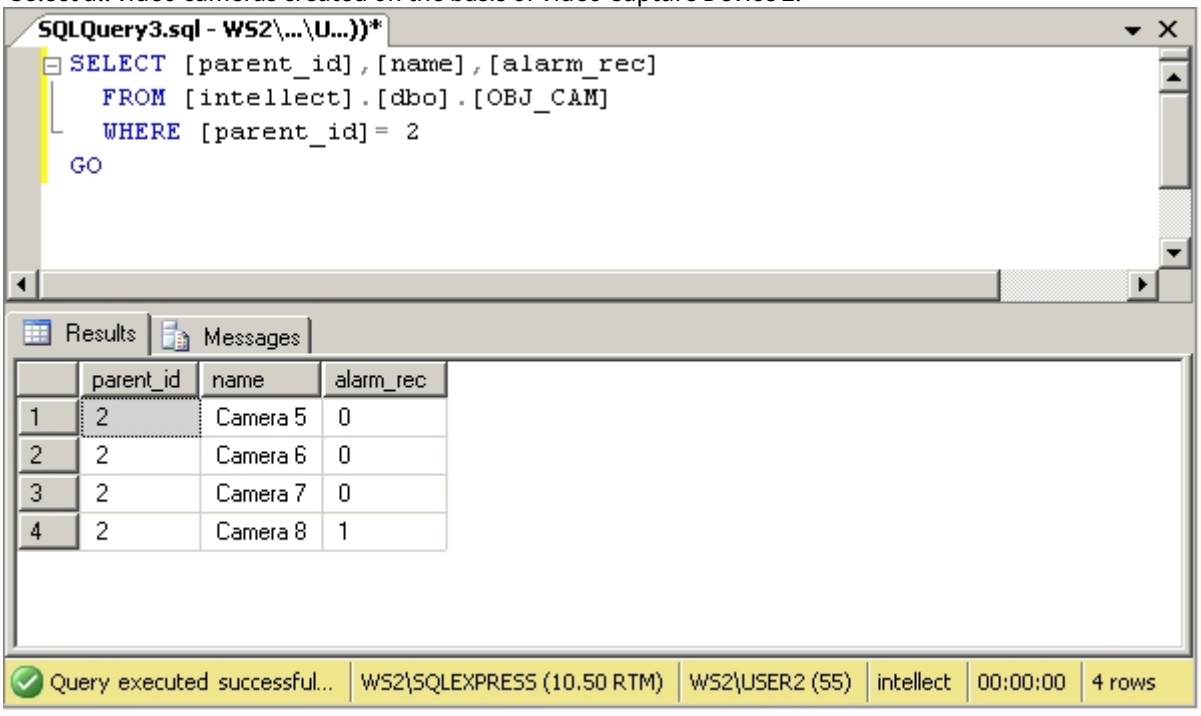


Note

To execute the query click Execute on the toolbar.

Example

Select all video cameras created on the basis of Video Capture Device 2.



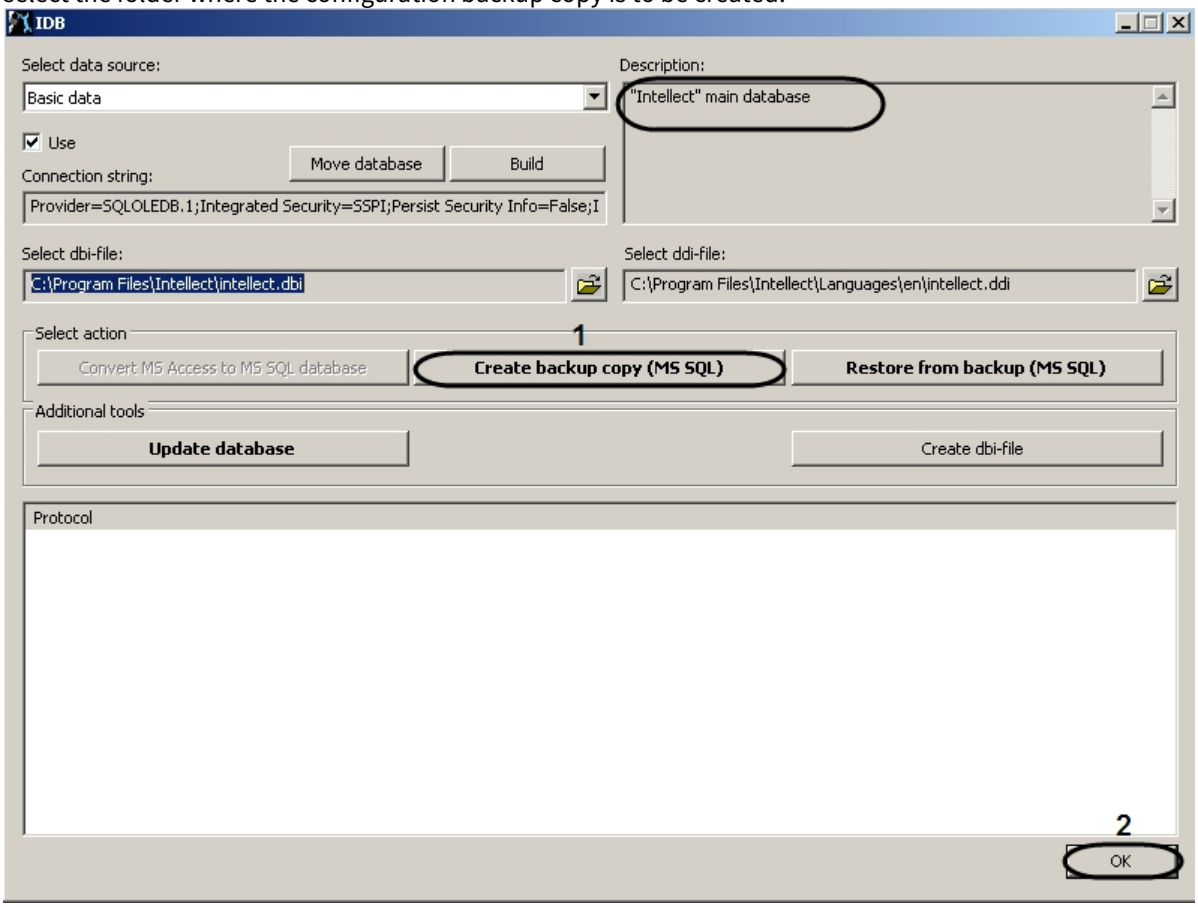
Viewing *Intellect* database is now completed.

