

Administrator's Guide

Last update 31/07/2020

Table of contents

1 Administrator's Guide. INTRODUCTION 25
1.1 Purpose of the INTELLECT™ intelligent video surveillance system 25
1.2 Setting up logical interrelations among objects in the Intellect software system 25
1.3 Purpose and structure of the guide 26
1.4 License method of the INTELLECT™ software 26
2 Software Lifecycle Policy 27
2.1 Software Lifecycle Phases 27
2.2 Software Technical Support 27
2.3 Standard Period for Release of Software Updates 27
2.4 Licensing Policy with Regard to Software Updates 27
3 General description of the INTELLECT™ software 28
3.1 INTELLECT™ software functionality 28
3.1.1 Video surveillance functionality 28
3.1.2 Audio monitoring functionality 29
3.1.3 Structuring guarded objects 29
3.1.4 Event registration functionality 29
3.1.5 Notification functionalities 29
3.1.6 Functions of workability control 29
3.1.7 Management functionality 30
3.1.8 Integration of the distributed video surveillance and audio monitoring system 30
3.2 Structure of the digital video surveillance and audio monitoring system based on INTELLECT™ software 30
3.2.1 Basic hardware components of the digital video surveillance system 31
3.2.2 Software 32
3.2.2.1 Operating system 32
3.2.2.2 Software kernels 32
3.2.2.3 Program modules 32
3.2.2.4 Interaction of basic modules with the Intellect kernel 32
3.2.2.5 Interaction of modules of other vendors with Intellect kernel 33
3.2.3 Internal video Server database 34
3.2.4 Communication environment 35
3.3 Intellect software package restrictions 35

3.4 Hashing procedure....37
3.5 Traffic encryption in the Intellect software....37
4 Requirements for the software and hardware platform....38
4.1 Requirements for base PCs....38
4.1.1 General requirements for PCs....38
4.1.2 Operating system requirements....39
4.1.3 Free disk space (video archive size) required....42
4.1.4 Defining disk space (audio archive size)....45
4.1.5 Define required disk space (size of event log database)....46
4.1.6 Define required disk space (VMDA metadata storage)....46
4.1.7 Intellect software working in virtual machines....47
4.2 Requirements for TCP/IP Network....48
4.2.1 Requirements for TCP/IP Network bandwidth for video signal transferring....48
4.2.2 Requirements for TCP/IP network bandwidth for database synchronization functionality....49
4.2.3 Requirements to the TCP/IP network quality....49
4.3 Requirements for PTZ and control panels....50
4.4 Requirements for audio input units....50
4.5 Requirements for IP devices of audio and video input....50
4.6 Requirements for GSM Equipment....51
4.7 Requirements for voice modems....51
4.8 Requirements for software which is used while integrating....51
4.9 Requirements for anti-virus software....51
4.10 Requirements for BIOS....51
4.11 Hardware requirements for Intellect and vertical solutions detection tools....52
5 Personnel skills requirements....53
6 Installing and removing INTELLECT™ software....54
6.1 Installing INTELLECT™ software....54
6.1.1 Description of INTELLECT™ software distribution package....54
6.1.2 Getting ready for Intellect installation....55
6.1.2.1 OS language settings....55
6.1.2.2 Unblocking a distribution kit downloaded from the Internet....58
6.1.2.3 System settings....58
6.1.3 Installation of INTELLECT™ software as a Server/Remote administrator workplace....59
6.1.4 Installation of INTELLECT™ software to the Client....73

6.1.5 Updating INTELLECT™ software ... 83
6.1.6 Using the Product.msi and Redist.exe for INTELLECT™ software installation ... 89
6.1.7 Possible installation problems and their solutions ... 90
6.1.7.1 Error while installing driver for the FX4 card ... 90
6.1.7.2 Error code 26352 ... 90
6.2 Repairing INTELLECT™ software ... 90
6.3 Removing INTELLECT™ software ... 93
6.3.1 Removing INTELLECT™ software from the Start menu ... 93
6.3.2 Removing INTELLECT™ software from the OS Windows panel Add or Remove programs ... 96
6.3.3 Removing INTELLECT™ software with the help of installation CD ... 98
6.3.4 Removing INTELLECT™ software installed as a Service ... 99
6.4 Installing INTELLECT™ software in a silent mode ... 100
6.5 Remote installation, removal and update of Intellect software ... 104
6.5.1 Remote installation of Intellect software ... 105
6.5.2 Remote update of Intellect software ... 106
6.5.3 Remote removal of Intellect software ... 106
6.6 Configuring Cluster Service for Intellect ... 106
6.6.1 Example. Combination of two Servers to the cluster and the Intellect software configuration ... 107
6.6.1.1 Previous configuration of servers ... 107
6.6.1.2 Combination of two Servers to the cluster and the Intellect software configuration ... 108
7 License key ... 110
7.1 Binding the license key to computer equipment ... 110
7.2 Match search in the license key ... 110
7.3 Features of the Intellect software operation when the object limit is exceeded ... 111
7.4 Decoding license key ... 112
8 Configuring system startup and shutdown ... 114
8.1 Configuration of Intellect™ software startup ... 114
8.1.1 Possible options for Intellect™ software startup ... 114
8.1.2 Configuring Intellect™ system automatic startup from Windows OS Startup ... 114
8.1.3 Configuring Intellect™ system automatic startup bypassing standard Windows OS ... 115
8.2 Configuring Intellect™ system shutdown ... 116
9 Working with the System settings dialog box ... 117
9.1 General information about the System settings dialog box ... 117
9.2 Startup and shutdown of the System settings dialog box ... 117

9.2.1 Startup of the System settings dialog box ... 117
9.2.2 Shutdown of the System settings dialog box ... 118
9.3 Setting procedure for system objects ... 119
9.3.1 Select an object. ... 119
9.3.2 Create an object. ... 119
9.3.3 Editing. ... 122
9.3.4 Deleting. ... 123
9.3.5 Changing the parent object. ... 124
9.3.6 Copying objects ... 124
10 INTELLECT™ software configuration and setup ... 126
10.1 Configuration procedure for servers, clients and remote workstations ... 126
10.1.1 Server settings ... 126
10.1.1.1 Server hardware and software platform ... 126
10.1.1.2 Setting up a Server ... 126
10.1.2 Configuring a Remote Admin Workstation ... 127
10.1.2.1 Remote Admin Workstation hardware and program platform ... 127
10.1.2.2 Remote Admin Workstation configuration ... 127
10.1.2.3 Videogate configuration ... 127
10.1.2.4 Configuring backup archive server ... 128
10.1.2.5 Configuring remote Web-server ... 128
10.1.3 OS settings for correct operation of Remote Admin Workstation or Server ... 129
10.1.4 Configuring Remote Clients (RC) ... 129
10.1.4.1 Remote Client hardware and software platform ... 129
10.1.4.2 Configuring Remote Client ... 129
10.1.4.3 OS settings for correct operation of Remote Client ... 130
10.2 Configuration of distributed architecture ... 130
10.2.1 General principles of designing the digital video surveillance system with distributed architecture ... 130
10.2.2 Configuring procedure for the distributed system ... 130
10.2.3 Selecting the structure of the distributed system ... 131
10.2.4 Synchronizing the databases of servers and remote workstations ... 131
10.2.5 Registration of servers, clients and remote workstations on the administering server ... 133
10.2.6 Configuring the interaction of distributed system components ... 134
10.2.7 Configuring time synchronization in the distributed system ... 137
10.2.8 Role-assignment in distributed system ... 138
10.2.9 Features of distributed system operation using NAT ... 139

10.3 Configuration of hardware 139
10.3.1 Configuring of using 64-bits modules 139
10.3.2 Configuring video subsystem 140
10.3.2.1 General information on configuring video subsystem 140
10.3.2.1.1 Video subsystem components description 140
10.3.2.1.2 Configuring video capture cards 141
10.3.2.1.3 Configuring IP-devices 141
10.3.2.1.4 Video signal compression and decompression 142
10.3.2.1.5 How to record digitized video signals 143
10.3.2.1.6 Digital video signal transmission to Remote Workplaces 144
10.3.2.1.7 Video signal display 144
10.3.2.2 Registrating Video Capture Devices and cameras in INTELLECT™ software 144
10.3.2.3 Configuring the video signals processing mode while using video capture cards and analog video cameras 144
10.3.2.3.1 Setting up format (PAL or NTSC) for the input analog video signal 144
10.3.2.3.2 Frame rate settings 146
10.3.2.3.2.1 Video capture card resources 146
10.3.2.3.2.2 Operation modes of the video capture cards' ADC 148
10.3.2.3.2.3 Frame rate setup procedure 148
10.3.2.3.2.4 Configuring video subsystem with disabled video channels 148
10.3.2.3.2.5 Actual frame rate 150
10.3.2.3.2.6 Changing frame scaling 151
10.3.2.3.2.7 Allocation of video capture card's resources 152
10.3.2.3.2.8 Video signal processing priorities 154
10.3.2.3.2.9 Setting video processing priority 156
10.3.2.3.2.10 Setting video recording priority 157
10.3.2.3.3 Brightness, contrast, color depth and color rendition format settings 157
10.3.2.3.3.1 Brightness and contrast settings 158
10.3.2.3.3.2 Color depth adjustment 160
10.3.2.3.3.3 Selecting the color rendition format 160
10.3.2.3.4 Configuring video compression 161
10.3.2.3.4.1 Compression rate settings 162
10.3.2.3.4.2 Key frame rate settings 162
10.3.2.3.4.3 Setting delta frame creation criterion 163
10.3.2.4 Creating and configuring a virtual Video Capture Device 164
10.3.2.4.1 Summary of virtual Video Capture Device 164

10.3.2.4.2 Creating and configuring a virtual Video Capture Device ... 165
10.3.2.4.3 Features of playing files in a virtual Video Capture Device ... 166
10.3.2.5 Configuring video archiving ... 167
10.3.2.5.1 General information on video archiving ... 167
10.3.2.5.2 Video archiving procedure ... 170
10.3.2.5.3 Selecting the disks for video archive storage ... 170
10.3.2.5.4 Using network disks ... 171
10.3.2.5.5 Disabling automatic recording upon alarm registration ... 172
10.3.2.5.6 Configuring video frame rate ... 173
10.3.2.5.7 Configuring video in the Hot record mode ... 174
10.3.2.5.8 Configuring video in the Pre-alarm record mode ... 175
10.3.2.5.9 Configuring video in the Post-alarm record mode ... 177
10.3.2.5.10 Configuring audio and video synchro recording ... 177
10.3.2.5.11 Selecting current disk for recording ... 178
10.3.2.5.12 Viewing current disk for recording ... 180
10.3.2.5.13 Configuring video camera archive depth ... 180
10.3.2.5.14 Video Archive Encryption ... 181
10.3.2.6 Additional information on camera ... 181
10.3.2.7 Configuring video detection tools ... 182
10.3.2.7.1 General description of Intellect software detection tools ... 182
10.3.2.7.2 Enabling, configuring and disabling basic video detection tools ... 182
10.3.2.7.2.1 General information on basic detection tools ... 182
10.3.2.7.2.2 Requirements to video parameters while working with detection tools and Tracker ... 183
10.3.2.7.2.3 Procedure for enabling and configuring basic detection tools ... 184
10.3.2.7.2.4 Connecting basic detection tools ... 184
10.3.2.7.2.5 Configuring basic detection tools ... 185
10.3.2.7.3 Configuring smart video detection tools ... 197
10.3.2.7.3.1 General information on forensic search ... 197
10.3.2.7.3.2 Requirements for video parameters to perform the forensic search in the archive ... 198
10.3.2.7.3.3 Hardware requirements for the Tracker with neural filter operation ... 198
10.3.2.7.3.4 Video requirements to be met for abandoned object detection tool of the Tracker object operation ... 199
10.3.2.7.3.5 Creating and configuring VMDA metadata storage ... 200
10.3.2.7.3.6 Recommendations on configuring smart video detection tools ... 201
10.3.2.7.3.7 Creating and configuring the Tracker object ... 201
10.3.2.7.3.8 Configuring object classification ... 206
10.3.2.7.4 Embedded detectors ... 216

10.3.2.7.4.1 Creating embedded detectors 216
10.3.2.7.4.2 Configuring embedded detectors 217
10.3.2.7.4.3 AxxonSoft tracking in Axis devices 218
10.3.2.7.4.4 Example of setting up and using the embedded detectors on Bosch FLEXIDOME IP dynamic 7000 VR IP camera .220
10.3.2.7.5 Face detection tool 224
10.3.2.7.5.1 General information on face detection tool 224
10.3.2.7.5.2 Requirements to video parameters while using face detection tool 224
10.3.2.7.5.3 Configuring Face detection tool 224
10.3.2.8 Configuration of multistream video 226
10.3.2.9 Video record from computer monitor 229
10.3.2.10 Configuring fisheye cameras 232
10.3.3 Configuring audio subsystem 233
10.3.3.1 General information on configuring audio subsystem 233
10.3.3.1.1 Audio digitizing devices 234
10.3.3.1.1.1 Video capture cards 234
10.3.3.1.1.2 Standard soundcards, microphones, loudspeakers and headphones 234
10.3.3.1.1.3 Multichannel audio capture devices 235
10.3.3.1.1.4 IP-devices 235
10.3.3.1.2 Configuring the digitization devices for audio signals 235
10.3.3.1.3 Digitized audio signal recording 235
10.3.3.1.4 Digital audio signal transmission to Remote Workstations and servers 236
10.3.3.1.5 Audio signal playback 236
10.3.3.2 Registration of audio cards and microphones in INTELLECT™ software 236
10.3.3.3 Configuring audio signals digitization and processing 236
10.3.3.3.1 Audio signals sample rate settings 236
10.3.3.3.2 Setting up the audio signal volume amplification 236
10.3.3.3.3 Setting up the Automatic Gain Control for sound cards of Olha line 237
10.3.3.4 Configuring audio signals recording 238
10.3.3.4.1 Audio signals recording modes 238
10.3.3.4.2 Selecting the disks for audio archive storage 239
10.3.3.4.3 Setting up the sound activated recording 240
10.3.3.4.4 Setting up the audio and video synchro recording 241
10.3.3.5 Configuring audio playback 242
10.3.3.5.1 Creating and configuring the Audio playback card object 242
10.3.3.5.2 Creating and configuring the Speaker object 243
10.3.3.6 Features of standard sound card use 244

10.3.3.6.1 General information on standard sound cards 244
10.3.3.6.2 Features of standard sound card setup 244
10.3.3.7 Using multi-channel audio capture devices 246
10.3.3.7.1 General information on multi-channel audio capture devices 246
10.3.3.7.2 Setting up multi-channel audio capture devices 246
10.3.3.8 Using IP-devices 247
10.3.3.8.1 General information on IP-devices 247
10.3.3.8.2 Setting up the transmission of video signals to IP-devices 247
10.3.3.8.3 Setting up the transmission of audio signals to IP-device Bosch 248
10.3.3.8.4 Setting up the transmission of duplex audio signals to IP-devices 251
10.3.4 Configuring events logging 251
10.3.5 Configuring the Event Viewer databases synchronization 253
10.3.5.1 General information on the Event Viewer databases synchronization 253
10.3.5.2 Configuring the Event Viewer database synchronization 253
10.3.5.3 Example of macro to start the Event Viewer databases synchronization 254
10.3.6 Configuring telemetry 255
10.3.7 Configuring operation of distributed architecture in the failover mode 255
10.3.7.1 General information about Failover mode 255
10.3.7.1.1 Purpose and features of the Failover mode 255
10.3.7.1.2 Examples of Failover system organization 256
10.3.7.1.2.1 1 main Server + standby Server 256
10.3.7.1.2.2 N main Servers + standby server 257
10.3.7.1.2.3 Two Servers being standby for each other 258
10.3.7.1.3 Limitations of the Failover mode 258
10.3.7.2 Configuring Failover mode 260
10.3.7.3 Limiting number of failovers running simultaneously 262
10.3.7.4 Configuring archive synchronization of main and backup Servers 262
10.3.8 Configuring the SNMP-service 264
10.3.8.1 SNMP service setting order 264
10.3.8.2 Creating the SNMP trap object 264
10.3.8.3 Events selection for transmitting to SNMP manager 266
10.3.8.4 Configuring the message conversion into SNMP format 267
10.3.8.5 Setting up the trap with SNMP-message 269
10.3.8.6 SNMP configuration for traps receiving on remote computer 270
10.3.9 Setting up and connecting the special keyboard 270

10.3.9.1 Setting up the Keyboard object in INTELLECT™ software ... 270
10.3.9.2 Settings the interpretation rules of the Special keyboard layout by Intellect program complex ... 271
10.3.10 Configuring the System restart service ... 272
10.3.10.1 General information on the System restart service module ... 272
10.3.10.2 Activating the hardware control of workability ... 273
10.3.10.3 Configuring the software control of workability ... 273
10.3.10.4 Getting the information on memory consumption for processes ... 275
10.3.11 Configuring backup archiving ... 275
10.3.11.1 Purpose and implementation of backup archiving in the Intellect software ... 275
10.3.11.2 Configuring the Backup archive module ... 276
10.3.11.2.1 Configuration procedure for the Backup archive object ... 276
10.3.11.2.2 Creating the Backup archive object ... 276
10.3.11.2.3 Selecting and configuring the cameras for the Backup archive ... 277
10.3.11.2.4 Selecting cameras as a group for the Backup archive ... 278
10.3.11.2.5 Setting the parameters of video archive transmission over LAN ... 280
10.3.11.2.6 Selecting disks to store the archive of the Backup archive module ... 281
10.3.11.2.7 Configuring the scaling of the video archive ... 282
10.3.11.2.8 Configuring the schedule of the video archive copying ... 283
10.3.11.2.9 Enabling cooperation of Backup archive with Failover service ... 284
10.3.11.3 Configuring the Backup audio archive module ... 285
10.3.12 Configuring the Videogate module ... 288
10.3.12.1 General information on the videogate ... 288
10.3.12.2 Order of setting up the Videogate object ... 289
10.3.12.3 Creating the Videogate object ... 289
10.3.12.4 Selecting and configuring the cameras for the Videogate module ... 291
10.3.12.5 Selecting video cameras as a group for the Videogate module ... 292
10.3.12.6 Selecting disks for storing the archive of the Videogate module ... 294
10.3.12.7 Configuring the record of the Videogate module archive ... 296
10.3.13 Notification services ... 297
10.3.13.1 Setting up the Alarm Message window ... 297
10.3.13.1.1 General description and usage details of the Alarm Message window ... 297
10.3.13.1.2 Creating and setting up the Alarm Message Window object ... 297
10.3.13.2 Setting up the Short Message Service (SMS) ... 299
10.3.13.2.1 General description and usage details of the Short Message Service ... 299
10.3.13.2.2 Creating and setting up the Short Message Service object ... 299

10.3.13.2.3 Creating and setting up the short messages 300
10.3.13.2.4 Creating and setting up the macro for sending the short message 300
10.3.13.3 Setting up the Mail Message Service (E-mail) 301
10.3.13.3.1 General description and usage details of the Mail Message Service 301
10.3.13.3.2 Creating and setting up the Mail Message Service 302
10.3.13.3.3 Creating e-mail messages 303
10.3.13.3.4 Creating and setting up a macro for sending the e-mail message 303
10.3.13.4 Setting up the Voice Message Service (V-dial) 304
10.3.13.4.1 General information and usage details of the Voice Message Service 304
10.3.13.4.2 Creating and setting up the Voice Message Service object 304
10.3.13.4.3 Creating voice messages 305
10.3.13.4.4 Creating and setting up the macro for sending the voice message 306
10.3.13.5 Setting up the Voice Notification Service 306
10.3.13.5.1 General description and usage details of the Voice Notification Service (VNS) 306
10.3.13.5.2 Creating and setting up the Voice Notification Service object 307
10.3.13.5.3 Creating and setting up the macro for sending the voice notification 307
10.3.13.6 Setting up messaging via Telegram bot 308
10.3.13.6.1 Configuring the Intellect to Telegram messaging function 308
10.3.13.6.2 Example macros for sending messages to Telegram 309
10.3.14 Replicating archive from unconnected servers using the removable storage 310
10.3.14.1 Order of archive replication from unconnected servers 310
10.3.14.2 Configuring the Data replication service object 310
10.3.14.3 Configuring the Target objects tree for data replication 311
10.3.14.4 Creating the query file 312
10.3.14.5 Copying the archive from the Source 312
10.3.14.6 Restoring the archive on the Target 313
10.3.15 Configuring the Web-server module 314
10.3.15.1 General description of the Web-server module 314
10.3.15.2 System requirements 315
10.3.15.3 Installing Java Runtime Environment 315
10.3.15.4 Authorization on the Web-server home page 316
10.3.15.5 Starting and setting up the Web-server module 317
10.3.15.6 Configuring the videoserver to connect Clients via the Web-server module 317
10.3.15.6.1 Creating the Web-server object 317
10.3.15.6.2 Selecting and configuring cameras for the Web-server module 319

10.3.15.6.3 Bulk selecting and configuring cameras for Web-server ... 320
10.3.15.6.4 Setting the parameters of connecting Clients to the Web-server ... 322
10.3.15.6.5 Configuring the authorization for the Web-server module. Default user ... 323
10.3.15.6.6 Enabling the processing of SDC (ECHD) requests and selecting the RTSP server ... 324
10.3.15.6.7 Configuring PTZ control priority for Web-server ... 325
10.3.15.7 Configuring the server for the clients connection via the Web-server 2.0 module ... 326
10.3.15.7.1 Creating the Web-server 2.0 object ... 326
10.3.15.7.2 Configuring the Events filter for the Web-server 2.0 module ... 327
10.3.15.7.3 Using the Web-server settings for the Web-server 2.0 module ... 328
10.3.15.7.4 Selecting maps ... 328
10.3.15.7.5 Applying changes of the user rights ... 329
10.3.15.7.6 Network settings of the Web Server 2.0 module ... 330
10.3.15.7.6.1 Changing the network interface used by the Web Server 2.0 module ... 330
10.3.15.7.6.2 Changing the port used by the Web Server 2.0 module ... 331
10.3.15.7.7 Configuring default response type for HTTP API requests ... 331
10.3.15.8 Web-server home page template and Java applet settings ... 331
10.3.15.9 Setting up the surveillance monitor interface of the Web-server module ... 333
10.3.15.10 Setting up the display of the data for traffic estimation in the Web-server ... 334
10.3.15.11 Setting up the Web-server module to act as a gate on a different HTTP-server ... 334
10.3.15.12 Change of certificates of push-notifications for the Web-server 2.0 module ... 334
10.3.16 Configuring RTSP Server module ... 335
10.3.17 Counting the system events ... 341
10.3.17.1 General Information on counting the system events ... 341
10.3.17.2 Configuring the Event Counter ... 341
10.3.17.3 Data output and counter control ... 342
10.3.18 Configuring PS-RTP server ... 343
10.3.19 Configuring ONVIF-Server module ... 346
10.3.19.1 General information about ONVIF-Server module ... 346
10.3.19.2 Configuring ONVIF-Server object ... 346
10.3.19.3 Configuring getting video using ONVIF-Server module ... 348
10.3.19.4 Features of embedded storage operation via ONVIF-Server ... 349
10.3.19.5 Filtering the ONVIF-Server events ... 350
10.3.19.6 Configuring ONVIF-Server module for the Multicast mode ... 353
10.3.20 Configuring integration with third-party systems ... 356
10.3.20.1 Configuring interaction with Manitou software ... 356

10.3.20.2 Configuring the integration with VideoIntellect software ... 358
10.3.20.2.1 Setting up the connection to VideoIntellect ... 358
10.3.20.2.2 Setting up the detector triggering reception from VideoIntellect ... 359
10.3.20.3 Configuring integration with VideoGuard system ... 359
10.3.20.4 Configuring BACnet integration ... 361
10.3.21 Configuring SIP-devices ... 362
10.3.21.1 Selecting the SIP-terminal type ... 363
10.3.21.2 Configuring the Intellect SIP-server ... 364
10.3.21.2.1 Network settings of the Intellect's SIP-server ... 364
10.3.21.2.2 Configuring SIP-device connection to Intellect SIP-server ... 364
10.3.21.2.2.1 Configuring the SIP-device ... 365
10.3.21.2.2.2 Configuring the SIP-device connection to Intellect ... 365
10.3.21.2.2.3 Configuring the tone DTMF commands ... 366
10.3.21.2.3 Configuring SIP operators on Intellect SIP-server ... 367
10.3.21.3 Configuring the Intellect SIP-client ... 368
10.3.21.3.1 Network settings of the Intellect's SIP-client ... 368
10.3.21.3.2 Configuring SIP-devices on the Intellect's SIP-client ... 368
10.3.21.3.3 Configuring SIP-operators on the Intellect's SIP-client ... 369
10.3.21.4 Configuring special numbers of Intellect's SIP-terminal ... 371
10.3.21.5 Configuring numbers of Intellect's SIP-terminal ... 372
10.3.21.6 Macros for working with SIP-devices ... 374
10.3.21.7 Selecting speaker, microphone and camera for SIP operator ... 374
10.3.21.8 Selecting the default SIP-operator ... 375
10.4 Configuration of interfaces ... 376
10.4.1 Intellect Software System's interface language ... 376
10.4.1.1 Installing the language ... 377
10.4.1.2 Switching languages in the Intellect Software System ... 378
10.4.2 Configuring the user interface ... 379
10.4.2.1 The user interface in the Intellect software ... 379
10.4.2.2 Setup procedure for the displays ... 379
10.4.2.3 Creating a Display object ... 379
10.4.2.4 Placing the interface components on the screen ... 381
10.4.2.5 Assigning the displays to the operator workstations ... 382
10.4.2.5.1 Assigning displays manually ... 382
10.4.2.5.2 Assigning displays via Wizard ... 383

10.4.2.6 Examples of the user interface configuration 383
10.4.3 Configuration of video display 384
10.4.3.1 Configuring video display on Video Surveillance Monitor 384
10.4.3.1.1 General information on video signal displaying 384
10.4.3.1.2 Video monitor setup sequence 385
10.4.3.1.3 Creating the Monitor object 385
10.4.3.1.4 Selecting the parameters of the Monitor interface box 386
10.4.3.1.5 Selecting and configuring video cameras 389
10.4.3.1.6 Selecting and configuring video cameras as a package 392
10.4.3.1.7 Configuring an auto select of video stream for displaying 394
10.4.3.1.8 Configuring the display mode for camera boxes 395
10.4.3.1.9 Selecting the display mode 397
10.4.3.1.10 Setting the Telemetry control priority using the Monitor object 398
10.4.3.1.11 Configuring the captions showing 399
10.4.3.1.11.1 Enabling the captions showing 399
10.4.3.1.11.2 Configuring captions display on a video image 400
10.4.3.1.12 Binding Audio player to the Monitor 402
10.4.3.1.13 Configuring a rotation angle of video image 402
10.4.3.1.14 Configuring Video surveillance windows interface 403
10.4.3.2 Configuring object's panoramic view by means of the Scene object 404
10.4.3.2.1 Creating the Scene object 405
10.4.3.2.2 Setting the parameters of the Scene interface box 405
10.4.3.2.3 Selecting and configuring cameras for the Scene object 406
10.4.3.3 Configuring video transmission to Remote Workstations 408
10.4.4 Configuration of audio 409
10.4.4.1 Configuring audio signals playback using the video monitor 409
10.4.4.2 Configuring audio signals playback using the Audio player object 409
10.4.4.2.1 Audio player setup sequence 409
10.4.4.2.2 Creating the Audio player object 410
10.4.4.2.3 Setting the parameters of the Audio player interface box 411
10.4.4.2.4 Setting up the recording and audio signals' playback 412
10.4.4.3 Features of audio signals export using the video monitor 414
10.4.4.4 Setting up the audio signal transmission to Remote Workstations and servers 414
10.4.5 Configuring the interactive map for object state indication and controlling the objects 415
10.4.5.1 General information on the structure of the interactive map of the guarded location 415

10.4.5.2 Configuring the interactive map ... 415
10.4.5.2.1 Setup procedure for the interactive map ... 415
10.4.5.2.2 Setting up the location of the map on the screen ... 416
10.4.5.2.3 Creating the layers of the interactive map ... 416
10.4.5.2.3.1 Configuring the external map server ... 421
10.4.5.2.4 Attaching objects to the layers of interactive map ... 422
10.4.5.2.5 Operations with objects in the Map editor utility ... 426
10.4.5.2.5.1 Operations with the objects, added to the layer ... 426
10.4.5.2.5.2 Editing the additional data and type of object's displaying ... 427
10.4.5.2.5.3 Editing the font, color, background or frame size of object's name ... 429
10.4.5.2.5.4 Editing the object's size ... 429
10.4.5.2.5.5 Editing the position of object ... 430
10.4.5.2.5.6 Editing color and transparency (polygon and ellipsis) ... 432
10.4.5.2.5.7 Adding or removing apexes to polygon or polyline ... 432
10.4.5.2.5.8 Setting order of displaying objects on map ... 433
10.4.5.2.5.9 Configuring object states displaying ... 434
10.4.5.2.6 Linking the layers of the interactive map ... 434
10.4.5.2.7 Cancelling the last action in Map editor ... 437
10.4.5.2.8 Configuring object ID is displaying ... 437
10.4.5.2.9 Editing object properties using the Properties panel ... 438
10.4.5.2.10 Configuring viewing Map editor utility ... 439
10.4.5.2.11 Searching object in the Map editor utility by its name and ID ... 439
10.4.5.3 Setting up the display of the alarm signals on multilevel maps ... 440
10.4.5.4 Configuring the smoothing method of the Map when scaling ... 441
10.4.5.5 Configuring the number of events displayed in the Map window ... 442
10.4.5.6 Configuring the event tooltips ... 442
10.4.5.7 Configuring the order of reactions in the object menu ... 443
10.4.5.8 Enabling the frame or video request function ... 444
10.4.6 Configuring the Backup archive panel object ... 445
10.4.7 Configuring the Operator protocol interface object ... 445
10.4.7.1 Creating the Operator protocol object ... 446
10.4.7.2 Configuring the position of the Operator protocol object ... 447
10.4.7.3 Setting up the event filter for the Operator protocol ... 447
10.4.7.4 Setting the options for handling events in the Operator protocol ... 449
10.4.7.5 Configuring the checklist ... 450
10.4.7.6 Configuring the Operator protocol interface ... 451

10.4.7.7 Connecting external DBs 451
10.4.7.7.1 Connecting an external configuration database 451
10.4.7.7.2 Connecting an external Event protocol database 452
10.4.7.7.3 Configuring the database server connection in a dialog mode 453
10.4.8 Configuring the Event Viewer interface object 455
10.4.8.1 Order of configuring the Event Viewer interface object 455
10.4.8.2 Configuring event filters for displaying in the Event viewer 455
10.4.8.3 Event viewer parameters 457
10.4.8.4 Parameters of displaying the Event Viewer interface box 458
10.4.9 Setting up the sound switch 460
10.4.9.1 Creating and configuring the Live sound switch object 460
10.4.9.2 Using the Live sound switch object 462
10.4.10 Setting up the Captions search window 463
10.4.10.1 The Captions search window setup procedure 463
10.4.10.2 Selecting the captioners 463
10.4.10.3 Specifying the captions search parameters 464
10.4.10.4 Setting up the Captions search window displaying 465
10.4.11 Configuring HTML interface 467
10.4.11.1 General description of HTML interface in Intellect software 467
10.4.11.2 Procedure of HTML interface configuring 467
10.4.11.3 Creating HTML interface object and setting its position 468
10.4.11.4 Creating and configuring the HTML page object 469
10.4.11.4.1 Creating the HTML page object 469
10.4.11.4.2 Open web-page by URL 469
10.4.11.4.3 Loading file from disk and saving to disk 470
10.4.11.4.4 Link to the HTML page object 471
10.4.11.5 Selecting start page for displaying in HTML interface 472
10.4.11.6 Selecting objects to track their states 472
10.4.11.7 Changing the displayed version of Internet Explorer 473
10.4.12 Setting up the voice notification 474
10.4.12.1 Setting up the voice notification using Audio player object 475
10.4.12.2 Setting up the voice notification using Sound notification object 475
10.4.13 Configuring the Display manager 476
10.4.14 Configuring the State statistics display 478
10.4.14.1 Configuring the State statistics window position on the screen 478

10.4.14.2 Selecting the objects to be included in State statistics and configuring the pixels number 479
10.4.14.3 Configuring the database connection 480
10.4.14.4 Configuring the interface parameters of the State statistics window 481
10.4.15 Configuring the Charts to display analog sensor readings 482
10.4.15.1 Setting the Charts window position on the screen 483
10.4.15.2 Configuring the chart display 484
10.4.16 Configuring the SIP Panel interface object 485
10.5 Configuration of users and permissions 486
10.5.1 Rights administration 486
10.5.1.1 The users' rights 486
10.5.1.2 User registration and removal 486
10.5.1.2.1 General information about user registration in Intellect software 486
10.5.1.2.2 User registration procedure 486
10.5.1.2.3 Administrator password registration 487
10.5.1.2.4 Department registration 488
10.5.1.2.5 Registration of Operator accounts 488
10.5.1.2.6 Removing user accounts 490
10.5.1.3 Registration of users' rights 490
10.5.1.3.1 Registration of operator rights 490
10.5.1.3.2 General information on the limits to the administrative functions 491
10.5.1.3.3 Limiting access to the tabs of the System Settings window 492
10.5.1.3.4 Limiting access to the system objects administration, control and viewing functions 492
10.5.1.3.5 Limiting access to shutting the system down 494
10.5.1.3.6 Limiting the rights to hide the interface components 495
10.5.1.3.7 Permissions for working with archives 496
10.5.1.3.7.1 Limiting access to archive playback 496
10.5.1.3.7.2 Limiting access to Backup archive playback 497
10.5.1.3.7.3 Permission protecting archive files from rewriting 498
10.5.1.3.7.4 Permissions for export and printout 499
10.5.1.3.7.5 Permissions to the hidden archive 500
10.5.1.3.7.6 Permission to remove archive video files 500
10.5.1.3.8 Configuring session auto termination when user is inactive 501
10.5.1.3.9 Configuring rights to use ONVIF Server 502
10.5.1.3.10 Combining (importing) permissions 503
10.5.1.3.11 Limiting access to sending commands (reactions) 504

10.5.1.4 Assigning the rights and password to operators for authorization in the Intellect ... 505
10.5.1.5 Setting up the default user ... 507
10.5.2 Configuration of the LDAP Service ... 508
10.5.2.1 General information about the LDAP Service module ... 508
10.5.2.2 Configuring the connection to the LDAP address book ... 509
10.5.2.3 Configuration of correspondence between address attributes and Intellect DB fields ... 510
10.5.2.4 Examples of LDAP Service configuration ... 511
10.5.2.5 Example macro for user import from LDAP address book ... 512
10.5.3 Active Directory configuration ... 513
10.5.3.1 General information about Active Directory and Intellect operation ... 513
10.5.3.2 Connecting the Intellect and Active Directory users ... 513
10.5.3.3 Connecting the Intellect user permissions to Active Directory groups ... 514
10.5.3.4 Starting the Active Directory synchronization ... 515
10.5.4 Configuring two-factor authentication ... 516
10.6 System settings (the Programming tab) ... 517
10.6.1 Configuring internal synchronization ... 517
10.6.2 Connection of objects with cameras ... 518
10.6.3 Creating and configuring Macro events ... 519
10.6.3.1 Configuring the macro events ... 520
10.6.3.2 Example of macro event ... 522
10.6.4 Creating and using macros ... 523
10.6.4.1 Creating macros ... 523
10.6.4.2 Examples of macros ... 528
10.6.5 Creating and using the Timer object ... 529
10.6.5.1 Creating and configuring the Timer object ... 529
10.6.5.2 Using the Timer object ... 531
10.6.6 Creating and using time schedules ... 533
10.6.6.1 Creating and configuring time schedules ... 533
10.6.6.2 Viewing time schedules states ... 538
10.6.6.3 Examples of time schedules usage ... 539
10.6.7 Subdivision of the guarded location into areas and regions ... 541
10.6.7.1 About areas and regions ... 541
10.6.7.2 Creating areas ... 541
10.6.7.3 Creating regions ... 542
10.6.7.4 Creating rules of states transition ... 544

10.6.7.5 Examples of using areas and regions ... 545
11 The Report System ... 548
11.1 General information on the Report System ... 548
11.2 Starting and shutting-down the Report system ... 548
11.2.1 Starting the Report system ... 548
11.2.2 Shutting-down the Report system ... 549
11.3 The Report window ... 550
11.3.1 The OptionsForm window ... 552
11.4 Connecting to databases ... 554
11.4.1 Connecting to the main database of the Intellect system ... 554
11.4.1.1 Selecting an Access database and setting up the connection ... 555
11.4.1.2 Selecting an SQL database and setting up its parameters ... 558
11.4.2 Connecting to the Events Log (PROTOCOL table) ... 564
11.5 Manual loading of the configuration and registered events from the database ... 565
11.6 Viewing the general information on the events in the database ... 566
11.7 Creating the log of changes made to the system configuration ... 567
11.8 Using the report templates in the Report system ... 569
11.8.1 Recommendations for template creation ... 569
11.8.2 Creating a report template ... 569
11.8.3 Deleting the report templates ... 571
11.9 Using screen and printed reports ... 571
11.9.1 Creating a screen report ... 571
11.9.1.1 Creating a screen report from the report template ... 573
11.9.2 Creating a printed report ... 574
11.9.2.1 Creating a printed report from a report template ... 576
11.9.3 Printing the report ... 578
11.9.4 Exporting the report to a file ... 579
11.10 Video recording playback from the Report system ... 581
11.10.1 Playback of the video recordings from the Report system ... 581
11.10.2 Selecting the playback mode of video recordings ... 583
11.11 Filtering the events in the screen report according to the additional information ... 584
11.12 The keyboard shortcuts list ... 584
12 Administrator's Guide. Conclusion ... 586
13 Appendices ... 587

13.1 Appendix 1. Interface 587
13.1.1 Description of the Main Control Panel Interface 587
13.1.2 Description of the System settings dialog box 587
13.1.2.1 Tabs panel 587
13.1.2.2 Object tree 588
13.1.2.3 Context menu of the system object 589
13.1.2.3.1 The Create object function 589
13.1.2.3.2 The Change parameter function 590
13.1.2.3.3 The Camera discovery tool function 591
13.1.2.3.4 The Delete object function 591
13.1.2.3.5 The Create folder function 591
13.1.2.3.6 The Move to folder function 593
13.1.2.3.7 The Save function 594
13.1.2.3.8 The Find function 595
13.1.2.3.9 The Reconnect function 597
13.1.2.3.10 The Send key to all function 598
13.1.2.3.11 The Send key function 599
13.1.2.3.12 The Save configuration function 600
13.1.2.3.13 The Load configuration function 600
13.1.2.3.14 Collapsing the tree 601
13.1.2.3.15 Expanding the tree 602
13.1.2.4 The Object setting panel 603
13.1.2.5 The Apply and Cancel buttons 606
13.1.2.6 The elements of the System settings dialog box 607
13.1.2.7 The Architecture tab 608
13.1.2.7.1 Connection settings table 608
13.1.2.8 The Hardware tab 609
13.1.2.8.1 Hardware tab components 609
13.1.2.8.2 The Settings panel of the Computer object 609
13.1.2.8.3 The Settings panel of the Video Capture Device object 614
13.1.2.8.4 The Settings panel of the Camera object 617
13.1.2.8.5 The Settings panel of the Detection zone object 630
13.1.2.8.6 The Settings panel of the Audio card object 633
13.1.2.8.7 The Settings panel of the Microphone object 635
13.1.2.8.8 The Settings panel of the Telemetry controller object 638

13.1.2.8.9 The Settings panel of the PTZ device object 640
13.1.2.8.10 The Settings panel of the Control panel object 644
13.1.2.8.11 The Settings panel of the Backup archive object 645
13.1.2.8.12 The Settings panel of the Keyboard object 649
13.1.2.8.13 The Settings panel of the System restart service object 651
13.1.2.8.14 The Settings panel of the Voice Notification Service object 653
13.1.2.8.15 The Settings panel of the Voice Message Service object 655
13.1.2.8.16 The Settings panel of the Voice message object 656
13.1.2.8.17 The Settings panel of the Short Message Service object 658
13.1.2.8.18 The Settings panel of the Short Message object 658
13.1.2.8.19 The Settings panel of the Mail Message Service object 660
13.1.2.8.20 The Settings panel of the Mail Message object 661
13.1.2.8.21 The Settings panel of the Web-server object 664
13.1.2.8.22 The Settings panel of the RTSP Server object 669
13.1.2.8.23 The Settings panel of the Operator query panel object 673
13.1.2.8.24 The Settings panel of the Alarm Message Window object 675
13.1.2.8.25 The Settings panel of the Videogate object 676
13.1.2.8.26 The Settings panel of the Event Counter object 678
13.1.2.8.27 The Settings panel of the Data replication service object 682
13.1.2.8.28 The Settings panel of the Failover service object 682
13.1.2.8.29 The Settings panel of the Backup audio archive object 684
13.1.2.8.30 The Settings panel of the Web Server 2.0 object 685
13.1.2.8.31 The Settings panel of the Edge storage object 687
13.1.2.8.32 The Settings panel of the RS-RTP server object 688
13.1.2.8.33 The Settings panel of the ONVIF-Server object 692
13.1.2.8.34 The Settings panel of the ONVIF-Server Profile object 696
13.1.2.8.35 The Settings panel of the Telegram bot object 698
13.1.2.8.36 The Settings panel of the SIP-terminal object 699
13.1.2.8.37 The Settings panel of the SIP-device object 704
13.1.2.8.38 The Settings panel of the SIP-operator object 708
13.1.2.9 The Interfaces tab 710
13.1.2.9.1 Interfaces tab components 710
13.1.2.9.2 The Settings panel of the Display object 710
13.1.2.9.3 The Settings panel of the Monitor object 711
13.1.2.9.4 The Settings panel of the Audio player object 721

13.1.2.9.5 The Settings panel of the Telemetry control panel object ... 724
13.1.2.9.6 The Settings panel of the Backup archive panel object ... 727
13.1.2.9.7 The Settings panel of the Map object ... 728
13.1.2.9.8 The Settings panel of the Layer object ... 733
13.1.2.9.9 The Settings panel of the Event viewer object ... 735
13.1.2.9.10 The Settings panel of the Operator protocol object ... 739
13.1.2.9.11 The Settings panel of the External window object ... 746
13.1.2.9.12 The Settings panel of the Scene object ... 748
13.1.2.9.13 The settings panel of the HTML Interface object ... 750
13.1.2.9.14 The settings panel of the HTML page object ... 752
13.1.2.9.15 The Settings panel of the Display manager object ... 753
13.1.2.9.16 The Settings panel of the State statistics object ... 755
13.1.2.9.17 The Settings panel of the Charts object ... 759
13.1.2.9.18 The Settings panel of the SIP-panel object ... 761
13.1.2.10 The Programming tab ... 763
13.1.2.10.1 The Settings panel of the Security zone object ... 763
13.1.2.10.2 The Settings panel of the Macro object ... 767
13.1.2.10.3 The Settings panel of the Program object ... 772
13.1.2.10.4 The Settings panel of the Time schedule object ... 773
13.1.2.10.5 The Settings panel of the Script object ... 776
13.1.2.10.6 The Settings panel of the Region object ... 778
13.1.2.10.7 The Settings panel of the Rule of states transition object ... 779
13.1.2.10.8 The Settings panel of the Macro event object ... 781
13.1.2.11 The Users tab ... 783
13.1.2.11.1 The Users tab components ... 783
13.1.2.11.2 The Settings panel of the Department object ... 783
13.1.2.11.3 The Settings panel of the User object ... 784
13.1.2.11.4 The Settings panel of the User permissions object ... 786
13.1.3 Information about program ... 789
13.2 Appendix 2. Relevant information on using Windows operating system ... 790
13.2.1 Working with Windows OS registry ... 790
13.2.1.1 General information about Windows OS registry ... 790
13.2.1.2 Using the registry editor ... 792
13.2.1.2.1 Starting and shutting-down the editor ... 792
13.2.1.2.2 Interface elements of the registry editor ... 793

13.2.1.2.3 Navigating the registry tree ... 794
13.2.1.3 Adding string parameters to the registry ... 794
13.2.1.4 Modifying the value of string parameters in Windows OS registry ... 797
13.2.1.5 Deleting parameters from the Windows OS registry ... 799
13.2.1.6 Configuring network drives visibility when UAC is enabled in Windows OS ... 801
13.2.2 Connecting network disks in Windows Vista and Windows 7 OS ... 803
13.2.3 Setting up serial (COM) ports in Windows ... 803
13.2.4 Working with Windows OS services for operating Intellect™ installed as a Service ... 804
13.2.4.1 General information on Intellect™ operation as a Service ... 804
13.2.4.2 Configuring the restart of the ITV Intellect Core Server service ... 805
13.2.4.3 Using network disks of INTELLECT™ installed as a Service ... 806
13.2.4.4 Enabling INTELLECT™ as a Service startup ... 806
13.2.4.5 Disabling INTELLECT™ as a Service startup ... 806
13.2.4.6 Configuring INTELLECT™ as a Service to work with Active Directory (AD) ... 807
13.2.5 The list of TCP ports used in INTELLECT™ ... 808
13.2.5.1 ACFA subsystem ... 814
13.2.6 Configuring Windows Firewall ... 820
13.2.7 Disable the Data execution prevention (DEP) function for Intellect software package ... 820
13.2.8 Configuring the best performance mode ... 822
13.2.9 Features of ElasticSearch service operation ... 823
13.2.9.1 Limiting RAM for Elasticsearch service ... 823
13.2.9.2 Running titles database update for restoration of ElasticSearch ... 824
13.3 Appendix 3. INTELLECT™ software database management ... 824
13.3.1 INTELLECT™ software database functions ... 824
13.3.2 Guidelines on INTELLECT ™ system database use ... 825
13.3.3 Converting the database from MS Access to MS SQL format ... 826
13.3.4 INTELLECT™ software database connection ... 831
13.3.5 Viewing INTELLECT™ software database ... 835
13.3.6 Moving Intellect configuration database to the latest version of MS SQL Server ... 840
13.3.7 Database synchronization setup ... 842
13.3.8 Stored procedures for adding or deleting a large number of objects ... 846
13.3.8.1 Running stored procedures ... 846
13.3.8.2 Examples of stored procedures use for adding or deleting Camera objects ... 847
13.3.8.3 Example of stored procedure use for adding Tracker objects ... 847
13.3.8.4 Example of stored procedure use for adding VMDA Detection objects ... 848

13.4 Appendix 4. Updating Java time zones for proper operation with archive in iOS client 848

1 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

1.1 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 guarded locations and operating various equipment.

1.2 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. Programming Guide (JScript).	

1.3 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.

1.4 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.

> **Note!**
>
> 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.

2 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

2.1 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.

2.2 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.

2.3 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.

2.4 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.