> **Note**
>
> To view databases of other formats, the SQL Server Management Studio utility can also be used. For this install the package of ODBC drivers and OLE DB provider that can be found at http://www.microsoft.com. To connect to database Server, use sp_addlinkedserver stored procedure. Its description and examples of use are at http://msdn.microsoft.com.

26.3.6 Moving Intellect configuration database to the latest version of MS SQL Server

To move configuration database to the latest version of MS SQL Server after INTELLECT™ update do the following:

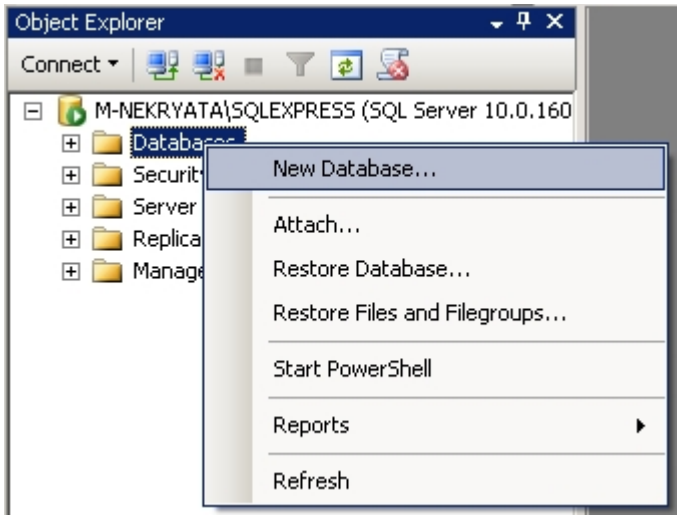
1. Run the idb.exe utility from the Intellect installation directory (e.g., C:\Program Files (x86)\Intellect). The dialog box of the idb.exe utility is opened.
2. To create backup copy of Intellect configuration database click **Create backup copy (MS SQL)** (1). In opened window select the folder where the configuration backup copy is to be created.



> **Note.**
>
> Configuration backup copy is a file with bak. extension.

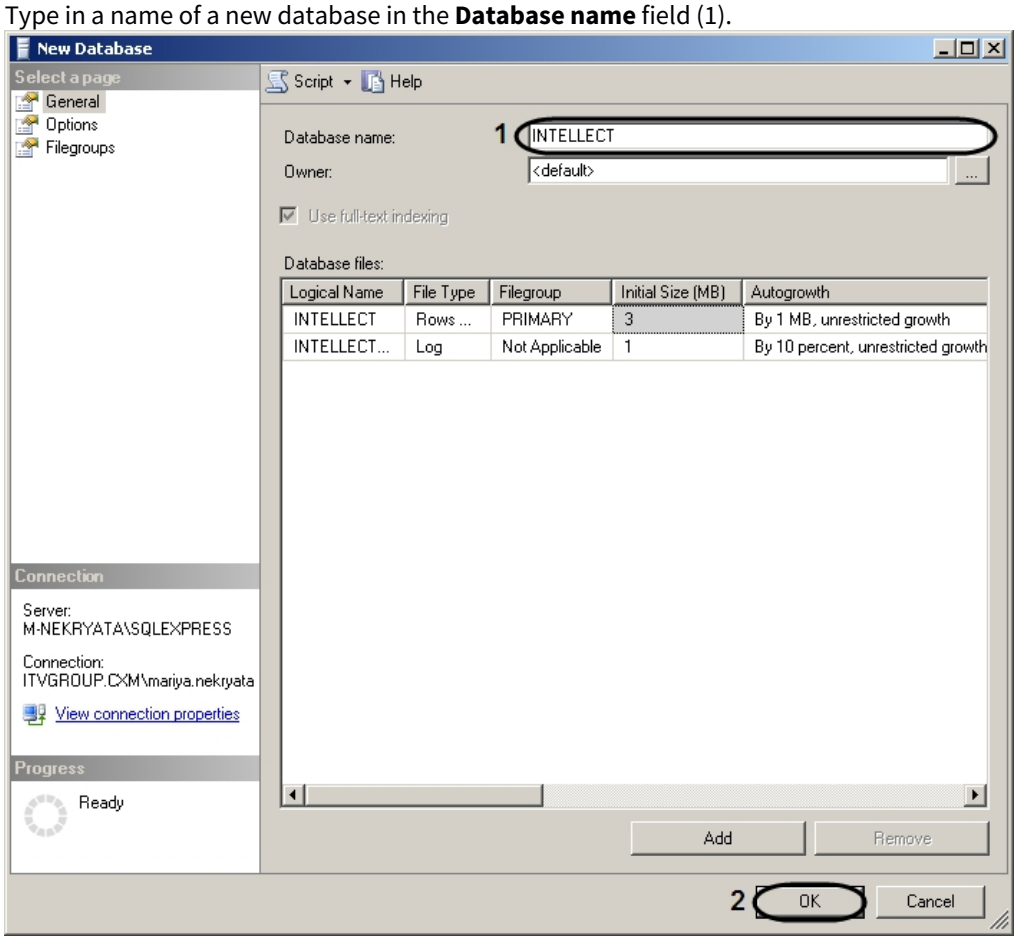
3. If the configuration backup copy is created without any errors (see the protocol of the idb.exe utility), then click **OK** (2). If there are some errors, then repeat 2 step or use MS SQL Server 2005 tools for creating database backup copies.
4. Remove previous version of MS SQL Server from computer.
5. Install a new version of MS SQL Server with SQL Server Management Studio (see Microsoft documentation).
6. Create an empty database.
    a. Run the SQL Server Management Studio utility. Click **Start => All Programs => Microsoft SQL Server => SQL Server Management Studio**.

b. Select **New Database** in the context menu of the **Databases** directory.



As the result the **New Database** window opens.

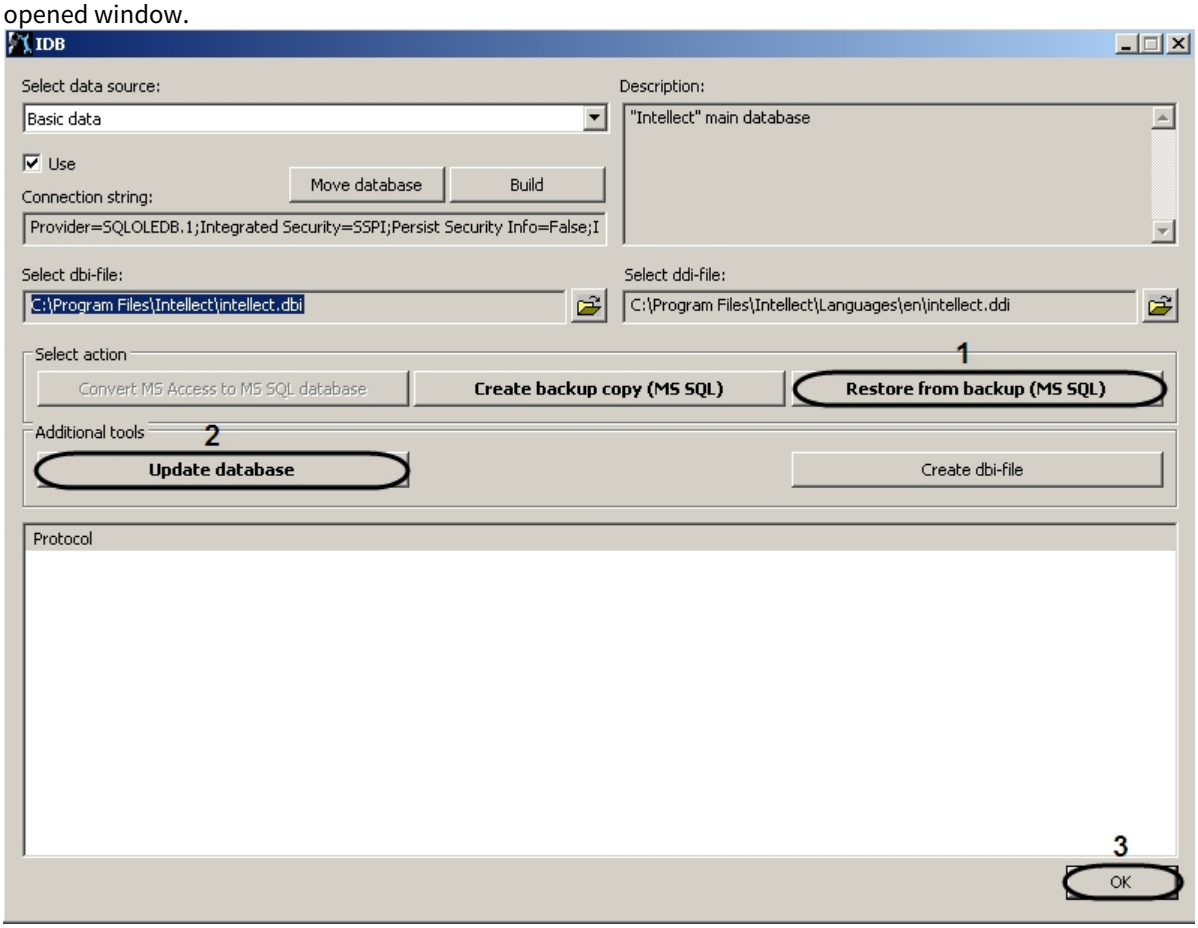
c. Type in a name of a new database in the **Database name** field (1).



d. Click **OK** (2).

7. Connect created database to Intellect using the idb.exe utility (see 1-16 steps in *INTELLECT™ software database connection* section).

8. To restore Intellect configuration database click **Restore from backup (MS SQL)** (1). Select configuration backup copy in opened window.



9. To update database click **Update database** (2).
10. Click **OK** to shut down the idb.exe utility (3).

Moving Intellect configuration database is completed.

26.3.7 Database synchronization setup

When INTELLECT™ software is applied by a large-scale system with distributed architecture, servers and Remote Admin Workstations databases should be synced. Database synchronization allows to store data both centrally (on a single server or Remote Admin Workstation) and in a distributed manner (data replication from different servers and Remote Admin Workstation databases of the video surveillance system). Database synchronization provides parallel operation with servers and Remote Admin Workstations databases and their automatic updating after they have been modified.

INTELLECT™ software databases on servers and Remote Admin Workstations are not synced by default. Usually INTELLECT™ software is configured to sync all databases with a single centralized administering server database.

Note.

If one or more databases are stored in MS Access format, they need to be converted to MS SQL format before the synchronization setup.