3 General description of the INTELLECT™ software

3.1 INTELLECT™ software functionality

On the page:

- Video surveillance functionality
- Audio monitoring functionality
- Structuring guarded objects
- Event registration functionality
- Notification functionalities
- Functions of workability control
- Management functionality
- Integration of the distributed video surveillance and audio monitoring system

This section provides information on the main basic user functions of the distributed digital video and audio surveillance system based on the INTELLECT™ software.
The INTELLECT™ software provides the following basic user functions:

3.1.1 Video surveillance functionality

1. Multiple camera/video servers split screen image simultaneously displayed on a single PC monitor.
2. Priority-oriented automatic selection of displayed video images from alarm or active cameras to bring the required scenes into Operator focus (selection of images depending on set parameters).
3. Flexible split screen configuration including the number of sources observed.
4. Priority window magnification (surveillance windows), magnified surveillance windows slideshow option for a selected camera.
5. Color coding of surveillance window (camera) state: “armed”, “alarm”, “recording”, etc.
6. Remote access to audiovisual streams from any workplace with both local and remote archive recording option.
7. Video recording can be performed:
    a. continuously;
    b. on schedule;
    c. on alarm with a pre-event recording option or by Operator’s command.
8. Pre-event video recording.
9. Freeze frame by Operator’s command selection and viewing, without interruption of the recording.
10. Image burn-in option.
    a. Current time;
    b. Current date;
    c. Camera No (ID).
11. Recording by Operator’s command.
12. Real time viewing of images from video cameras.
13. Priority-oriented viewing of critical video stream based on alarm detection.
14. Web interface-based surveillance.
15. Audio- and video-archive management.
16. Viewing of recorded video with search and retrieve options (time/event type/camera ID criteria).
17. Synchro playback of footage recorded by several cameras.
18. Recorded time calculation.
19. Timestamp based footage search.
20. Image processing:
    a. Digital zooming;

   b. Contrast maximizing;
   c. Image sharpening;
   d. masking;
   e. Dynamic outlining.

21. Management of end devices using:
   a. the 3rd party programmable interface panel;
   b. the universal control panel for end devices;
   c. a PC mouse;
   d. a joystick.

22. Viewing video server footage from any system workplace using the TCP/IP communications environment.
23. Storage and exporting of single frames and video sequences.
24. Integrated use of various types of multi-zone detectors:
   a. main motion detector;
   b. motion;
   c. focus loss;
   d. video signal stability;
   e. changes in the image background;
   f. light-struck camera lens;
   g. closing camera lens;
   h. infra-red

25. Detector zone(s) masking.
26. Image de-interlacing.
27. Analog video-signal output.

3.1.2 Audio monitoring functionality

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

3.1.3 Structuring guarded objects

1. Virtual subdividing of guarded objects.
2. Multilevel hierarchical object mapping to obtain:
   a. Automatic switching and recursive structural event analysis possibility;
   b. Graphical representation of active objects on the map (on different levels) for simple device control via the shortcut menu.

3.1.4 Event registration functionality

1. Event log maintenance.

3.1.5 Notification functionalities

1. Automatic notification using:
   a. SMS (Short Message Service);
   b. email;
   c. V-dial auto dialing service;
   d. Audible/voice notification.

3.1.6 Functions of workability control

1. Software control of workability - the "Restarting system service" object.

2. Hardware control of workability - Watchdog

3.1.7 Management functionality

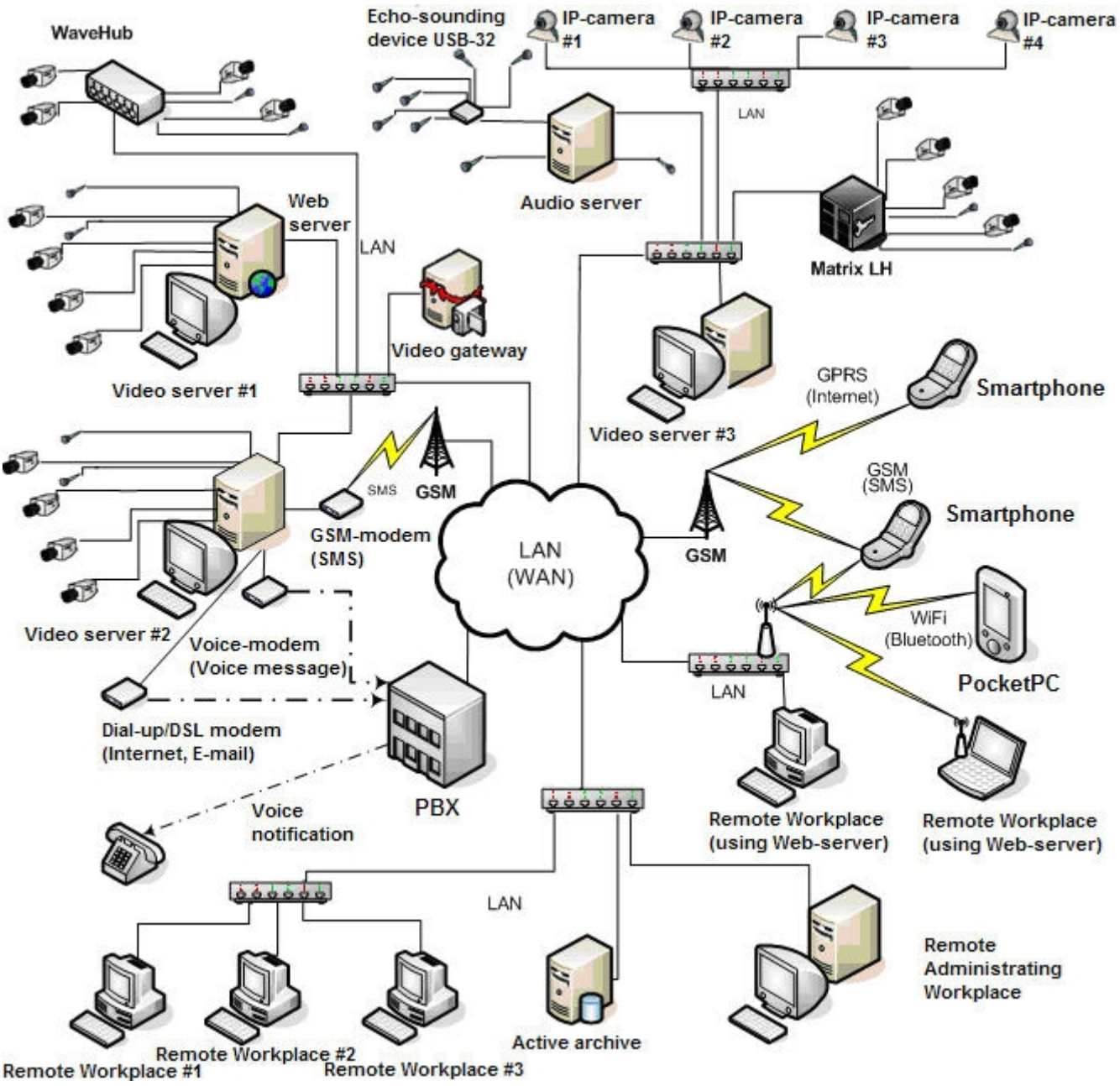
Macro commands programming of user specific functions.

3.1.8 Integration of the distributed video surveillance and audio monitoring system

1. Remote interaction of the software cores and automated replication of internal databases (containing system setup parameters and data about 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 system setup parameters and registered events, followed by their processing in compliance with standards and specialized adjustable algorithms, including generation of notifications and system responses.
3. Software-rogrammable optimization of video data flows within the distributed digital video surveillance system when there is a lack of channel capacity (optional videogate functionality).

3.2 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.



3.2.1 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.

3.2.2 Software

3.2.2.1 Operating system

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

3.2.2.2 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.

3.2.2.3 Program modules

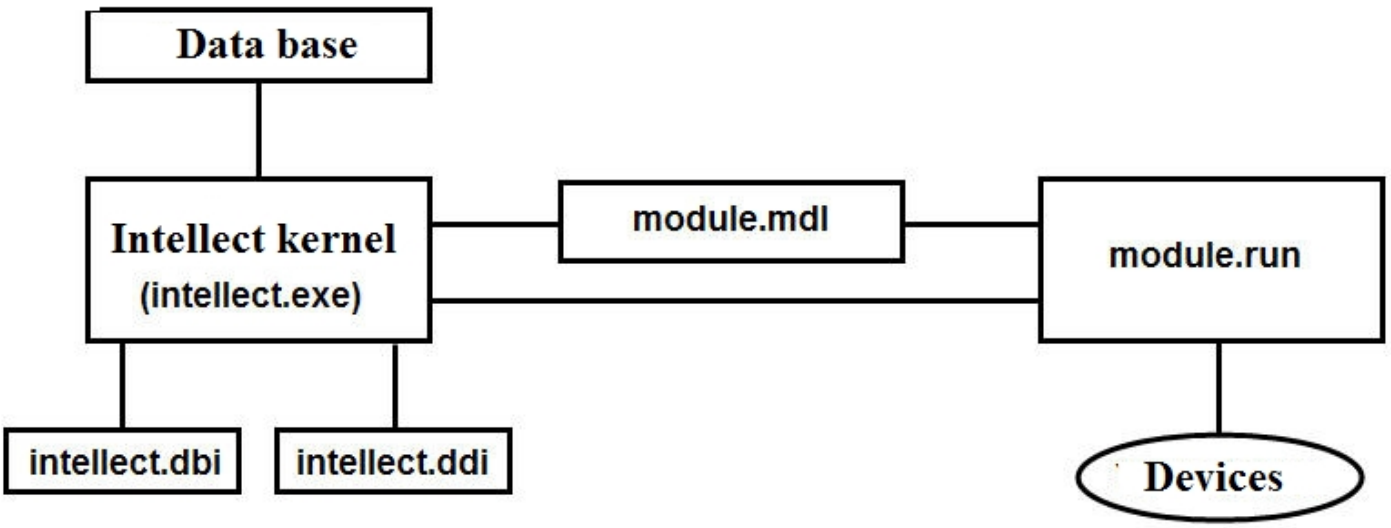
Program modules support direct interworking of the hardware, and also serve as a source of data about controllable objects. The software kernel of the system processes the incoming data from various program modules, providing their integration. The kernel sends ICMP packages to program modules every 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 executive file) will be launched.

3.2.2.4 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.

3.2.2.5 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;

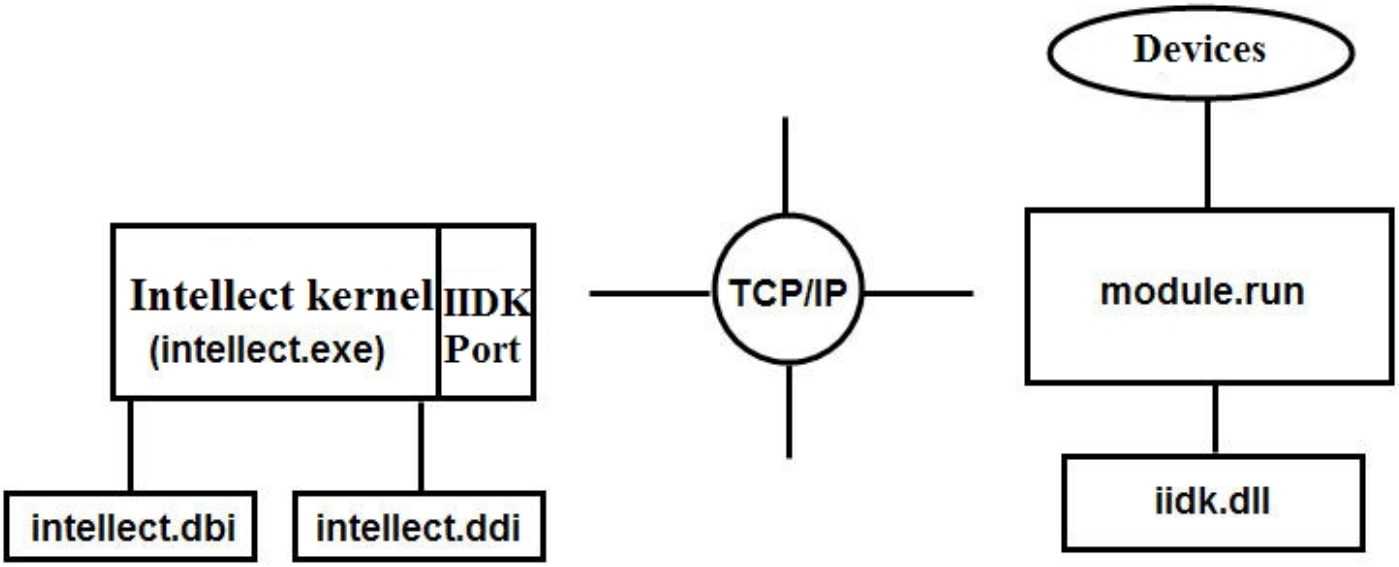
To enable the above mechanism, the **IIDK interface** object should be created in the Intellect software tree based on the **Computer** object at the stage of *Intellect* software configuration.

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.

3.2.3 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 is installed with Intellect software on default.To get information about technical features and limitations of free version see http://www.microsoft.com.

Note.

If an error occurs while installing Microsoft SQL Server 2008 R2 Express it is necessary to create “Repair.bat” file, following the instructions, given at the site “http://support.microsoft.com/kb/958043”.

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.

3.2.4 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.

3.3 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. Scaling on Videogate can be performed using MJPEG, Motion Wavelet, MPEG, H.264 and MxPeg codecs. If the scaling rate is 25 fps, then the first minute of video will be displayed at lower speed (~12 fps). For MXPeg codec the maximum allowed scaling 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. It is required to set digitizing rate equals to 8000, 16000 or 32000 if channels from FS 5\6\16- boards will be in use when configuring the LinuxHub audio card. Otherwise, receiving of audio from FS5\6\16 cards is not guaranteed. Any other rate can be set when the audio is to be received only from the embedded audio card.
30. 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.
31. Video displaying on Server using SC3B0N16 (WS216) and SC390N16 (WS16) cards is performed only with 352x288(PAL)/ 352x240(NTSC) resolution.
32. Only key frames are played back when the archive is played back fast in H264 and MPEG4 formats.
33. Video signals are not transferred to Intellect-based vertical modules using the Videogate module. These modules always receive video signal directly like other modules.

34. There is no sound transmission to the RMW via the Videogate if different subnets are in use.
35. 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.
36. Intellect does not support NVIDIA® Mosaic™ multi-display technology.

3.4 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).

3.5 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.

4 Requirements for the software and hardware platform

4.1 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.

4.1.1 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.

Minimal 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 the type of processor, which is installed.
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.		1	It is recommended to use 64-bit OS (Windows 7 x64 Ultimate, Windows 7 x64 Professional or Windows Server 2008 R2 x64) when total number of cores is more than 8. Processor supporting AVX instructions is required for the Tevian 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 + 20Gb 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 (not compulsory).
Video card	Discrete: Nvidia GeForce GT520 1GB RAM or more productive. On-board: Intel HD Graphics 530 or more productive.		1	Not compulsory, if the image is not required to be displayed on a monitor.
Audio card	Standard audio cards, MidiMan Delta, Comart Hera and Olkha 9P.		1	Not compulsory, 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	Not compulsory
OS	OS Windows supported versions (see Operating system requirements section).		1	Internet access is recommended to be switched off.
Architecture	x86, x64		-	-

Important!

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.

4.1.2 Operating system requirements

Intellect software is compatible both with 32 and 64 bit licensed versions of Microsoft Windows operating system. File system – NTFS.

Windows version	Supported architecture	Supported release	Note	
Windows Server 2008 R2 SP1 [3,4]	x64	Enterprise	OS edition, enabling to use all realized product features.	Full Installation type is supported.Server Core Installation type is not supported
		Datacenter	OS edition, enabling to use all realized product features.	
		Standard	OS edition, enabling to use all realized product features.	

Windows version	Supported architecture	Supported release	Note	
		Web	OS edition, enabling to use all realized product features.	
		HPC	OS edition, enabling to use all realized product features.	
		Foundation	OS edition, enabling to use all realized product features.	
Windows 7 SP1 [3]	x86, x64	Starter (x64 edition does not exist)	Restrictions, posed by OS edition (2GB of main memory, 1 physical processor, 1 monitor) - see. http://www.microsoft.com	
		Home Basic	Restrictions, posed by OS edition (1 physical processor) - see http://www.microsoft.com	
		Home Premium	Restrictions, posed by OS edition (1 physical processor) – see http://www.microsoft.comhttp://www.microsoft.com/	
		Professional	OS edition, enabling to use all realized product features.	
		Enterprise	OS edition, enabling to use all realized product features.	
		Ultimate	OS edition, enabling to use all realized product features.	
Windows Storage Server 2008 R2 SP1 [4]	x64	Essentials	Restrictions, imposed by OS release (1 physical processor) – see. http://www.microsoft.com	Full Installation type is supported.Server Core Installation type is not supported
		Workgroup	OS edition, enabling to use all realized product features.	
		Standard	OS edition, enabling to use all realized product features.	
		Enterprise	OS edition, enabling to use all realized product features.	
Windows Small Business Server 2011 SP1[4]	x64	Standard	OS edition, enabling to use all realized product features.	Full Installation type is supported.Server Core Installation type is not supported
		Essentials	OS edition, enabling to use all realized product features.	
		Premium Add-on	OS edition, enabling to use all realized product features.	
Windows Home Server 2011 SP1[4]	x64	-	OS edition, enabling to use all realized product features.	Full Installation type is supported.Server Core Installation type is not supported

Windows version	Supported architecture	Supported release	Note	
Windows Server 2012 [1,4]	x64	Foundation	Restrictions, posed by OS edition (1 physical processor) – see http://www.microsoft.com	Full Installation type is supported. Server Core Installation type is not supported.
		Essentials	Restrictions, posed by OS edition (2 physical processors) — see http://www.microsoft.com	
		Standard	OS edition, enabling to use all realized product features.	
		Datacenter	OS edition, enabling to use all realized product features.	
Windows Storage Server 2012 R2 [1,4]	x64	Standard	OS edition, enabling to use all realized product features.	
Windows 8 [3]	x86, x64	Windows 8 (Windows 8 Core)	OS edition, enabling to use all realized product features.	
		Windows 8 Pro	OS edition, enabling to use all realized product features.	
		Windows 8 Enterprise	OS edition, enabling to use all realized product features.	
Windows 8.1 [3]	x86, x64	Core	OS edition, enabling to use all realized product features.	
		Pro	OS edition, enabling to use all realized product features.	
		Enterprise	OS edition, enabling to use all realized product features.	
Windows Server 2012 R2 [1,4]	x64	Foundation	Restrictions, posed by OS edition (1 physical processor) – see http://www.microsoft.com	Full Installation type is supported. Server Core Installation type is not supported.
		Essentials	Restrictions, posed by OS edition (2 physical processors) — see http://www.microsoft.com	
		Standard	OS edition, enabling to use all realized product features.	
		Datacenter	OS edition, enabling to use all realized product features.	
Windows 10 [3]	x86, x64	Home	OS edition, enabling to use all realized product features.	
		Pro	OS edition, enabling to use all realized product features.	
		Enterprise	OS edition, enabling to use all realized product features.	
Windows Server 2016[1,4]	x64	Essentials	OS edition, enabling to use all realized product features.	
		Standard	OS edition, enabling to use all realized product features.	Full Installation type is supported. Server Core and Nano Core Installation types are not supported.
		Datacenter	OS edition, enabling to use all realized product features.	
Windows Server 2019[1,4]	x64	Standard	OS edition, enabling to use all realized product features.	
	x64	Datacenter	OS edition, enabling to use all realized product features.	

Windows version	Supported architecture	Supported release	Note
Windows 10 IoT [3]	x86, x64	Enterprise ***Attention! Core edition is not supported.***	OS edition, enabling to use all realized product features.

[1] The latest drivers are to be installed on video adapter for proper operation of interface objects in INTELLECT™ and vertical solutions in server OS.

[2] The *FACE-Intellect* is not compatible with this OS version

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

[4] 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.

Note.

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

Attention!

For stable and proper *Intellect* operation, the swap file (the size is selected according to system requirements) is to be enabled in OS.

Note.

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

Note.

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

4.1.3 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)					

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 (FS15) **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

4.1.4 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*

4.1.5 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

4.1.6 Define required disk space (VMDA metadata storage)

When using the forensic search in an archive the VMDA metadata storage is creating and configuring (see Creating and configuring VMDA metadata storage section).

Size of VMDA metadata storage depends on resolution, frame frequency, minimal and maximal object size, tracker sensibility).

It's possible to use the following formula to count the disk space to save database of object trajectory if record is performed round the clock

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

4.1.7 Intellect software working in virtual machines

Intellect software package supports working in the following virtual machines:

Virtual machine	Client OS	Additional information
VMWare Workstation 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 Moscow or your AxxonSoft branch or by contacting the technical consulting department at expert@itv.ru.

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.

4.2 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

4.2.1 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 secured site.

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

Communication mode	Link capacity	Black and white image			Color image		
		standard	high	full	standard	high	full
Ethernet	10 Mb/sec	71	53	39	64	51	38
Ethernet	100 Mb/sec	711	533	388	640	512	376
Ethernet	1 Gb/sec	7282	5461	3972	6554	5243	3855

*max. one surveillance camera, provided that maximum compression and/or image flow gapping is supported.

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.

4.2.2 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.

4.2.3 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.

4.3 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

4.4 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

4.5 Requirements for IP devices of audio and video input

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

> **Note.**
>
> The updated list of IP devices compitable with Intellect system and the range of IP device's functionalities supported by the *Intellect* system 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 section) and functions performed on the basis of these devices. For instance, virtual memory consumption (for video.run process) increases when VMDA detectors are in use (see Configuring smart video detection tools section). One camera with configured VMDA detector can use 30-40 Mb (depending on camera resolution) of virtual memory. At most 2 Gb of virtual memory is allocated for the video.run process. Enable 64-bit modules if more than 25 **Tracker** objects are to be used on one Server with video resolution higher than 800x600 (see the Configuring of using 64-bits modules section).

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 using the ONVIF protocol, it may be necessary to synchronize the time and the time zone between the Server and the device.
2. For the Intellect with 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 bit rate at 8 or 12 Kb/s, if the digitizing rate is 8 kHz: the bite rate should be 16, 24, 32, 48 or 64 Kb.
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 update drivers and codecs , taking into account the changed distributive structure, irrespective of the general Intellect version update.

4.6 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.

4.7 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.

4.8 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.

4.9 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.

4.10 Requirements for BIOS

Processor's operation frequency is important for the productivity of the *Intellect* software, especially for video decoding. The higher frequency, the higher productivity of the *Intellect* software on this platform.

The energy saving mode is activated on default in BIOS on modern computers. Usage of this mode on multiprocessor system leads to partial load of CPU cores and reduces productivity of I/O subsystem.

So for more productivity of the *Intellect* software configure BIOS as follows:

1. Disable all Enhanced Intel SpeedStep (EIST) technologies.
2. Disable saving modes by customizing settings of maximum capacity.
3. Disable "green" technologies, such as Energy saving, Turbo boost, Smart throttling.

Note.

Different vendors of motherboards name such technologies the different way. So for each model of motherboard it's required to specify technology name in the corresponding documentation.

4.11 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	+	+	+
Fire detection	+	+	+
Stopped vehicle detection	+	-	-
People counter detection	+	-	-
Train detection	+	-	-
Glow detection	+	-	-
Sweethearting detection	+	+	+
Barcode detection	+	-	-
Fluid level detection	+	-	-
Neurotracker	+	+	+
Person location tracker	+	+	+
Face-Intellect			
Face detection with any external capture	+	-	-
Auto-Intellect			
Any LPR module	+	-	-

5 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.

6 Installing and removing INTELLECT™ software

6.1 Installing INTELLECT™ software

6.1.1 Description of INTELLECT™ software distribution package

INTELLECT™ software is offered as a software installation package (distribution package) on a compact disk.



The distribution disk (software bundle) contains all software components necessary for the installation of INTELLECT™ software on the base PC.

The software is made operable with the intellect.sec key file. The key file is a part of the software bundle and can be found in the Key folder on the CD. 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™ software as a Server/Administrator's workplace
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

File or folder	Description
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.

6.1.2 Getting ready for Intellect installation

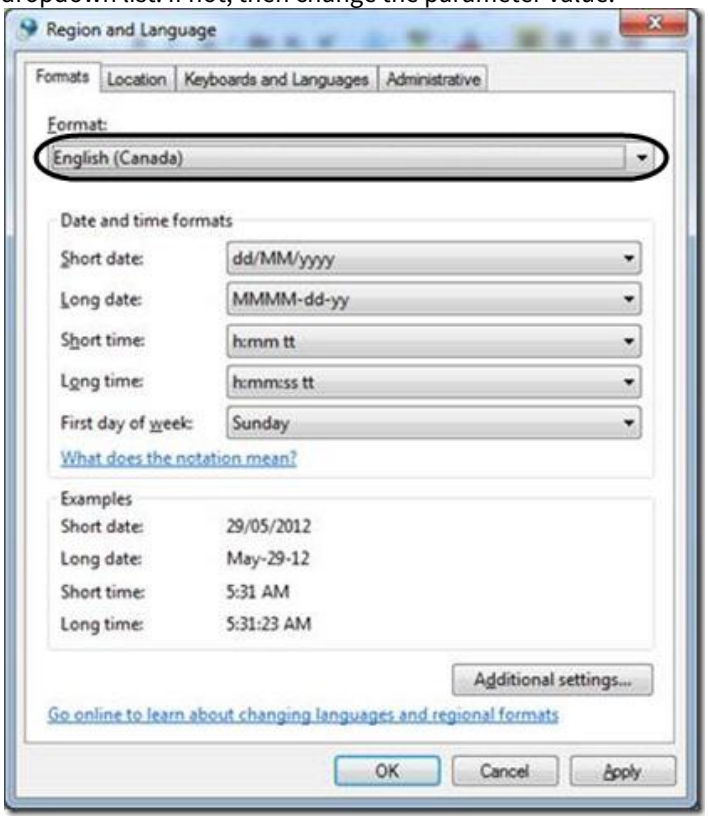
On the page:

- OS language settings
- Unblocking a distribution kit downloaded from the Internet
- System settings

6.1.2.1 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:

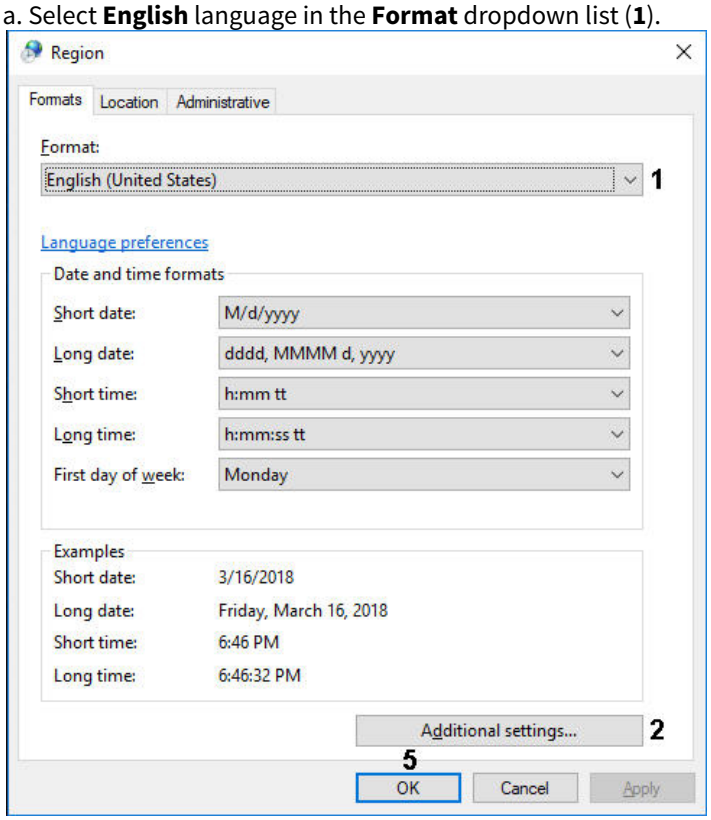
1. Go to the **Start – Control Panel – Regional and Language Options** menu. The **Regional and Language Options** window is displayed.
2. Go to the **Formats** tab. Make sure that the language that is used for Intellect installation is selected in the **Format** dropdown list. If not, then change the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



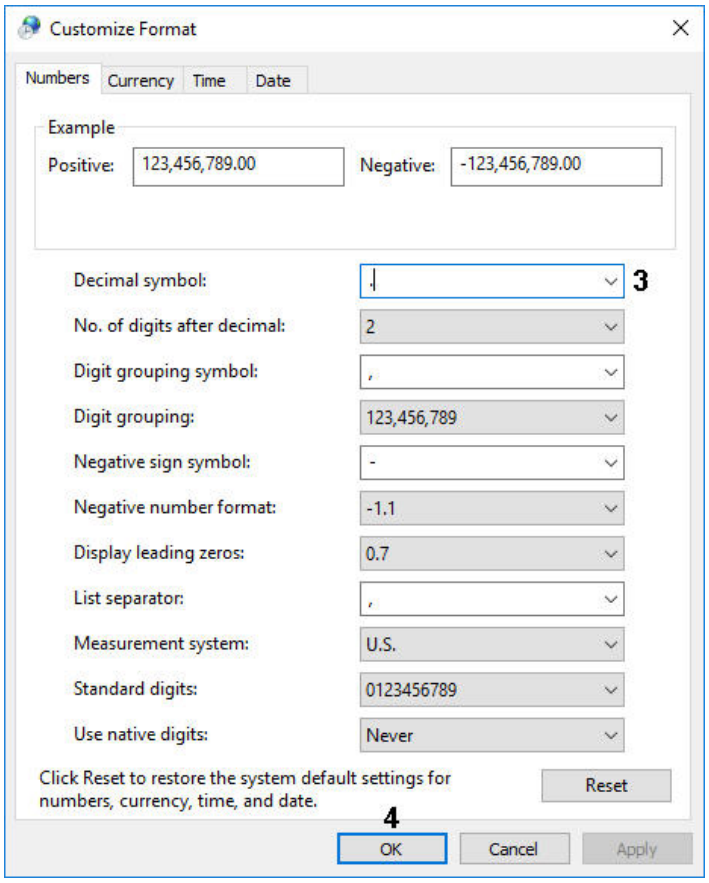
Important!

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**).

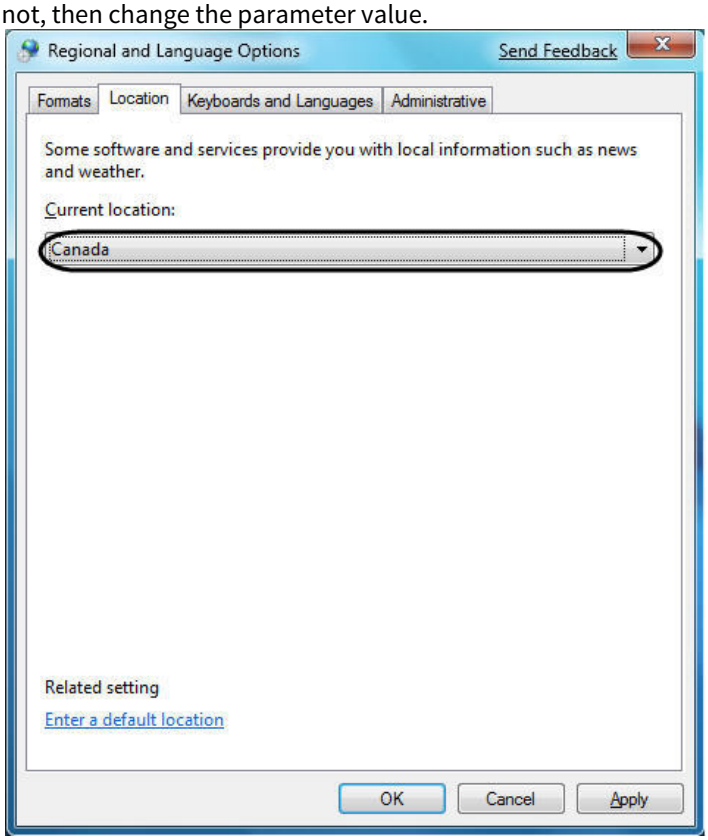


b. Click the **Additional settings...** (2) button and make sure the '.' value is selected for the **Decimal symbol (3)** parameter in the **Numbers** tab. If not, then change the parameter value manually.

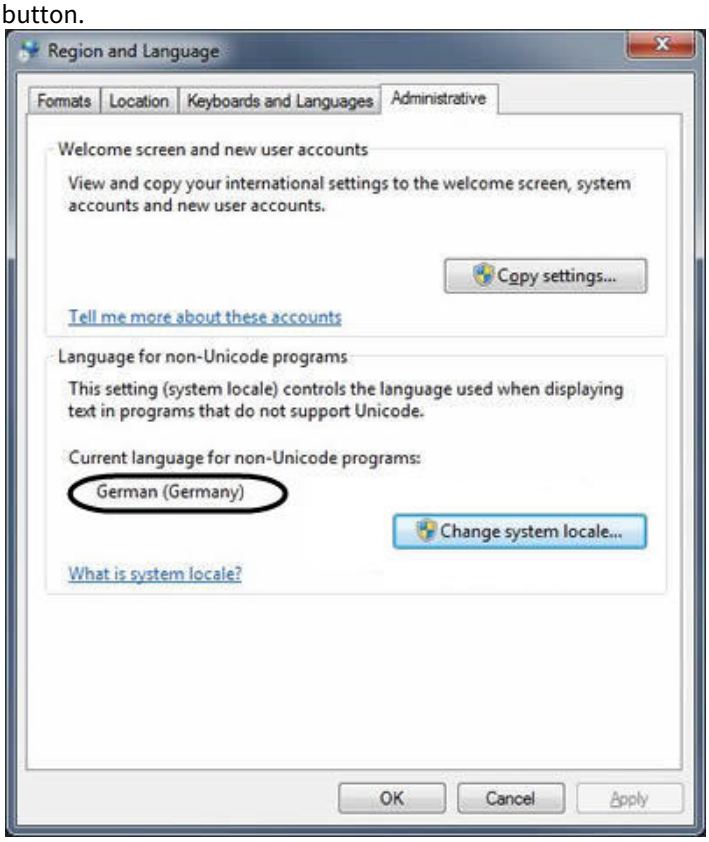


c. Click **OK** (**4**).
d. Click **OK** (**5**).

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.



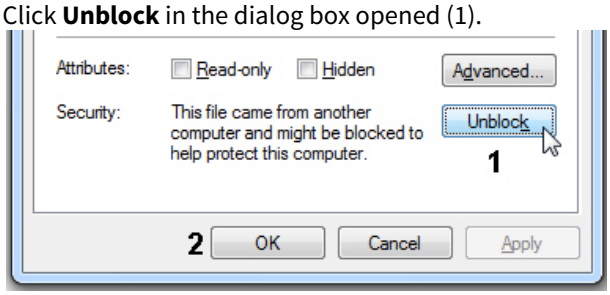
4. Go to the **Administrative** tab. Make sure that the language that is used for Intellect installation is specified in the **Current language for non-Unicode programs** field. If not, then change the parameter value using the **Change system locale...** button.



6.1.2.2 Unblocking a distribution kit downloaded from the Internet

Unblock the archive with *Intellect* software distribution kit downloaded on-line before unpacking it to ensure correct installation. To do that:

1. Left-click the downloaded archive.
2. Select **Properties** in the opened menu.
3. Click **Unblock** in the dialog box opened (1).



4. Click **OK** (2).
5. Unpack the archive and run *Intellect* installation.

Unblocking a distribution kit is completed.

6.1.2.3 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.

6.1.3 Installation of INTELLECT™ software as a Server/Remote administrator workplace

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:

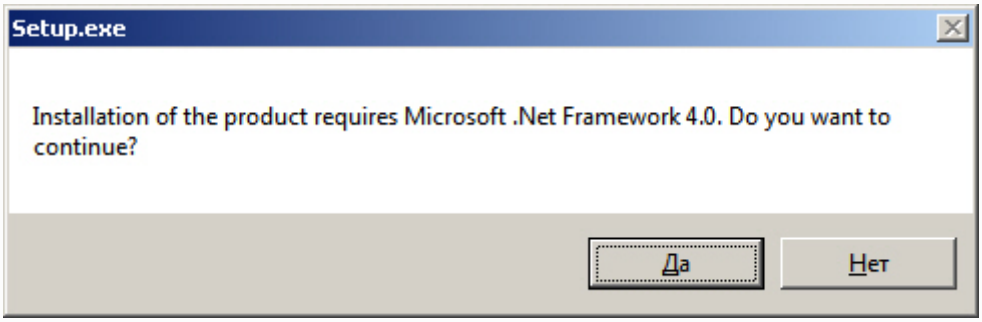
1. Insert INTELLECT installation disk in the CD-ROM drive, its contents will be displayed in a dialog box.



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.

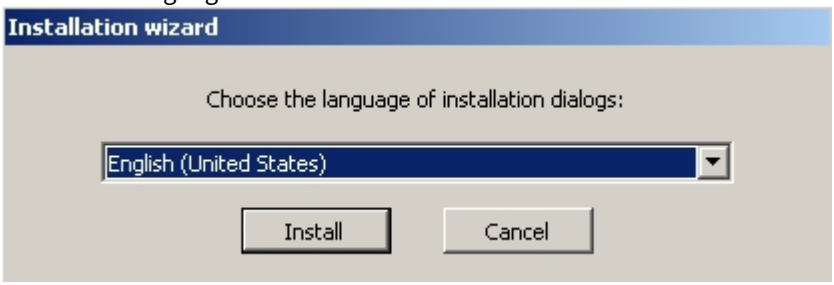


Click **Yes** for Microsoft.Net Framework 4.0 auto installation.

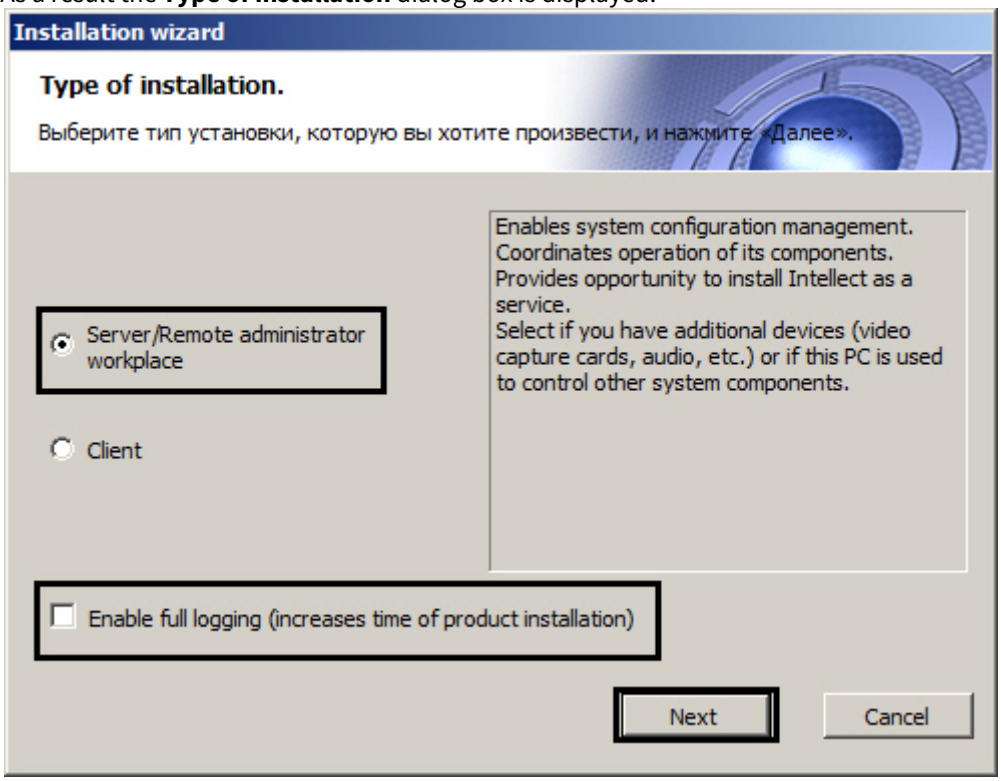
Important!

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**.



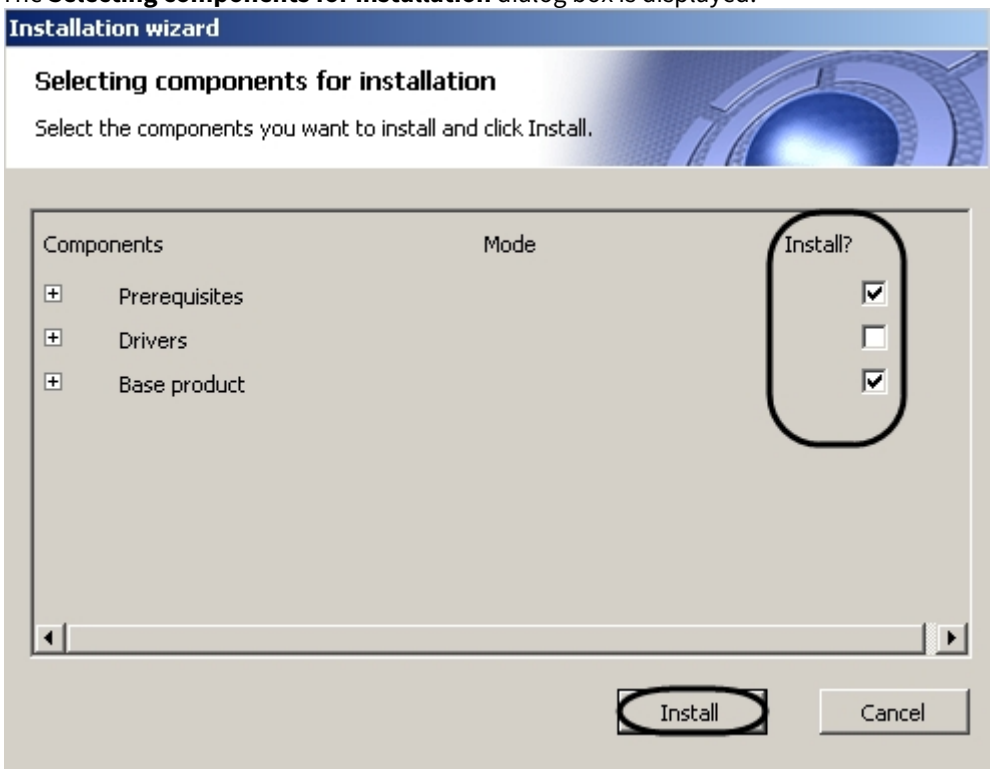
As a result the **Type of installation** dialog box is displayed.



4. Select the **Server/Remote administrator workplace** 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.

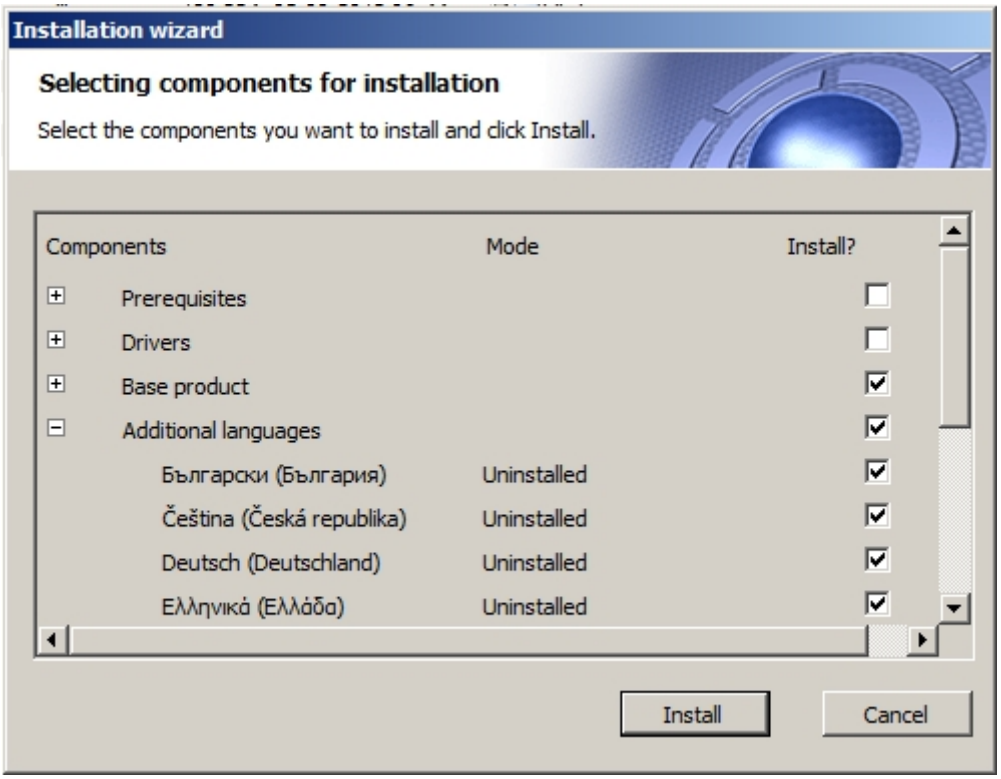


7. Set the checkboxes next to the components that are to be installed.

> **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.

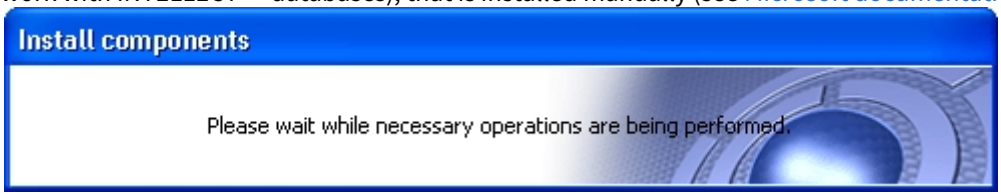
If you are not installing from a disk, you will also be able to select the languages to be installed. To do this, download the language pack from ITV's official website (http://www.itv.ru/) before beginning the installation and put the archive's files into the languages folder in the installer's directory.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



Note

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

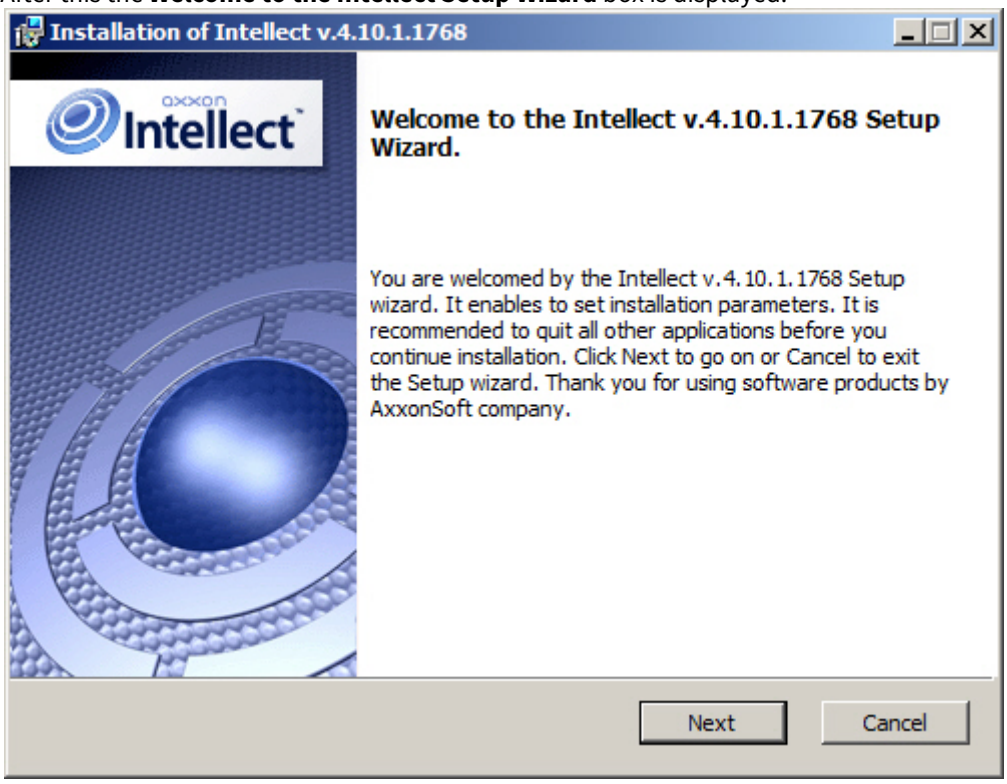
8. Click the **Install** button.
The selected components are automatically installed except Microsoft SQL Server Express 2014 database (necessary for work with INTELLECT™ databases), that is installed manually (see Microsoft documentation).