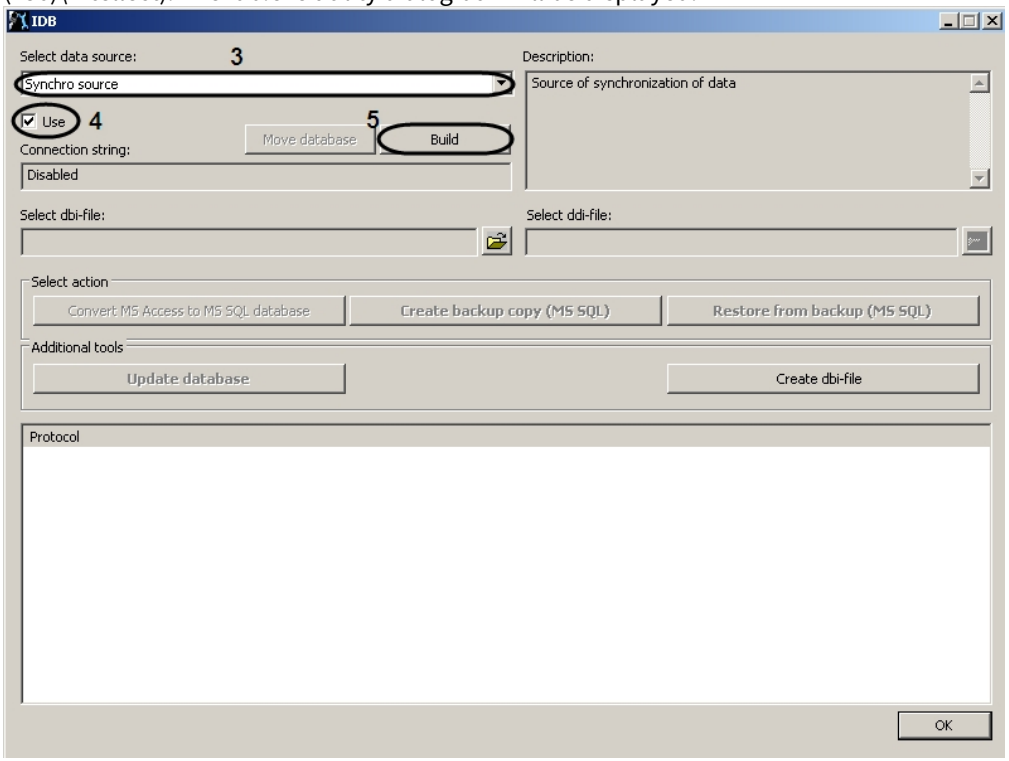
The administering Server acts as a synchronization source. The second-level Server/RAW will accept all database changes from the administering Server. Synchronization should always be performed from the second-level Server to the administering Server, or from the RAW to the administering Server.

Important!

You shall install all industry-specific solutions used for the particular distributed system on your Administration Server, otherwise all .ddi and .dbi files as well as the updated database containing these files must be present there.

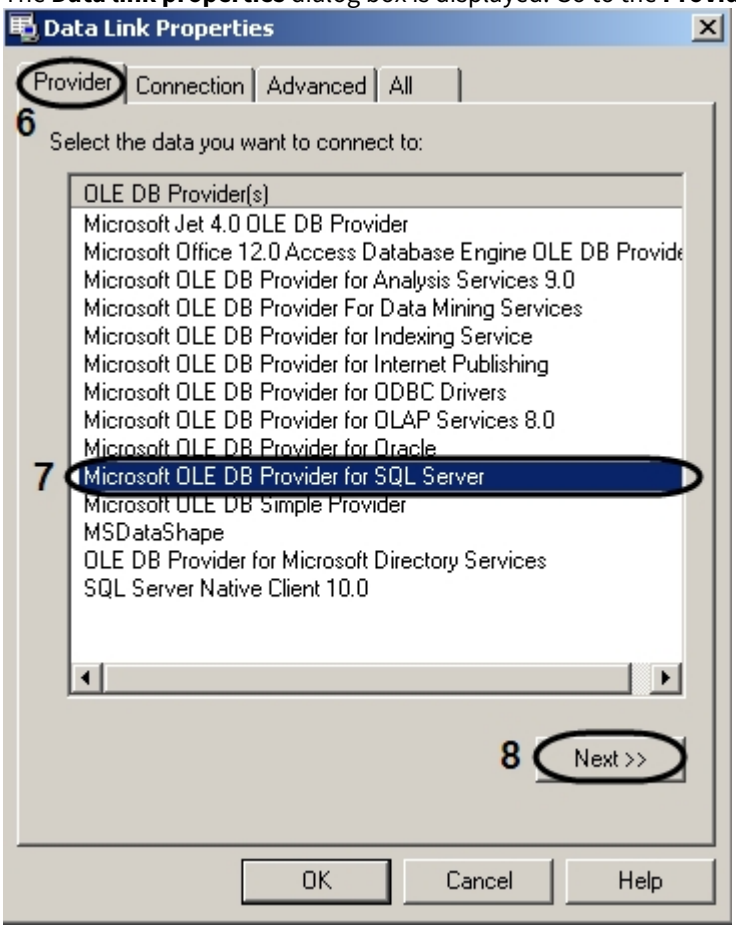
To sync the INTELLECT™ software “Configuration” database with the administering server database (or any other one), follow the procedure on RAW/second-level Server:

1. Make sure that MS SQL Server software is.
2. Start the idb.exe utility from the root of the INTELLECT™ software installation directory (for example, C:\Program Files (x86)\Intellect). The idb.exe utility dialog box will be displayed.



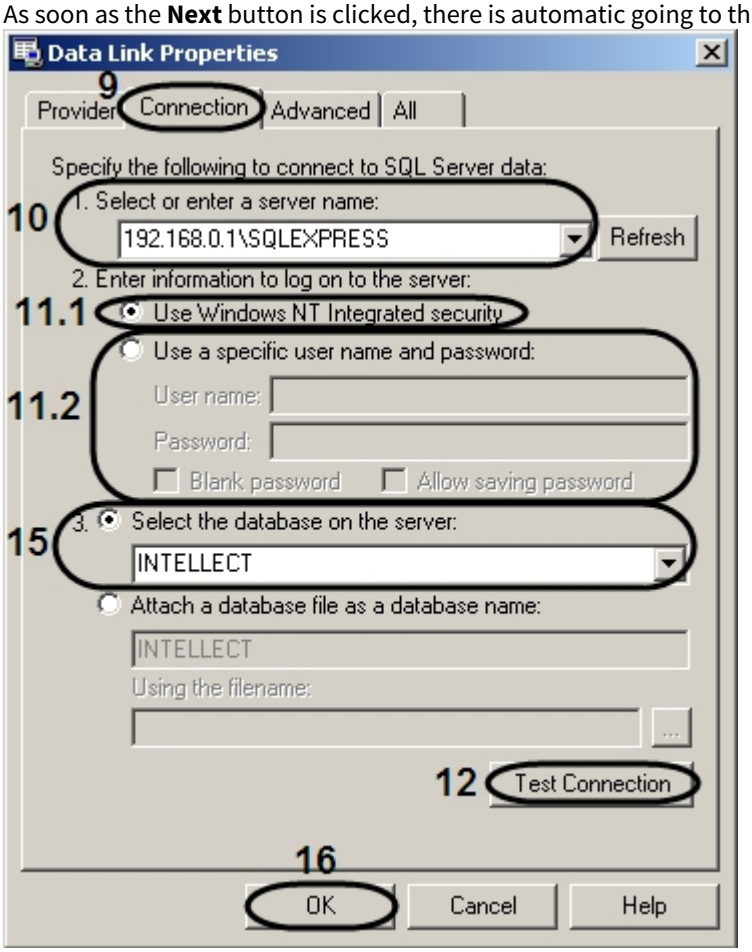
3. Select the **Synchro source** item from the **Select source database** list.
4. Set the **Use** checkbox.
5. Click **Build**.

6. The **Data link properties** dialog box is displayed. Go to the **Provider** tab in the **Data link properties** dialog box.



7. Select **Microsoft OLE DB Provider for SQL Server** from the **OLE DB Provider(s)** list.
8. Click **Next**.

9. As soon as the **Next** button is clicked, there is automatic going to the **Connection** tab.

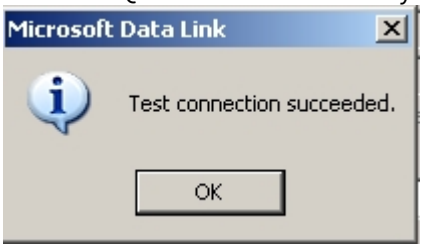


10. In the **1.Select or enter a server name** select from the list or input manually the address of MS SQL server containing the database that is to be used as a source to sync with the current database.
11. The **2.Enter information to log on to the server** group is used to enter the type and authentication parameters of the MS SQL server connection. MS SQL server authentication is performed through the user account, authorized in the Windows OS, or by user name (login) and password that protect the MS SQL server connection.
    The method and parameters of authentication at the MS SQL server are set during MS SQL server installation.
    Different parameters need to be entered, with different authentication techniques for MS SQL server connection:
    a. If MS SQL server authentication is performed through a user's Windows OS account, switch to to the **Use Windows NT Integrated security** position. The user's current account on the computer, from which the synchronization is performed, should be logged into the computer with MS SQL server and the database to be synced with.
    b. If MS SQL server authentication is performed through user login and password, follow the sequence:
        i. switch to the **Use a specific user name and password** position;
        ii. in the **User name** field: enter the user name (login) to connect to the MS SQL server.
        iii. if access to the MS SQL server is password protected, remove the **Blank password** checkbox and enter the database access password into the **Password** field.
        iv. set the **Allow saving password** checkbox.
        v. go to the **All** tab.
        vi. in the **Persist Security Info** field, set the **True** value. This is necessary to correctly save the user password.

> **Note**
>
> Each time you change the server connection parameters, you must set the **Persist Security Info** field value to **True**.

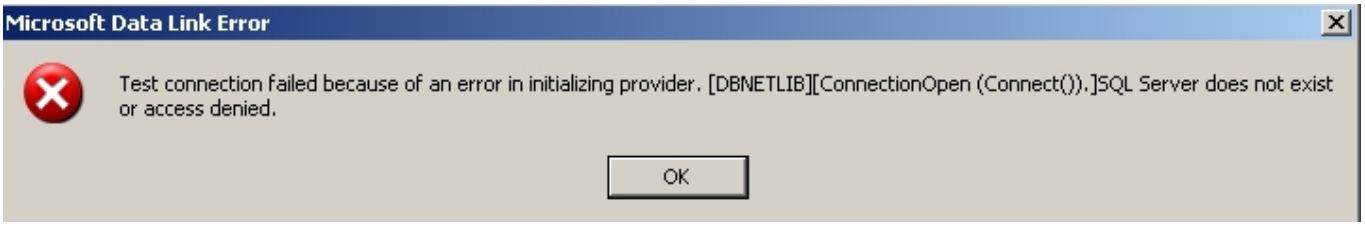
12. Click **Test Connection**.

13. If the MS SQL server was successfully connected, the “Test connection succeeded” message is displayed.



Click **OK** to close the window.

14. If the MS SQL server name and/or authentication parameters of MS SQL server connection were entered inaccurately, the error message will appear.



Click **OK** to close the window. Then enter the correct password and try MS SQL server connection again.

15. From the **Select the database on the server** list choose the name of the database to be synced with the current base.
16. Click **OK** in the **Data link properties** dialog box. The window will close.
17. Click **OK** in the right bottom corner of the idb.exe utility window.

Database synchronization setup is completed.