Important!

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

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

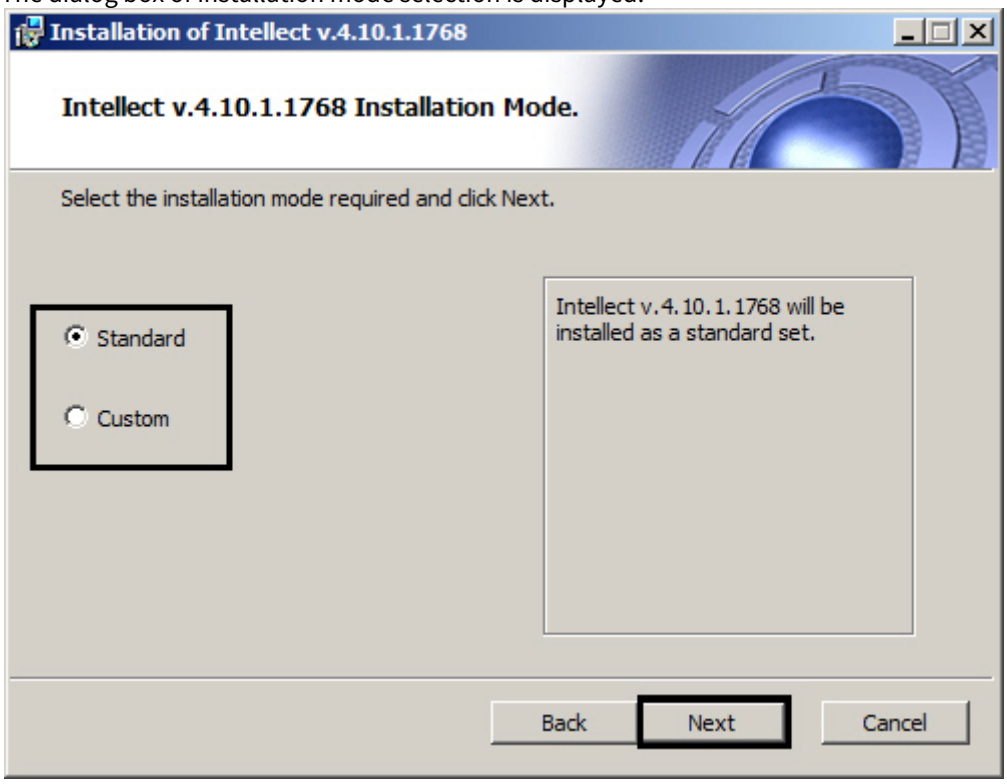


9. Click the **Next** button.
   The **License Agreement** dialog box is displayed.

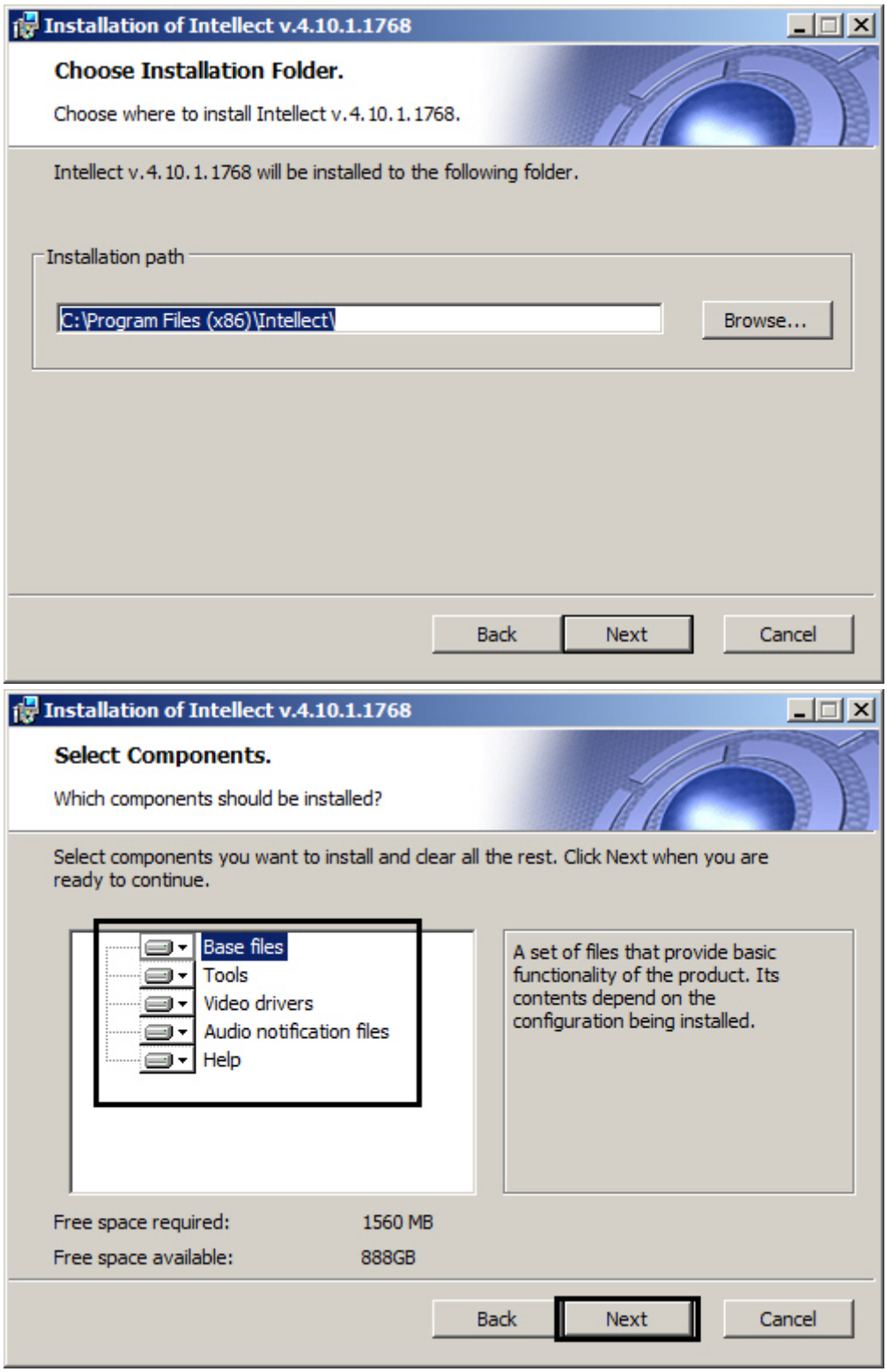


10. Read the License agreement and accept its terms by setting the switch into the **I accept the terms of the License agreement** position, otherwise the INTELLECT™ installation will be stopped.

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



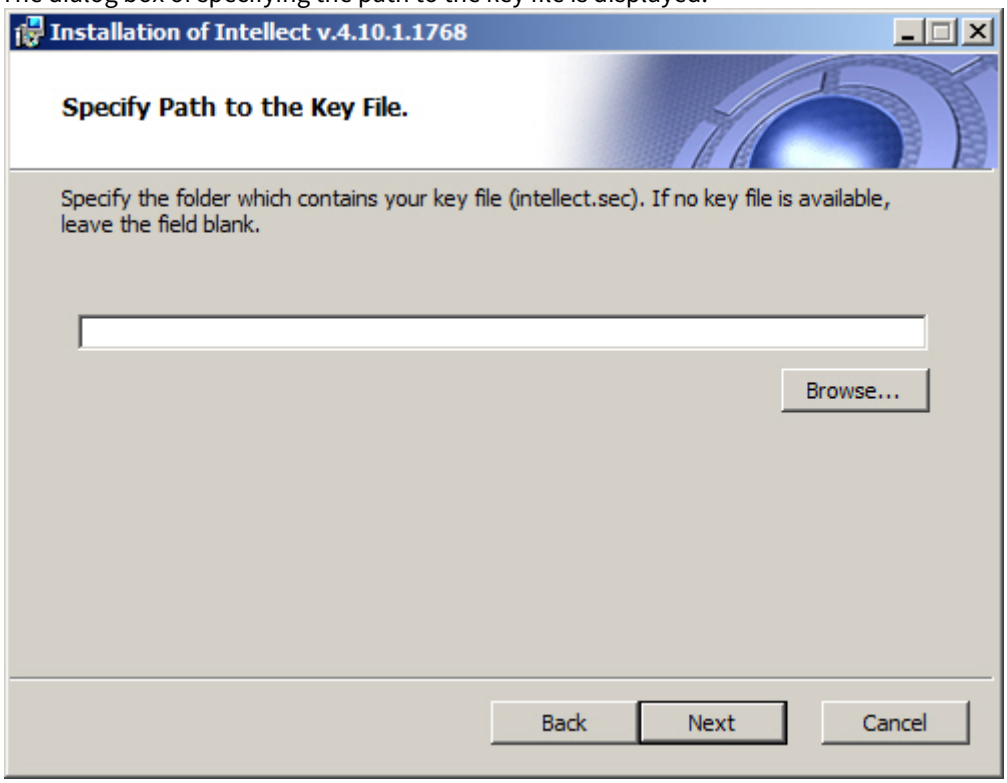
12. Select the installation mode.
13. Click the **Next** button.
    When the **Custom** installation mode is selected, the dialog box of choosing the installation folder is displayed, and then the **Select components** dialog box is displayed. This step is omitted when the **Standard** installation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



Note

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

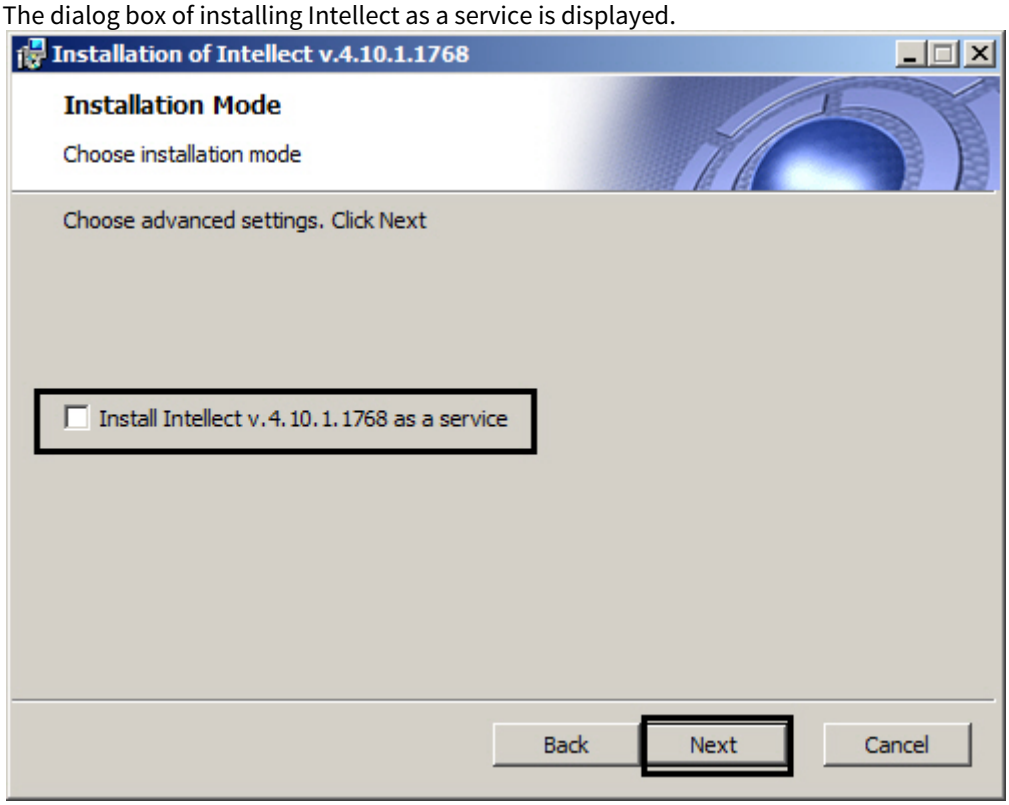
The dialog box of specifying the path to the key file is displayed.



Note

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

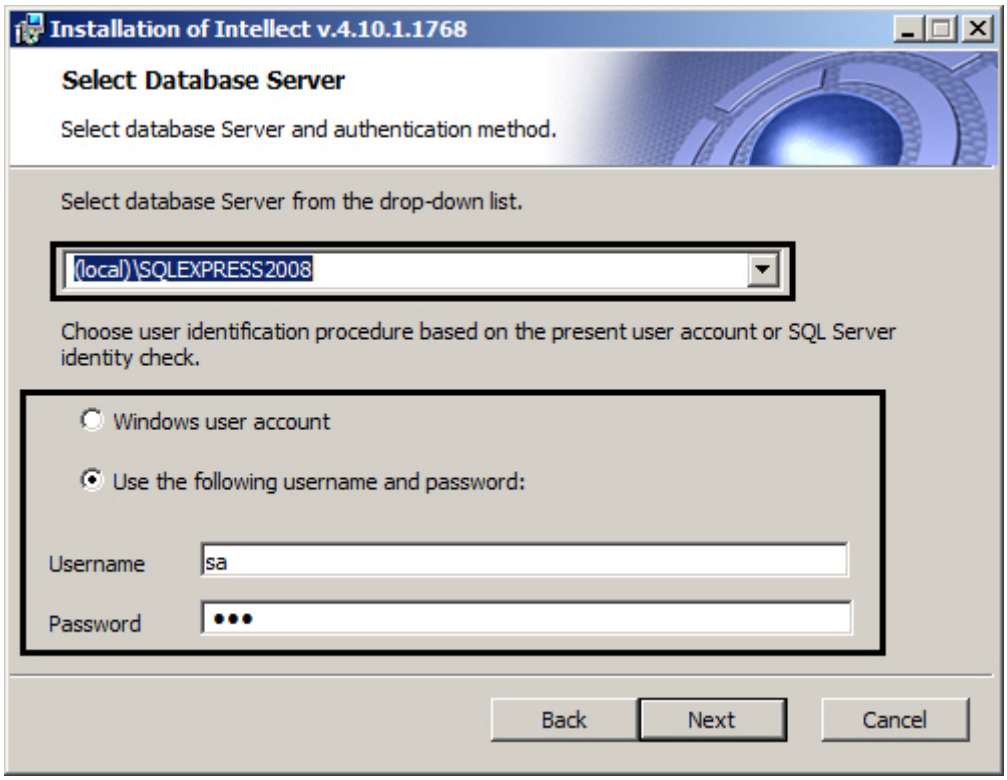
14. Click the **Next** button.
The dialog box of installing Intellect as a service is displayed.



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 intrrfaces 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 higer 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.

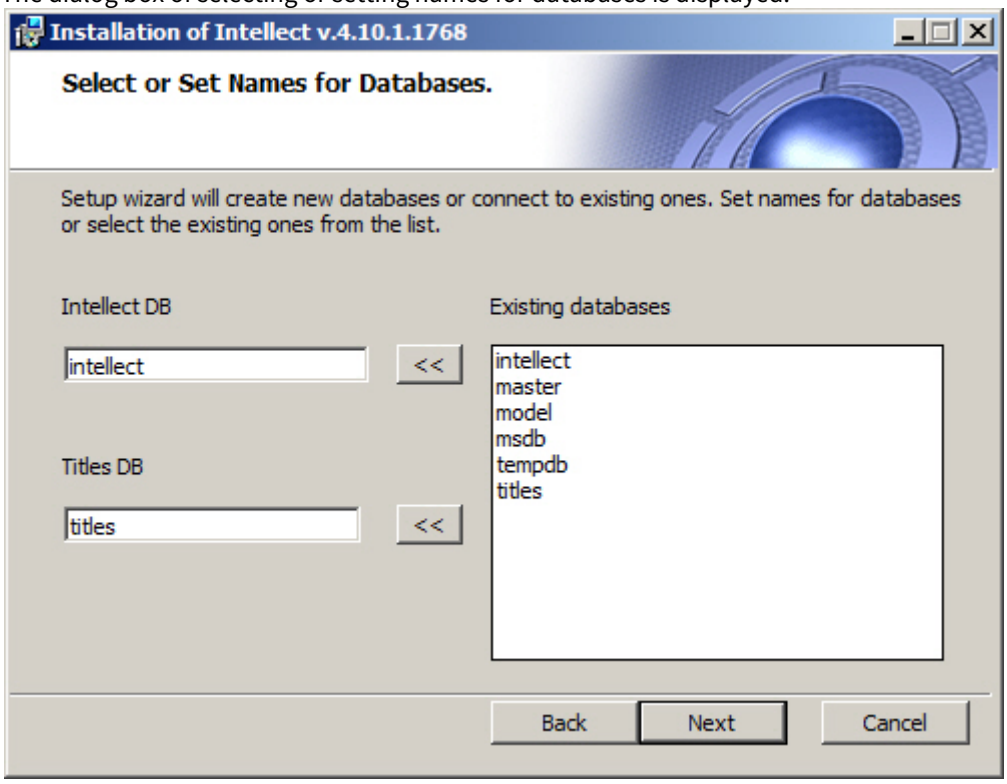
> **Note**
>
> If INTELLECT™ is installed as a service, select the SQL Server identity check, i.e. set the **Use the following username and password** checkbox and specify the username and password to login the Server database. If the database is to be connected via the Windows account, then for proper 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.

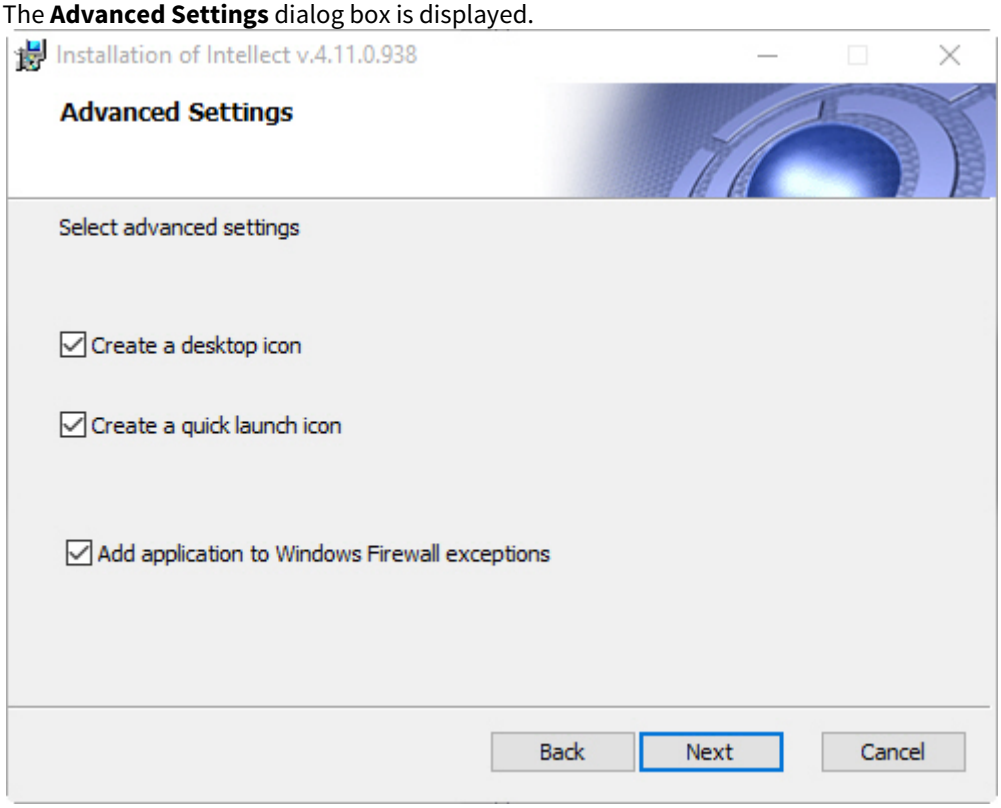
19. To continue the installation, click the **Next** button.
    The dialog box of selecting or setting names for databases is displayed.



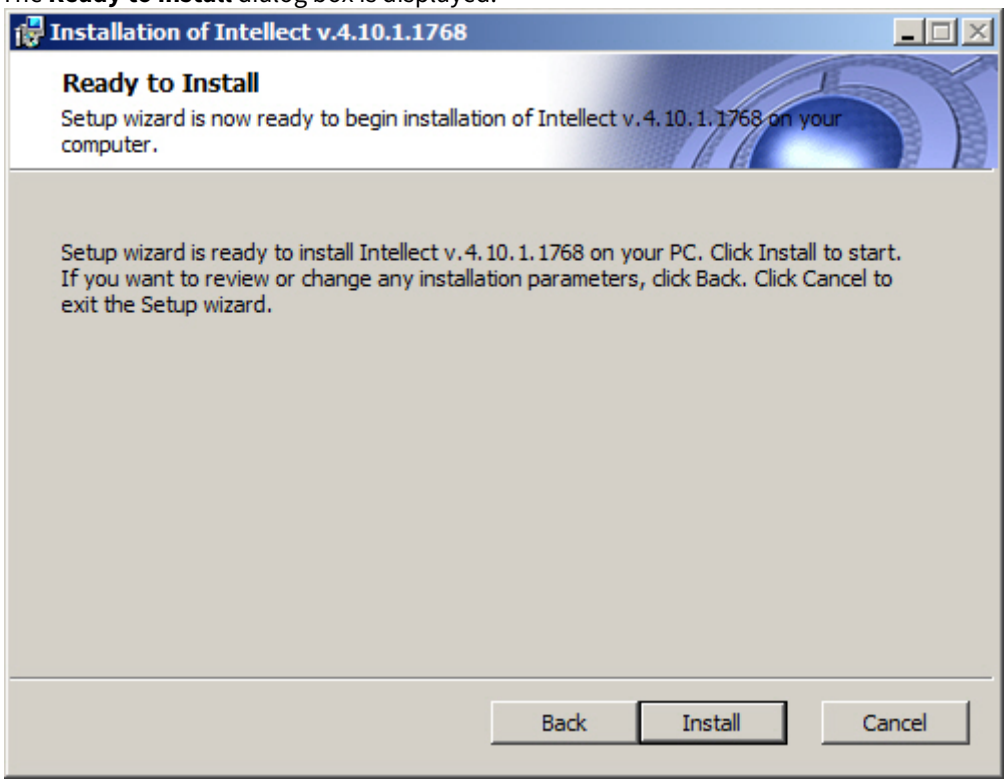
20. By default the *Intellect* database is in use as the main database. To set another database select the required database from the **Existing databases** list and click the << button near the **Intellect DB** field.
21. By default the titles database is in use as a database of titles. To set another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



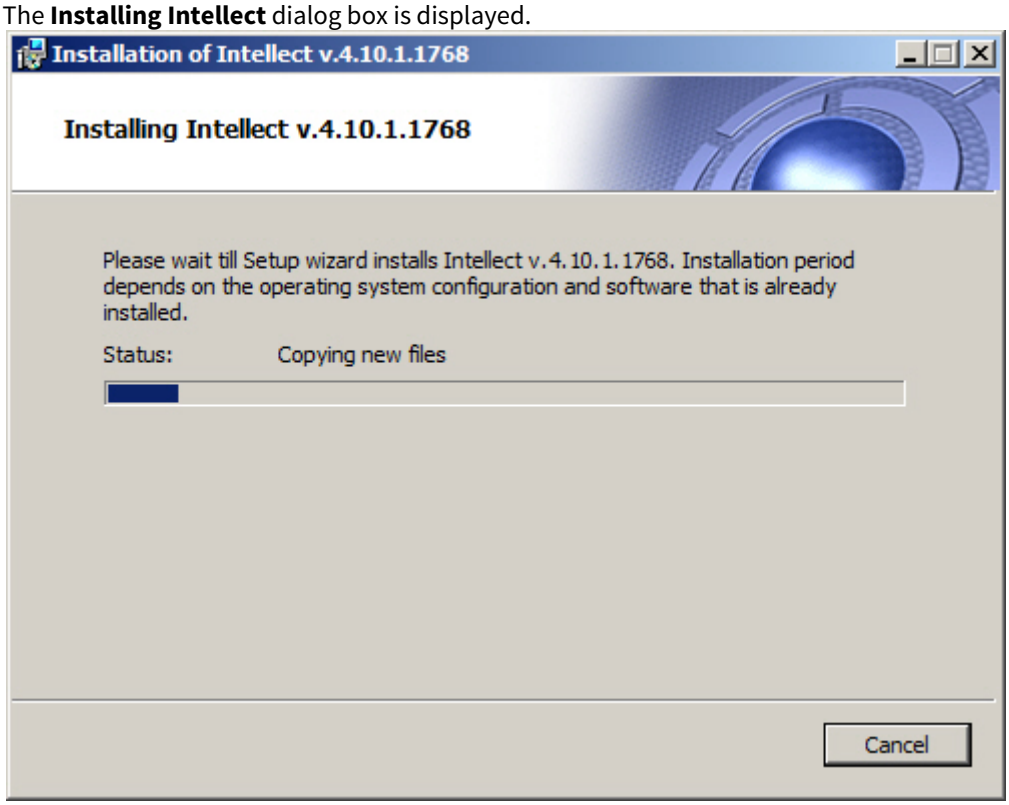
23. If a desktop icon is to be created, set the corresponding checkbox.
24. If a quick launch icon is to be created, set the corresponding checkbox.
25. If it is required to add *Intellect* and all its components to the Windows Firewall exceptions, set the corresponding checkbox.
26. Click the **Next**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



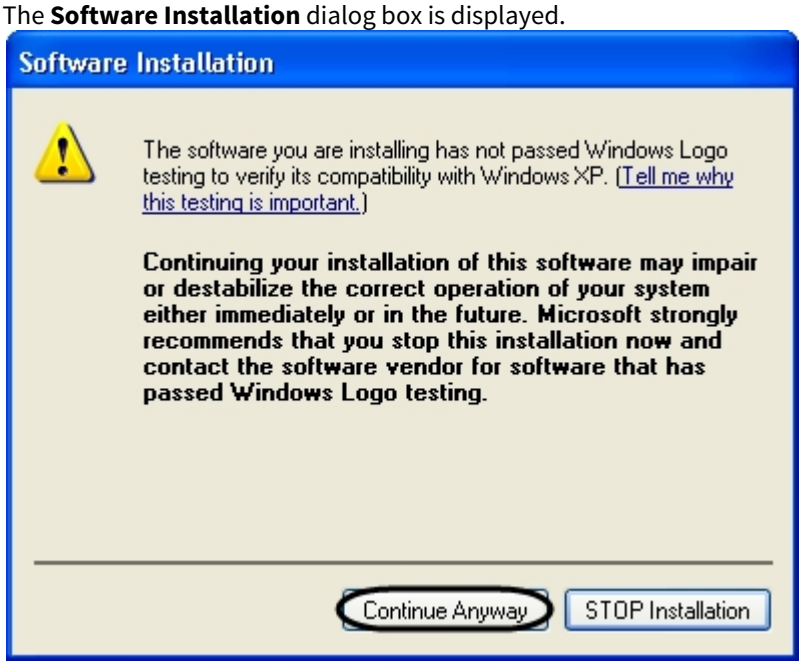
Note

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

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



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



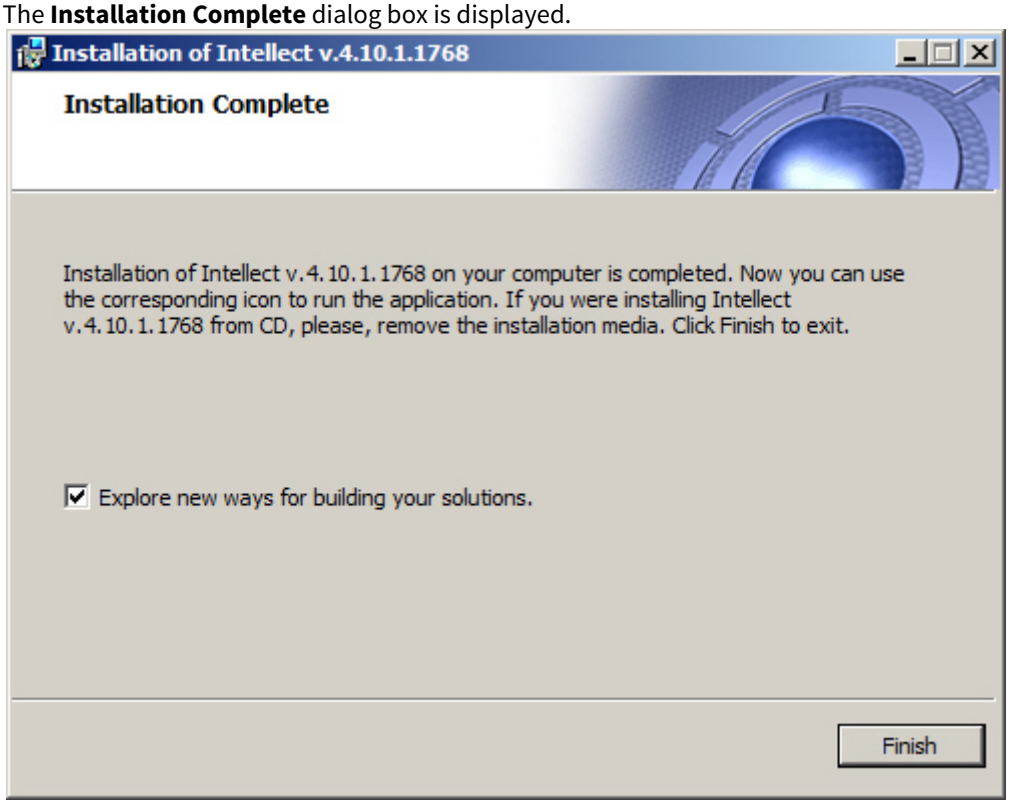
Note

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

30. To continue the installation, click the **Continue Anyway** button.
The **Installation Complete** dialog box is displayed.



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

Note

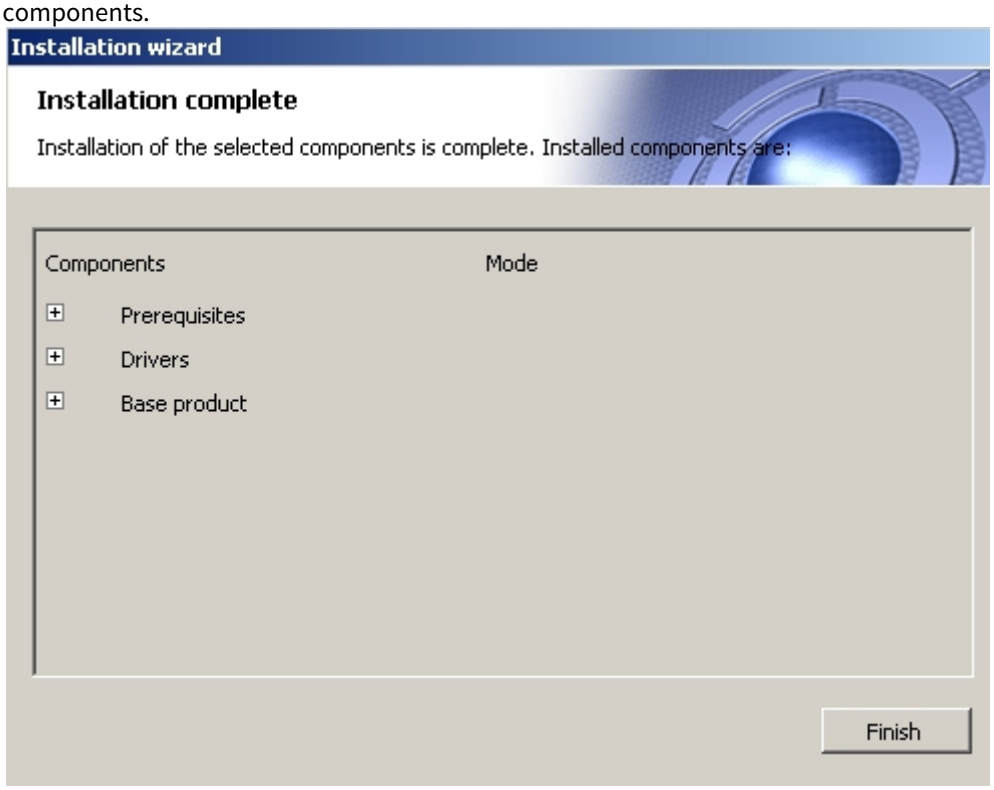
Then the Axxon Driver Pack will be installed. Starting from the Axxon Driver Pack 3.51, this driver package requires the Windows KB2999226 update to be installed. If this update is not installed on the system, a corresponding warning will be displayed. To continue the installation, it is necessary to 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 Axxon Driver Pack installation from the command prompt with the SOFT_INSTALL = "yes" parameter.

```
C:\>start /i IPDriverPack-x64.msi SOFT_INSTALL="yes"
```

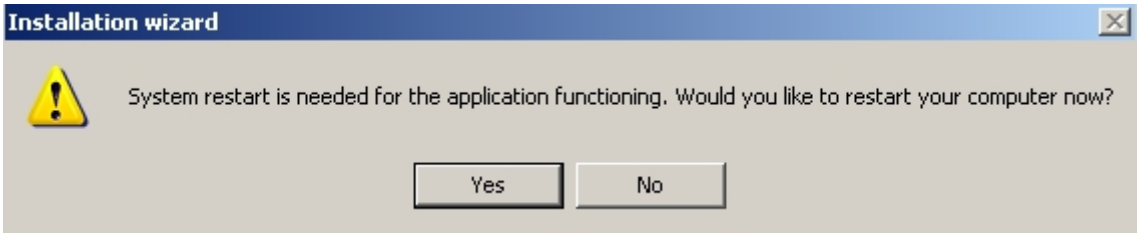
Then the Installation wizard dialog box is displayed, containg the information on the mode (installed or not) of *Intellect*

components.



33. Click the **Finish** button.

The dialog box offering to restart the system is displayed.



Note

The option with installation completion and system restarting is the most recommended.

The *Intellect* as a Server is now installed.

6.1.4 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.

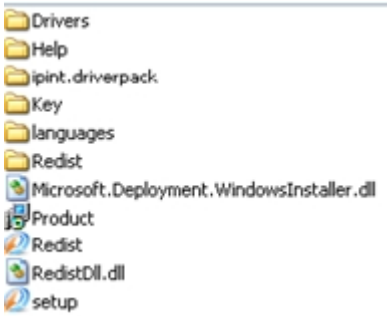
Note.

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:

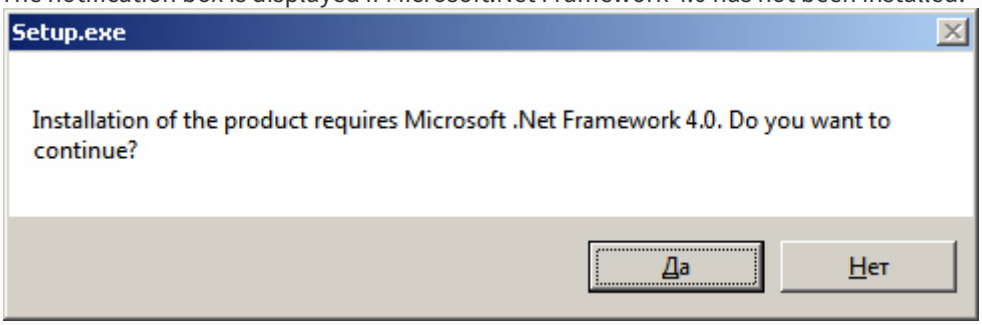
1. Insert INTELLECT installation disk in the CD-ROM drive, its contents will be displayed in a dialog box.



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.

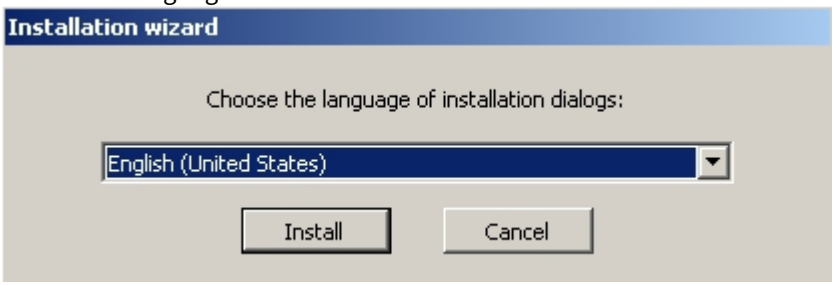


Click **Yes** for Microsoft.Net Framework 4.0 auto installation.

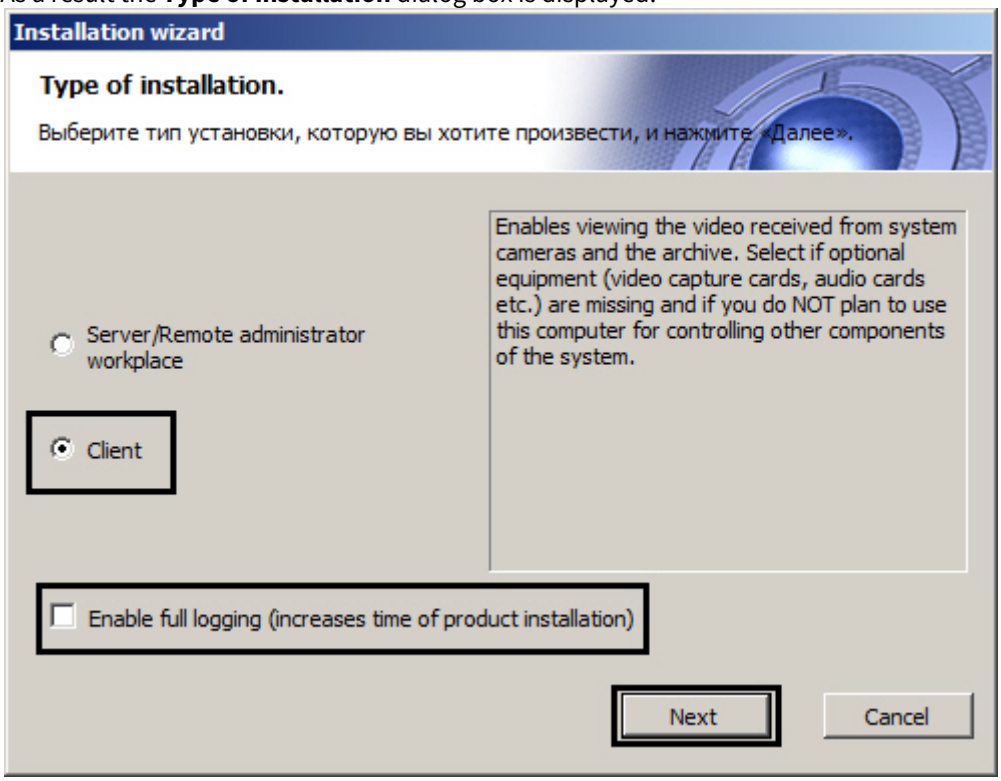
Attention!

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**.



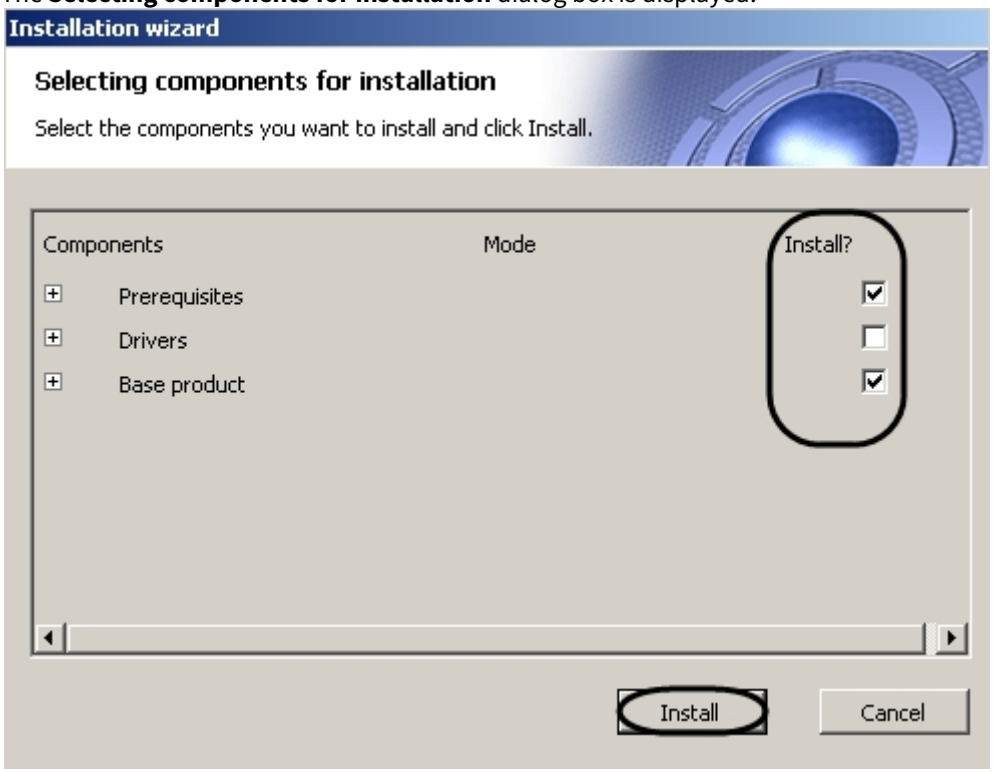
As a result the **Type of installation** dialog box is displayed.



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.

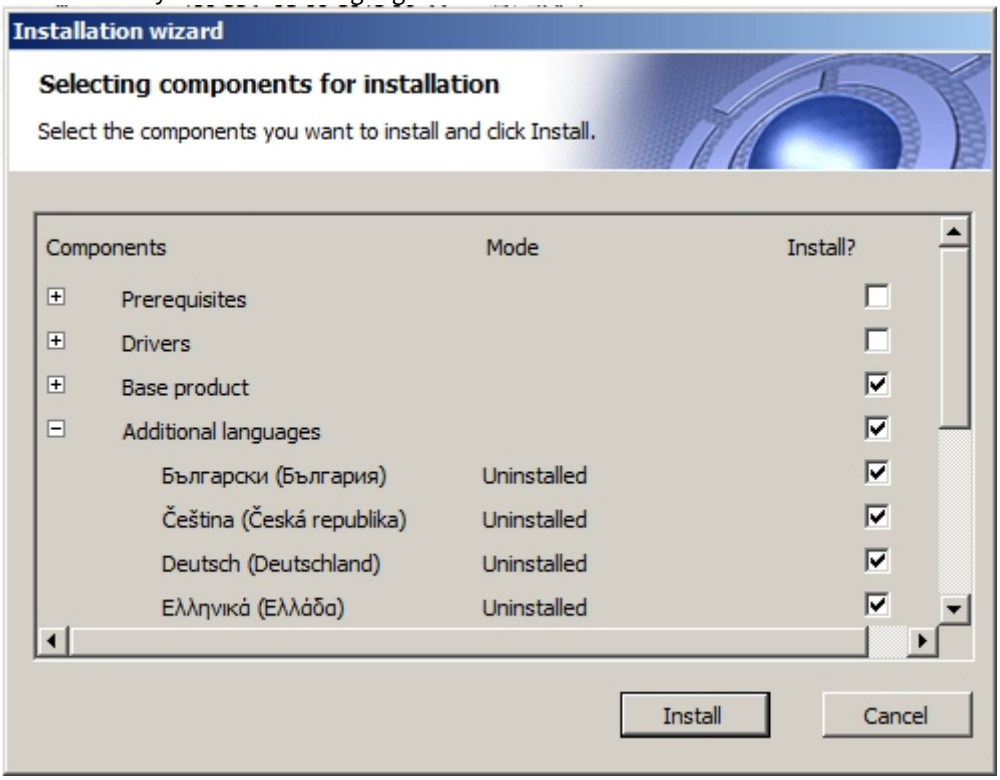


7. Set the checkboxes next to the components that are to be installed.

> **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 ITV's official website (http://www.itv.ru/) 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

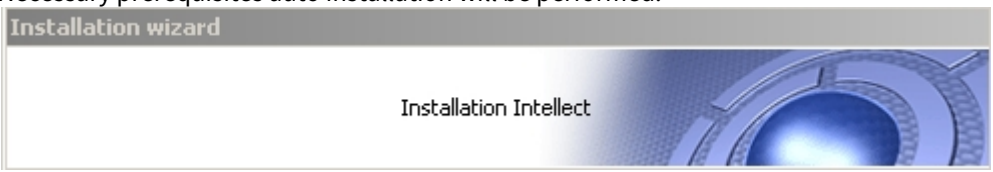
offer the ability to select the languages to be installed.



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).

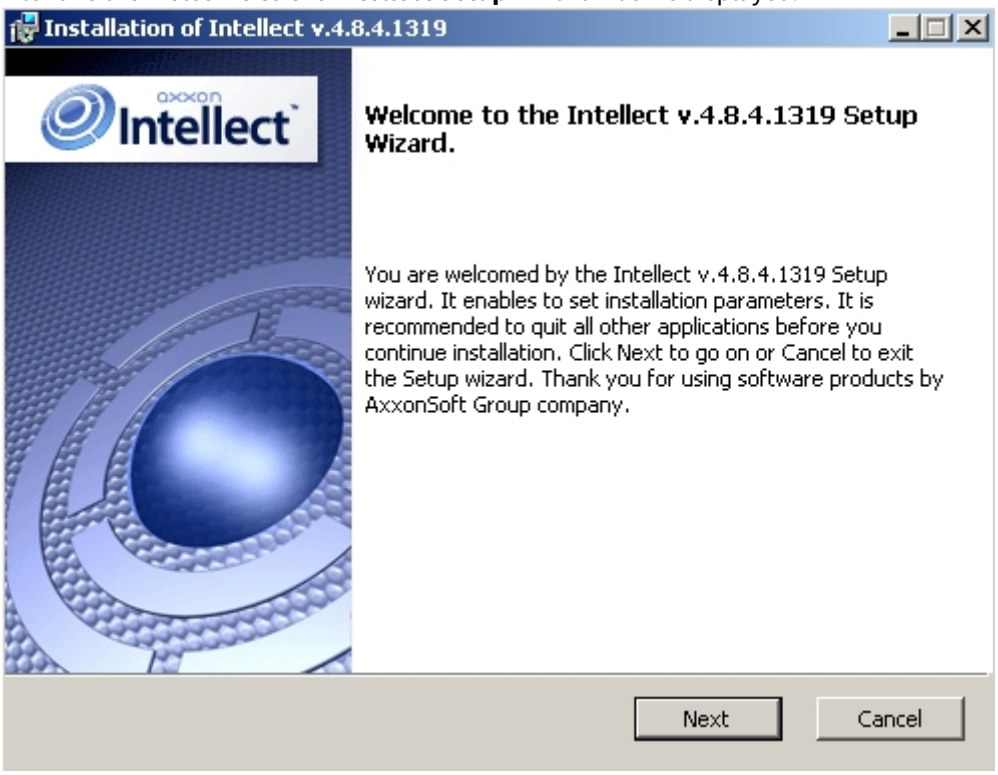
Click the **Install** button.
Necessary prerequisites auto installation will be performed.



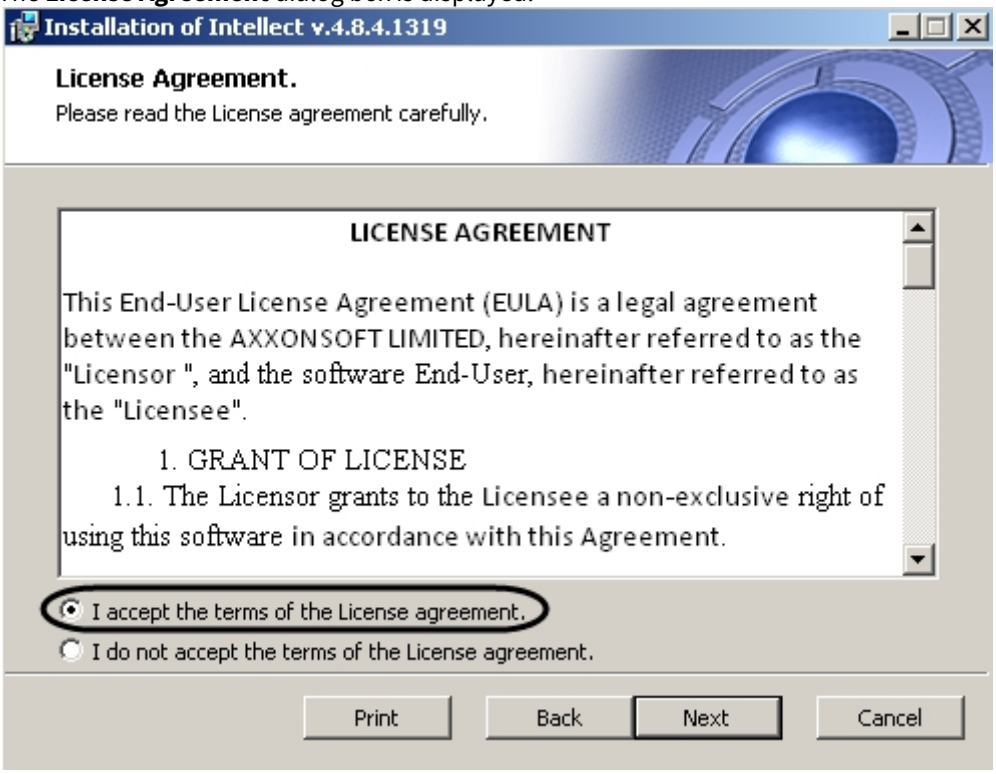
Attention!

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

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

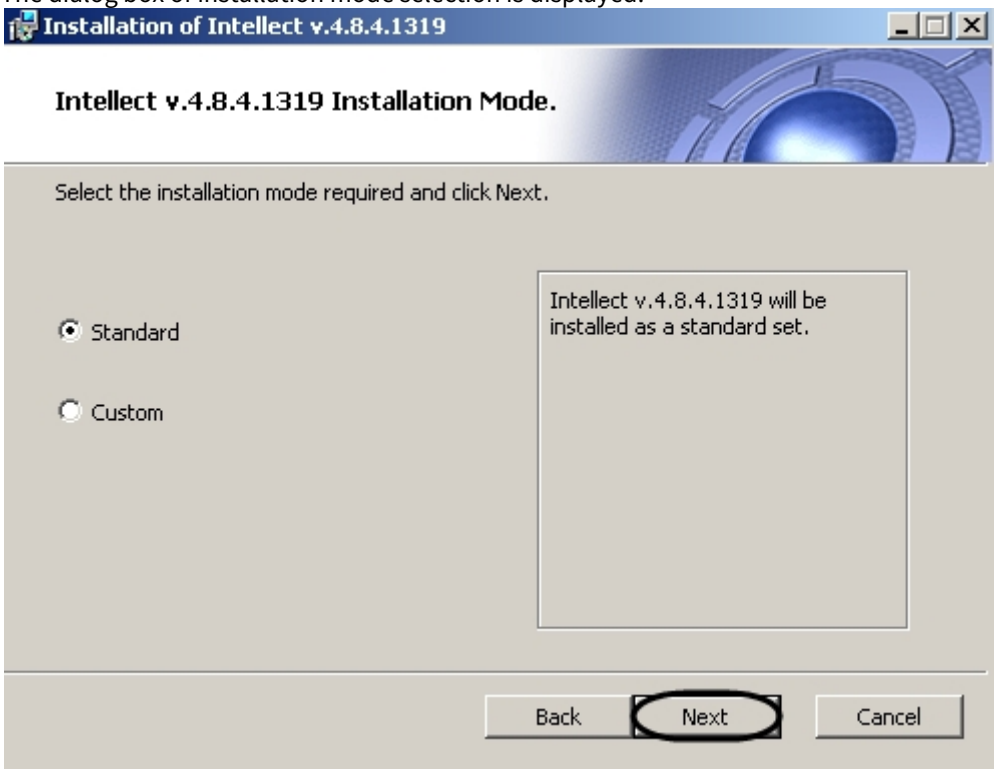


8. Click the **Next** button.
   The **License Agreement** dialog box is displayed.

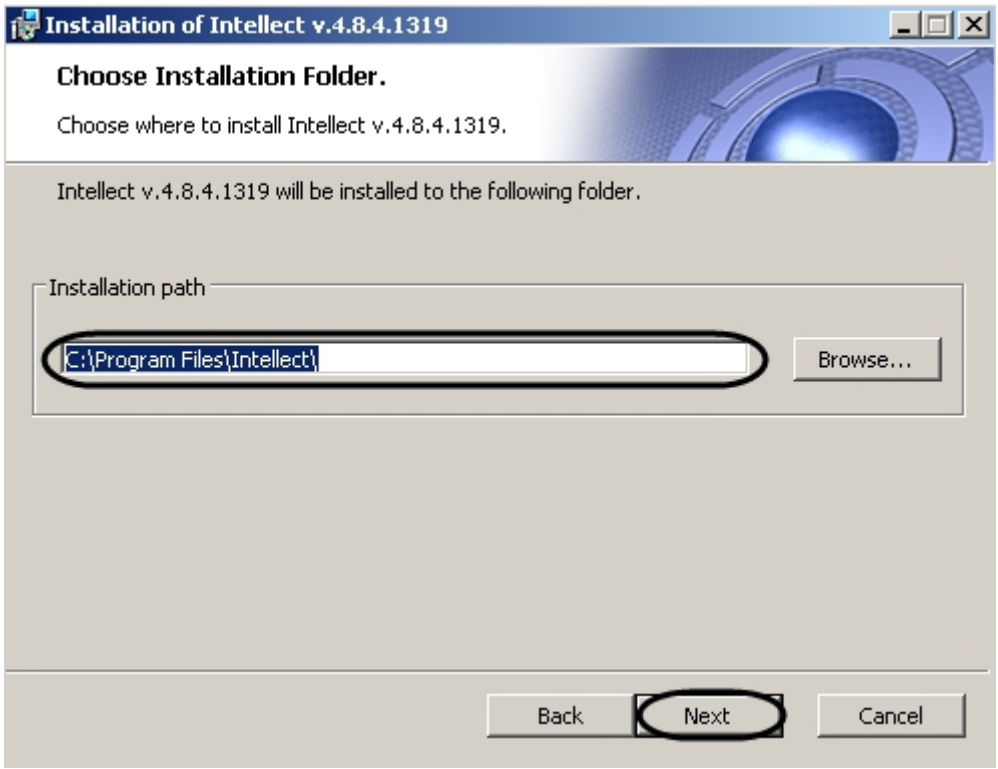


9. Read the License agreement and accept its terms by setting the switch into the **I accept the terms of the License agreement** position, otherwise the INTELLECT™ installation will be stopped.

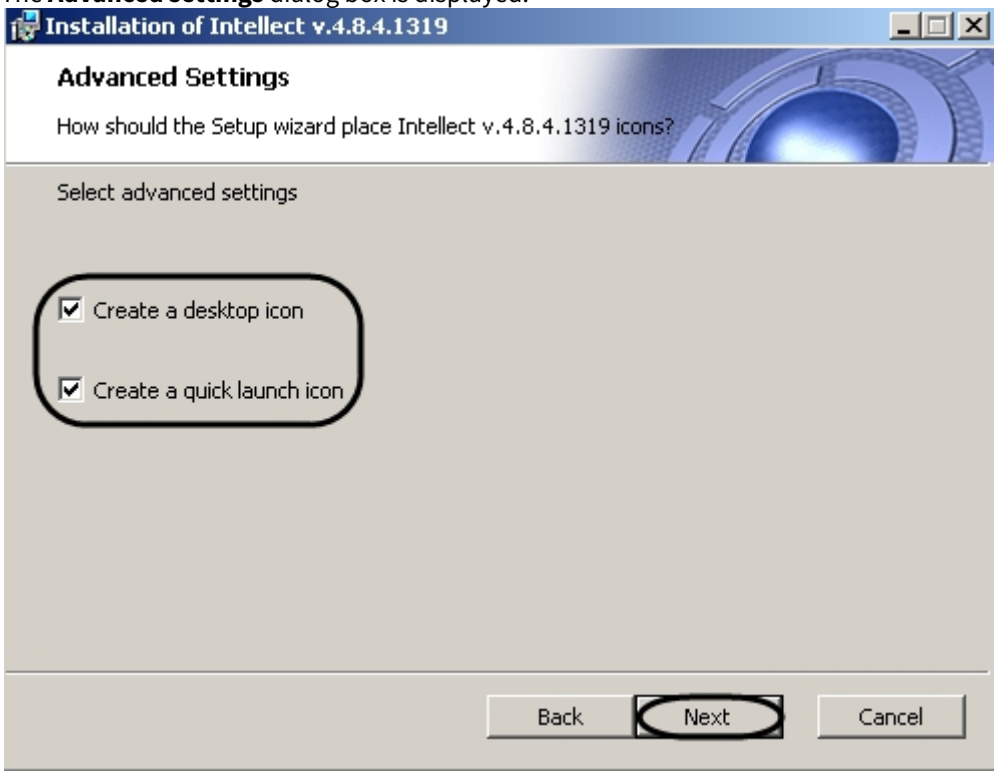
10. Click the **Next** button.
    The dialog box of installation mode selection is displayed.



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.

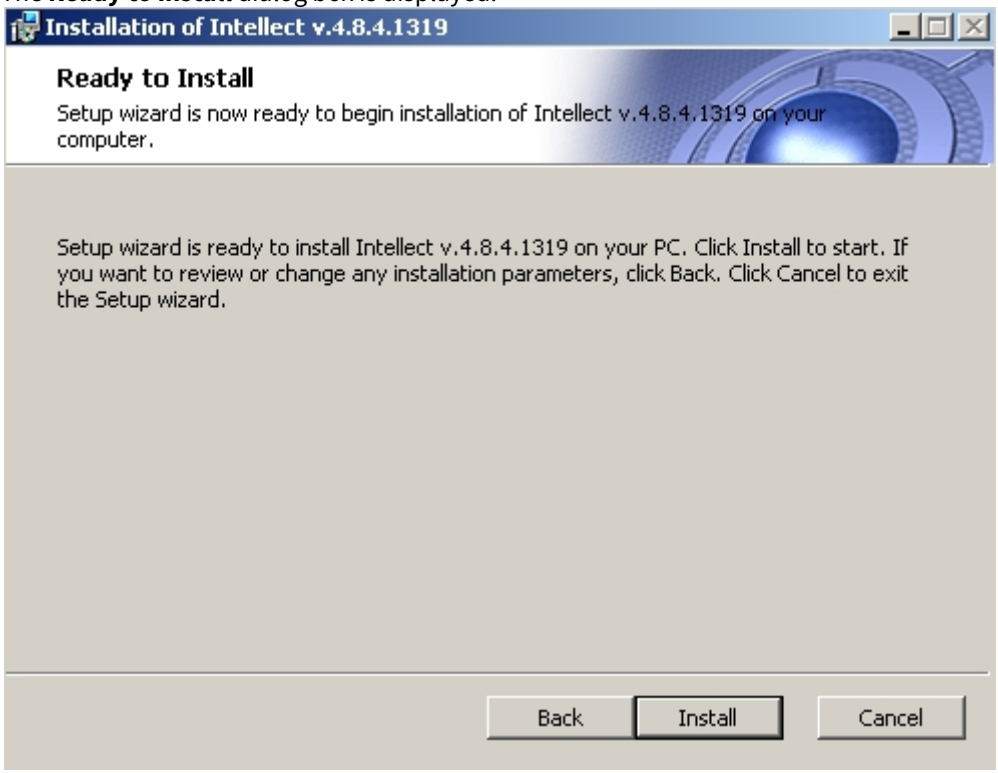


The **Advanced settings** dialog box is displayed.



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.

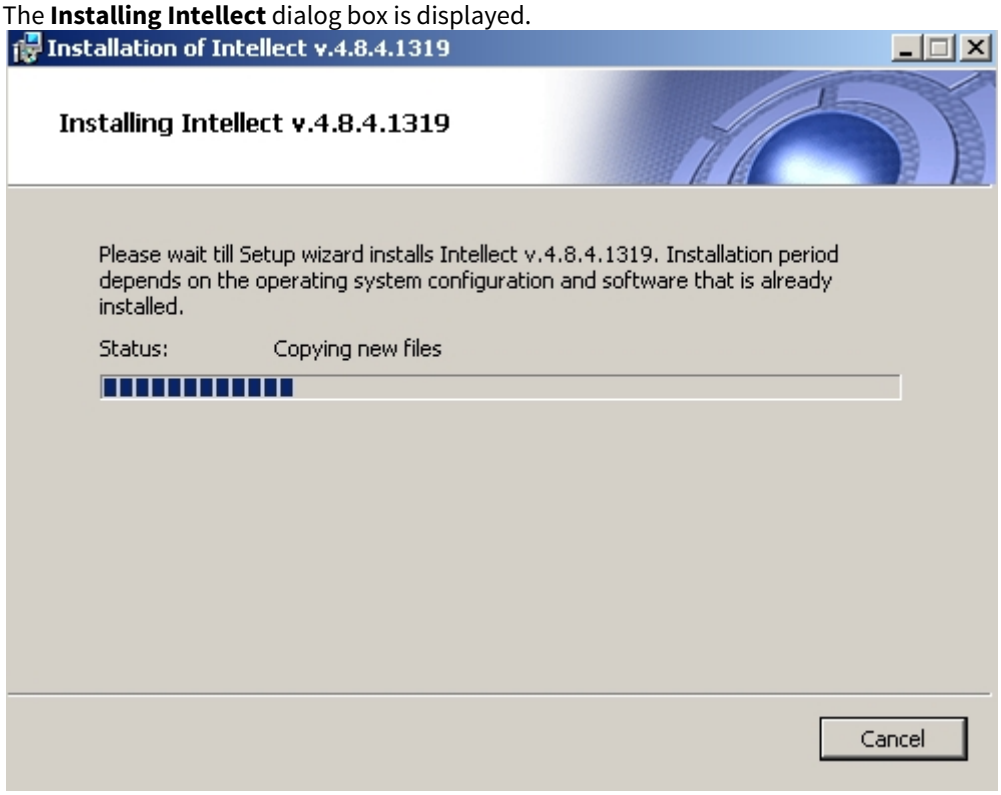
The **Ready to install** dialog box is displayed.



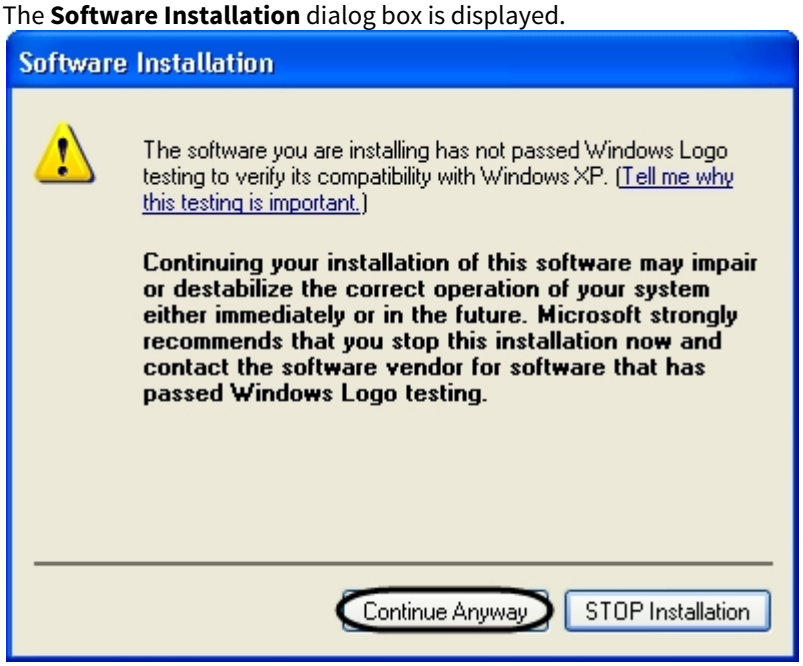
Note.

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

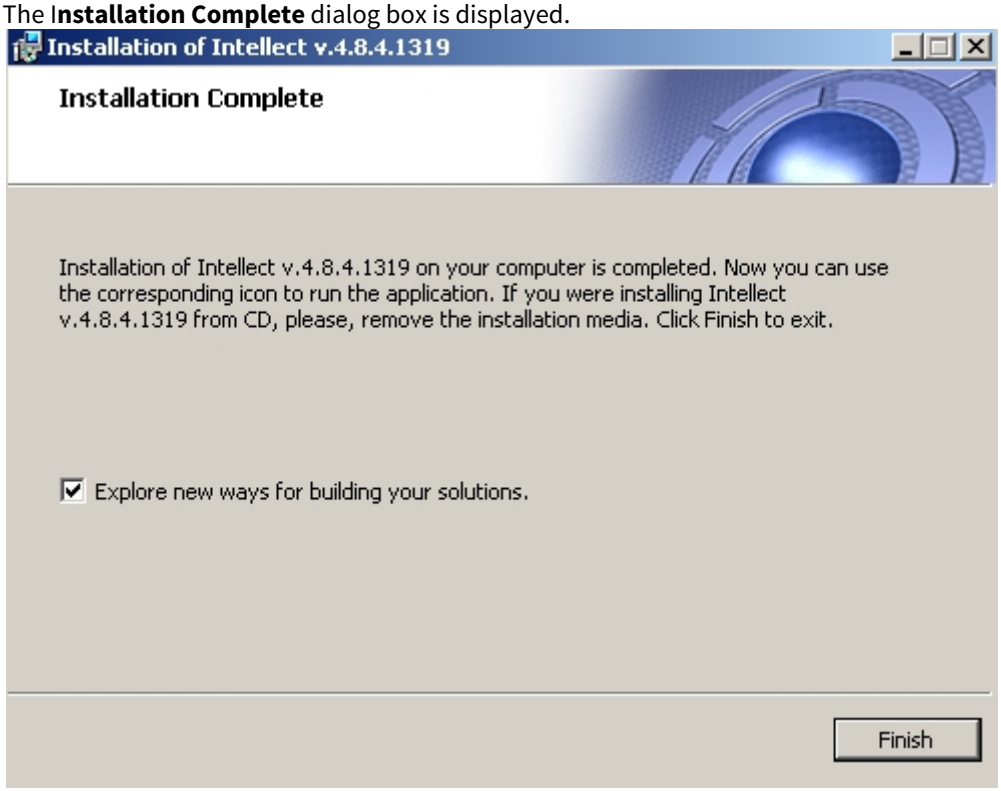
16. Click the **Install** button.
The **Installing Intellect** dialog box is displayed.



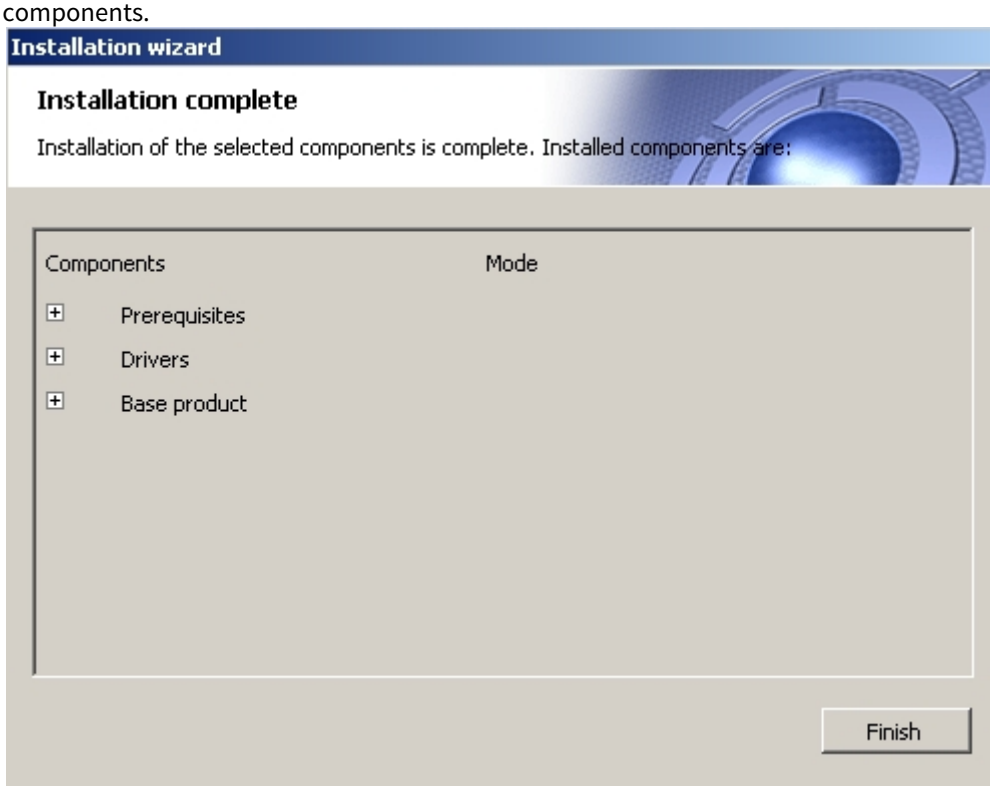
The **Software Installation** dialog box is displayed.



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.

6.1.5 Updating INTELLECT™ software

If you install INTELLECT™ software on computer where an earlier version is used, then installation will be in the updating mode.

Note.

Update the *Intellect* software on Remote Clients while its updating on the Server or on Remote Admin Workstation.

The compatible versions of the *Intellect* software should be installed on Remote Clients and on Server/Remote Admin Workstation, i.e. the first two digits of version number should be the same (e.g. versions 4.10.4 and 4.11.0 are not compatible, but versions 4.10.3 and 4.10.4 are compatible).

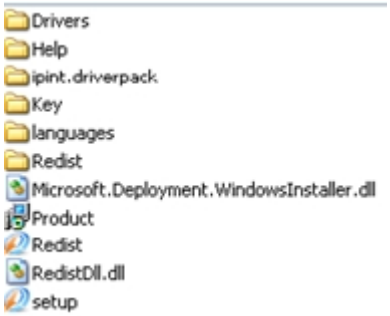
Intellect since version 4.10.2 is not compatible with earlier versions in the distributed configuration.

Important!

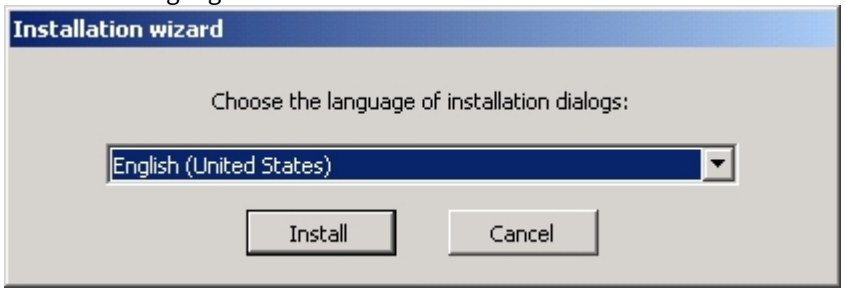
It is recommended to create database backup before updating – see Creating the database backup copy.

To update INTELLECT™ software, do the following:

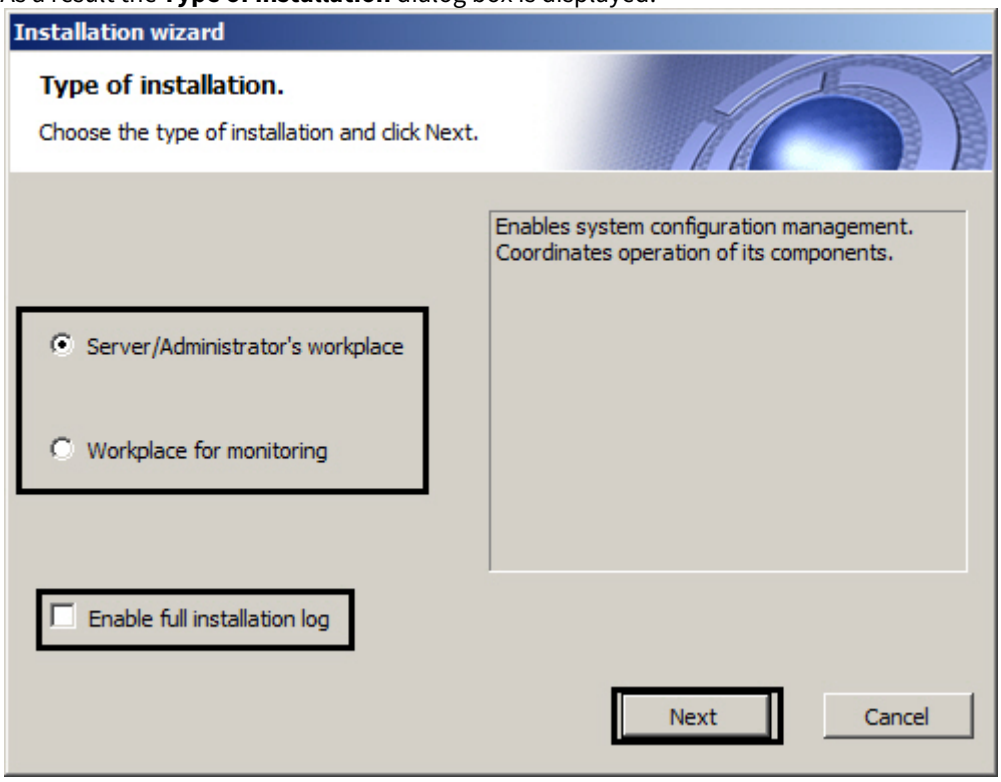
1. Insert INTELLECT installation disk in the CD-ROM drive, its contents will be displayed in a dialog box.



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



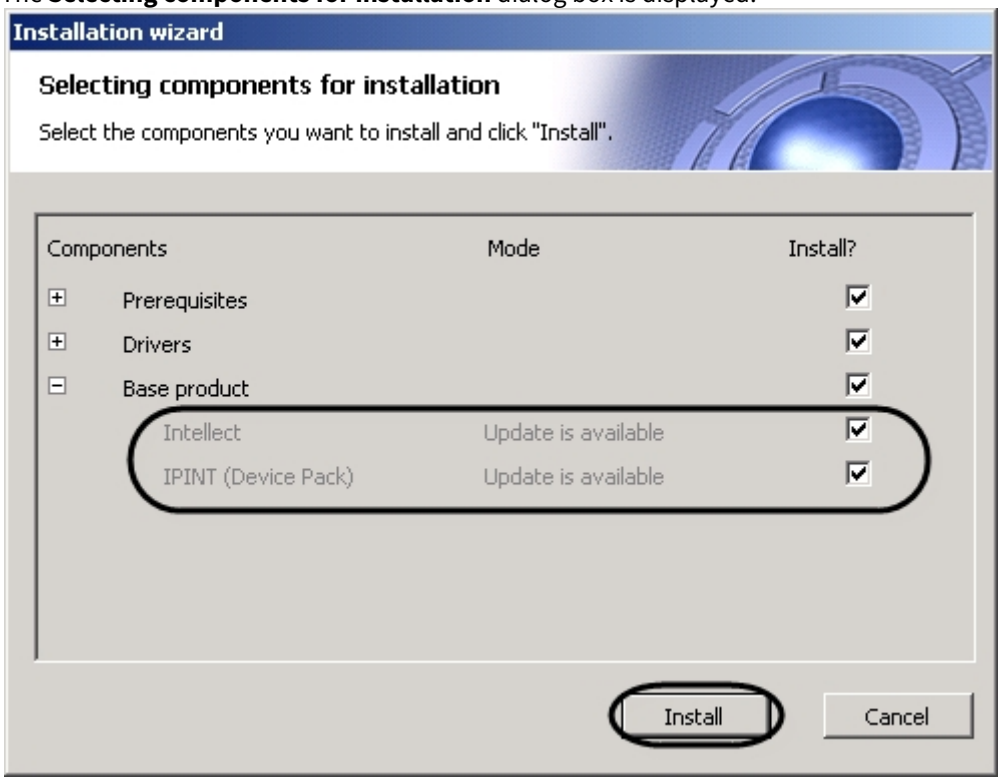
As a result the **Type of installation** dialog box is displayed.



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, the “Support.exe” tool is to be used (see The utility for collecting configuration data on servers and RWS for the Technical Support *section).*

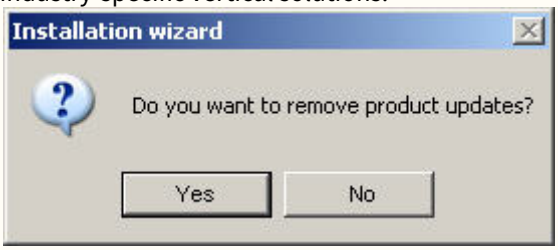
6. Click the **Next** button.
   The **Selecting components for installation** dialog box is displayed.



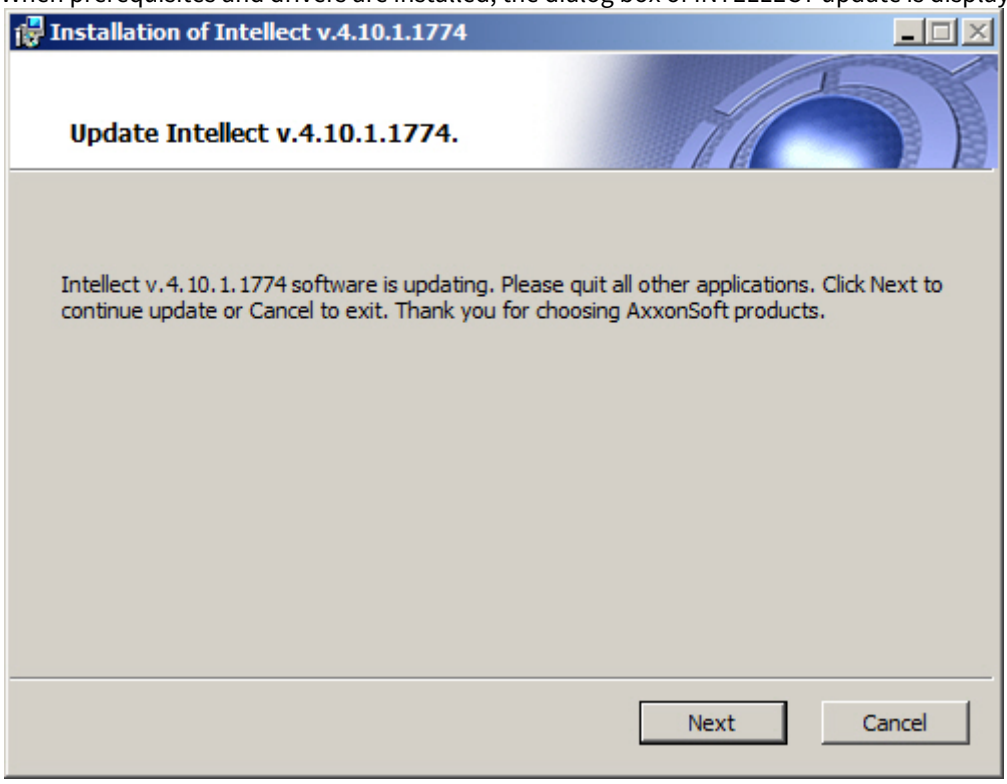
7. Set the checkboxes next to the components that are to be installed.

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

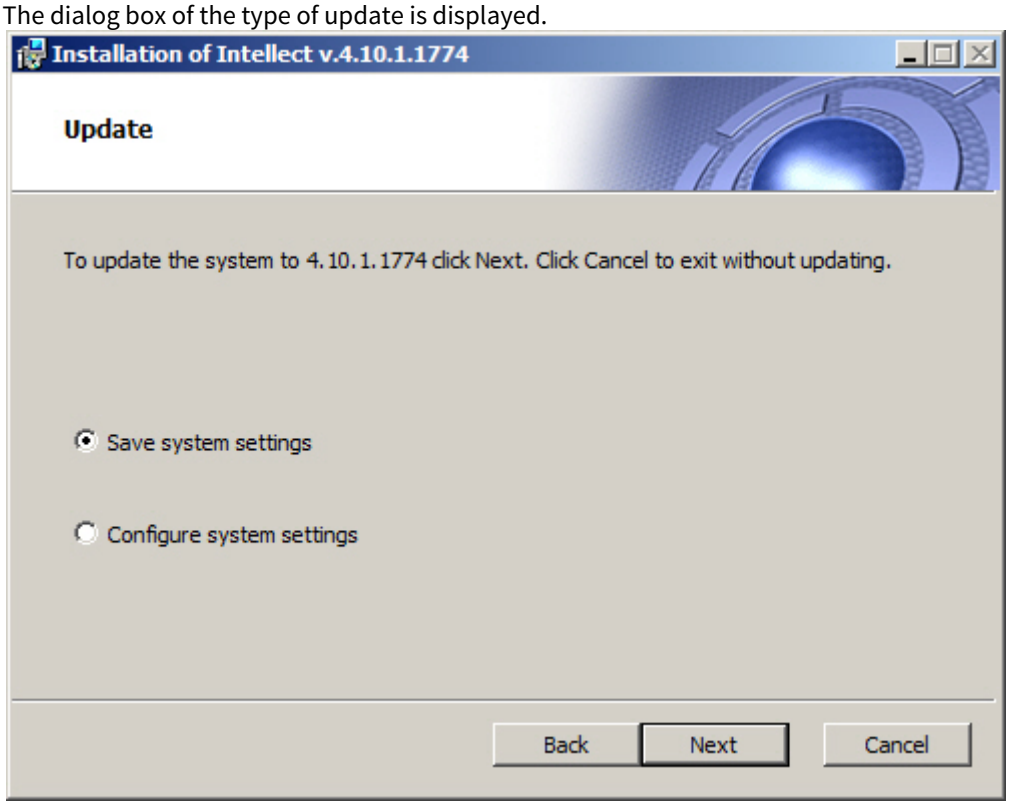
8. Click the **Install** button.
   The selected prerequisites and drivers will be installed.

> **Attention!**
>
> 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 4.10.4 to 4.11.0), compatibility is lost with industry-specific vertical solutions built for old versions. This is why, during the installation process, you are asked to remove industry-specific vertical solutions.
>
> 
>
>
> To remove industry-specific vertical solutions that are installed on the computer, select **Yes**. Otherwise, problems can occur when starting *Intellect* after update.

When prerequisites and drivers are installed, the dialog box of INTELLECT update is displayed.



9. Click the **Next** button.
   The dialog box of the type of update is displayed.

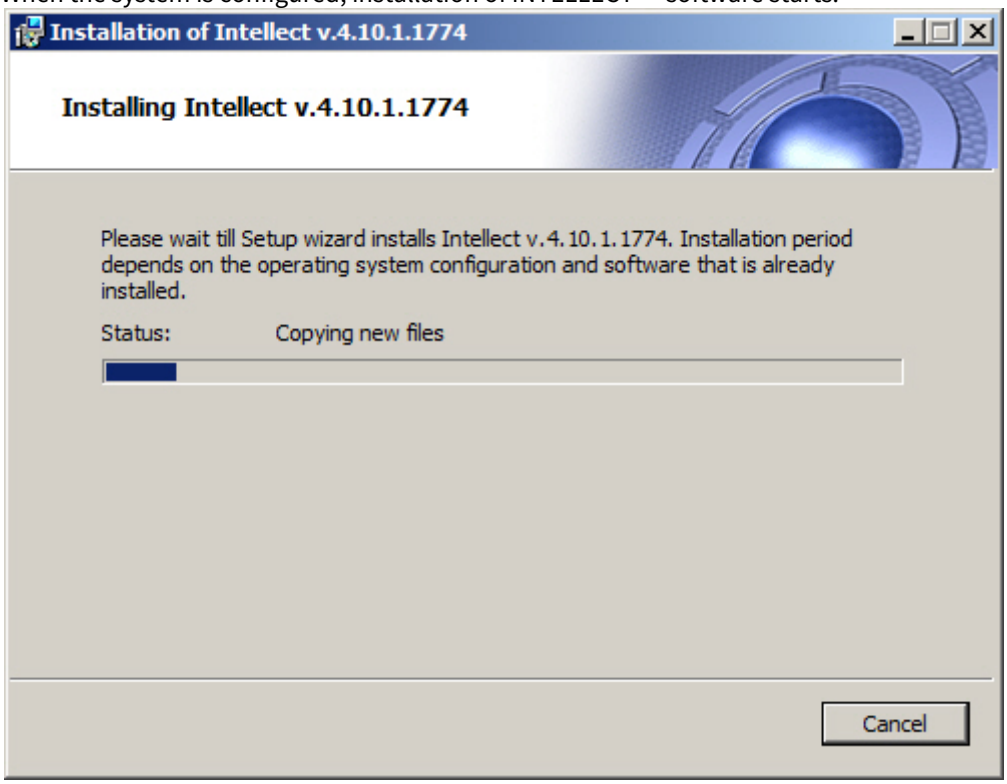


10. Select one of the offered types of update. The types of update are described in the table below

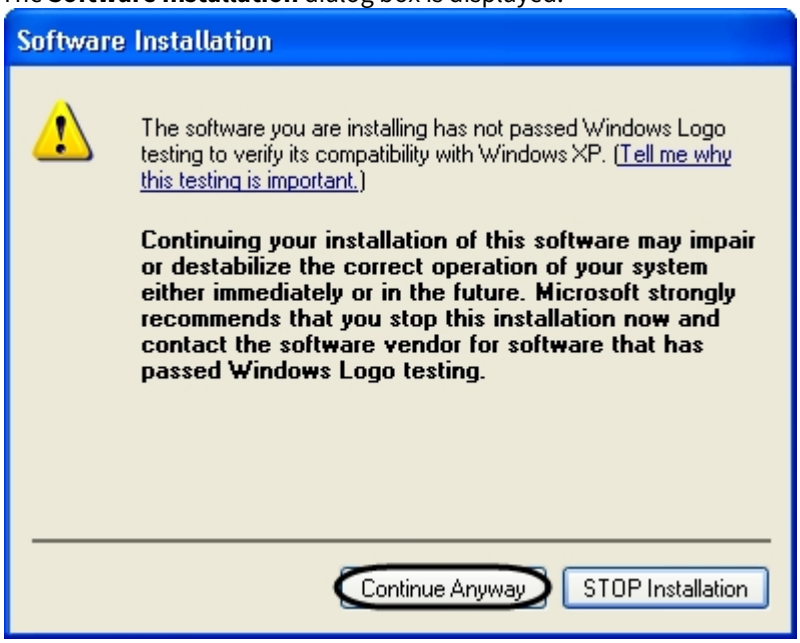
The types of update	Description
Save system settings	Use of settings chosen for installation of an earlier version

Configure system settings	Switch to step-by-step system configuration. Step-by-step configuration is described in Installation of INTELLECT™ software as a Server/Remote administrator workplace section.

11. Click the **Next** button.
When the system is configured, installation of INTELLECT™ software starts.



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



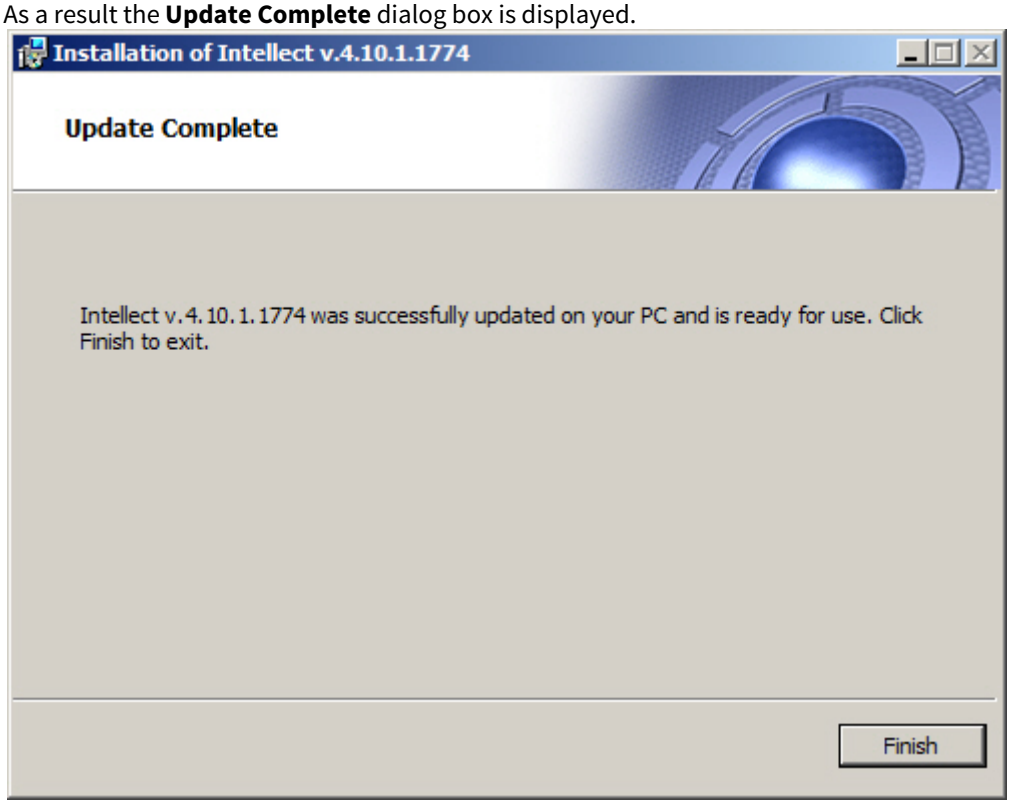
Note.

Error of driver installation for the FX4 card can occur while the *Intellect* software update 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://technet.microsoft.com/en-us/library/security/3033929

12. To continue installation, click the **Continue Anyway** button
As a result the **Update Complete** dialog box is displayed.



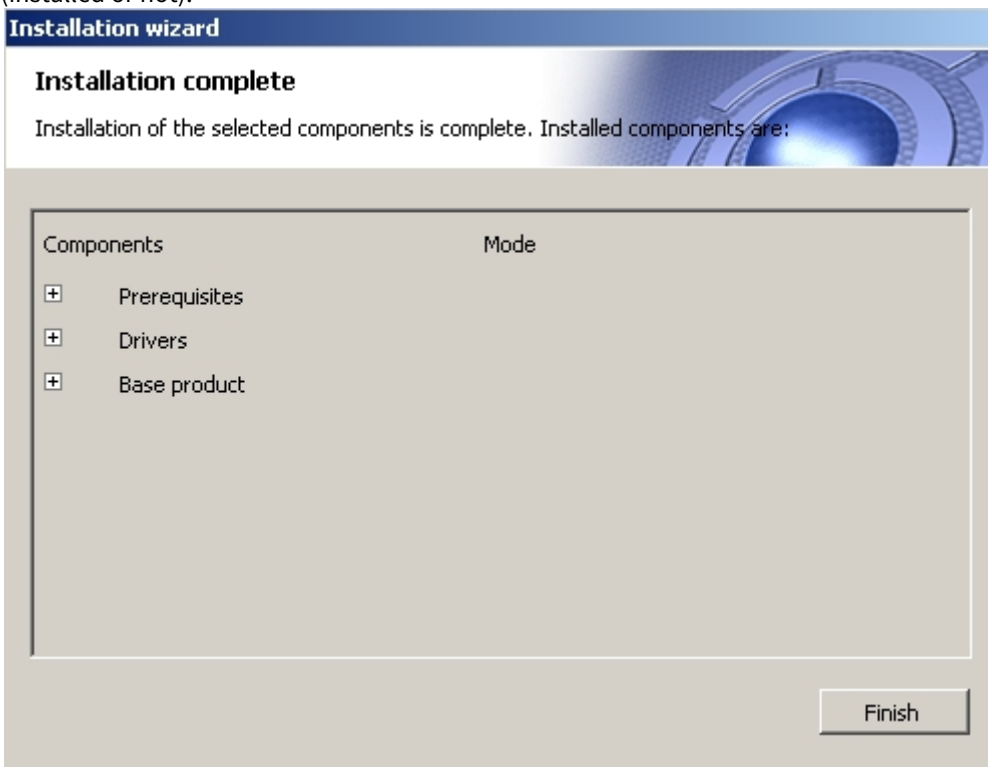
13. Click the **Finish** button.

Note.

Then the Axxon Driver Pack will be installed.

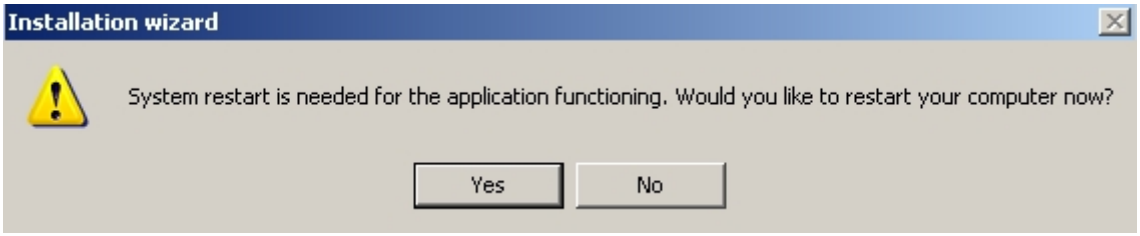
The **Installation complete** dialog box is displayed. It contains the information about INTELLECT components mode

(installed or not).



14. Click the **Finish** button.

The dialog box offering to restart the computer is displayed.



> **Note.**
>
> It is recommended to select the option of closing the program with computer restart.

INTELLECT software is now updated.

6.1.6 Using the Product.msi and Redist.exe for INTELLECT™ software 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.

6.1.7 Possible installation problems and their solutions

On the page:

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

6.1.7.1 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

6.1.7.2 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.

6.2 Repairing INTELLECT™ software

The repair mode is used to re-install all INTELLECT™ software components. Use this function when, for example, some files were accidentally deleted from the installation directory.

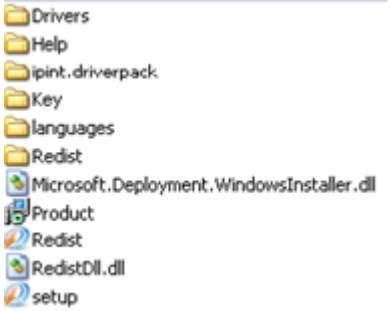
To launch repair mode, restart INTELLECT™ software installation from the installation CD, without deleting the previous version of the program. If INTELLECT™ software was initially installed from hard drive, for correct repairing make sure that installation kit is located in the same directory as when installation was performed or enable *.msi files cashing in the OS.

Note.

To ensure that INTELLECT™ software is installed correctly all applications should be closed before the installation startup.