Requirements for TCP/IP Network

26.3.8 Stored procedures for adding or deleting a large number of objects

On the page:

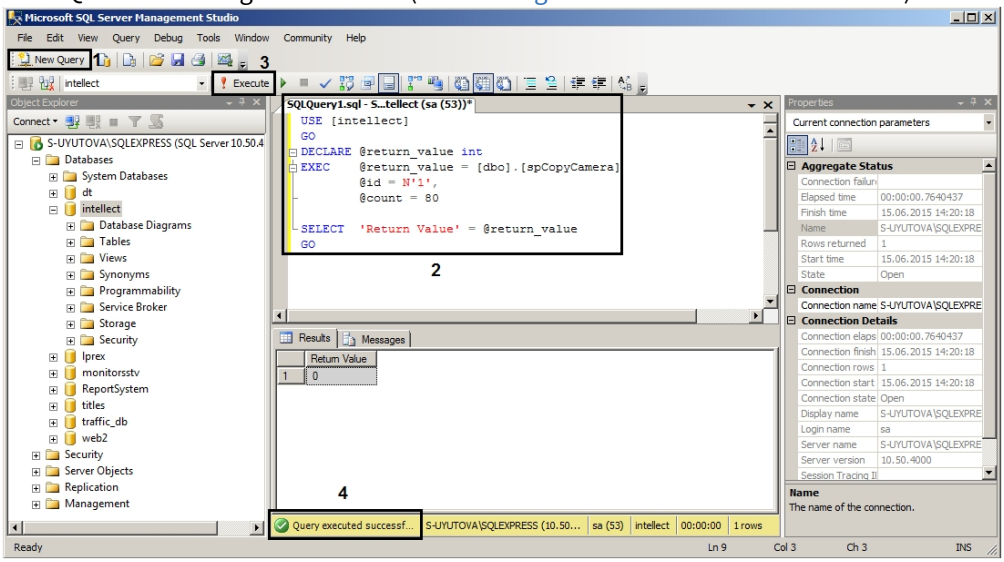
- Running stored procedures
- Examples of stored procedures use for adding or deleting Camera objects
- Example of stored procedure use for adding Tracker objects
- Example of stored procedure use for adding VMDA Detection objects

Intellect database has built'in pre-installed stored procedures for adding and deleting a large number of **Camera**, **Tracker**, **VMDA Detection** objects.

26.3.8.1 Running stored procedures

Run stored procedures in SQL Server Management Studio as follows:

1. Run SQL Server Management Studio (see Viewing INTELLECT™ software database).



2. Click the **New Query** button (1).
3. Specify the SQL query (2, see examples below).
4. Click the **Execute** button (3). If the query is executed successfully, then the corresponding message appears at the bottom of the window (4).

You can find examples of using stored procedures below.

26.3.8.2 Examples of stored procedures use for adding or deleting Camera objects

If lots of **Camera** objects are to be created or deleted, this can be done using dbo.spCopyCamera and dbo.spDeleteCameras stored procedures correspondingly.

1. Take Camera 1 as an example and create 80 cameras with the same settings as Camera 1 has.

```
USE [intellect]
GO
DECLARE @return_value int
EXEC    @return_value = [dbo].[spCopyCamera]
                @id = N'1',
                @count = 80
SELECT  'Return Value' = @return_value
GO
```

2. Delete cameras from 3 to 33.

```
USE [intellect]
GO
DECLARE @return_value int
EXEC    @return_value = [dbo].[spDeleteCameras]
                @fromId = 3,
                @toId = 33
SELECT  'Return Value' = @return_value
GO
```

26.3.8.3 Example of stored procedure use for adding Tracker objects

Take Tracker 1 based on Camera 1 as an example and copy under all other cameras.

```
USE [intellect]
GO
DECLARE @return_value int
EXEC    @return_value = [dbo].[spCopyVmda]
        @id = N'1'
SELECT  'Return Value' = @return_value
GO
```

26.3.8.4 Example of stored procedure use for adding VMDA Detection objects

Take VMDA Detection 1 based on Tracker 1 as an example and copy under all other trackers.

```
USE [intellect]
GO
DECLARE @return_value int
EXEC    @return_value = [dbo].[spCopyVmdaDetector]
        @id = N'1'
SELECT  'Return Value' = @return_value
GO
```

26.3.9 Removing the events from the PROTOCOL table using SQL queries

You can manually remove the events from the PROTOCOL table using SQL queries as follows:

> **Attention!**
>
> Once you remove the events, it cannot be undone. We recommend you to create a backup before removal (see Creating the database backup copy).

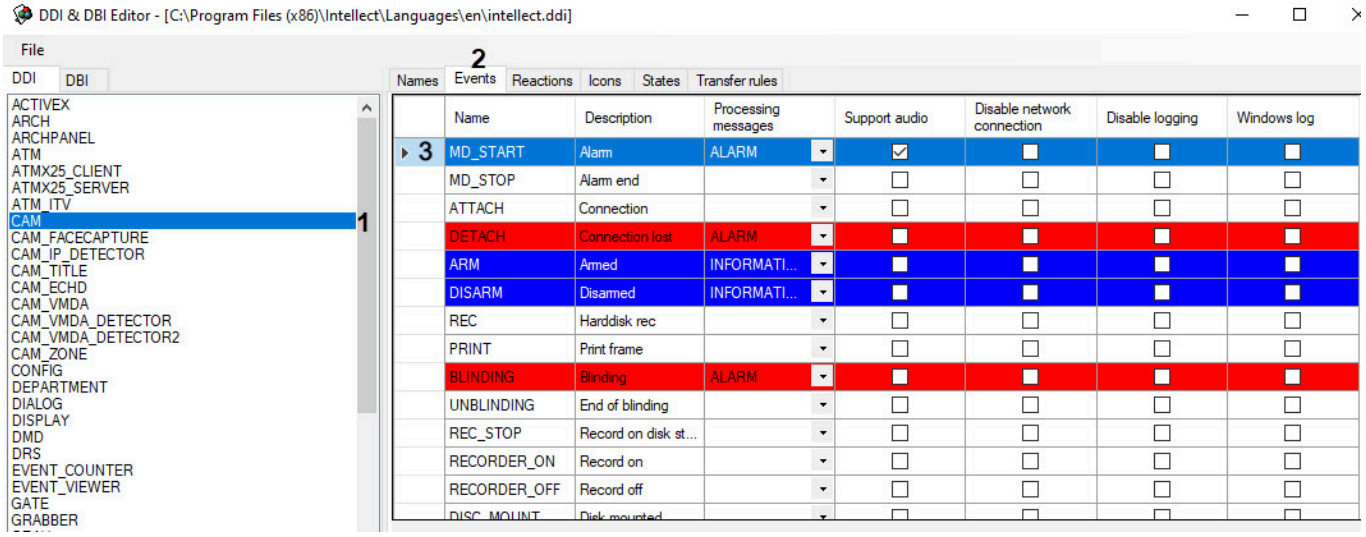
1. Shut down *Intellect*.
2. Determine the events which should be removed from the events database.
3. Open the intellect.ddi file using the ddi.exe utility (see The ddi.exe utility for editing database templates and external settings files):
   a. select the object the events from which you want to delete;
   b. go to the **Events** tab to view the names of the events to be deleted in the database.
4. In SQL Server Management Studio, run a query to remove the selected events:

```
delete FROM [intellect].[dbo].[PROTOCOL] where action = 'action'

where

[intellect].[dbo].[PROTOCOL] – is the name of the table with events;

action – is the name of the event to be deleted in the database.
```