To repair INTELLECT™ software, do the following:

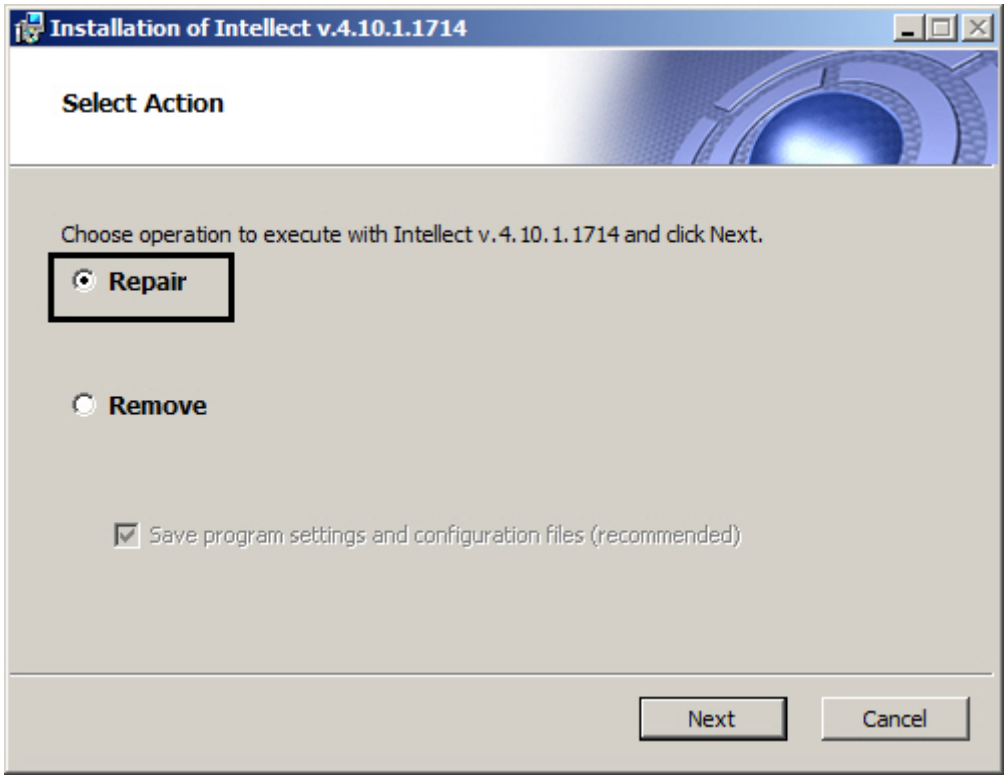
1. Insert the INTELLECT installation disk in the CD-ROM drive and display its contents in a separate window of your PC.



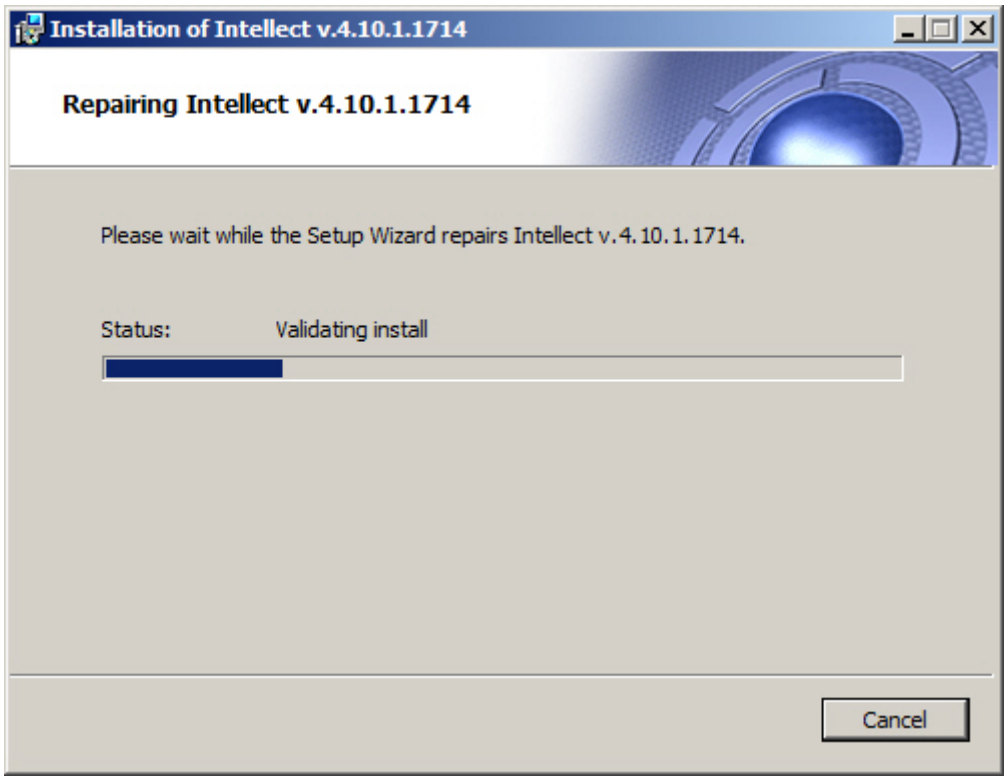
2. Run setup.exe file, designed for running the Intellect software install program.
   As a result the **Select Action** dialog box is displayed.

   Note.

   The following files may be run for repairing the Intellect software instead of *Setup.exe:*
   a. *Product.msi – to repair the INTELLECT™;*
   b. *Redist.exe – to install additional components.*



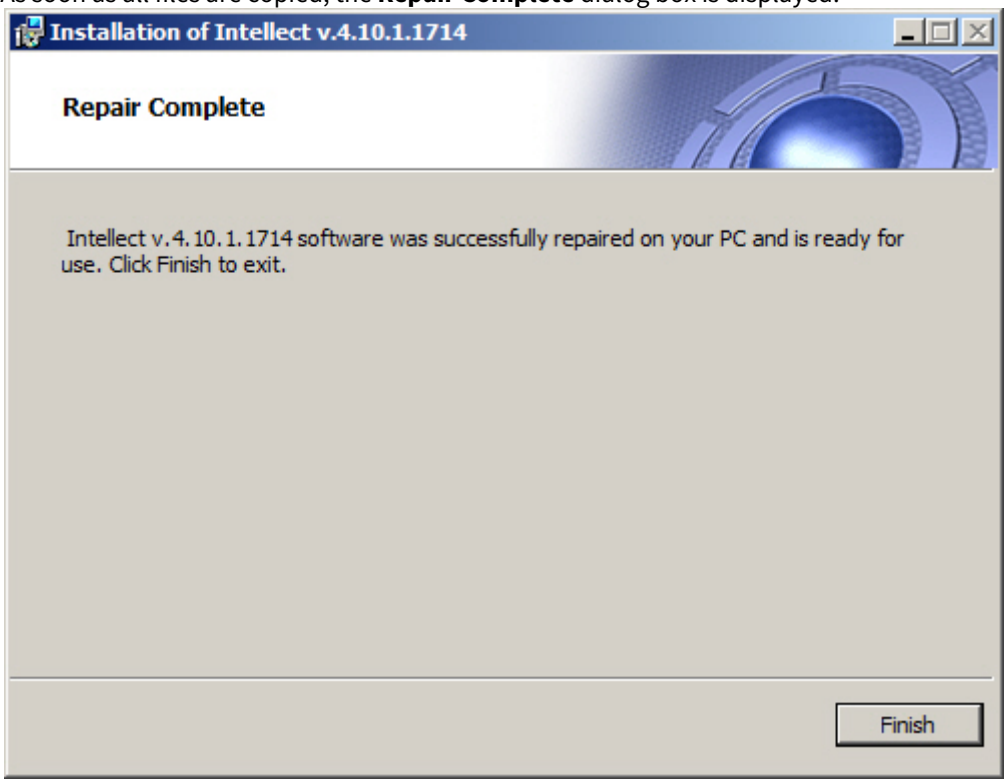
3. To select INTELLECT™ software components repair mode, select **Repair** installation type and click **Next**.
   The **Repairing Intellect** dialog box is displayed.



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



4. To continue INTELLECT™ software installation, click **Continue Anyway**.
   As soon as all files are copied, the **Repair Complete** dialog box is displayed.



5. Click the **Finish** button.

INTELLECT™ software is now repaired.

6.3 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.

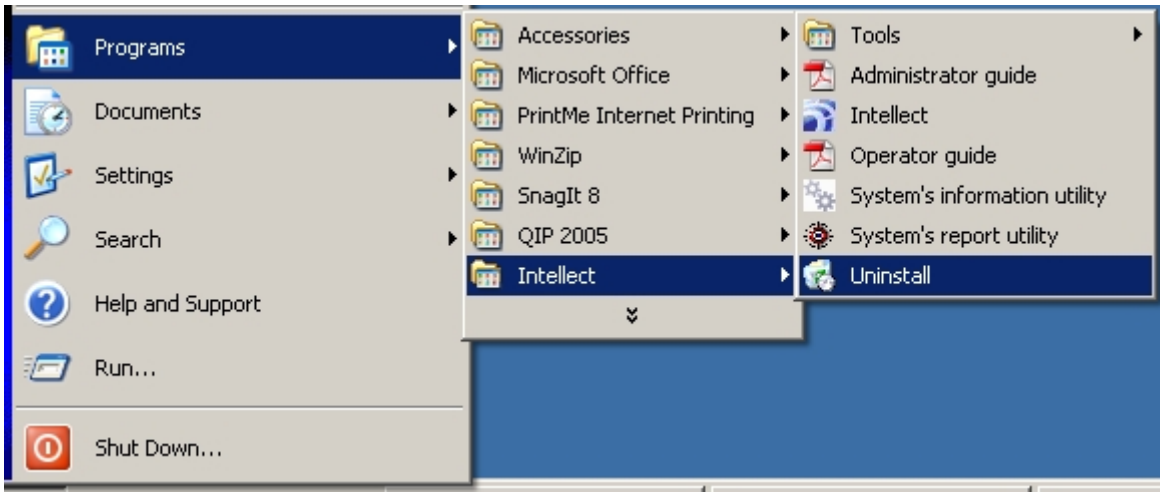
The *Intellect* software removal process can be launched using one of the following ways:

1. Using the Start menu;
2. With the help of OS Windows panel «Add or remove programs»;
3. With the help of installation CD.

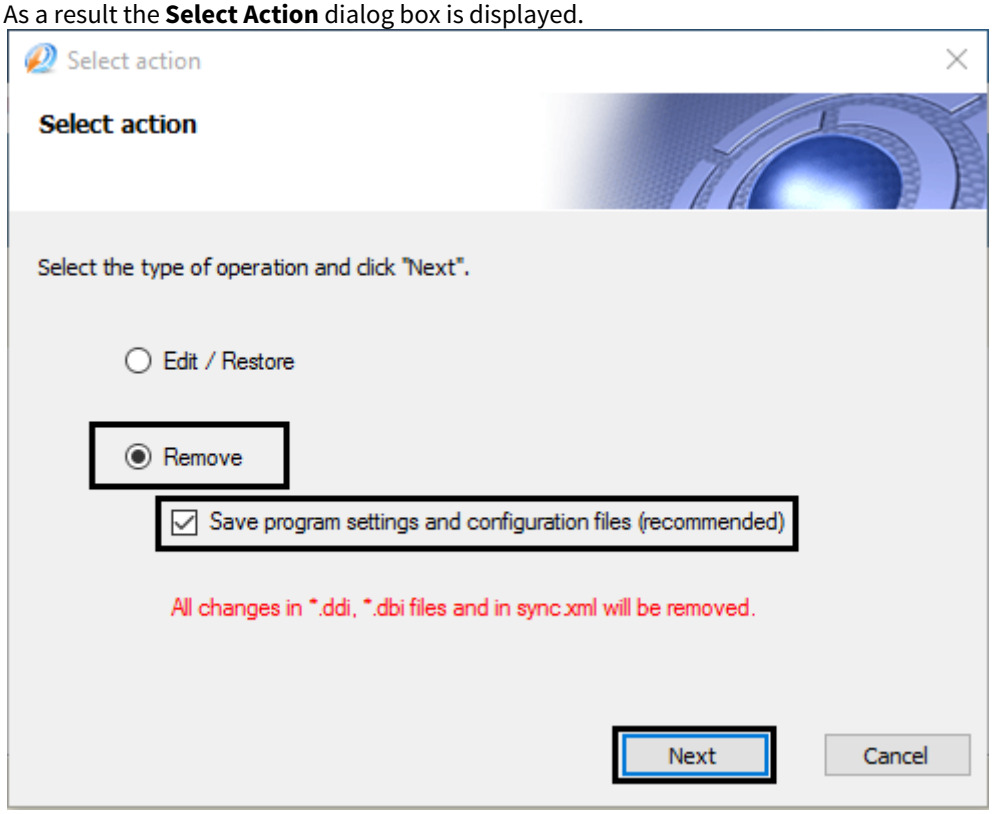
6.3.1 Removing INTELLECT™ software from the Start menu

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

1. In the command prompt select the following: **Start -> Programs -> Intellect** and then **Uninstall** in the drop down list, as shown in the figure.



As a result the **Select Action** dialog box is displayed.



2. Select the **Remove** type.
3. If INTELLECT™ software settings are to be saved in the database, set the **Save program settings and configuration files (recommended)** checkbox.

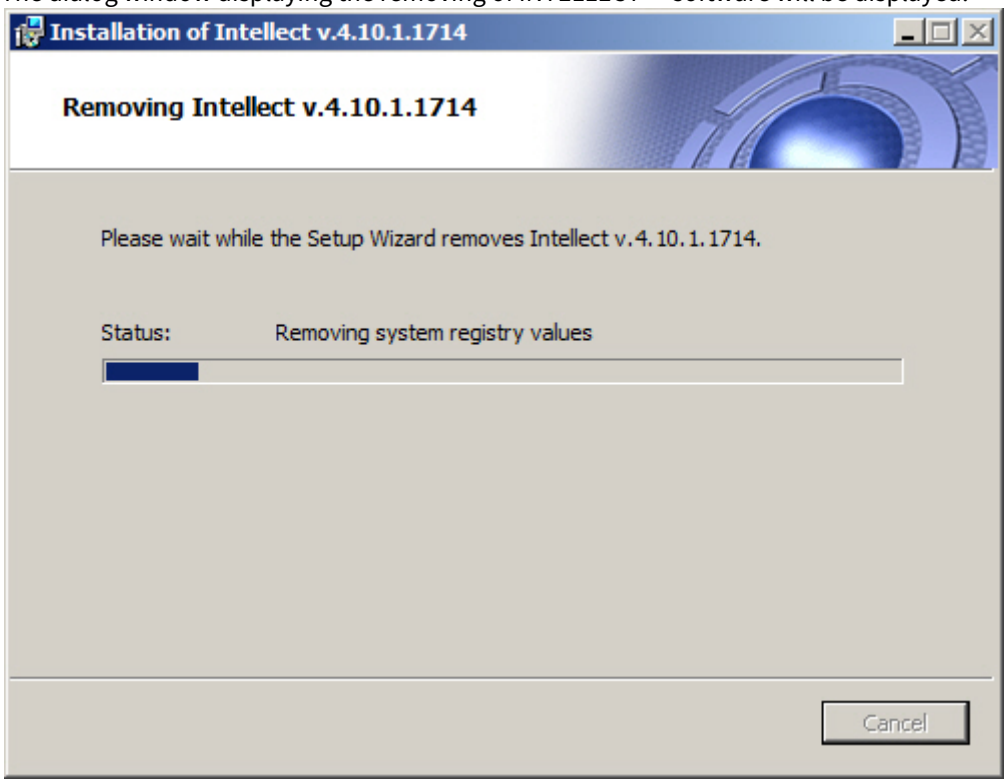
> **Note.**
>
> If the “sync.xml” file was changed, then after removing with saving of the configuration it will not be deleted, but the next time you install INTELLECTTM software it will be overwritten.
> If using the ddi.exe utility the user has changed ddi or dbi files install along with *Intellect* software, then these files will be deleted when removing with saving of the configuration. If the user has created new ddi or dbi files, they will be saved.

4. Click the **Next** button.

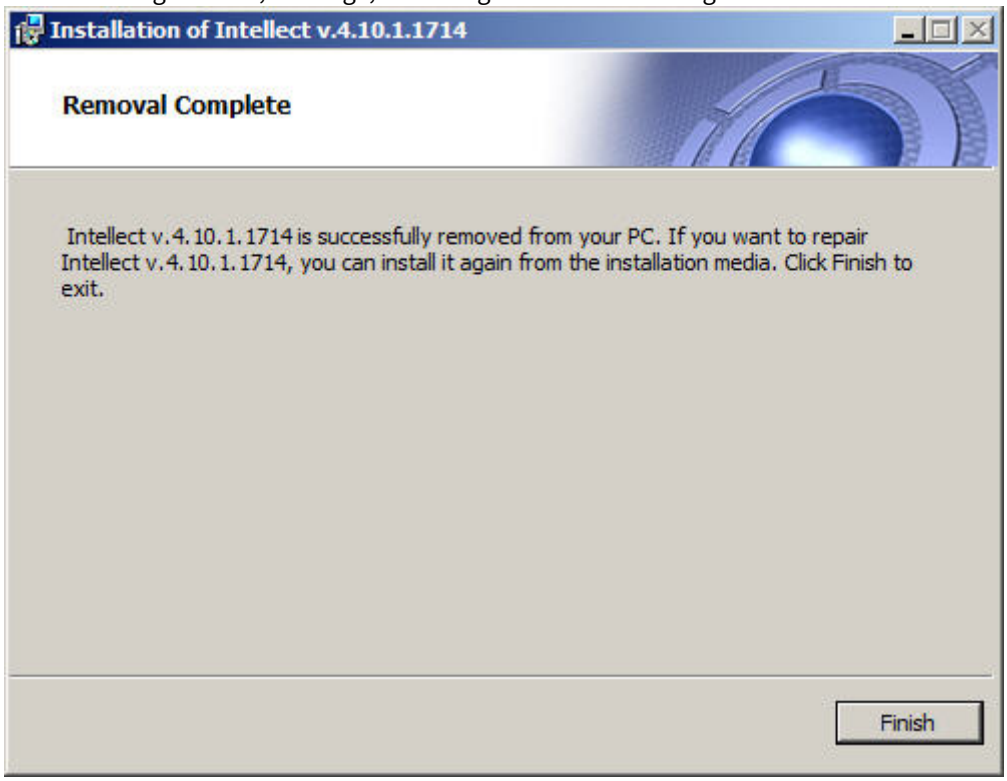
Note.

Click the **Cancel** button to interrupt INTELLECT™ software removing.

The dialog window displaying the removing of INTELLECT™ software will be displayed.



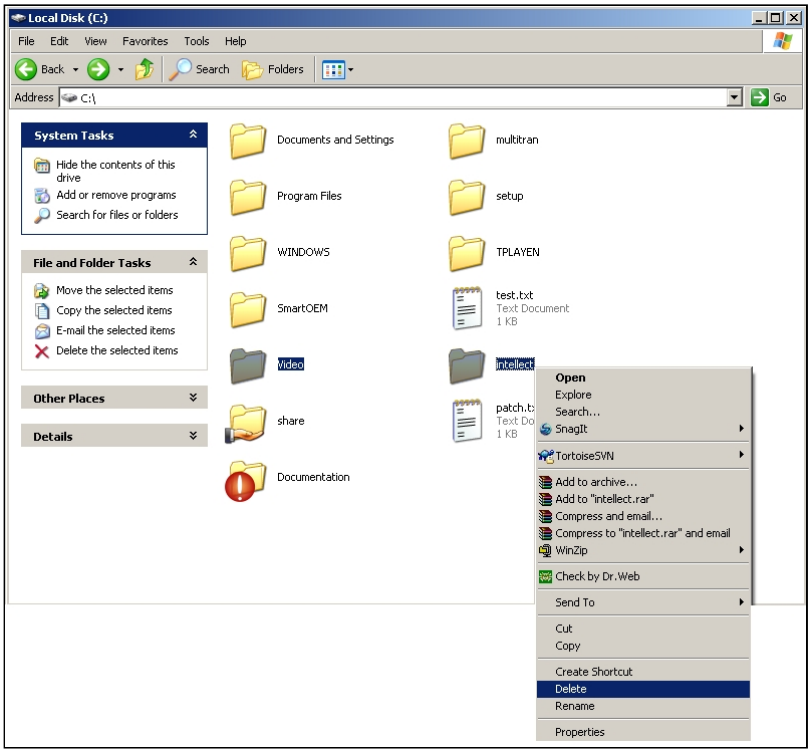
After removing the files, message, informing about the removing of INTELLECT™ software will be displayed.



5. Click the **Finish** button.

Note.

For complete deletion of INTELLECT™ software files delete the installation catalog and all the created Video folders for storing the audio and video recordings manually.



Note.

Please take into consideration, that the name of the INTELLECT™ software installation folder may differ from the default name (C:\Intellect).

Note.

In certain cases, Windows OS should be restarted before the INTELLECT™ software installation folder is deleted (for instance, Folders/Intellect).

Note.

We do not recommend deleting the INTELLECT™ software installation folder, if you need to re-install INTELLECT™ software. The folder contains:

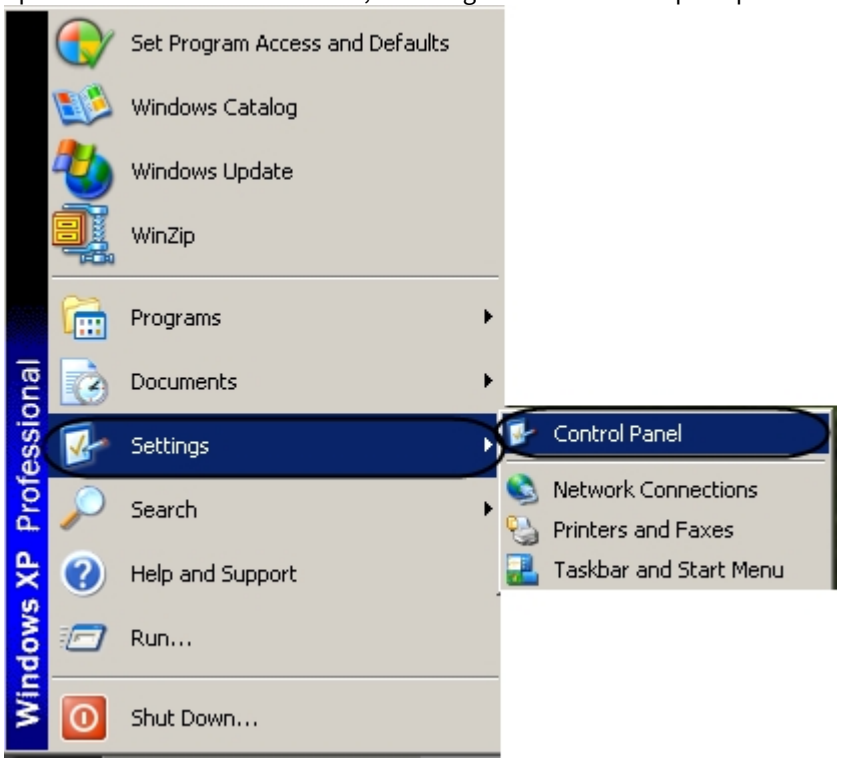
1. folders with video records and frames of video records exported during INTELLECT™ software operation;
2. log files containing the information about INTELLECT™ software module operations;
3. backup copies of these files.

At this stage the deletion process of Intellect software from the **Start** menu is over.

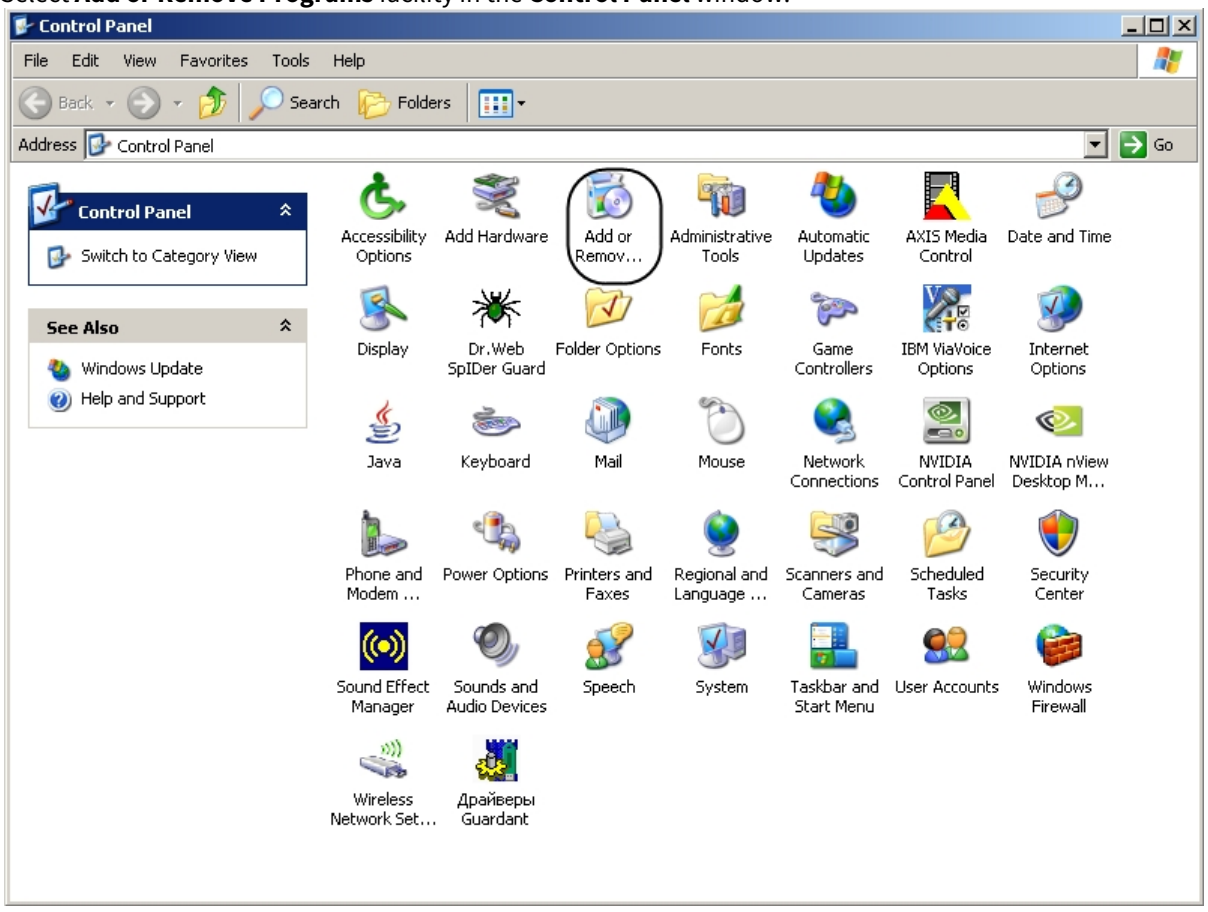
6.3.2 Removing INTELLECT™ software from the OS Windows panel Add or Remove programs

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

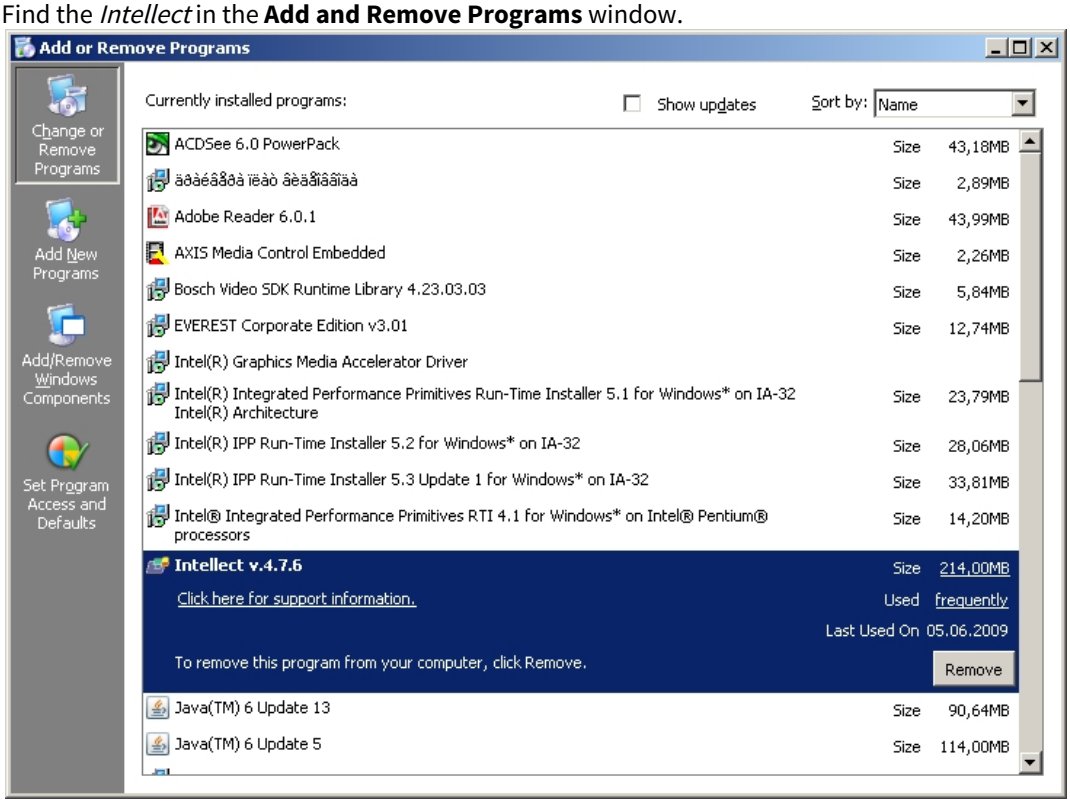
1. Open the **Control Panel** window, selecting in the command prompt: **Start ->Settings ->Control Panel**.



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™ software 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.

6.3.3 Removing INTELLECT™ software with the help of installation CD

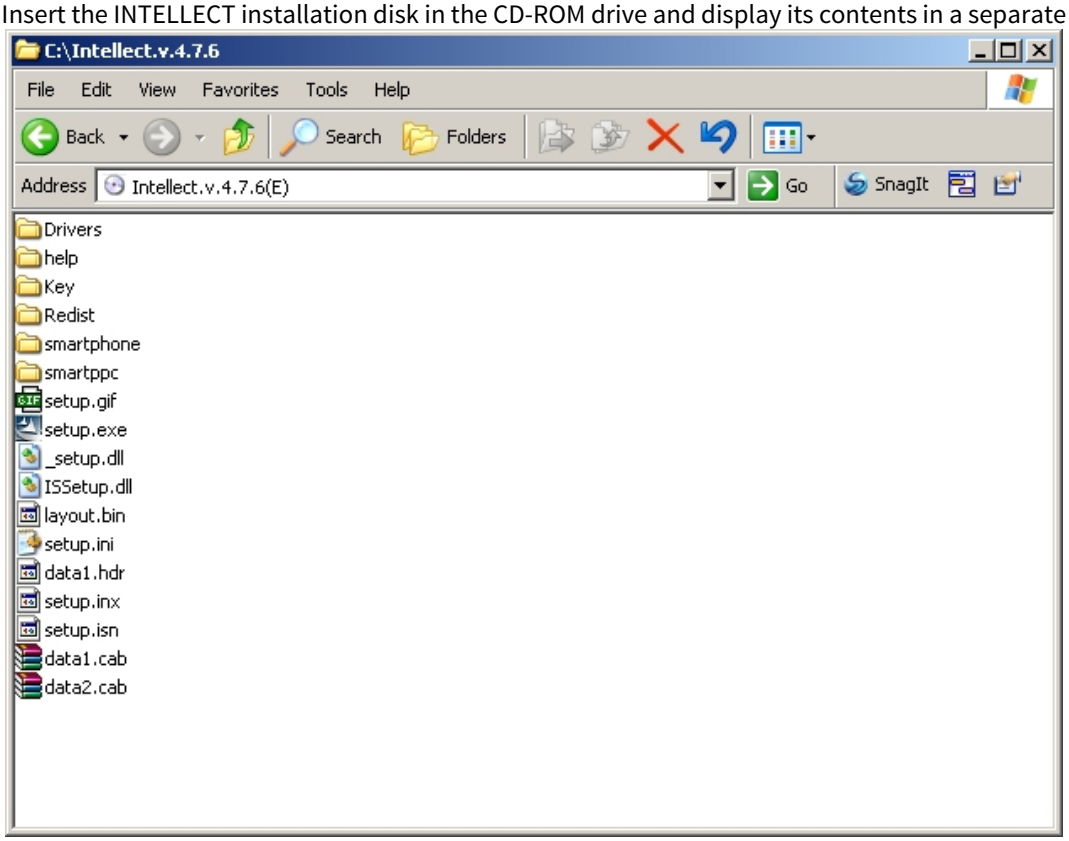
Installation program *Intellect* works in a deletion mode. This mode is required when all the components of the *Intellect* software should be deleted.

Run the installation CD with *Intellect* software manually without removing the previous version 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. Insert the INTELLECT installation disk in the CD-ROM drive and display its contents in a separate window of your PC.



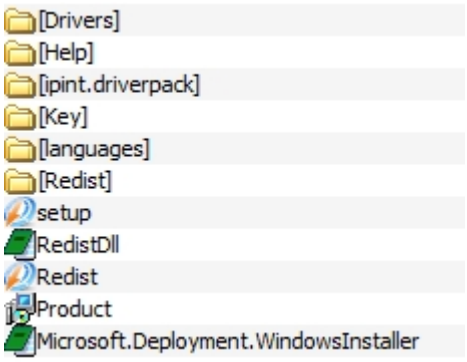
2. Launch the file Setup.exe
   As a result the **Select Action** dialog box is displayed.
3. Follow steps 2-5 of the instruction in section Removing INTELLECT™ software from the Start menu.

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

6.3.4 Removing INTELLECT™ software installed as a Service

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

1. Insert the INTELLECT installation CD in the CD-ROM drive and display its contents in a separate window of your PC.



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, with the help of installation CD is over.

6.4 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.

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	The Intellect software deletion saving the configuration
/removeall	The Intellect software deletion without saving the configuration
/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.

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\").

6.5 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. At the time of writing this documentation the utility description is located on http://msdn.microsoft.com/ru-ru/library/aa394531.aspx.

> **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.

6.5.1 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="ru" TRANSFORMS="%Path_to_folder_with_distributive%\Setup\ru\ru.mst" CMD_INSTALLTYPE="Server"

Where

REBOOT=ReallySuppress – cancel computer reboot when installation finished,

LANGUAGE="ru" – select the language of product. Default product language is English.

TRANSFORMS="% Path_to_folder_with_distributive %\Setup\ru\ru.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).

6.5.2 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.

6.5.3 Remote removal of Intellect software

For remote removal of the Intellect software, do 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 – name under which the Intellect software installed. It is usually «Intellect v.Build_number».

These names can be found in the catalogue in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall section.

6.6 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 fot 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 http://technet.microsoft.com/en-us/library/bb625087.aspx).

6.6.1 Example. Combination of two Servers to the cluster and the Intellect software configuration

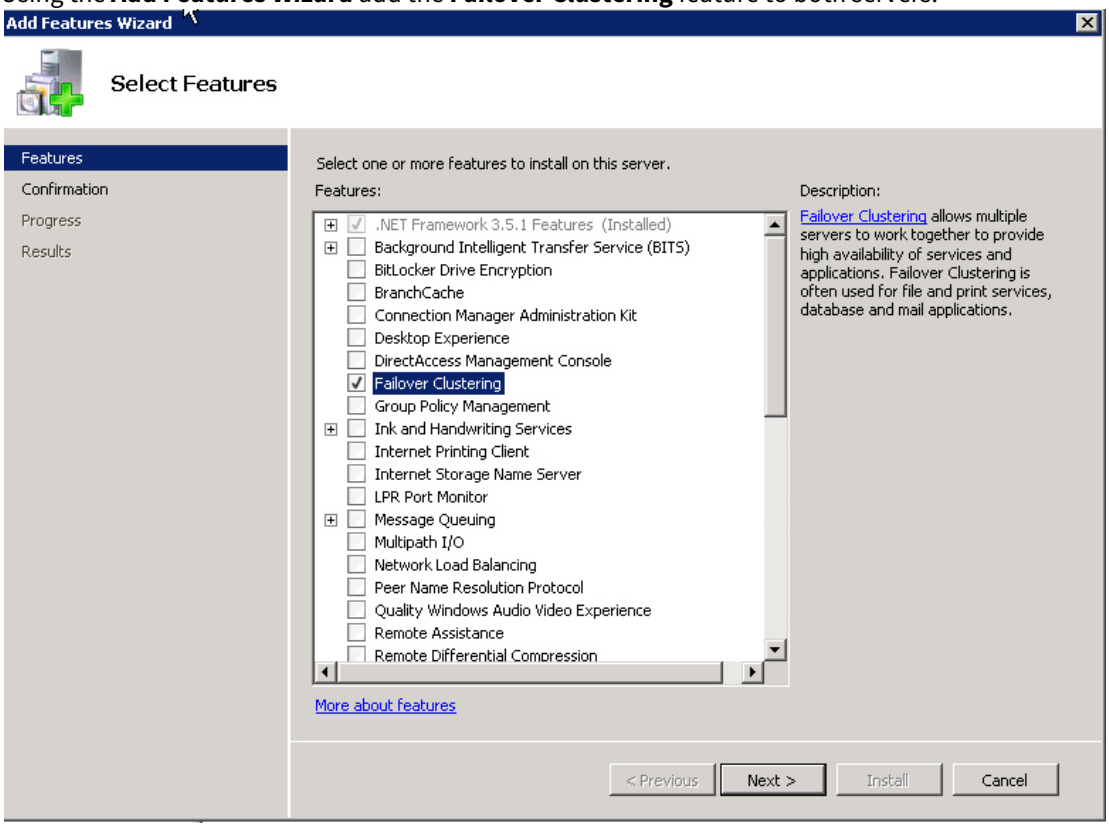
On the page:

- Previous configuration of servers
- Combination of two Servers to the cluster and the Intellect software configuration

6.6.1.1 Previous configuration of servers

Before combination of Servers to the cluster, do the following:

1. Install the 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.

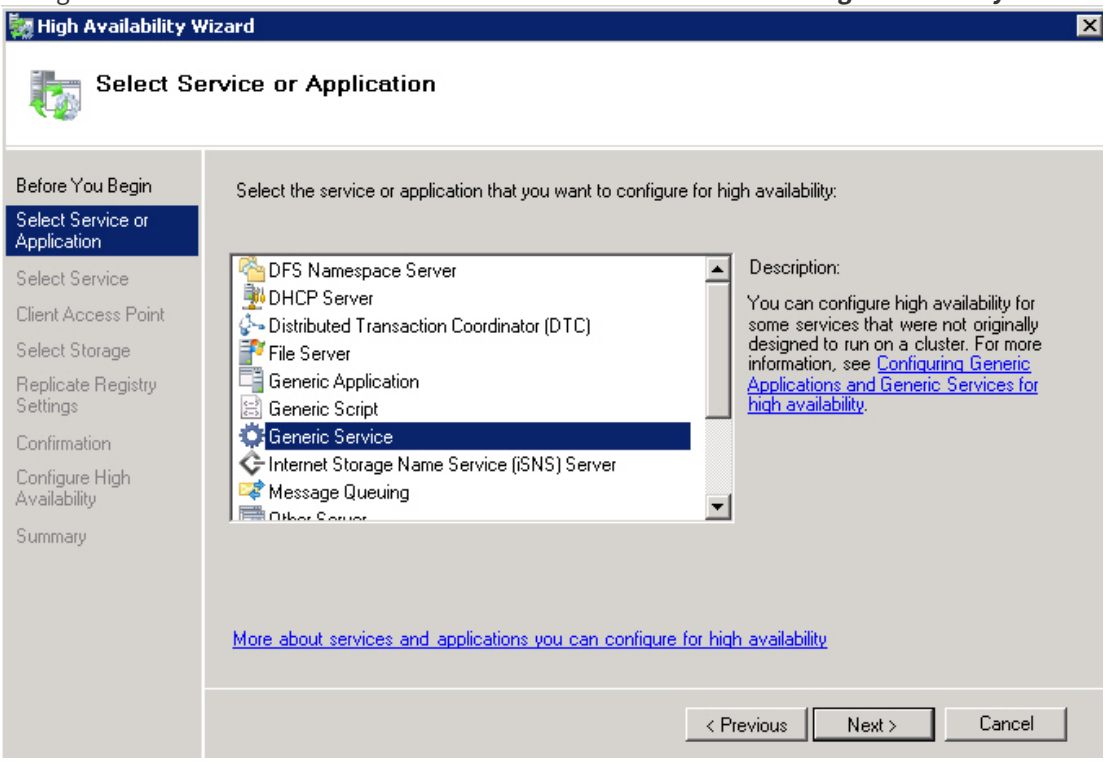


4. Enter the following parameter for the RAID supporting as a storage for cluster to the register:
   Location - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ClusDIsk\Parameters
   Name - AllowBusTypeRAID
   Type - DWORD
   Value - 1
5. Restart both servers.
6. Create three disks on the common 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 over disks to online mode, create sections on all disks and format them.
11. Switch over disks to offline mode.
12. Enter the **second server** and initialize disks such way.

6.6.1.2 Combination of two Servers to the cluster and the Intellect software configuration

To combine two Servers to the cluster and configure the *Intellect* software, do the following:

1. Install the *Intellect* software of proper version on both Servers before combination them to cluster.
2. Set the ITV\INTELLECT\IntellectRunService\InheritServiceEnvironment parameter with the value 1 in the registry.
3. Stop **SQL Server (SQLEXPRESS)** and **ITV Intellect Core Server** services on both Servers and switch over them to the manual type of start.
4. Start the **Cluster failsoft executive program** 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 failsoft cluster.
7. Specify NetBios name and IP-address for the failsoft cluster (this data will be in use for connection of settings panel).
8. Complete the cluster creation.
9. Configure the role on cluster. Select **Add service - Generic Service** in the **High availability Wizard**.



10. Select the **ITV Intellect Core Server** service.

11. Configure NetBios name and IP-address for the service (these parameters will be used for connection to the Intellect software).
12. Complete the role configuration.
13. Set the dependence on Name and IP-address on the **Dependence** tab in the settings of service.
14. Set the **Use network name for computer name** (the name will be transmitted in capitals apart of the registry in settings of cluster) checkbox 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 service.
18. Select the **ITV 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, replace database files on the disk of the failsoft array and connect the database again.
20. Set the user name and password for database connection in the idb.exe.
21. Start the Tweaki.exe and rename the computer to the name of failsoft cluster.
22. In the cluster setting select **Additional actions - Replace primary cluster resources - Select unit**. Specify the second Server.
23. In the SQL disconnect ald databases and connect new databases from the disk in failsoft array.
24. Change the user name and password for database connection in the idb.exe.
25. Start the **ITV Intellect Core Server** in the **Cluster failsoft executive program**.
26. Start the *Intellect* software. Ensure in the start accuracy.

Combination of two Servers to the cluster and the *Intellect* software configuration are completed.

7 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.

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 to the equipment is performed by three means:

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

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.

7.1 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.

At the moment of writing the documentation the binding of following elements has been realized:

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

> **Note.**
>
> Before releasing 4.8.3 version in INTELLECT™ the license key was generated using the information about other equipment. If the license key was generated for INTELLECT™ software of earlier version ,then its features are saved — see documentation about earlier versions https://doc.axxonsoft.com/confluence/display/ASdoc/AxxonSoft+documentation+repository

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.

7.2 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:

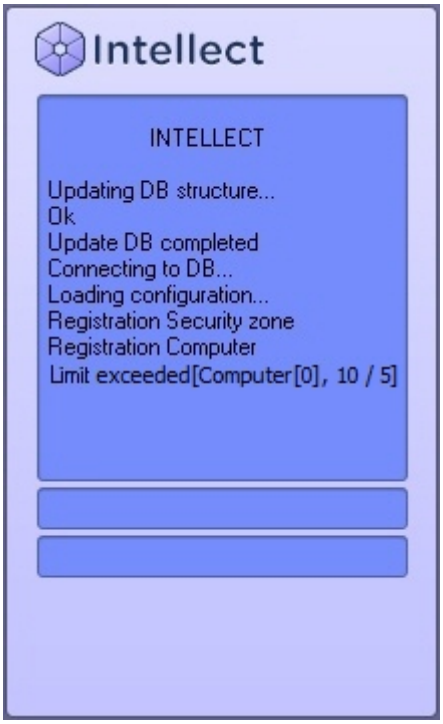
1. Computer HID is read where the Intellect software is run.
2. License key is read.

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.

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

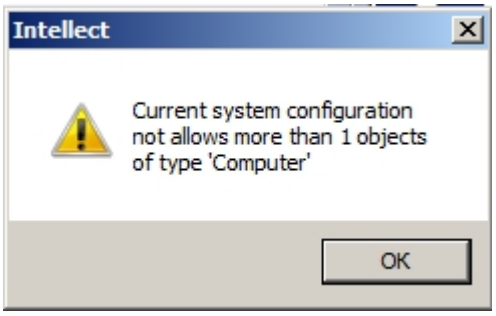
When the INTELLECT ™ software is started with the key and exceeded object limit, there is the message with the name of object because of which the limit is exceeded and the number of objects "created / permitted". The internal ID of the object type in the license key is shown in square brackets.



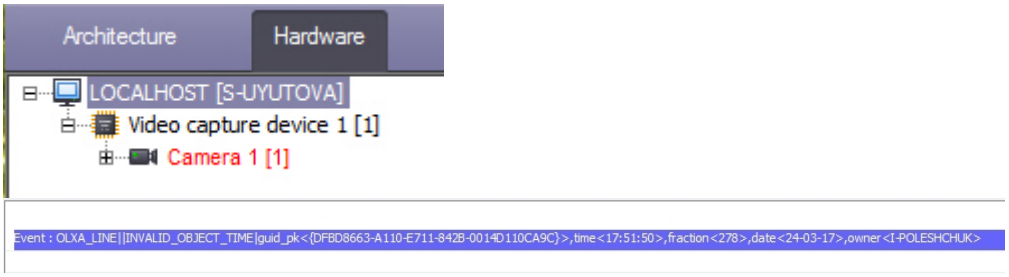
In this case to start the INTELLECT ™ software operation, do the following:

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 you try to add an object that is not provided by the key, there will be the message that current system configuration does not allow more than 1 object of this type.



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 use of an expired object, connect ITV|AxxonSoft Manager in order to update the intellect.sec license key. If the object is no longer required, it can be deleted (see Deleting).

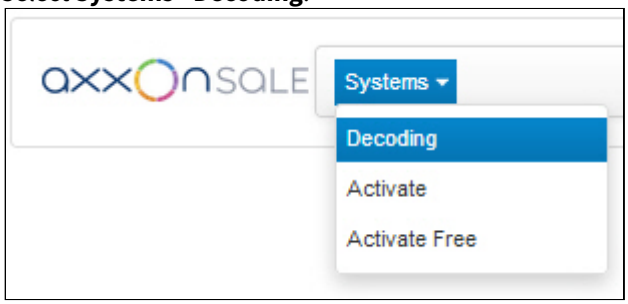
The time of action of the object can not be longer than the validity of the temporary key.

7.4 Decoding license key

It is possible to 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.

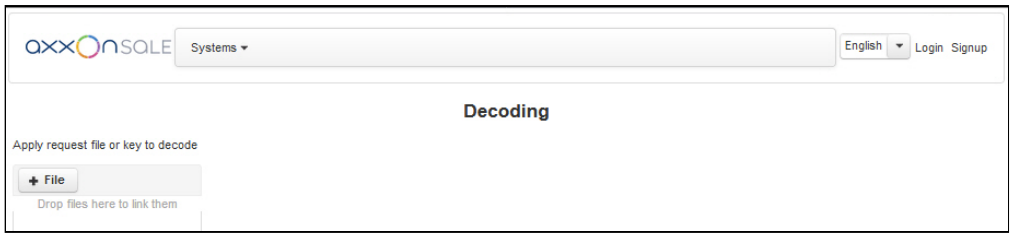
For this do the following:

1. Go to https://sale.axxonsoft.com/
2. Select **Systems** - **Decoding**.

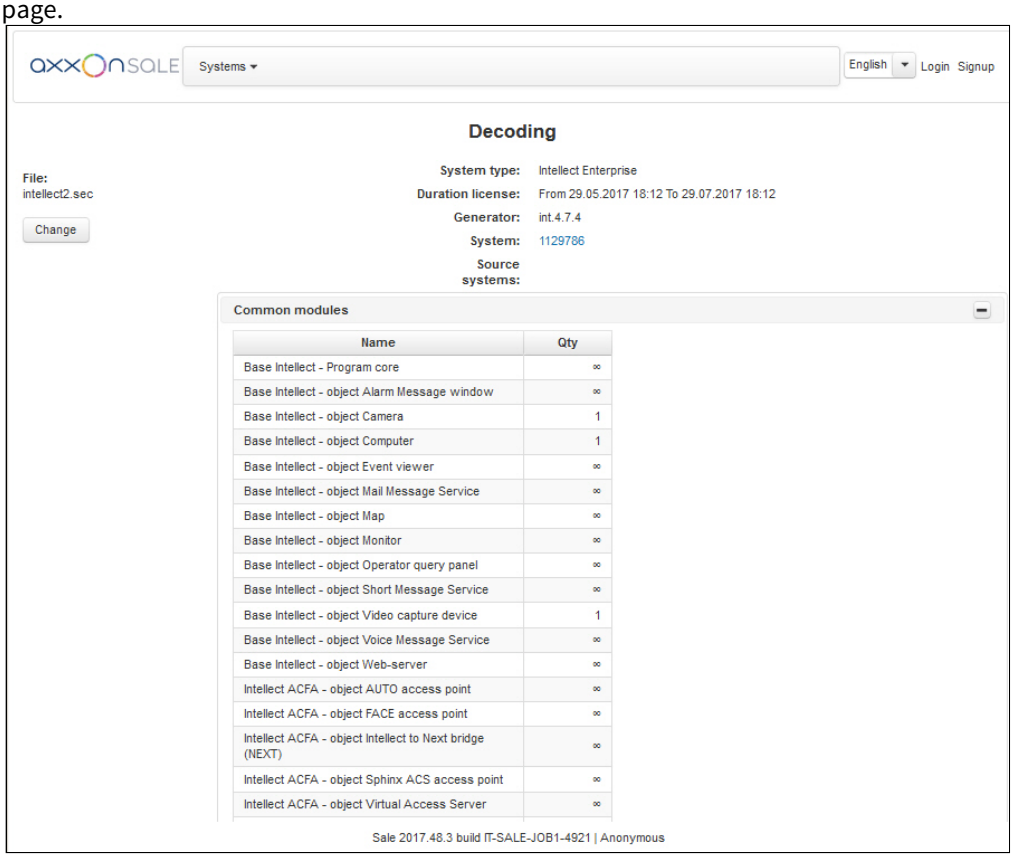


3. Add intellect.sec license file to the **File** form.

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



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



8 Configuring system startup and shutdown

8.1 Configuration of Intellect™ software startup

8.1.1 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.

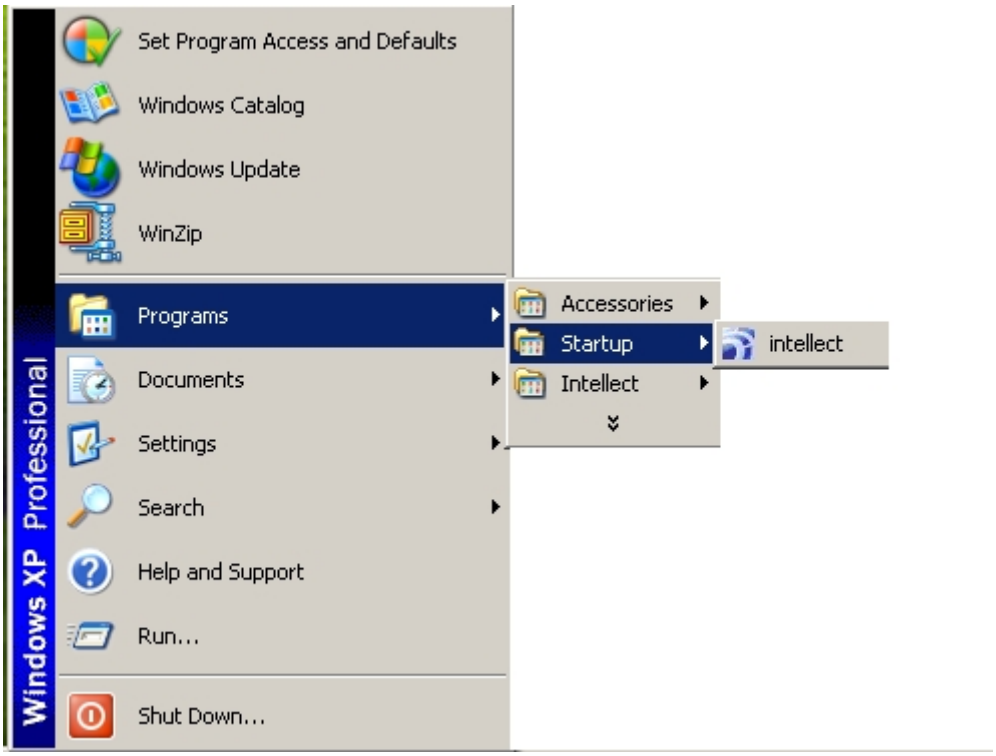
Note.

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.

8.1.2 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 from the **Startup** function, the *Intellect*™ system icon should be placed in the **Startup** group of the **Start** menu.



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.

8.1.3 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. This procedure requires assigning a name (login) and a password of the user, which will be used for the PC authorization 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.

8.2 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..

9 Working with the System settings dialog box

9.1 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.

9.2 Startup and shutdown of the System settings dialog box

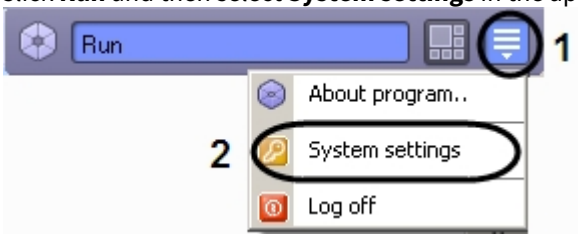
9.2.1 Startup of the System settings dialog box

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.



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

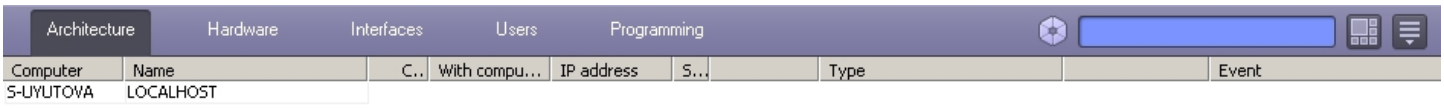


Note.

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.

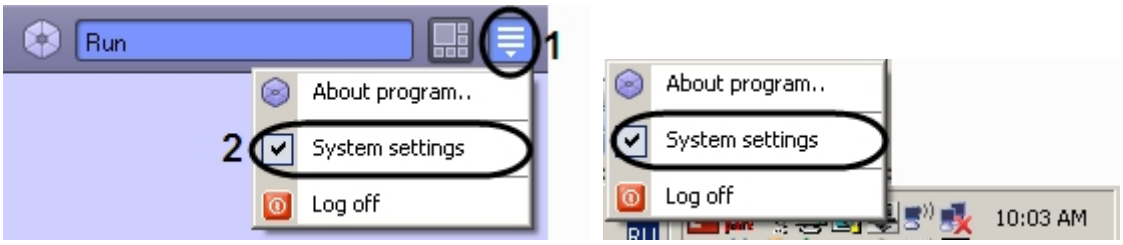
If captions are displayed incorrectly in the interface because there is no such font in the system, then install the font located in the Redist\Font folder. Information on how to install fonts in Windows up to 7 can be found at https://support.microsoft.com/en-us/help/314960/how-to-install-or-remove-a-font-in-windows.

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.

9.2.2 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.

9.3 Setting procedure for system objects

On the page:

- Select an object.
- Create an object.
- Editing.
- Deleting.
- Changing the parent object.
- Copying objects

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

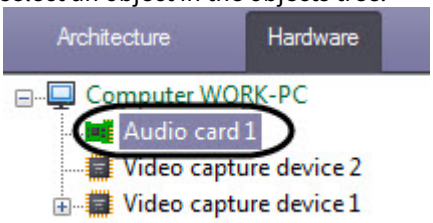
1. ### 9.3.1 Select an object.

   To select an object, do the following:

   a. open the **Hardware** tab containing objects tree;

   b. select an object in the objects tree.

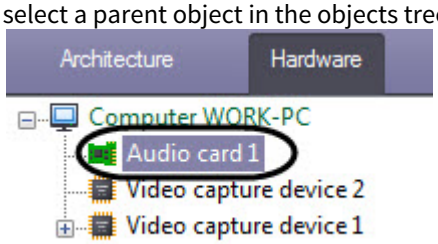
2. ### 9.3.2 Create an object.

   To create an object, do the following:

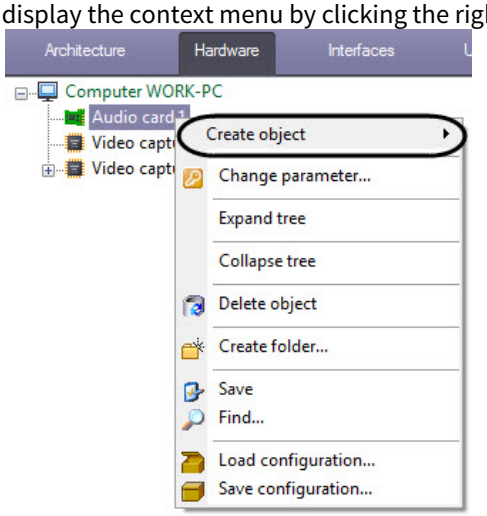
a. open the **Hardware** tab containing objects tree;



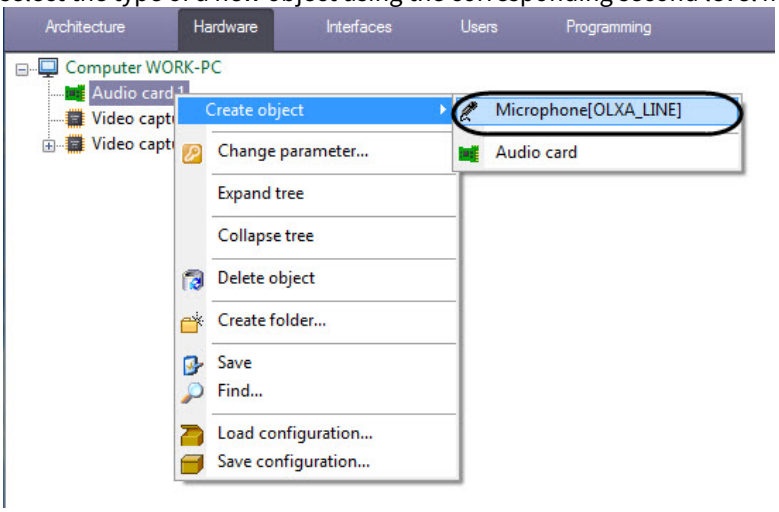
b. select a parent object in the objects tree, which should be used as a basis for the creation of a child object;



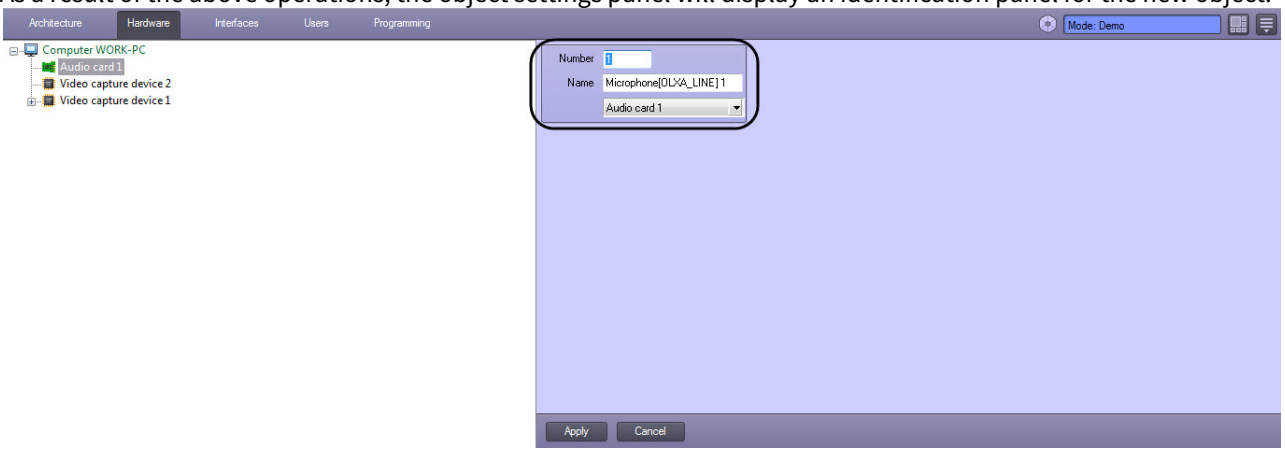
c. display the context menu by clicking the right mouse button and select **Create object**;



d. 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.



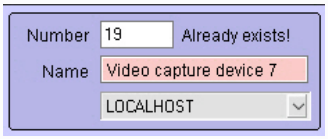
e. specify a unique identification number in the **Number** field (1) and the unique name of a new object, **Microphone** in the example on the figures, in the field **Name** (2).



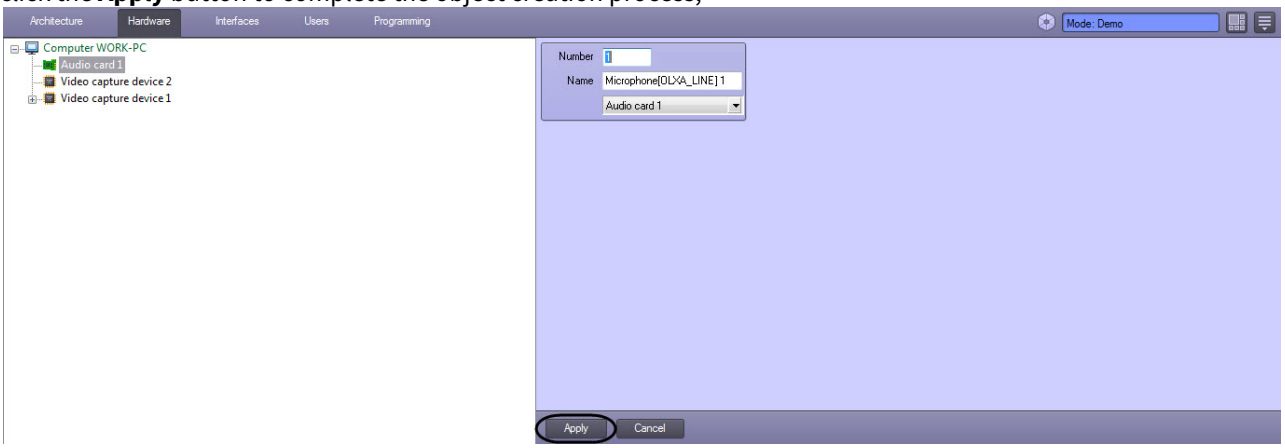
Note.

Entering of > and < symbols is forbidden in the **Name** filed. They will be removed when settings applying if these symbols are used in the object name.

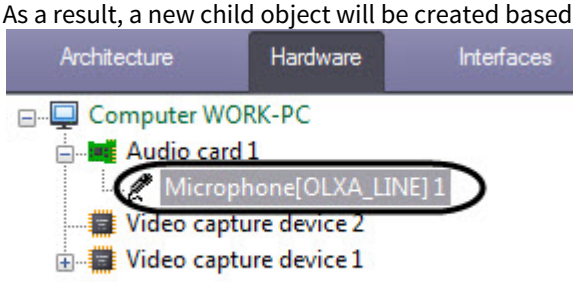
If the identifier or the name are not unique, the corresponding message is displayed on the panel while the field is highlighted in red.



f. click the **Apply** button to complete the object creation process;



g. 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 child objects using the ⊞ icon, and collapse the list using the ⊟ icon.

3. 9.3.3 Editing.

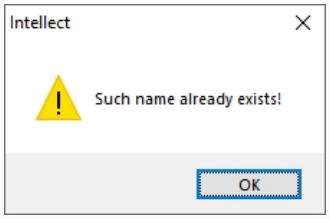
Editing means any modification of the object settings, i.e., changes in the object parameter values. The tools panel of the system object is the key configuration instrument of the object setup.
To edit an object, do the following:

a. select a system object the parameters of which are to be modified (1);
b. modify the object parameters using the tools panel of the object (2);

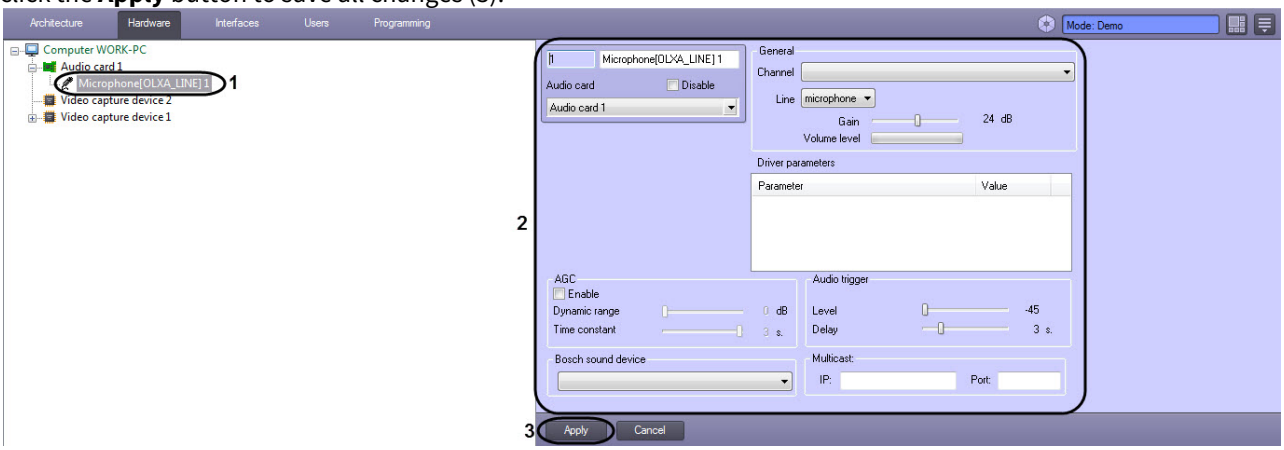
Note.

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:



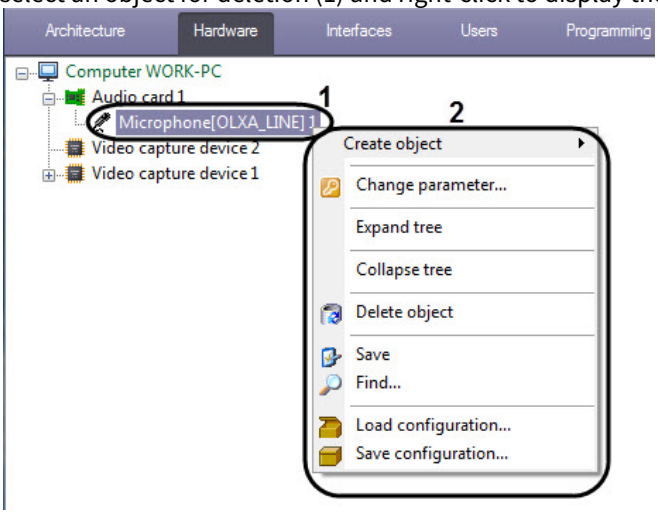
c. click the **Apply** button to save all changes (3).



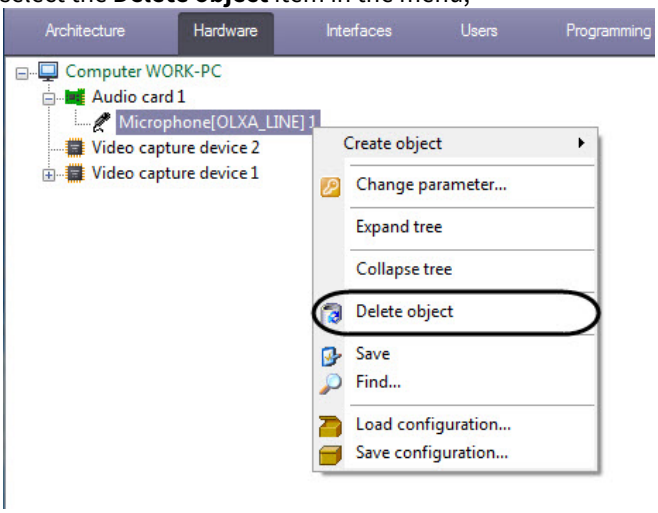
4. 9.3.4 Deleting.

To delete an object, do the following:

a. select an object for deletion (1) and right-click to display the context menu on the monitor (2);



b. select the **Delete object** item in the menu;



Now a dialog box requesting confirmation of the object deletion will appear on the monitor.

c. Click the **OK** button.

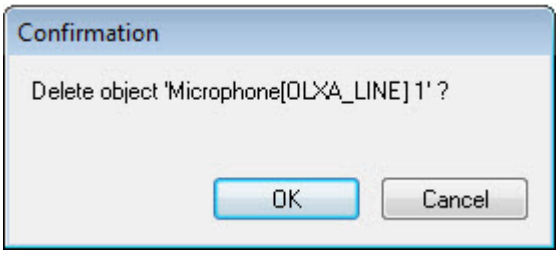
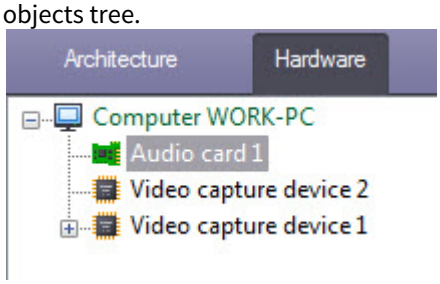


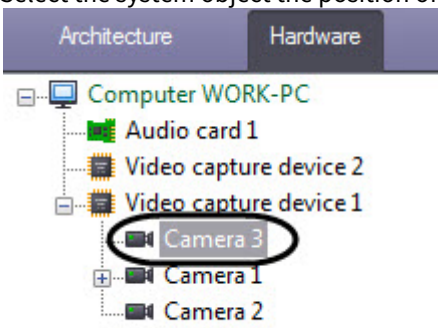
Figure below shows the result of an object deletion (objects tree contents after the object has been deleted). The object, in the example on figures the object is **Microphone**, which has been deleted is no longer displayed in the objects tree.



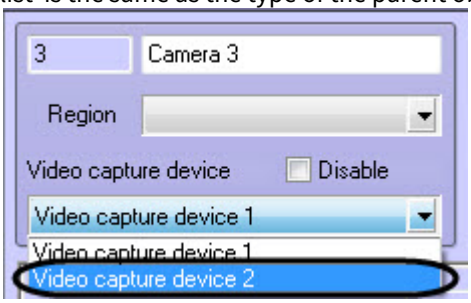
5. ## 9.3.5 Changing the parent object.

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

a. Select the system object the position of which is to be changed in the objects tree.

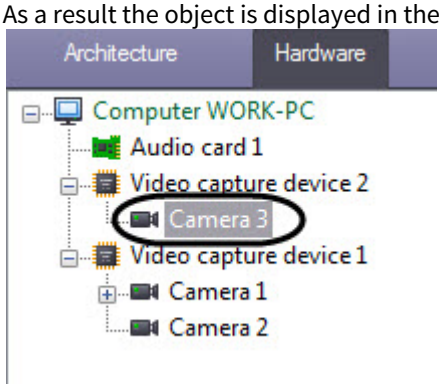


b. Select a new parent object in the drop-down list on the settings panel of the object. The name of the drop-down list is the same as the type of the parent object.



> **Note.**
>
> If the object is moved to another computer, INTELLECT™ is to be restarted on both computers – on one the object is moved to and on another the object is moved from.

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



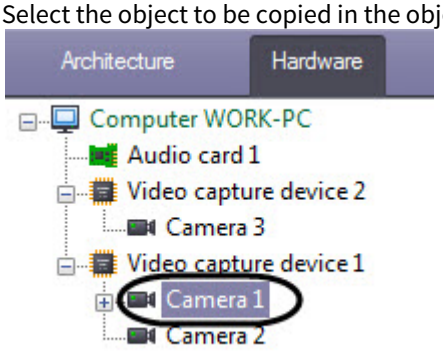
6. ## 9.3.6 Copying objects

The copy function enables cloning objects created in *Intellect* object tree (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.

Copy objects as follows:

a. Select the object to be copied in the object tree.

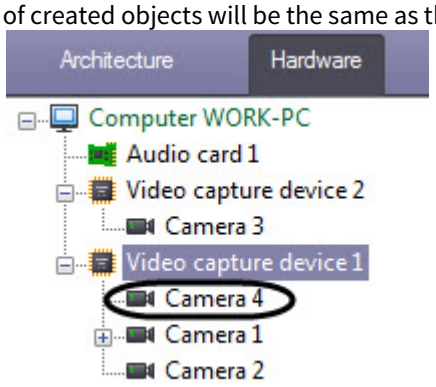


b. To copy the object press Ctrl+C.

c. Select the parent object under which the copy of the selected object is to be created or one of the objects created under the parent object.
If the copy is to be created under the same parent object as the source object, then this step can be skipped.

d. Paste the object using one of the following key combinations:
   i. **Ctrl+V** – paste only the copied object.
   ii. **Ctrl+Shift+V** – paste the copied object with all child objects.

e. The object or objects will be created with the default names and a vacant IDs will be assigned to them. Parameters of created objects will be the same as those of corresponding source objects.



Note.

Once copied object can be pasted multiple times.

10 INTELLECT™ software configuration and setup

10.1 Configuration procedure for servers, clients and remote workstations

10.1.1 Server settings

10.1.1.1 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™ software as a Server/ Administrator's workplace section).
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.

10.1.1.2 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).

10.1.2 Configuring a Remote Admin Workstation

10.1.2.1 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™ software as a Server/Administrator's workplace section).
4. License activation key.
5. MS SQL server software to control the *Intellect*™ database.

10.1.2.2 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).

10.1.2.3 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).

10.1.2.4 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).

10.1.2.5 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).

10.1.3 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 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).
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\ITV\Intellect\BackupFolder key is in the registry (HKEY_LOCAL_MACHINE \Software\Wow6432Node\ITV\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.

10.1.4 Configuring Remote Clients (RC)

10.1.4.1 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).

10.1.4.2 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).

10.1.4.3 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.

10.2 Configuration of distributed architecture

10.2.1 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

10.2.2 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).

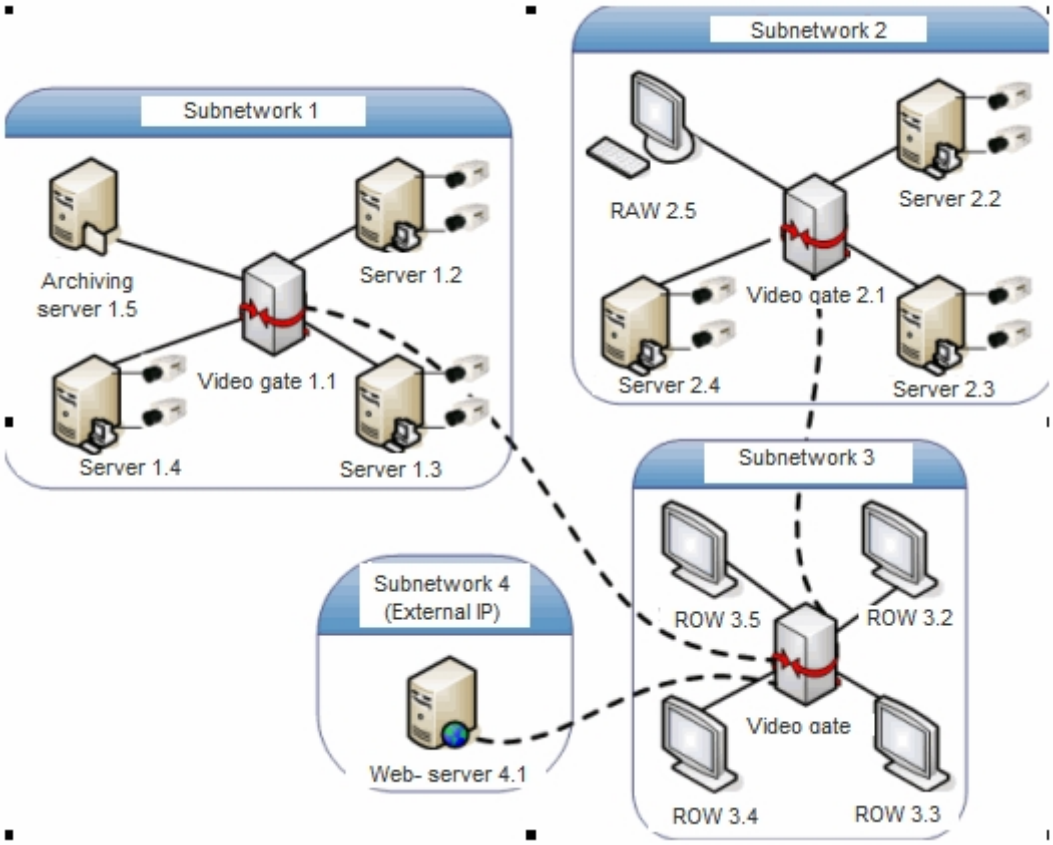
3. Register the servers, Remote Admin Workstations and Remote Clients from the same subnet on the administering server of this subnet (or at node Remote Admin Workstations and servers, that optionally realize the administering server function, if there are any subnets). If any selected subnets are present 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).

10.2.3 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.



10.2.4 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*:

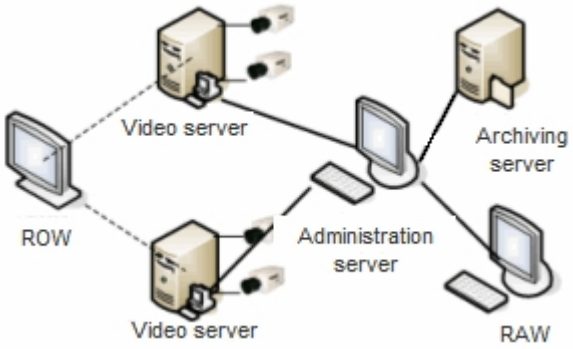
1. Configuration synchronization (see Database synchronization setup).
2. Configuration and protocol synchronization (see Database synchronization setup and make changes to sync.xml file).

   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).

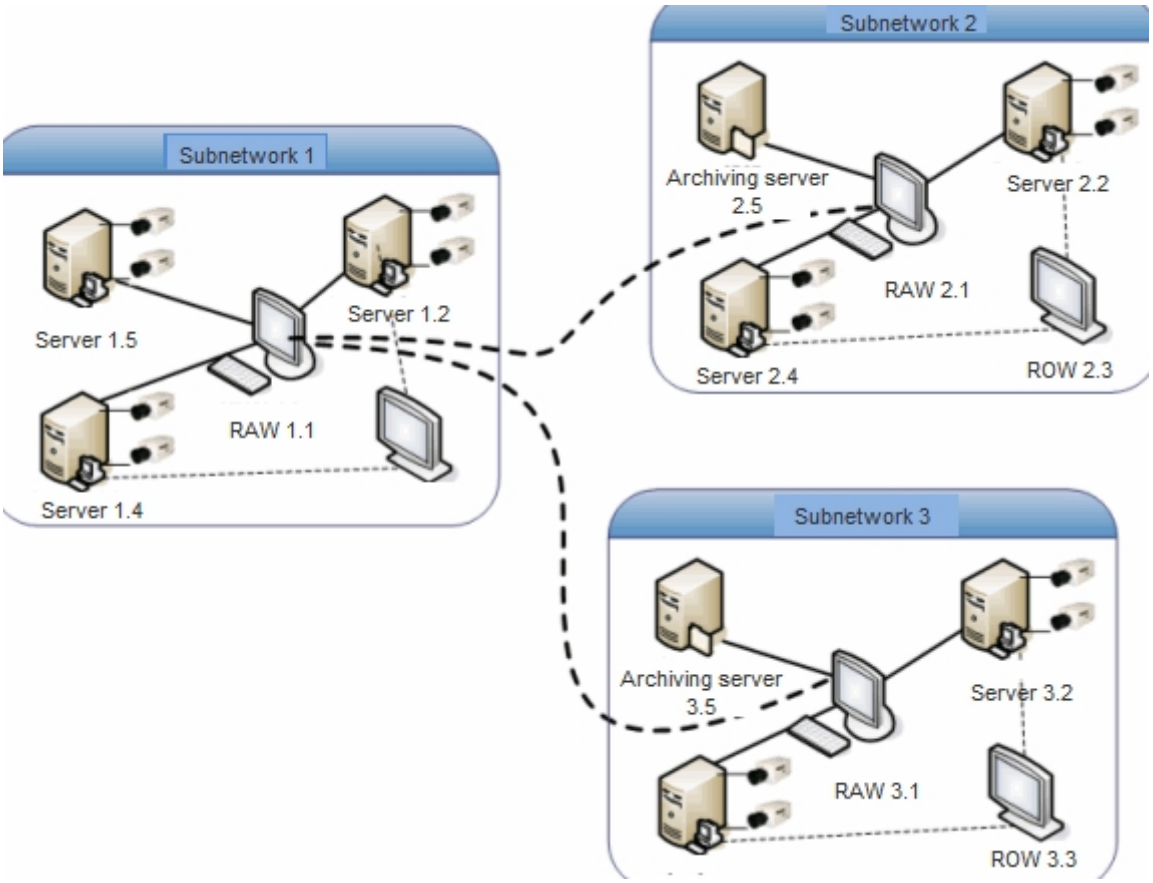
In the simplest case, database synchronization is performed for all servers and Remote Admin Workstations with the database of the administering server.



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.

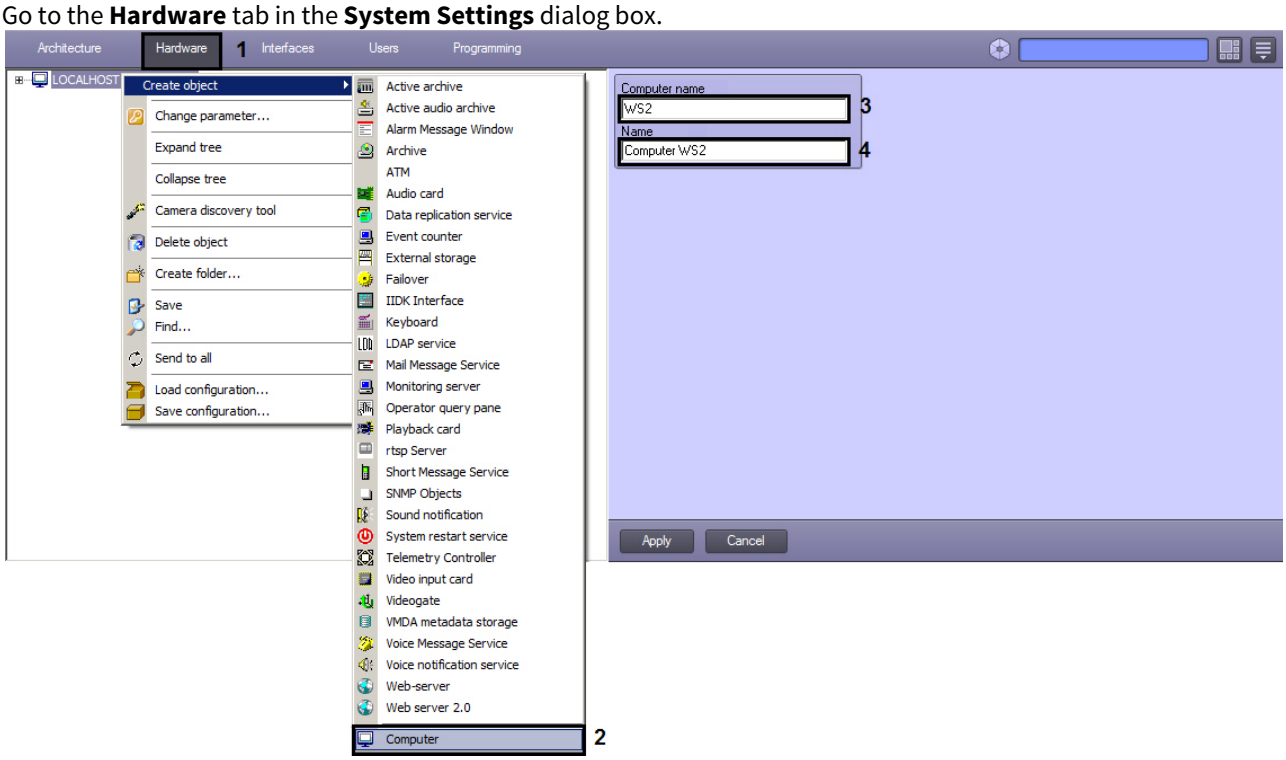
10.2.5 Registration of servers, clients and remote workstations on the administering server

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.

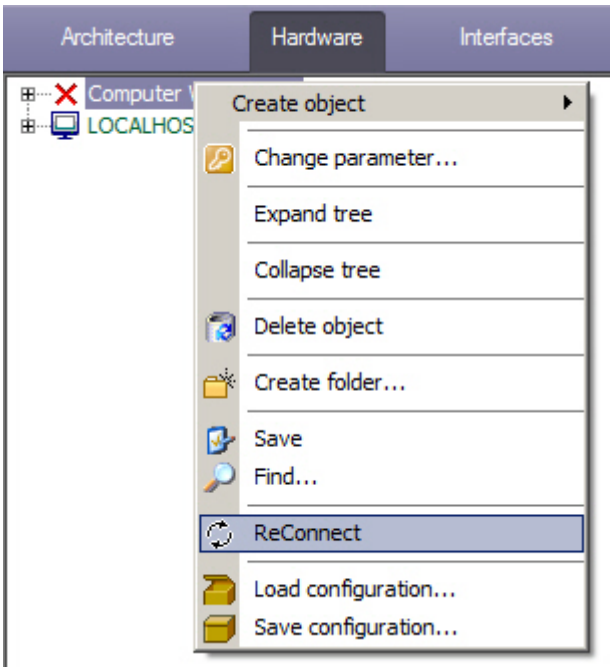
> **Note.**
>
> The maximum length for the network name is 15 characters. If the network name is longer than 15 characters, then first 15 characters are to be specified as the network name in this field.
>
> The computer name may only consist of Latin characters and digits.

   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.

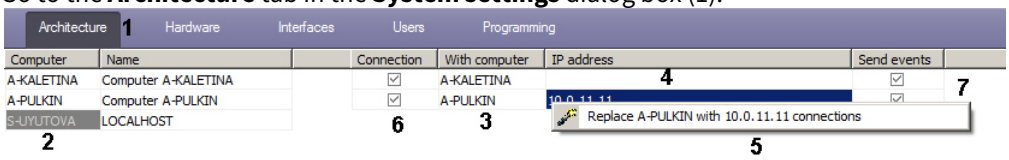
10.2.6 Configuring the interaction of distributed system components

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.

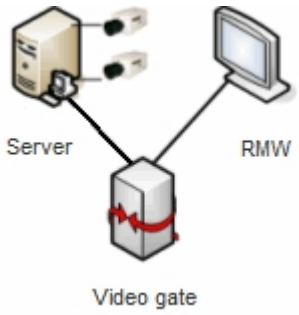
> **Note**
>
> In order to set all checkboxes in the **Connection** or **Send events** columns, highlight a box in the required column and click Ctrl+A. To set all the checkboxes unchecked, highlight a box and click Shift+A.

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.

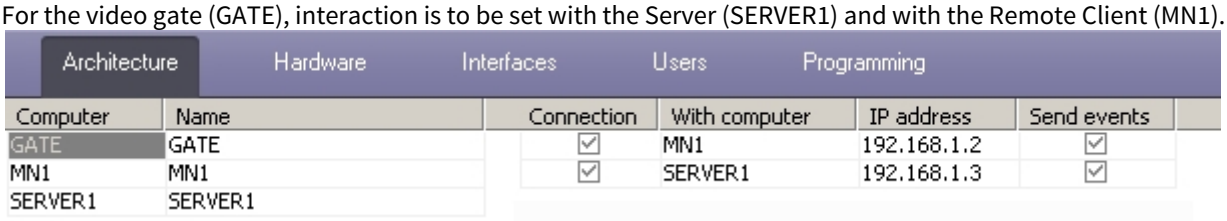
Let's consider setup of a Server and Remote Client connection via video gate as an example. A diagram of interaction of relevant components is shown in the figure.

> **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.

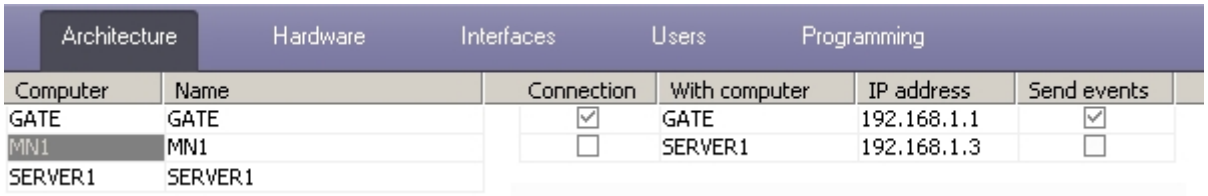


According to the diagram, shown in the figure above, interaction must be disabled between the server (SERVER1) and Remote Client (MN1). As a result, the **Architecture** tab is to display the settings:

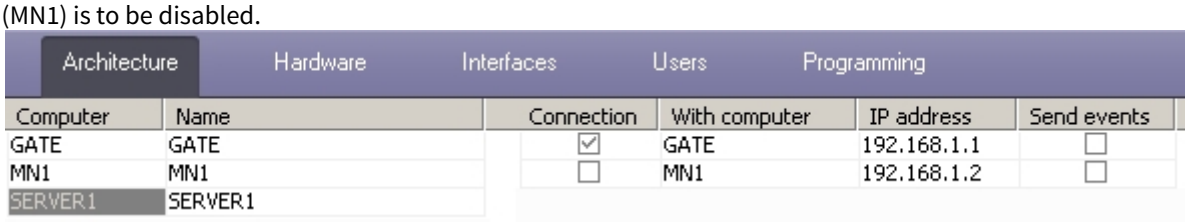
1. For the video gate (GATE), interaction is to be set with the Server (SERVER1) and with the Remote Client (MN1).



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.



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.



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.

10.2.7 Configuring time synchronization in the distributed system

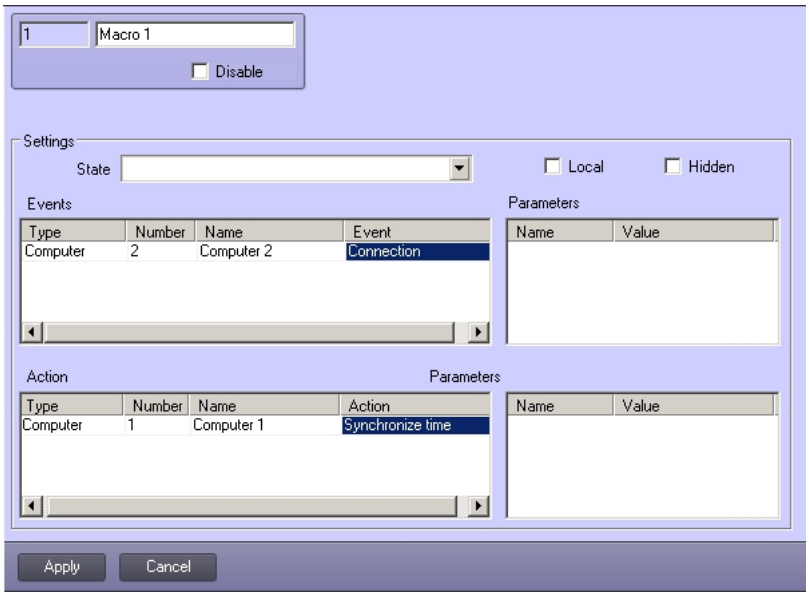
If Server is to synchronize its time with Servers connected to it when INTELLECT™ is started, do one of the following:

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 Programming Guide (JScript)).

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:



10.2.8 Role-assignment in distributed system

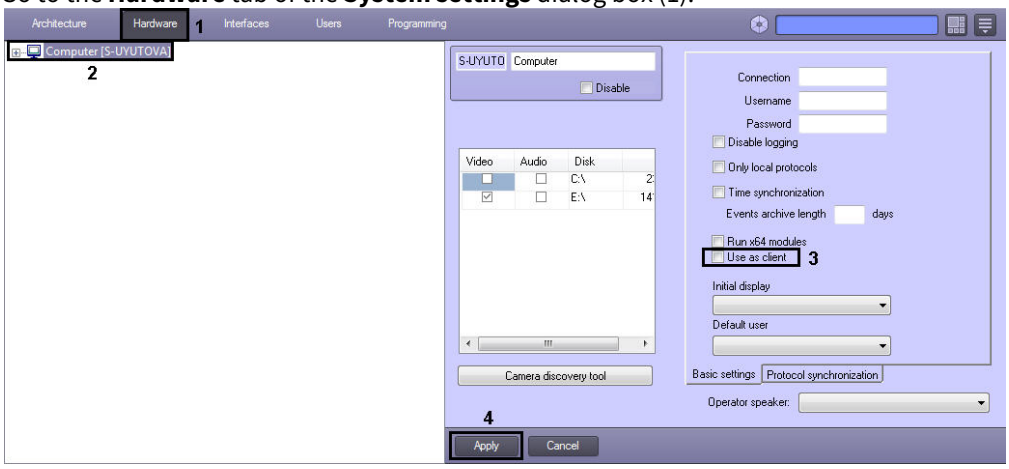
If it is certain that a computer is to be used as the Client only in the distributed systems (more than 30 computers), then it is to be specified on the settings panel of the corresponding **Computer** object. In this case software operation will be optimized.

> **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).

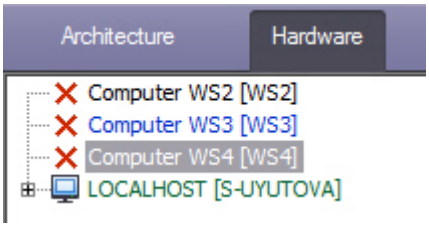


2. Select the **Computer** corresponding to the Client (2).
3. Set the **Use as client** checkbox checked (3).
4. Click the **Apply** button (4).