As a result, the selected events will be removed from the PROTOCOL table using an SQL query.

For example, if it is necessary to remove all the **Alarm** events of the **Camera** object, then do the following:

1. In the intellect.ddi file, select the **Cam** object (**1**).



2. Go to the **Events** tab (**2**).
3. Find the name of the **Alarm** event to be deleted in the database: **MD_START** (**3**).
4. In SQL Server Management Studio, run the query:

```
delete FROM [intellect].[dbo].[PROTOCOL] where action = 'MD_START'
```

As a result, the **Alarm** events from cameras will be removed from the events table.

26.3.10 Removing the event table from the Intellect database

If necessary, you can clear the table with events from the **INTELLECT** database. For example, if the database has become very large.

> **Attention!**
>
> Once you remove the event table, it cannot be undone. We recommend you to create a backup before removal (see Creating the database backup copy).

To remove the events table from the *Intellect* database, do the following:

1. Shut down *Intellect* on the server where the database to be cleared is stored.
2. Launch the *SQL Server Management Studio* utility and connect to the server. For details, see Viewing the Intellect database.
3. Go to the folder with tables Databases/intellect/Tables.
4. Delete the **PROTOCOL** table.
5. Quit *SQL Server Management Studio*.
6. Run the **idb.exe** utility (Start -> Programs -> Intellect -> Update database).
7. Click the **Update database** button in the utility and wait for the message about the completion of the update (see Interface elements of the idb.exe window).
8. Close the **idb.exe** utility with the **OK** button.

As a result, the event table will be deleted.

26.3.11 Compressing the database size

> **Attention!**
>
> The article provides an example of advanced settings. We recommend that you do not perform them if you do not have the appropriate qualifications, and instead contact AxxonSoft staff for help.

You cannot compress the database if the **Report System** is used (see The Report System).

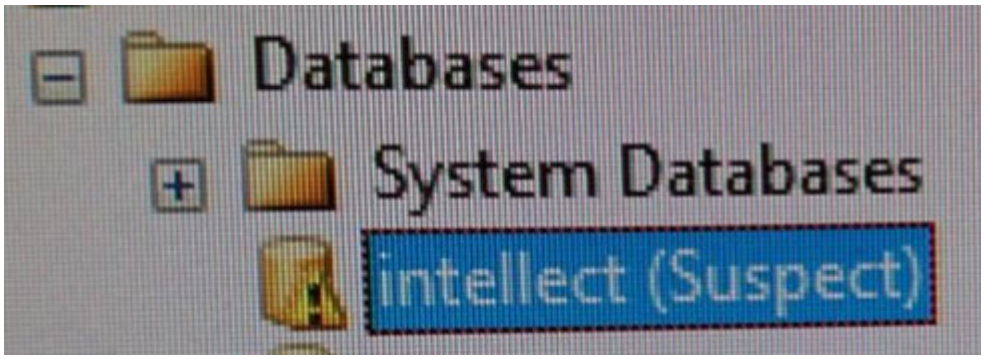
To compress the database and reduce the size of the log files, do the following:

1. Shut down *Intellect.*
2. Launch the *SQL Server Management Studio* utility and connect to the server. For details, see Viewing the Intellect database.
3. Open the **Databases** list.
4. Adjust the compression settings:
   a. Right-click on the name of the database to be compressed and select **Properties** from the context menu.
   b. In the window that opens, go to the **Options** tab.
   c. Set the **Recovery Model** parameter to **Simple.**
   d. In the **Automatic** section, set the **Auto Shrink** parameter to **True**.
   e. Click **OK**.
5. Start the compression process:
   a. For database:
      i. right-click on the name of the database;
      ii. in the drop-down menu, sequentially select **Tasks** → **Shrink** → **Files**;
      iii. in the window that opens, in the **File type** column, select **Data**;
      iv. click **OK**.
   b. For log file:
      i. right-click on the name of the database;
      ii. in the drop-down menu, sequentially select **Tasks Shrink File**;
      iii. in the window that opens, in the **File type** column, select **Log**;
      iv. click **OK**.

The database is now compressed.

26.3.12 Restoring the Intellect database from the Suspect mode

The *Intellect* database can go into Suspect mode because of a sudden server reboot or file system damage.

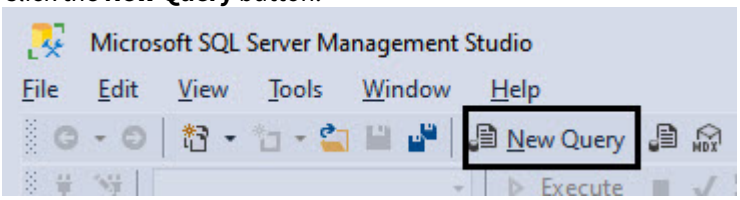


To restore the database from this mode, do the following:

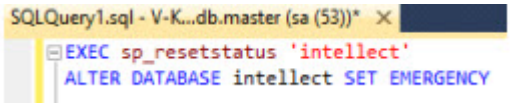
1. Check system disk for errors:
   a. run command line as administrator;
   b. enter the command <chkdsk c:> to search for errors;
   c. if there are errors, use the </f> parameter to fix them;
   d. perform step b again to recheck the system disk.
2. If no errors were found at step 1, start the recovery:
   a. Launch Microsoft SQL Server Management Studio Express (SSMSE).

b. Connect to the required MS SQL instance.

c. Click the **New Query** button:



d. In the window that opens, enter the following commands:
EXEC sp_resetstatus 'intellect'
ALTER DATABASE intellect SET EMERGENCY

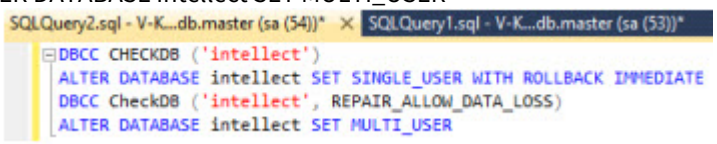


e. After you enter the commands, click the

button.

f. Click the **New Query** button.

g. In the window that opens, enter the following commands:
DBCC CHECKDB('intellect')
ALTER DATABASE intellect SET SINGLE_USER_WITH_ROLLBACK IMMEDIATE
DBCC CheckDB('intellect', REPAIR_ALLOW_DATA_LOSS)
ALTER DATABASE intellect SET MULTI_USER



h. After you enter the commands, click the

button.
The recovery process will start.

> **Note**
>
> To check the recovery status, you need to create a request. You can do it by clicking the **New Query** button in a new window and entering the following command:
> SELECT
> [command]
> ,[start_time]
> ,[percent_complete]
> ,[estimated_completion_time]/60000. AS [estimated_completion_time_min]
> FROM sys.dm_exec_requests
> WHERE [command] LIKE '%DBCC%'

```
SELECT
    [command]
    ,[start_time]
    ,[percent_complete]
    ,[estimated_completion_time] / 60000. AS [estimated_completion_time_min]
FROM sys.dm_exec_requests
WHERE [command] LIKE '%DBCC%'
```

After you enter the commands, click the Execute button (or pressing **F5** on the keyboard). After that, a line containing the percentage of completion and the remaining time will appear in the window below. To refresh the line, click the Execute button (**F5**).

As a result, the *Intellect* database will be restored.

26.4 Appendix 4. Updating Java time zones for proper operation with archive in iOS client

Issues affecting the ability to access archive video from the iOS client may occur due to changes in Russian time zones.

These issues are due to discrepancies in how Windows and Java handle time zones. The inconsistency is only indirectly related to Intellect and will be solved in the next official Java release.

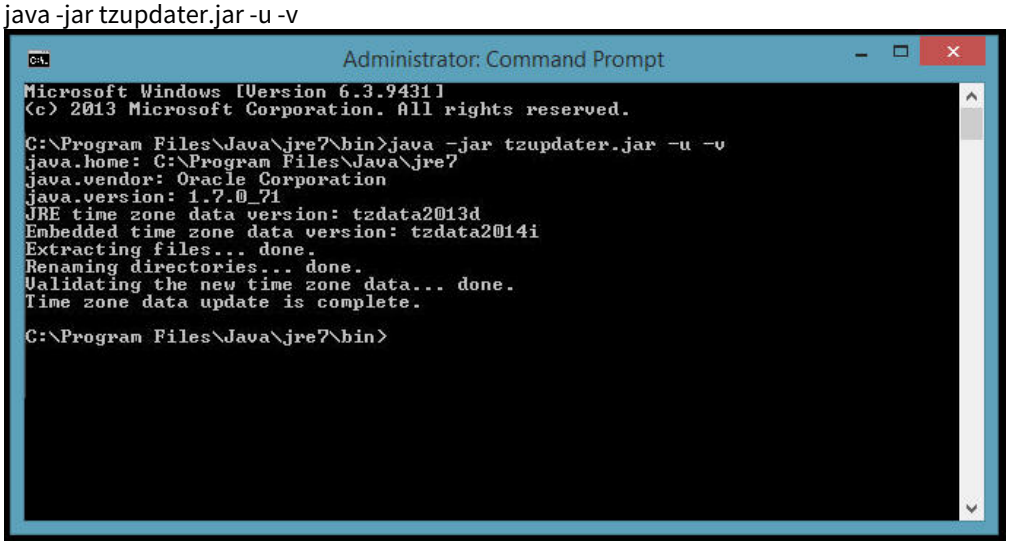
As a temporary workaround, perform the following actions:

1. Quit *Intellect*.
2. Update Java to the latest version from the official website http://www.oracle.com/.
3. Download the update tzdata2014i.1.4.9, or newer, for Java time zones.

> **Note.**
>
> See the official site for details on the update http://www.oracle.com/technetwork/java/javase/tzdata-versions-138805.html?ssSourceSiteId=ocomen).
> Download the utility for updating time zones at http://www.oracle.com/technetwork/java/javase/downloads/tzupdater-download-513681.html.

4. Update Java time zones with the help of tzdata2014i.1.4.9 (or newer). To do this, you must:

1. Copy tzupdater.jar from downloaded tzupdater-1_4_9-2014i.zip to the folder JRE_HOME /bin (where JRE_HOME represents your Java install directory).
2. In the command line, run the following command with administrator rights:
java -jar tzupdater.jar -u -v



If the update is successful, you will view a message: "Time zone data update is complete".