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

10.2.9 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.

10.3 Configuration of hardware

10.3.1 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 versions of the following modules are not available in *Intellect*:

1. The **Scene** object (see Configuring object's panoramic view by means of the Scene object).
2. Some detection tools from *Detector Pack* (at the moment of writing the documentation - the barcode detection tool only).
3. *Arena* module and *Auto-Uragan* license plate recognition as a part of *Auto Intellect*.
4. *ACFA Intellect* modules.

Some modules of *Intellect* and vertical solutions support operation in 64-bits mode only:

1. Some detection tools from *Detector Pack* (at the moment of writing the documentation - smoke, fire, sweethearting and fluid level detection tools).
2. *IntelliVision* module as a part of *Auto Intellect.*
3. *VisionLabs* and *Tevian* modules as a part of *Face Intellect*.

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:

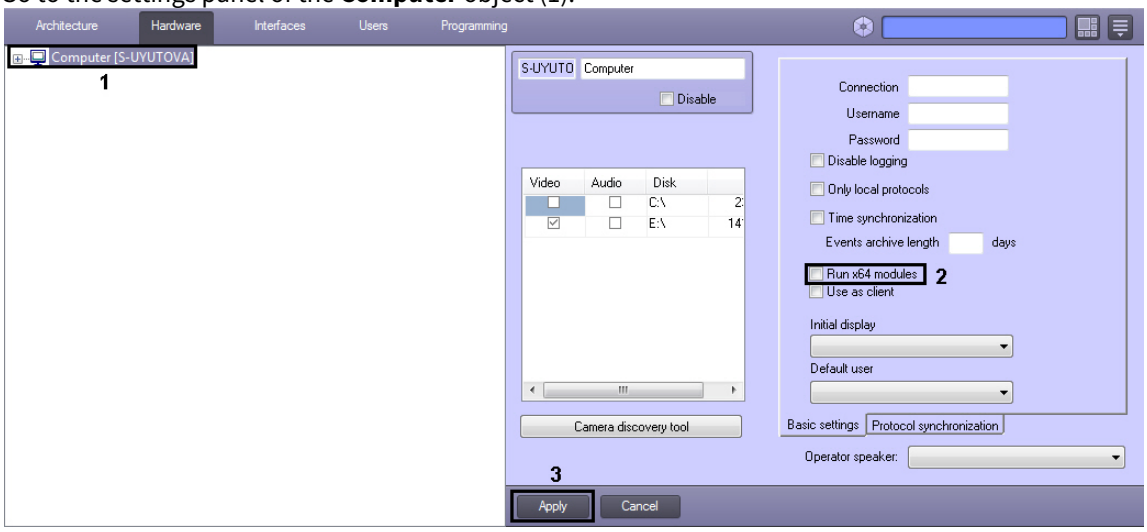
1. if the large number of cameras are to be displayed simultaneously (over 100 cameras);
2. if the large number of cameras are to be displayed in the ultrahigh resolution (over 50 cameras with 5Mpxls resolution in format without local unpacking);
3. if the large number of channels of forensic detections 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.

10.3.2 Configuring video subsystem

10.3.2.1 General information on configuring video subsystem

10.3.2.1.1 Video subsystem components description

In the video surveillance systems based on INTELLECT™ software by video subsystem you mean 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

10.3.2.1.2 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

10.3.2.1.3 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 of audio and video input

Configuring IP devices

10.3.2.1.4 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 Workplace 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.
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.

Decompressor	Description
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.

10.3.2.1.5 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

10.3.2.1.6 Digital video signal transmission to Remote Workplaces

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 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 Workplace, video signals are compressed.

Configuring video transmission to Remote Workstations

10.3.2.1.7 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 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

10.3.2.2 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).

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

10.3.2.3.1 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.

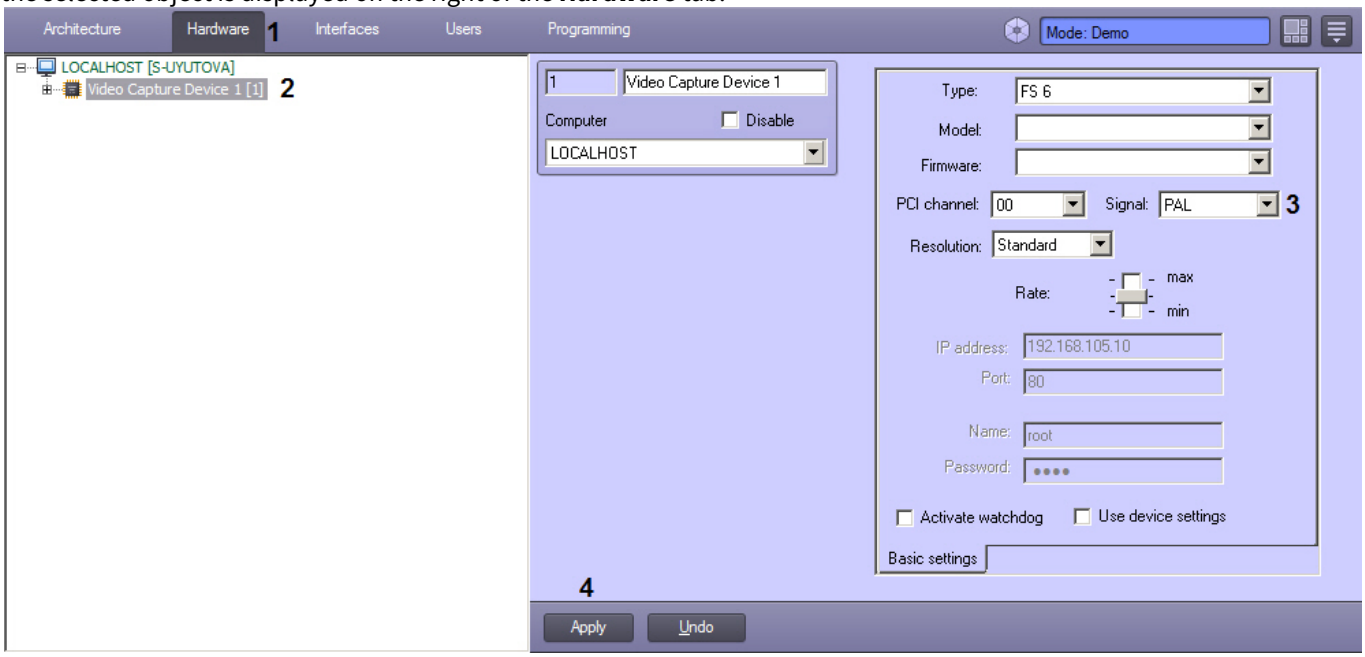
While using Stretch VRC6004, VRC 6008, VRC 6416, VRC 7008L and VRC 6404HD video capture cards, the input video signal (PAL or NTSC) is selected automatically depending on cameras, connected to the card. Changing the parameter does not affect the card workability.

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.

10.3.2.3.2 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 scaling
- Allocation of video capture card's resources
- Video signal processing priorities
- Setting video processing priority
- Setting video recording priority

10.3.2.3.2.1 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™ software 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.

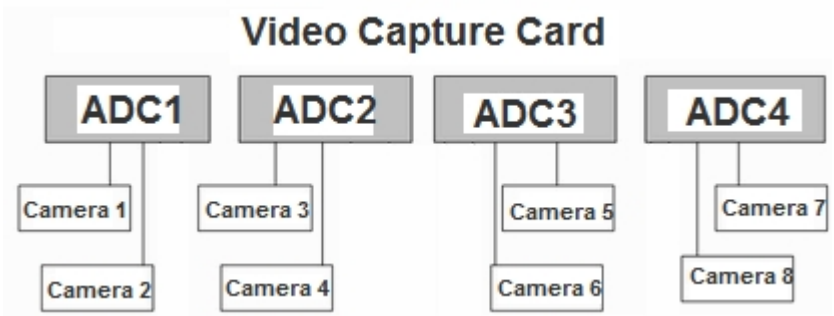
ADC resources are generally characterized by the maximum total frame rate of video signals. By default ADC resources are uniformly distributed between cameras to the assigned cameras. So, the more camera video signals are digitized and processed by the ADC, the lower the frame rate of the single video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

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

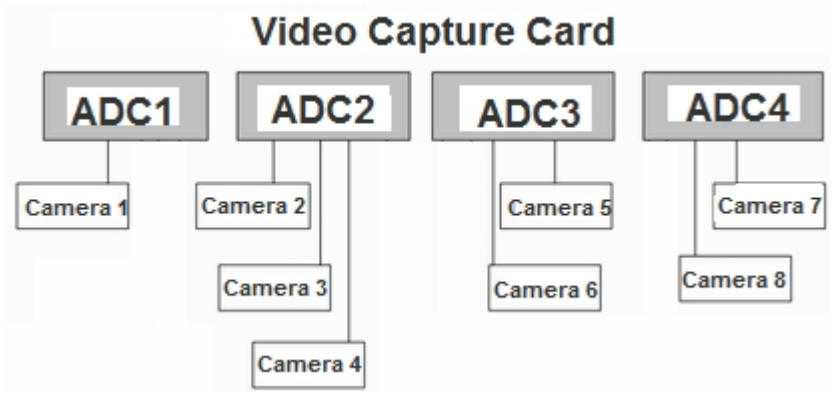
If all allowable cameras are connected to a video capture card, then only uniform distribution on ADC is possible. In this case every ADC of a video capture card digitizes and processes video signal from an equal number of cameras. So, the maximum frame rate is the same for all video signals (except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

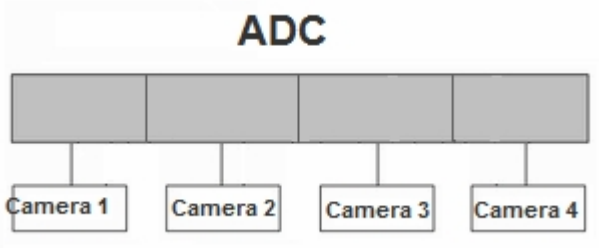
Reallocation of cameras between ADCs allows increasing the frame rate for some cameras by means of others. Reallocation of resources of one ADC to the cameras is much less effective than camera reallocation between the ADC. Therefore this is to be done only if camera reallocation to the ADC is impossible 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.

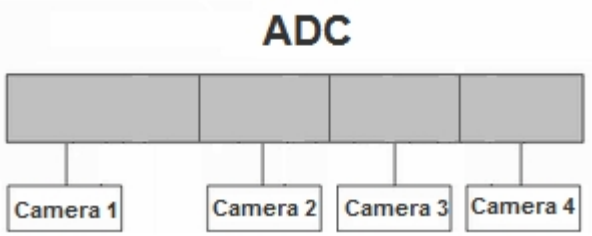
So, for a single ADC, when the frame rate of a certain camera increases, the frame rates of other cameras decrease.

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

10.3.2.3.2.2 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.

10.3.2.3.2.3 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 scaling.
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.

10.3.2.3.2.4 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.

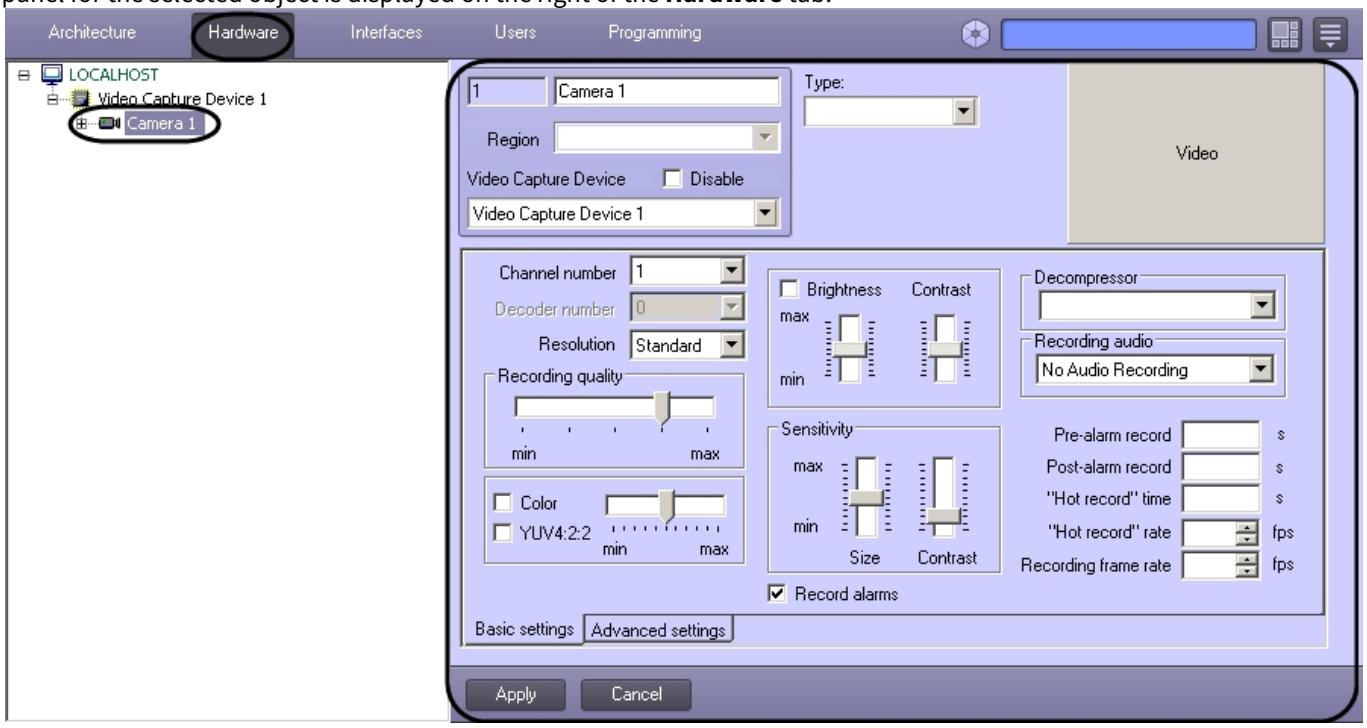
Several **Camera** objects are disabled in turn.

To prevent allocation of ADC resources, the **Camera** objects are to be disabled in INTELLECT™, assigned to the disabled video channels.

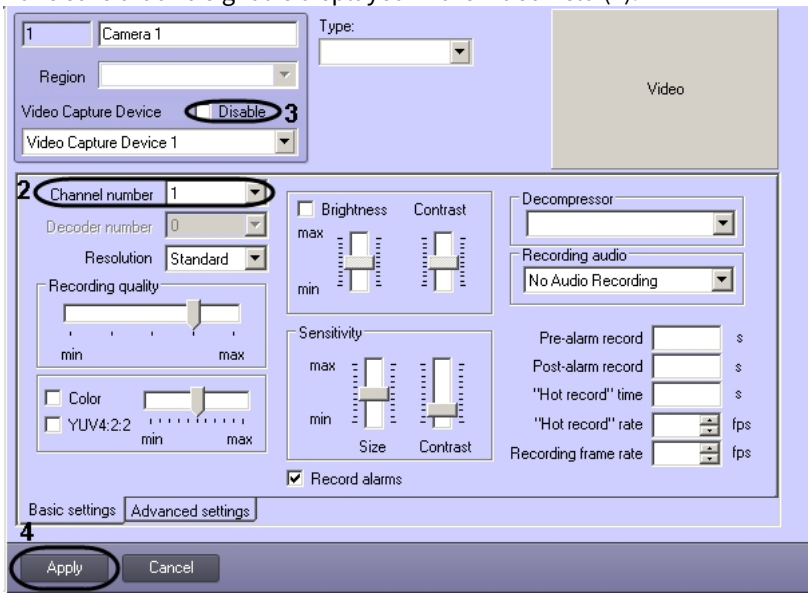
To disable the **Camera** objects in INTELLECT™ system, do the following:

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.

10.3.2.3.2.5 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™ software using the tweaki.exe utility (see Tweaki.exe utility for advanced setup of the Intellect software system section).

In Intellect™ software, 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™ software 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™ software 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).

10.3.2.3.2.6 Changing frame scaling

By default INTELLECT™ software 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.

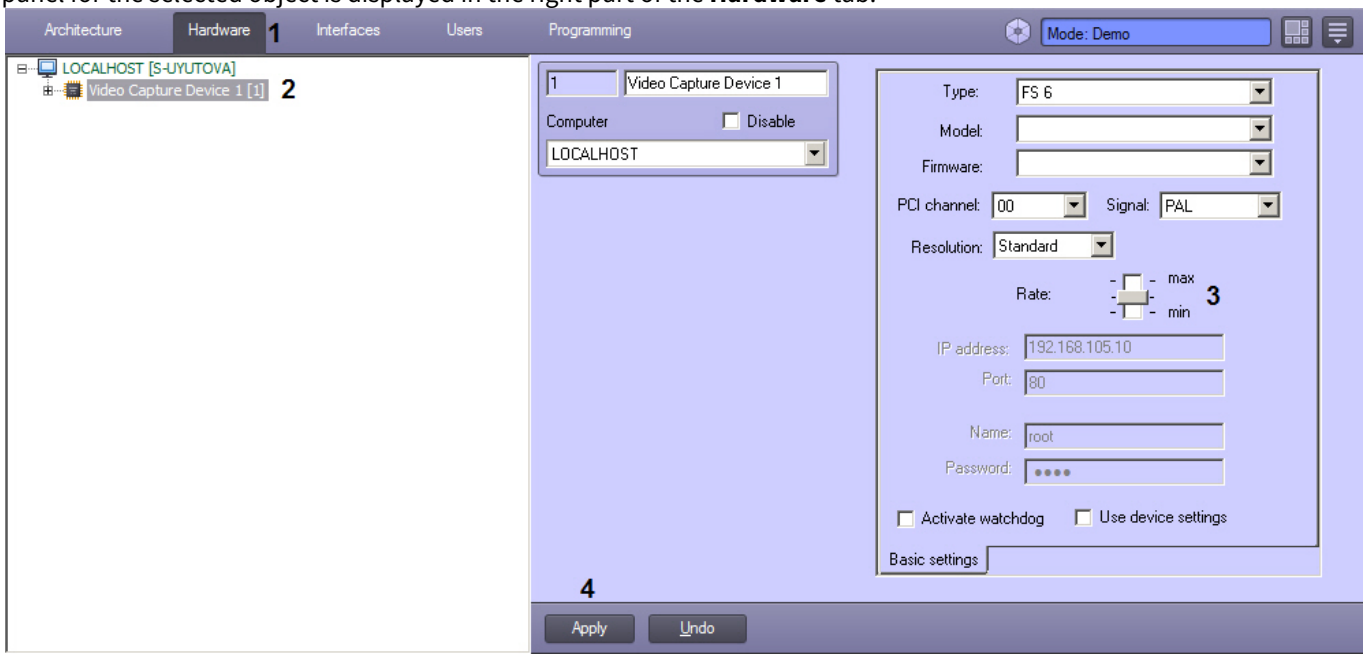
By default the total frame rate of video signals, which are digitized and processed by the same ADC, is 2 times lower than the maximum allowed one. This ratio is provided by frame scaling, which allows every second frame to be processed by the program.

Settings allow reducing (total frame rate increases) or increasing (total frame rate decreases) the scaling.

Frame scaling is changed separately and independently for every ADC.

To change scaling 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 scaling 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™ software.

> **Note.**
>
> Without restart, changes in video signal scaling may be applied incorrectly.

10.3.2.3.2.7 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.

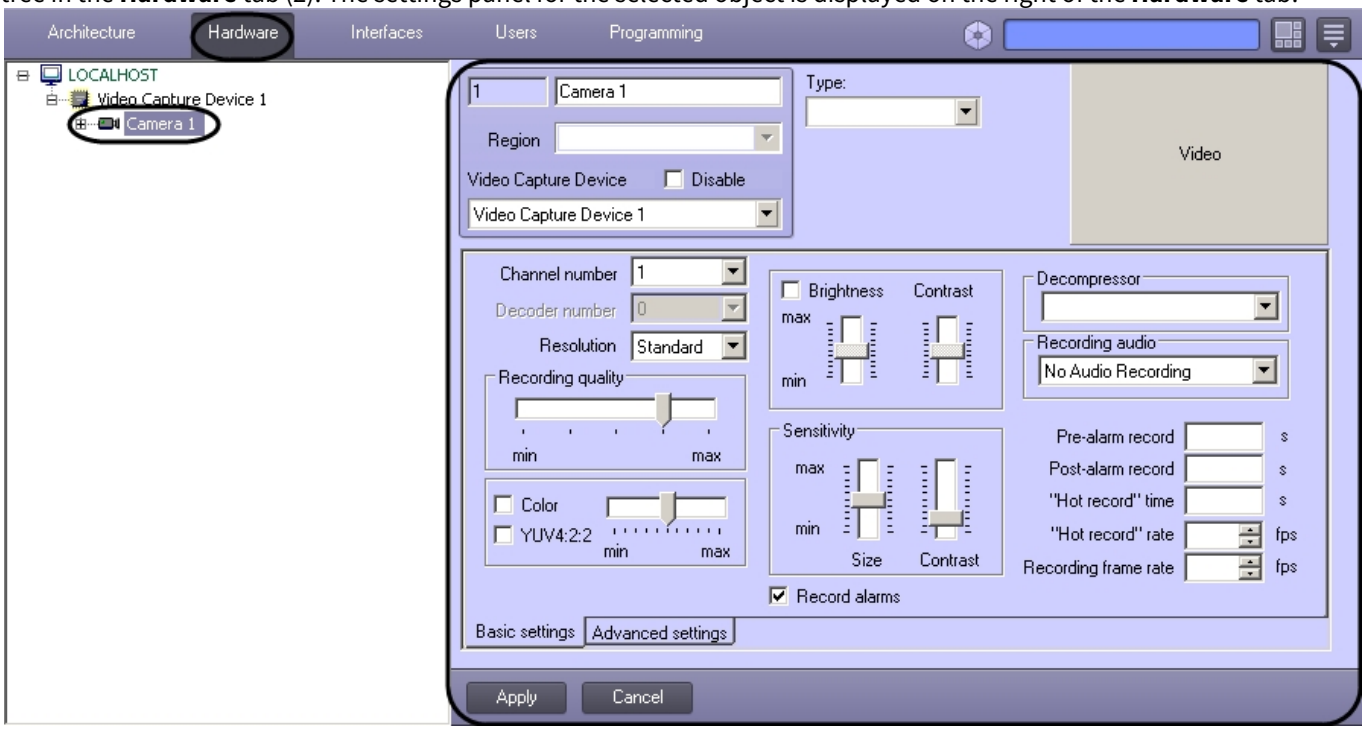
If the number of cameras connected to a video capture card is less than their maximum allowed number, it is possible to reallocate them between different ADCs of the video capture card. Reassigning of cameras allows increasing the frame rate for some cameras by means of a decrease in the frame rate of 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.



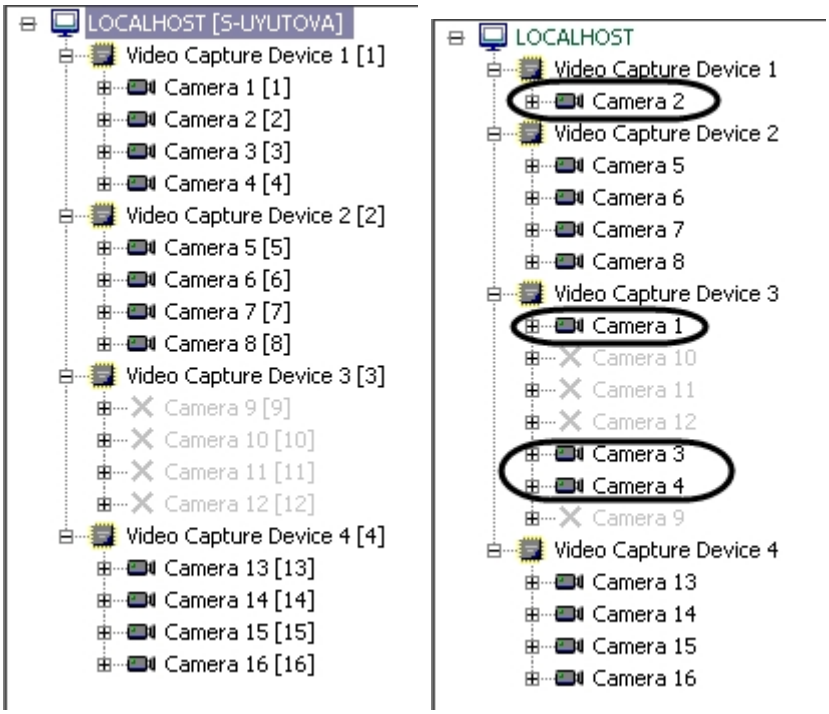
3. To increase the frame rate of a camera up to the Real time rate (25 fps in PAL format and 30 fps in NTSC format), reallocate other cameras serviced by the same ADC as with the camera above , to other ADCs.

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 Camera2 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:

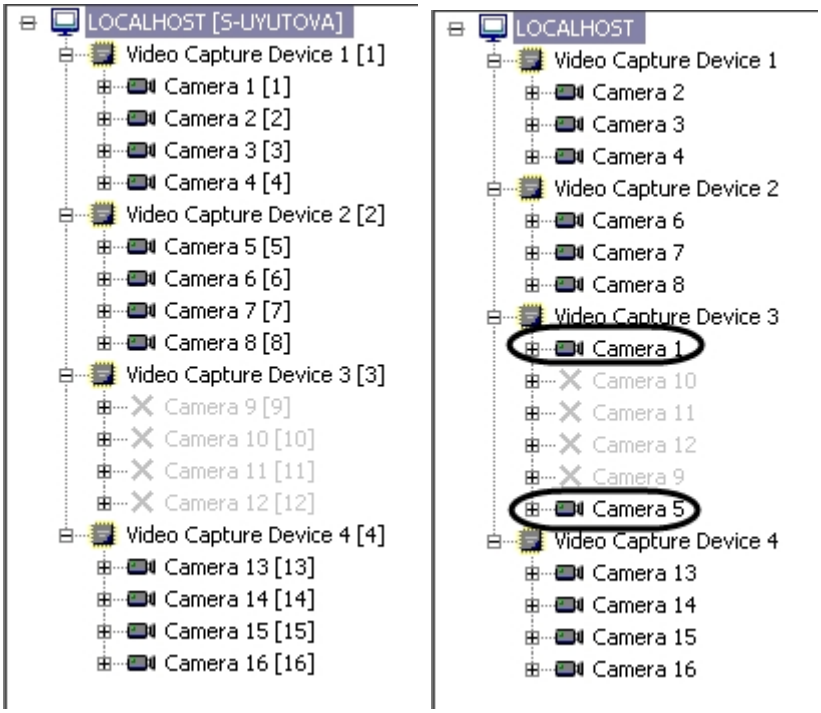
1. Select the **Camera 1** object in the objects tree. The settings panel for the selected object is displayed.
2. Select **Video Capture Device 3** in the **Video Capture Device** list.
3. Click the **Apply** button.
4. The **Camera 1** object moves to the subdirectory of the **Video Capture Device 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™ software.
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 **Camera5** 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).

10.3.2.3.2.8 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™ software 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.

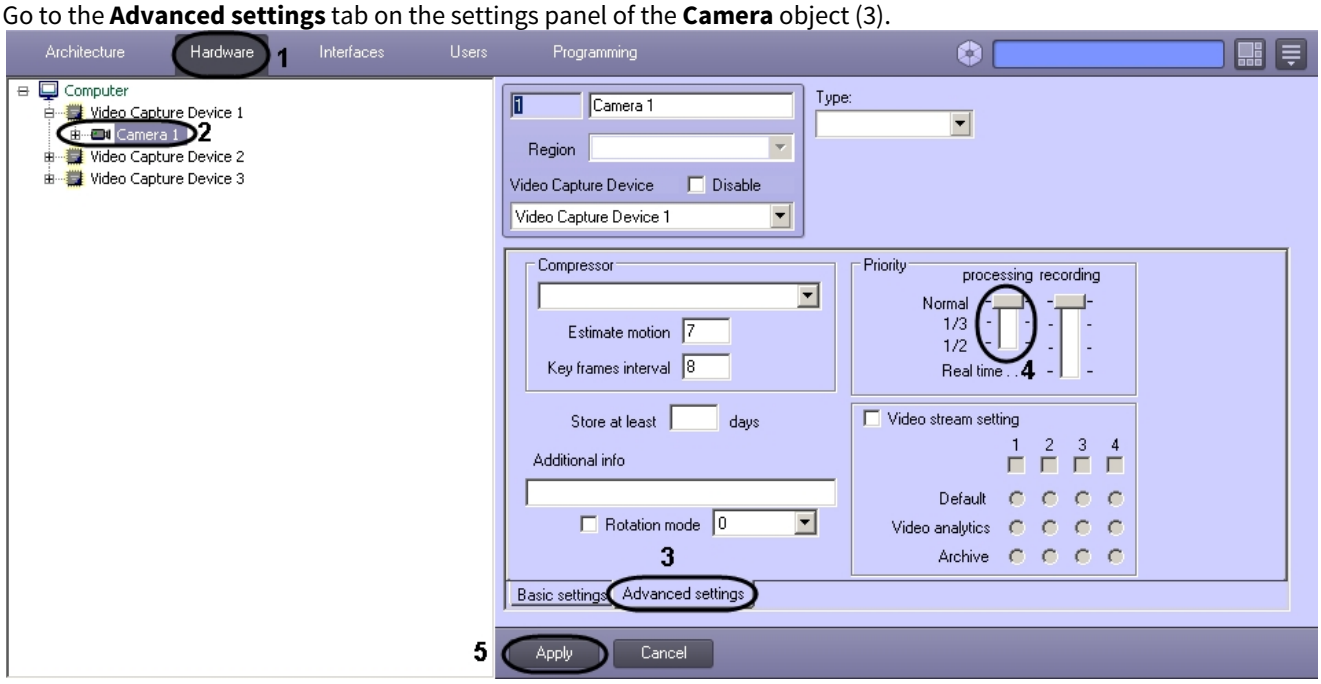
10.3.2.3.2.9 Setting video processing priority

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.

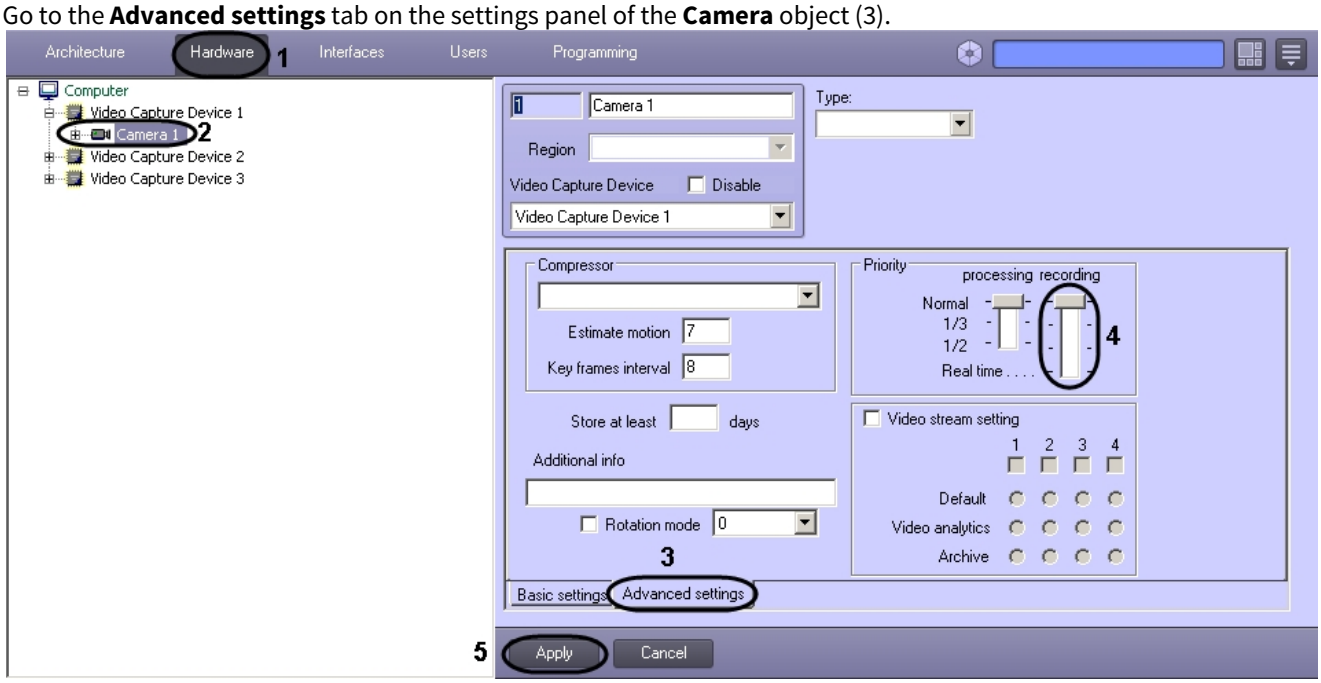
10.3.2.3.2.10 Setting video recording priority

While processesing 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.

10.3.2.3.3 Brightness, contrast, color depth and color rendition format settings

On the page:

- Brightness and contrast settings
- Color depth adjustment
- Selecting the color rendition format

10.3.2.3.3.1 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.

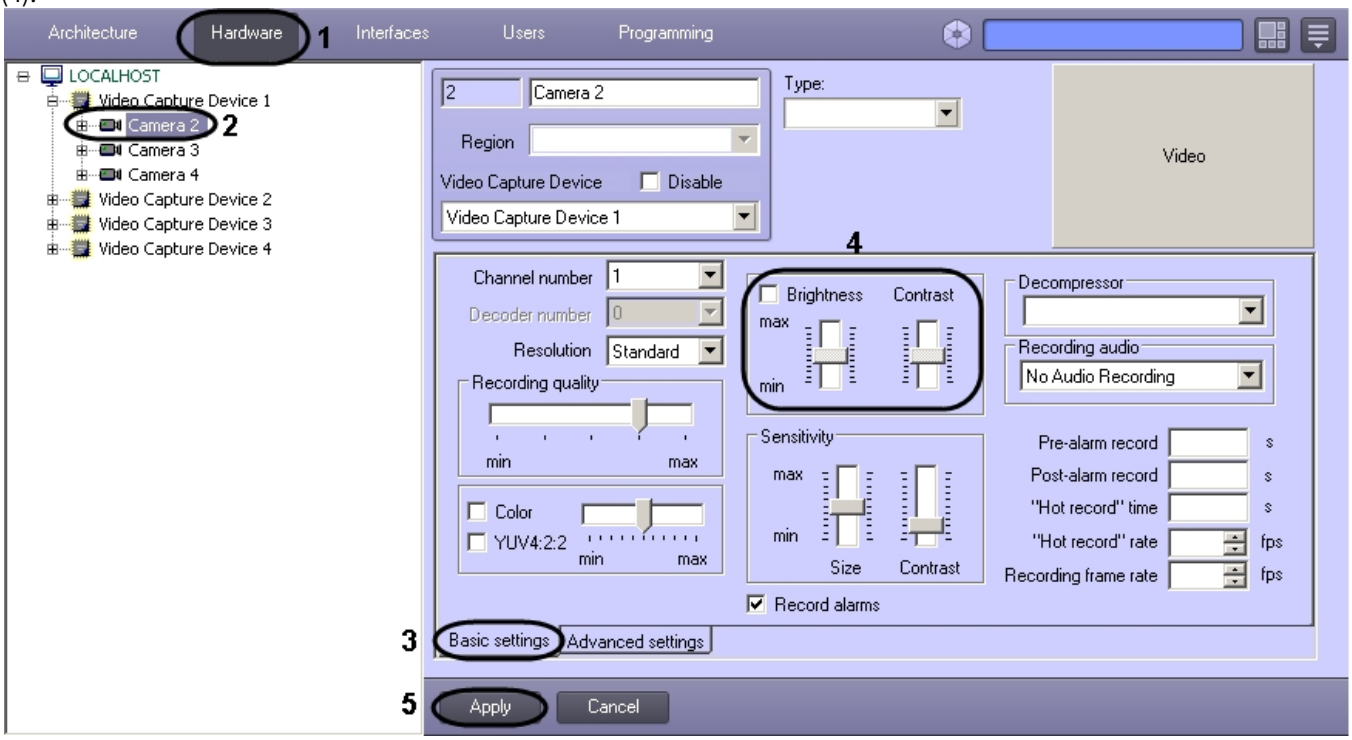
> **Note.**
>
> Manual Brightness and Contrast Control of IP-cameras is enabled by default.

Brightness and contrast are changed separately and independently for every camera.

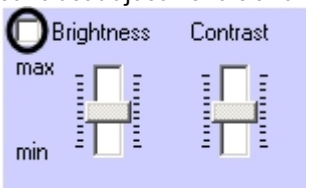
To adjust brightness and contrast, do the following:

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).

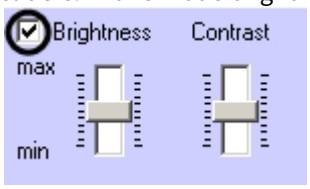


4. Auto brightness and contrast adjustment mode is activated by default. Active brightness and contrast auto adjustment mode is indicated by the absence of the check in the **Brightness** and **Contrast** boxes. In this mode manual brightness and contrast adjustment is unavailable. So, the **Brightness** and **Contrast** sliders are deactivated.

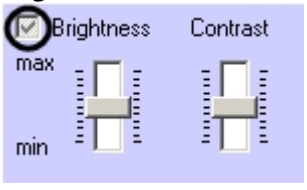


The mode is activated by default. To return to this mode, uncheck the checkbox next to the **Brightness** and **Contrast** sliders.

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.

10.3.2.3.3.2 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.

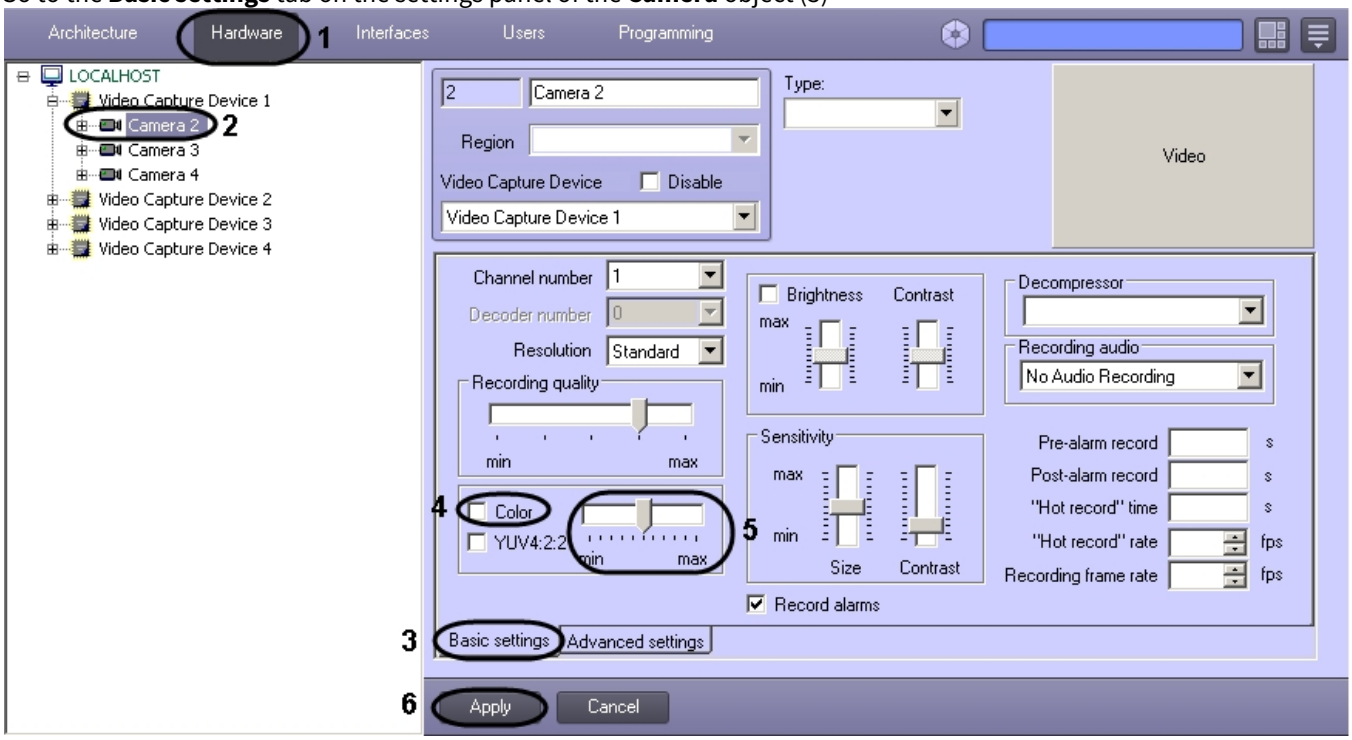
Color depth is set for each camera individually.

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.

10.3.2.3.3.3 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.

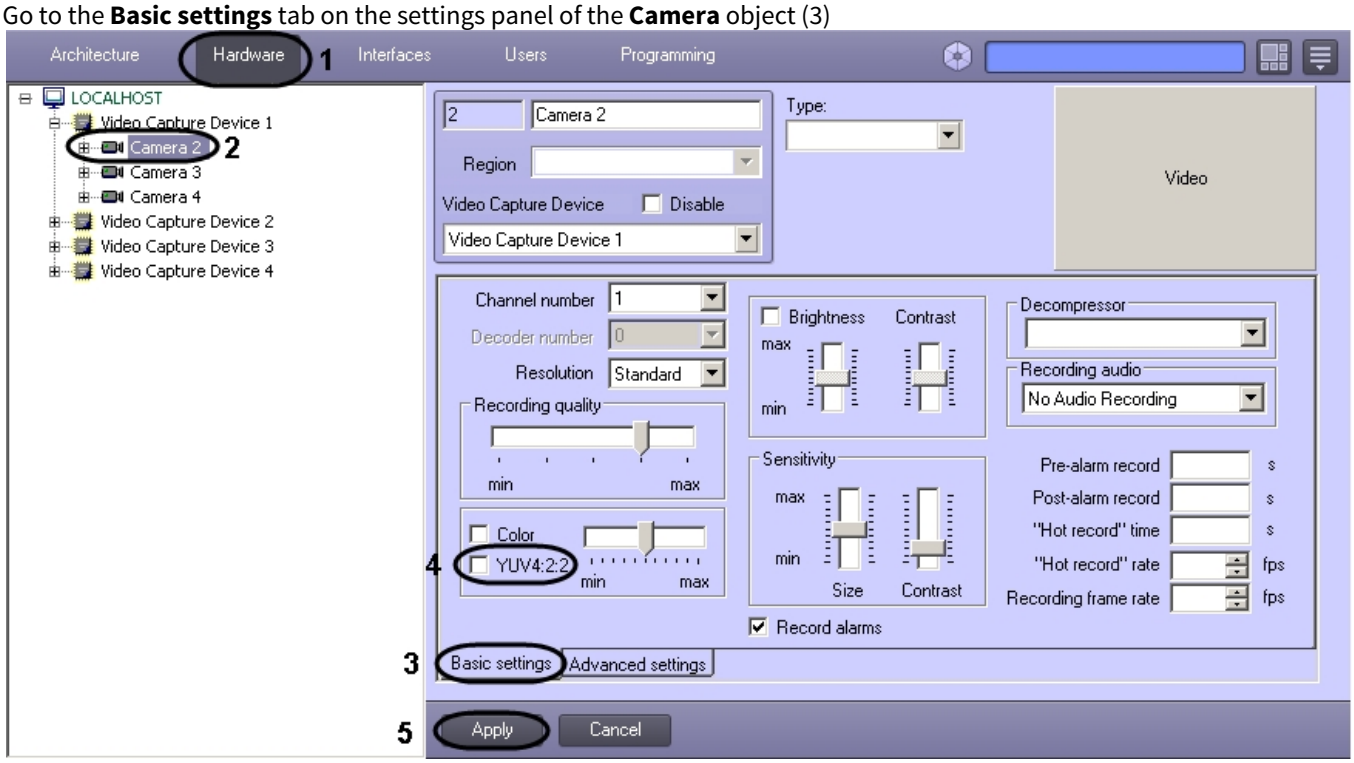
INTELLECT™ software has digitization options in both formats: YUV 4:2:0 and YUV 4:2:2.

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.

10.3.2.3.4 Configuring video compression

On the page:

- Compression rate settings
- Key frame rate settings
- Setting delta frame creation criterion

10.3.2.3.4.1 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.

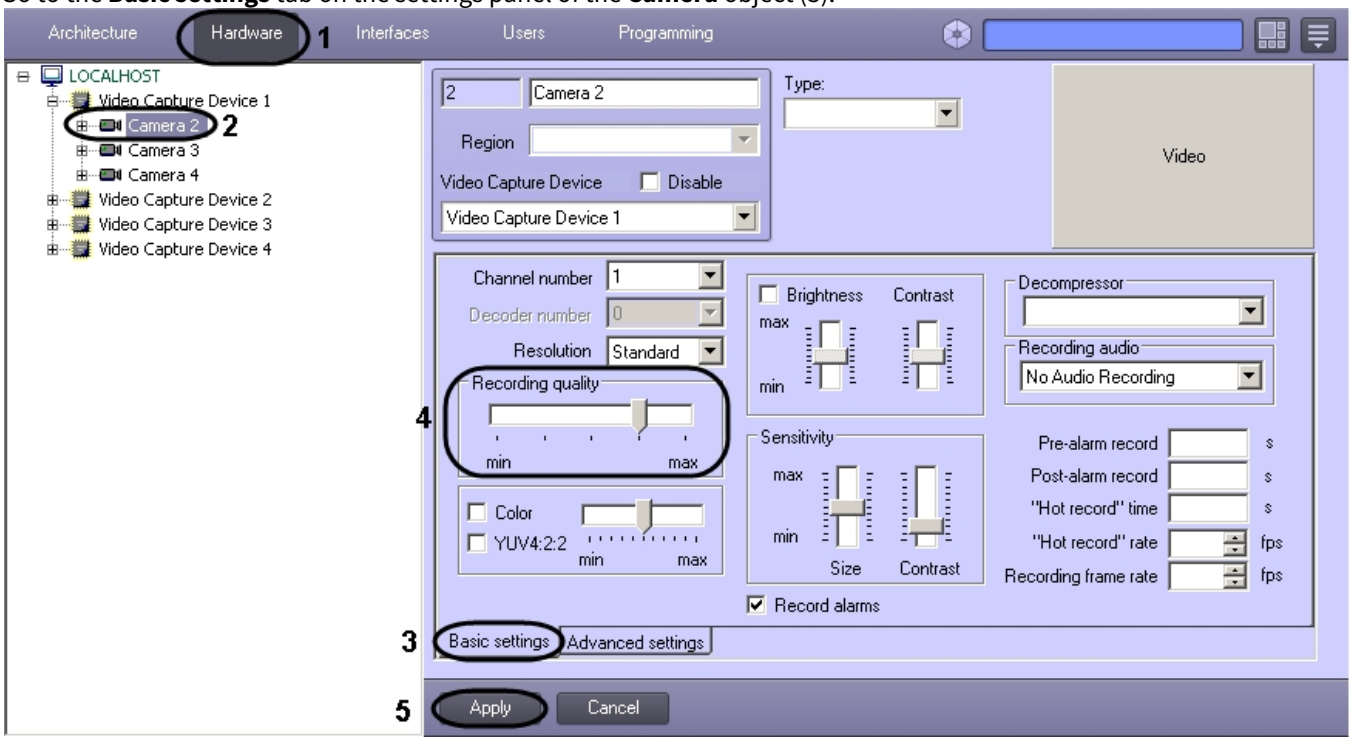
Video compression rate is configured for each camera individually.

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).

10.3.2.3.4.2 Key frame rate settings

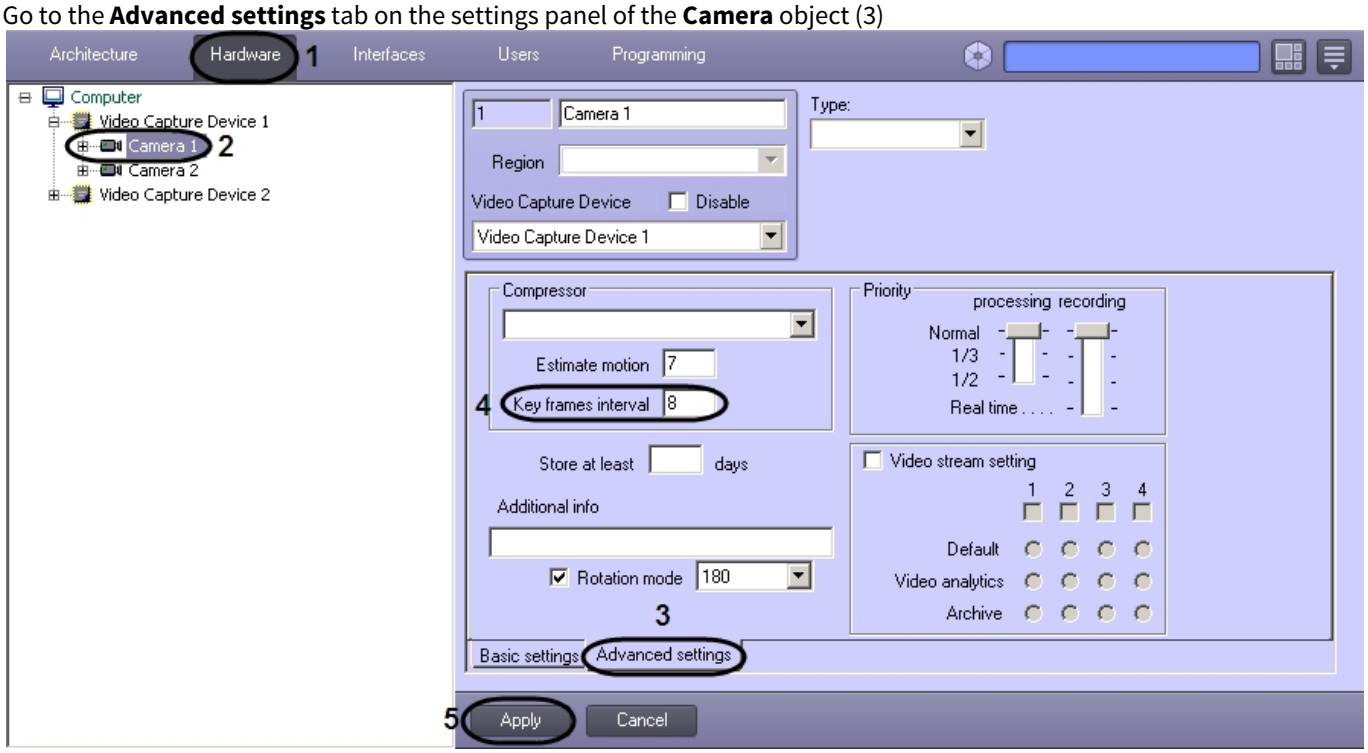
INTELLECT™ software uses Motion Wavelet algorithm for video processing and compression. Processed by this algorithm, the video is the sequence of key - and delta frames. A key frame is a full frame of an image. A delta frame (differential frame) is an image containing only pixel blocks which differ from 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 8th 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.

10.3.2.3.4.3 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.

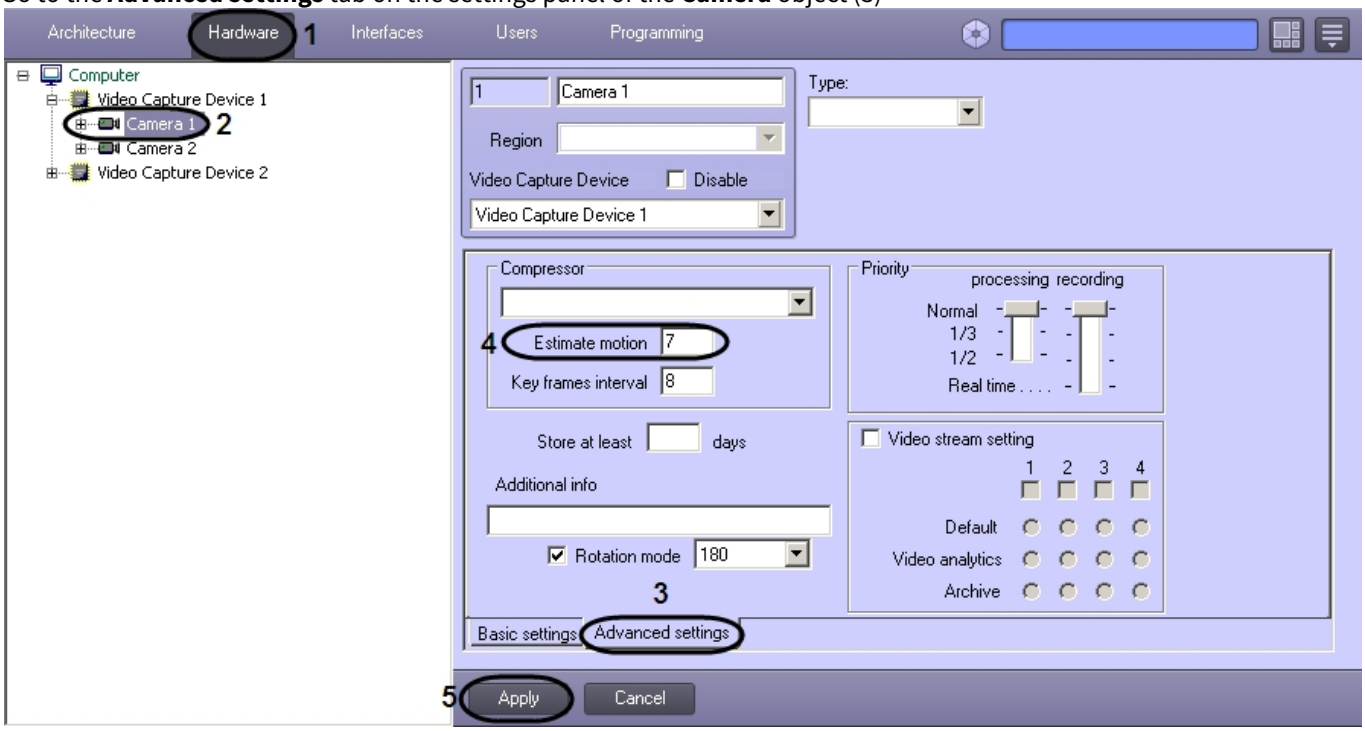
Legitimate values of pixel block brightness lie within 0-225 range. The block becomes a part of the delta frame by default, if the difference between its average brightness in the current frame and in the previous key frame exceeds 7 units. If this value is increased, the size of the delta frame is decreased, 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.

10.3.2.4 Creating and configuring a virtual Video Capture Device

On the page:

- Summary of virtual Video Capture Device
- Creating and configuring a virtual Video Capture Device
- Features of playing files in a virtual Video Capture Device

10.3.2.4.1 Summary of virtual Video Capture Device

One can work with a virtual Video Capture Device in INTELLECT™ software package. This way assumes that INTELLECT™ operates in a test mode and consists of imitation of video stream feed to virtual Video Capture Device by playing back ready-made video recording. There are two types of virtual video capture devices in *Intellect*:

1. **Virtual bench**. It is designed to play back video recordings in mkv, mp4 and avi formats for which DirectShow codecs are installed in Windows OS.
2. **Virtual**. It is designed to play back video recordings in internal *Intellect* format and files in .avi format.

Important!

Video recordings with B-frames are not supported.

Virtual Video Capture Devices do not support multistreaming. To ensure correct operation of a virtual Video Capture Device, including video displaying and archiving, disable multistreaming (see Configuration of multistream video).

It is not recommended to use LAV Splitter for playing clips in the Virtual Video Capture Device. FFDSHOW video decoder is preferable.

Note

If only Windows Media Player 11 (or its older versions) is installed on Windows OS to view video recordings, then it is to be updated to Windows Media Player 12 or DirectShow filters (codecs) of third-party vendors are to be in use.

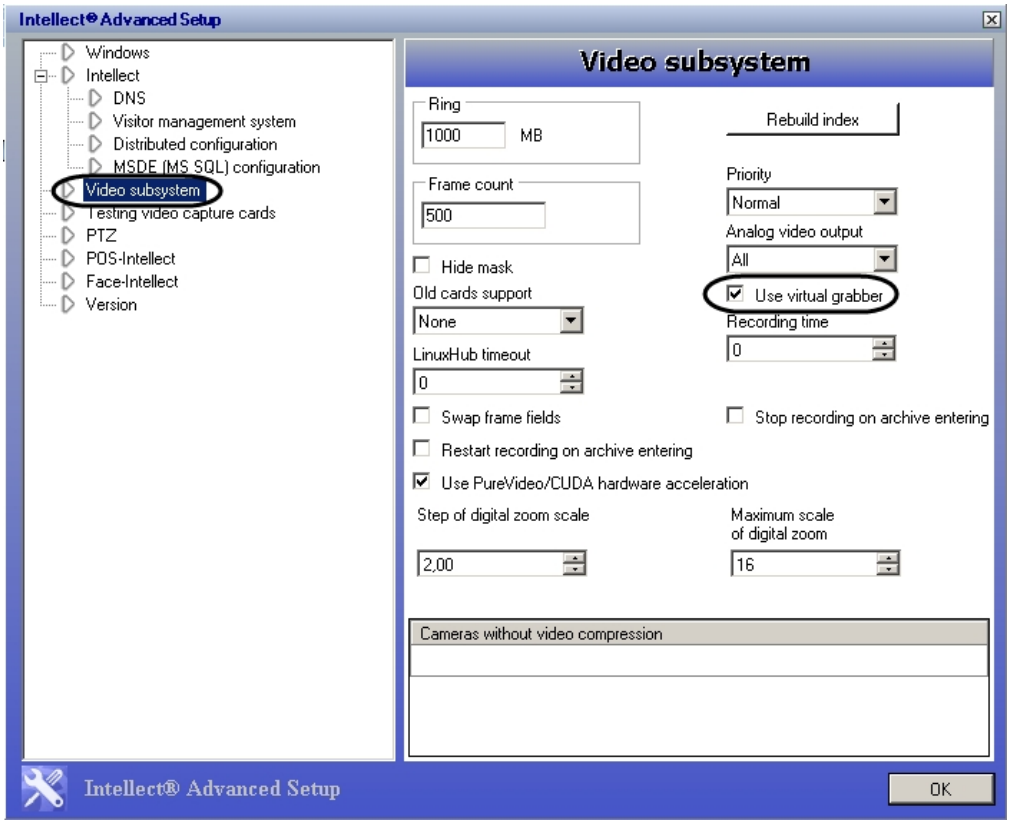
Note

Enable **Desktop Experience Feature** when using the virtial video capture device on Server OS and avi files.

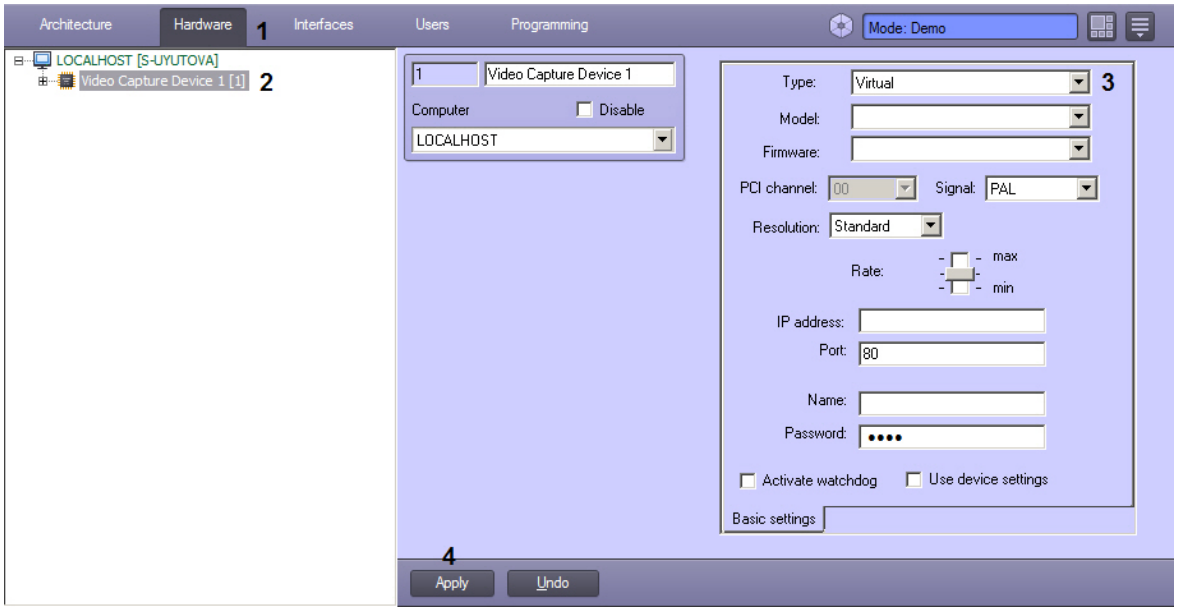
10.3.2.4.2 Creating and configuring a virtual Video Capture Device

Create and configure a virtual Video Capture Device as follows:

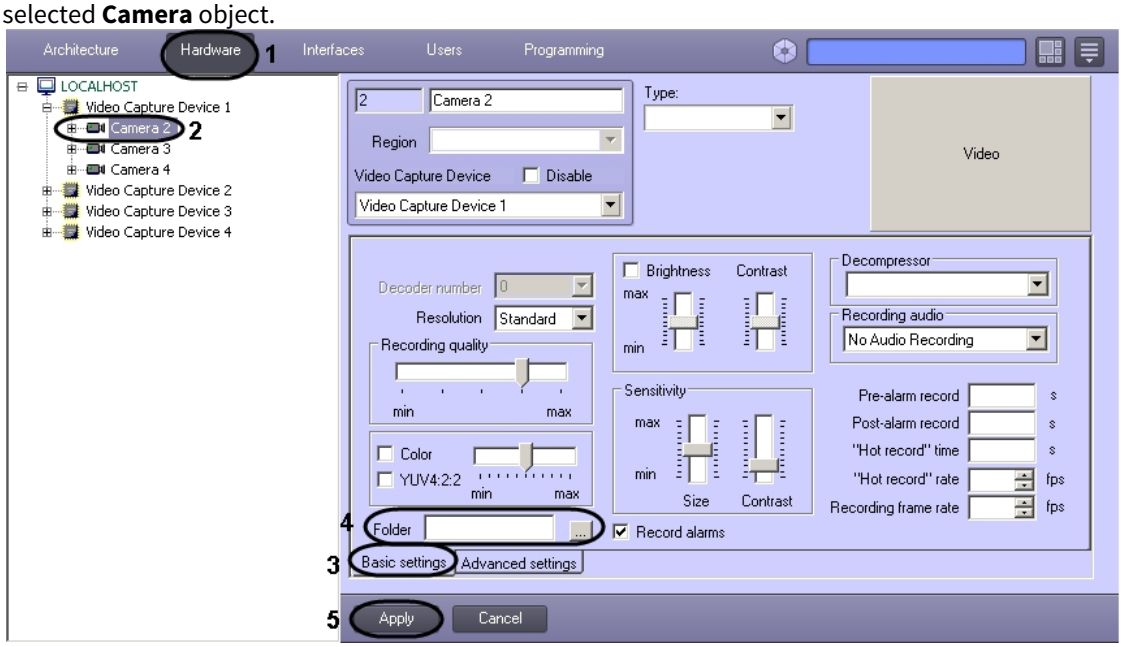
1. Set the **Use virtual grabber** checkbox (The Settings panel of the Video subsystem section), having shut down INTELLECT™ beforehand.



2. 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 video stream feed.



3. Specify the storage for video recording that is to be used for video signal imitation in the **Basic settings** tab of the selected **Camera** object.



If *Intellect* does not detect files for playback within 1 minute after clicking the **Apply** button, the file search is interrupted.

Attention!

The selected folder must not contain video recordings of internal INTELLECT™ format and AVI-files at the same time.

10.3.2.4.3 Features of playing files in a virtual Video Capture Device

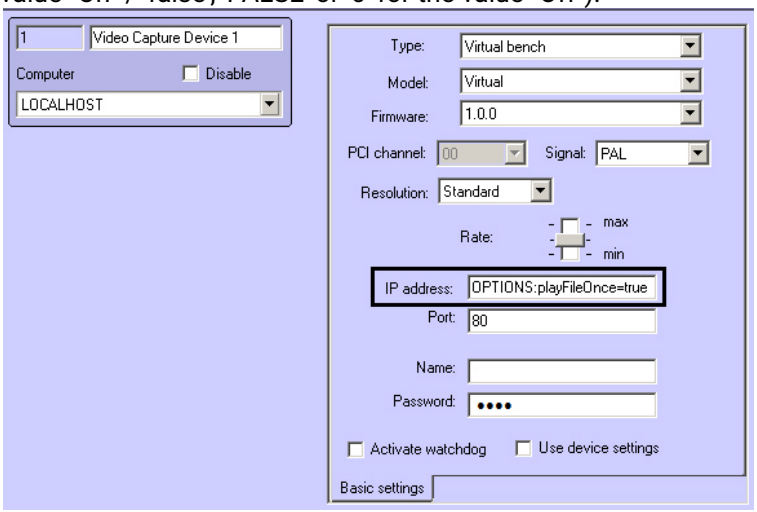
As a result of the above settings, video recording file from the selected folder will be played back in a loop.

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 in **Virtual bench** type device in one of the following ways:

1. Enter "**OPTIONS:playFileOnce=true**" in **IP address** field on the **Video Capture Device** settings panel:

a. the OPTIONS: enables the use of advanced options.
b. the playFileOnce flag corresponds to the "Single Play" option (the parameter name must be specified strictly case-sensitive).
c. after the '=' symbol, the value to be applied is indicated (the correct values are 'true', 'TRUE', or '1' for the value "On" / 'false', 'FALSE' or '0' for the value "Off").



2. Set the playFileOnce = 1 registry key (see Registry keys reference guide).

If there are several files in the folder they are to be played back in the order set in the latest modification. Files can also be sorted by names and time of creation while being played back. The sorting order is set by the VirtualGrabberSortMode registry parameter (see Registry keys reference guide).

When playing files, the system sends events to the Debug window showing the playback status – see CAM. There also are reactions for controlling videos playback in virtual grabber using scripts see GRABBER.

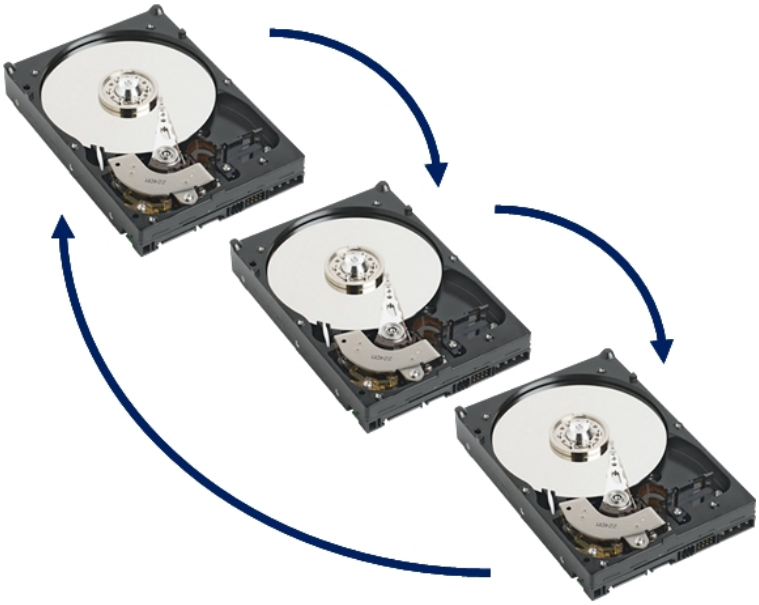
10.3.2.5 Configuring video archiving

10.3.2.5.1 General information on video archiving

Video archiving allows saving the footage according to the settings and analyse the fragments of interest for the user.

The archive is saved on the Server storage. 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.exe utility.

The archive represents the storage for the video recordings that are made in INTELLECT™ software. Loop recording is used here. When the hardwares run out of the space allocated to archive storage, the rewriting of footprint starts. It is made on the principle of overwriting the earliest recordings.

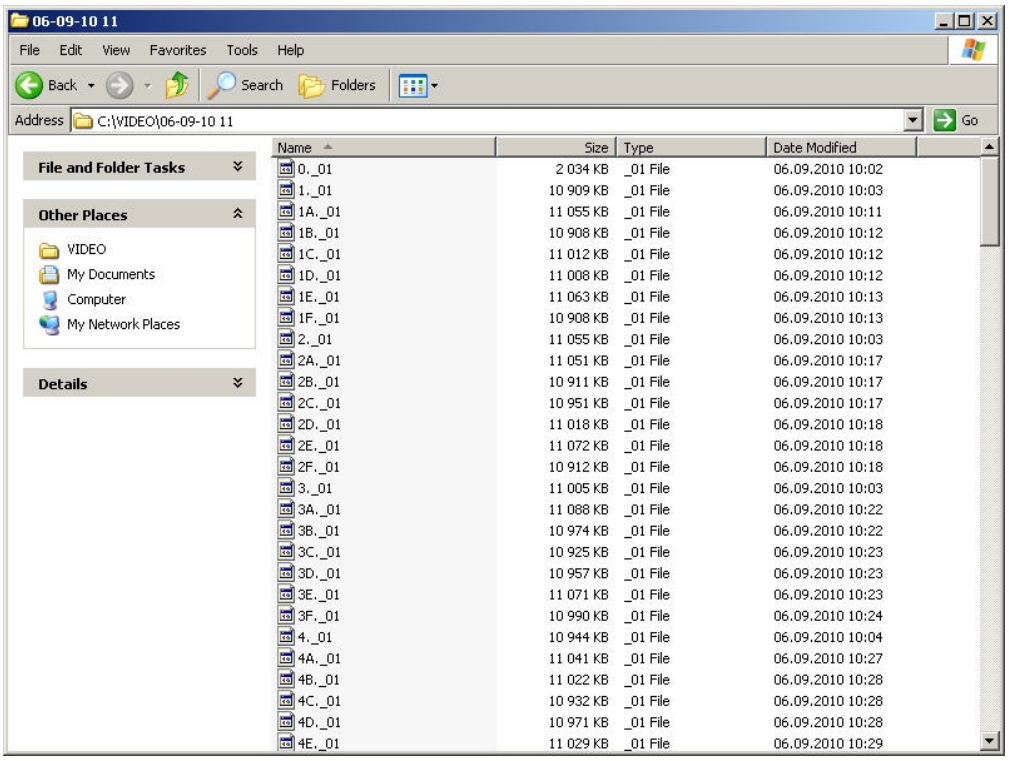


Video archive is stored in the VIDEO folder on the selected system disk. Child directories with titles in «DD-MM-YY HH» (Date, Hour) format are stored in the VIDEO folder. Archive files for the current hour are here. Video file extension indicates the number of video camera that is used for video archive.

Important!

Intellect software creates and stores video archive in its own format. One can view the archive files without converting with the Video surveillance window, using the converter.exe utility or using the AxxonPlayer utility (if you chose the required period).

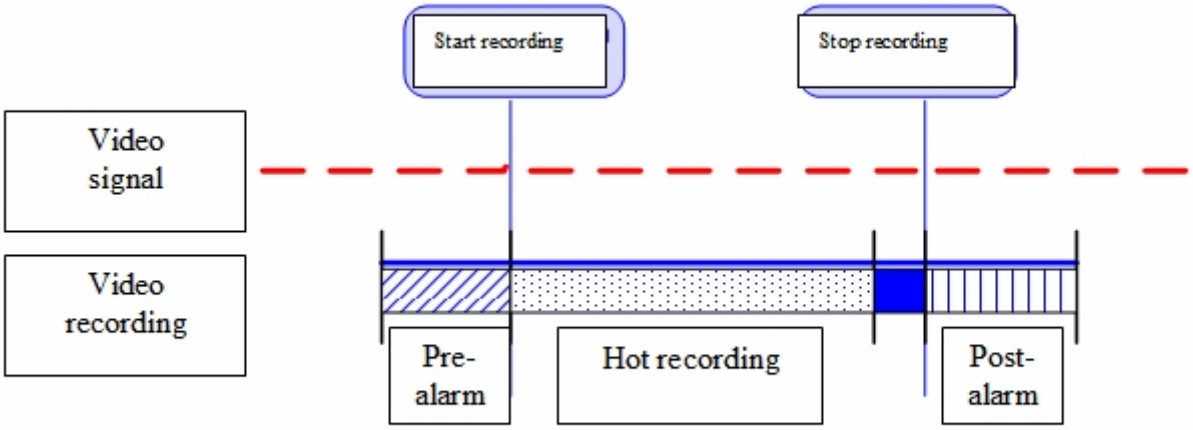
Video archive can also be exported to other formats. For that, the above instruments as well as the AviExport utility can be used. See also Operator's Guide , the Export and print out section.



Video signal recording may be initialized by one of three methods:

1. Forced recording by Operator command;
2. Automatic recording upon alarm registration;
3. Automatic recording upon a macro/script/program execution.

To make the analysis of the causes and effects of an alarm event more effective, INTELLECT™ software performs expanded schemes of 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 recorded before the recording start time on the camera alarm. Pre-alarm event recording option facilitates the analysis of event causes.

   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.

2. Post-alarm event recorded after the recording end time on camera alarm. Post-alarm event recording option facilitates the analysis of event consequences.
3. Hot recording – video recording segment with higher frame rate. Increasing frame rate on the **Hot recording** segment makes event analysis more effective. The **Hot recording** segment always starts from the recording start time on the alarm event registration. The **Hot recording** segment is finished at the recording end time (depending on the **Hot recording** settings and event duration).

Further use of video recording segments is restricted by INTELLECT™ software. The list of restrictions is given in the table.

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

10.3.2.5.2 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.

10.3.2.5.3 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.

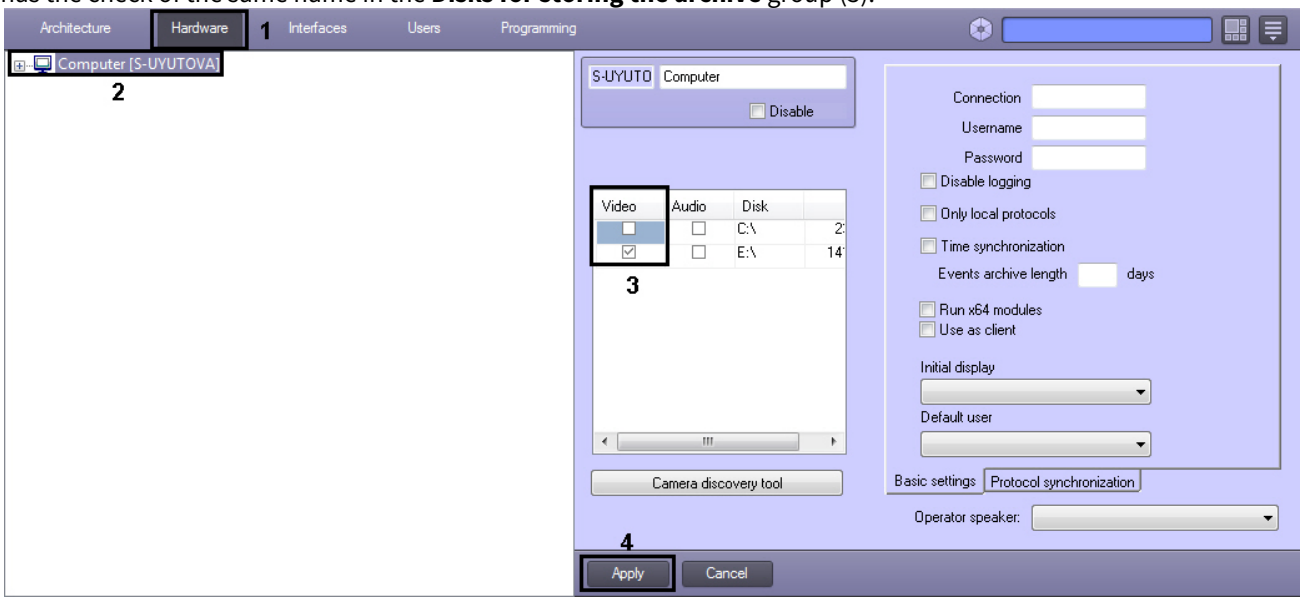
Note.

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

10.3.2.5.4 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 swiched 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.

Important!

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

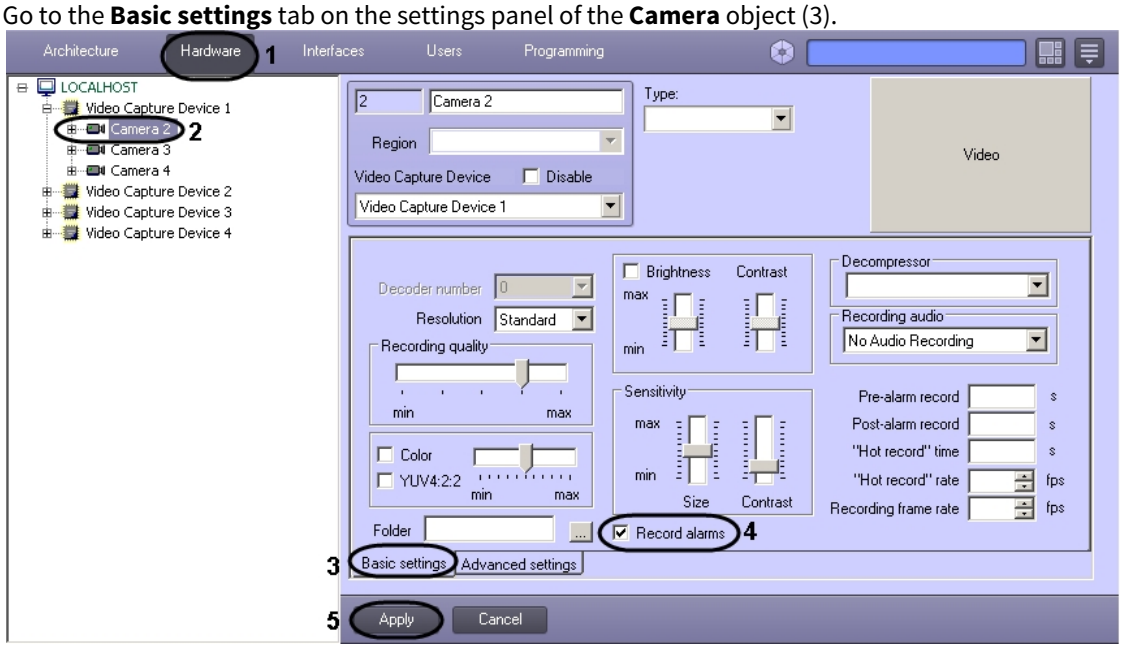
10.3.2.5.5 Disabling automatic recording upon alarm registration

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

10.3.2.5.6 Configuring video frame rate

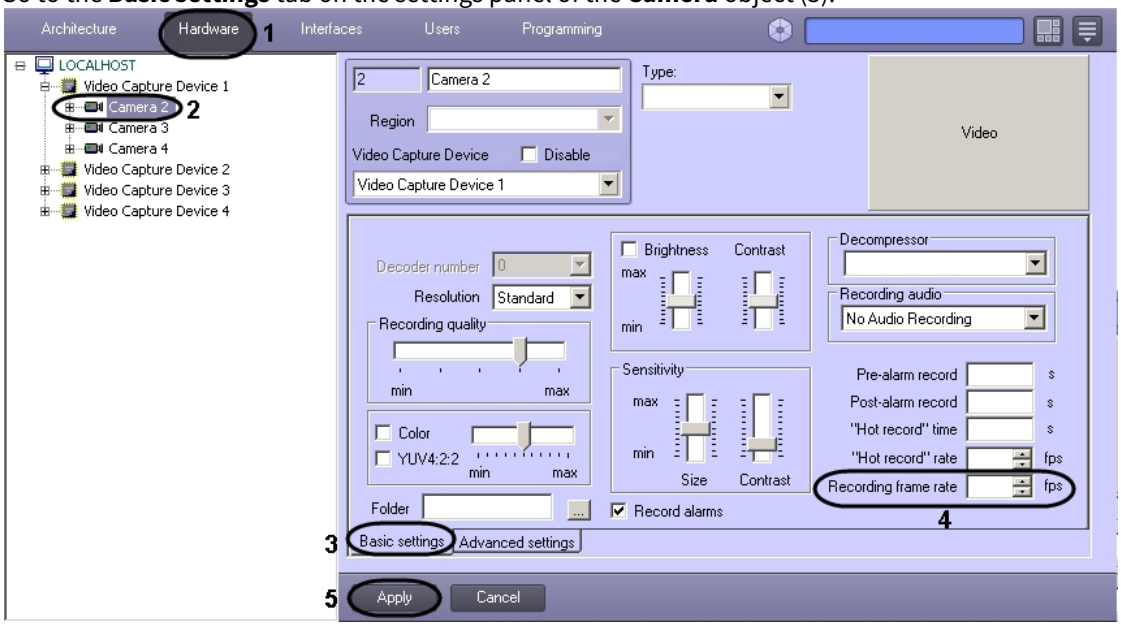
By default, video is recorded to the archive with the same frame rate as the video capture card digitizes it. Thus, to reduce the archive size, the frame rate can be configured.

> **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).

10.3.2.5.7 Configuring video in the Hot record mode

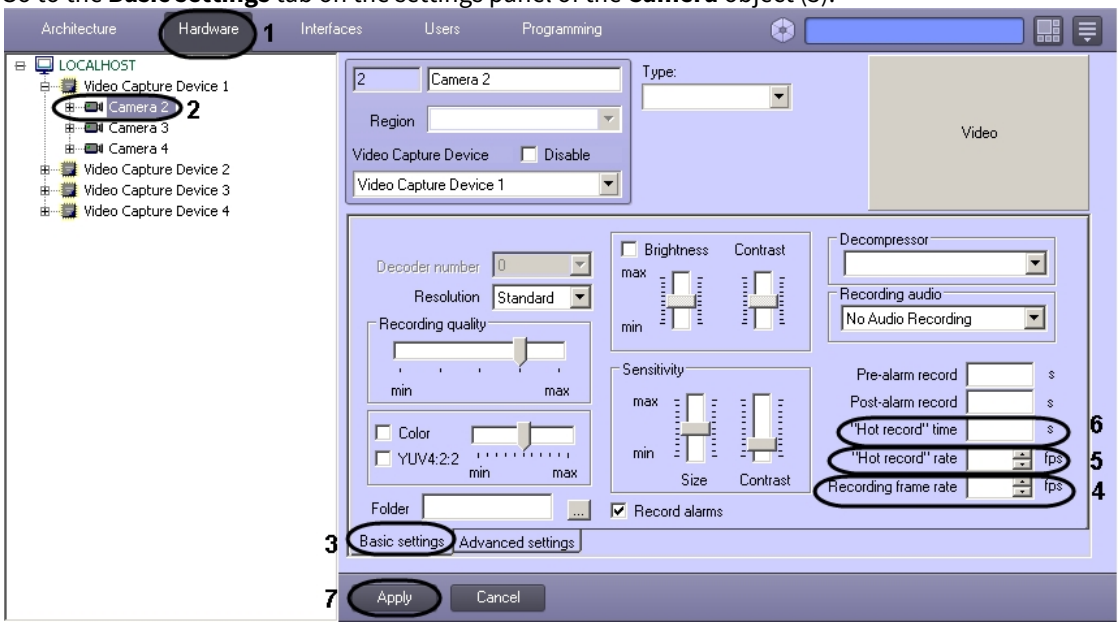
In the **Hot record** mode the video is recorded with a larger frame rate compared to the set value.

> **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. 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 **Recording frame rate** field specify the frame rate of the video to be recorded (4).
5. In the **Hot record rate** field specify the frame rate for the alarm hot recording (5).
6. In the **Hot record time** field specify the interval in sec during which the video is being recorded at the rate that has been set in the **Hot record rate** field, from the moment of alarm registration (6).

> **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 specifyied interval.

7. Click the **Apply** button (7).

> **Note.**
>
> 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.

10.3.2.5.8 Configuring video in the Pre-alarm record mode

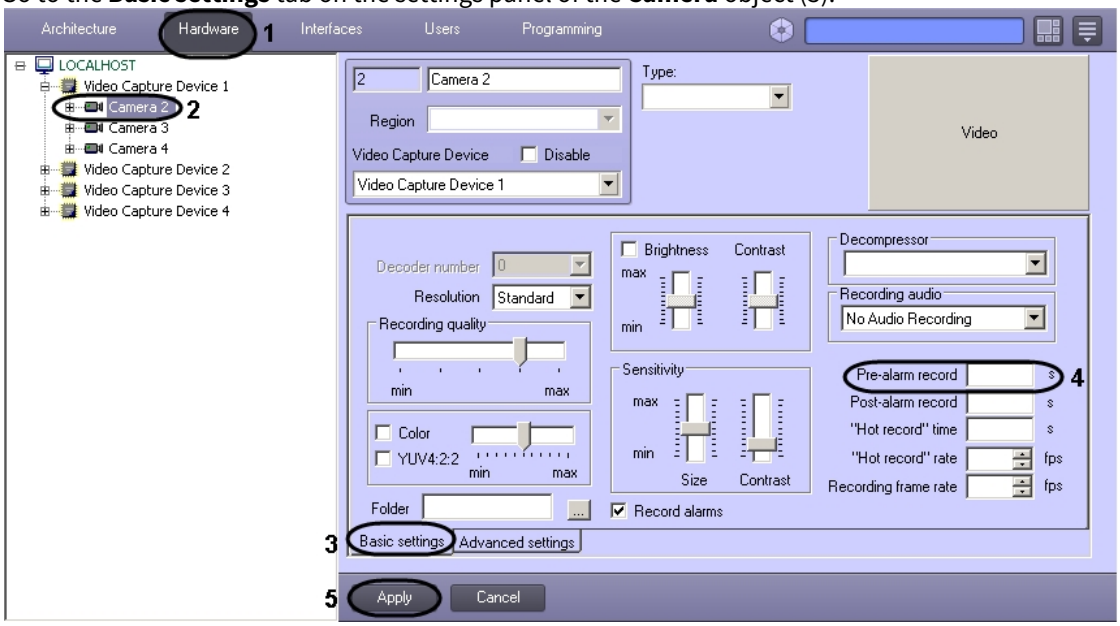
The **Pre-alarm record** mode is the record mode for recording pre-alarm events for a specified period before recording an alarm. Pre-alarm record is performed at the hot record rate. If the hot record rate is not specified, then at standard record rate.

> **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 Programming Guide (JScript)).

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

Example.

Camera performs pre-record for 15 seconds with the hot record speed 25 fps. Size of 500-frames fragment is 20Mb. It is required to define size of pre-record buffer for such camera.

At first define the average frame size:

Frame size = Fragment size / 500 = 20Mb/500 frames=0,04Mb.

So, the size of pre-record buffer is:

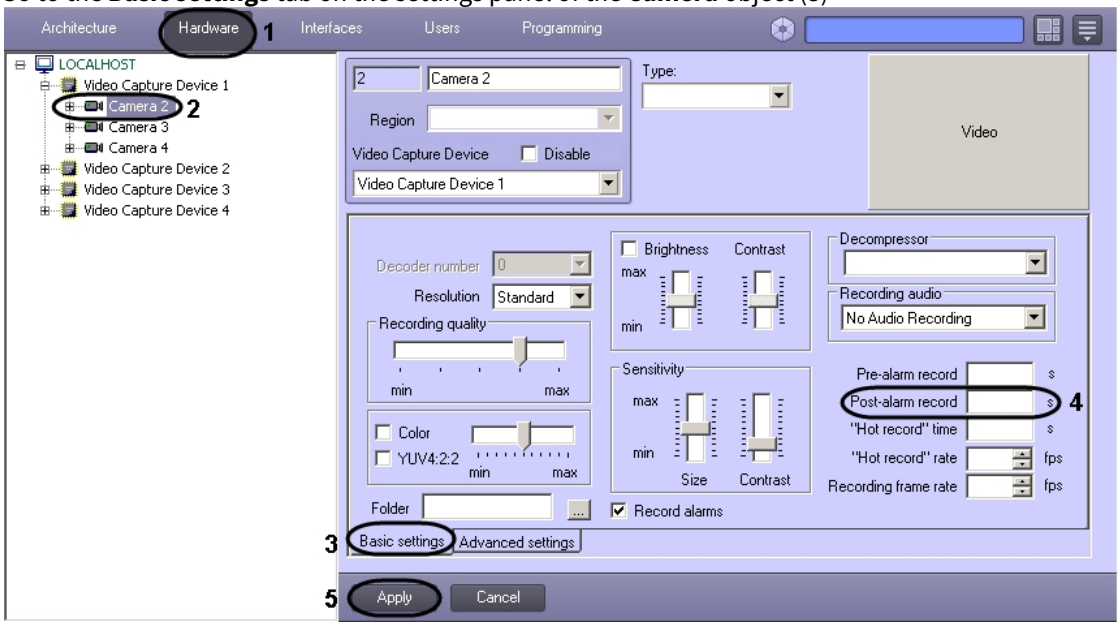
The memory consumption in the pre-record mode for one camera, Mb = Pre-record time, sec * Frame frequency in the pre-record mode, fps * Frame size, Mb = 15 sec * 25 fps * 0,04 Mb = 15Mb.

10.3.2.5.9 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).

10.3.2.5.10 Configuring audio and video synchro recording

INTELLECT™ software provides audio and video synchro recording option.

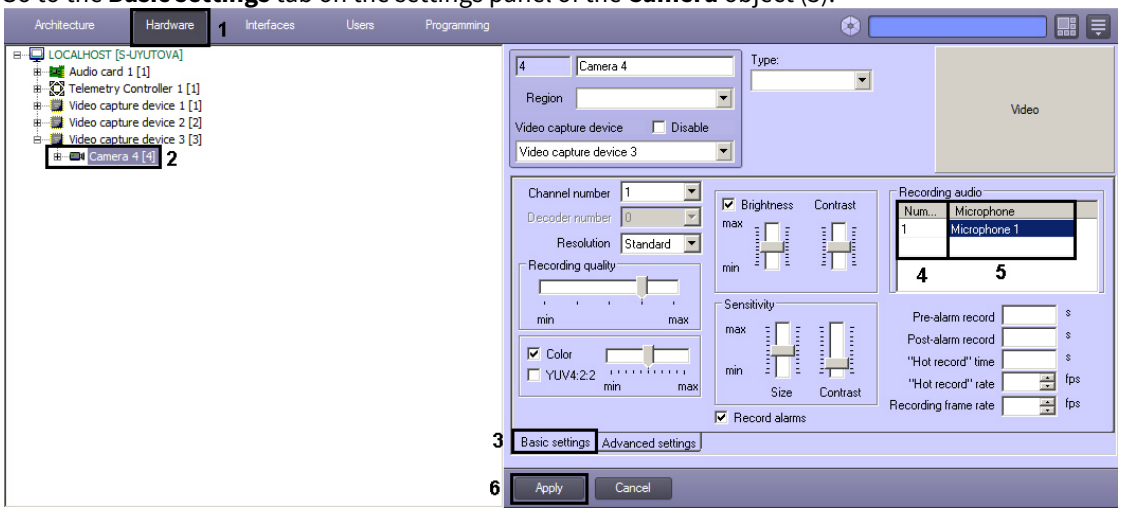
Audio signal recording beginss at the recording start time and ends at recording end time. In synchro record mode, audio files are stored with video files in the Server archive in the "VIDEO" folders on the Server archive local disks.

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, 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.

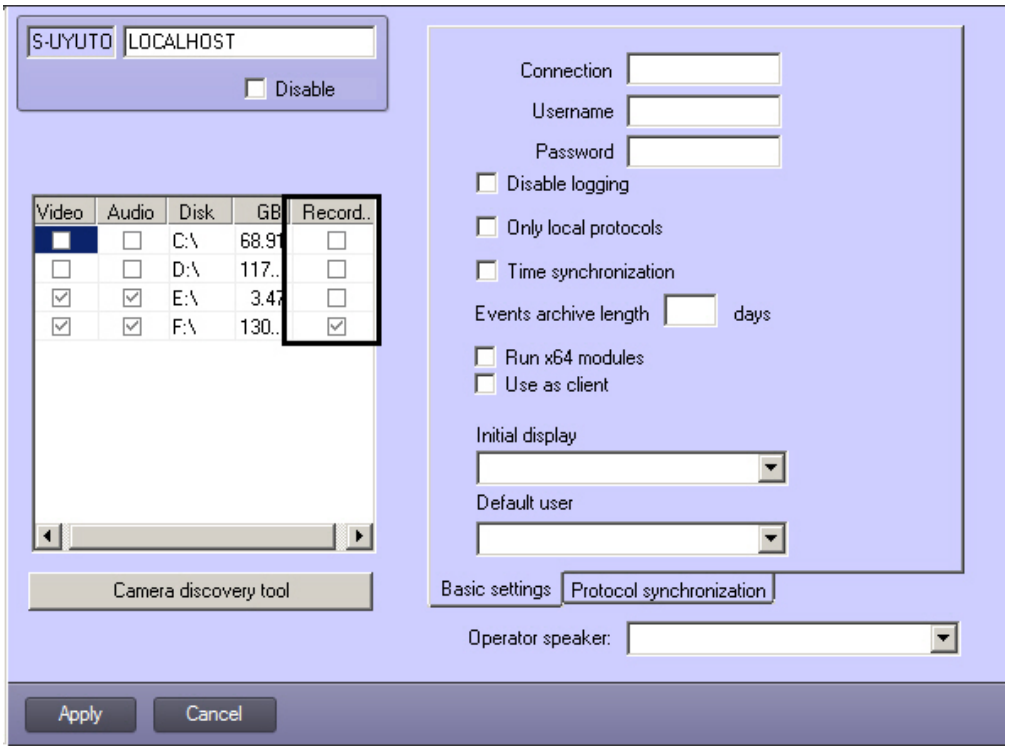
7. Click the **Apply** button (6).

Camera and microphone are now configured for audio and video synchro recording.

> Synchronous playback of video and audio recordings
>
> Audio and video synchro recording

10.3.2.5.11 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.

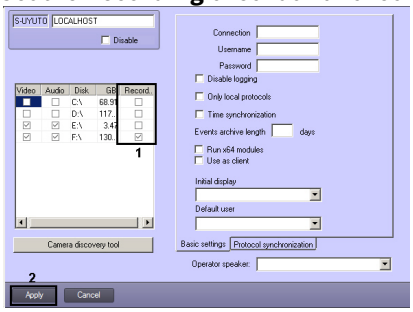


The *select current disk for recording* feature allows switching once to the disk from the list of active disks specified by the user (not to the following in the list) while loop recording in the list.

> **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.

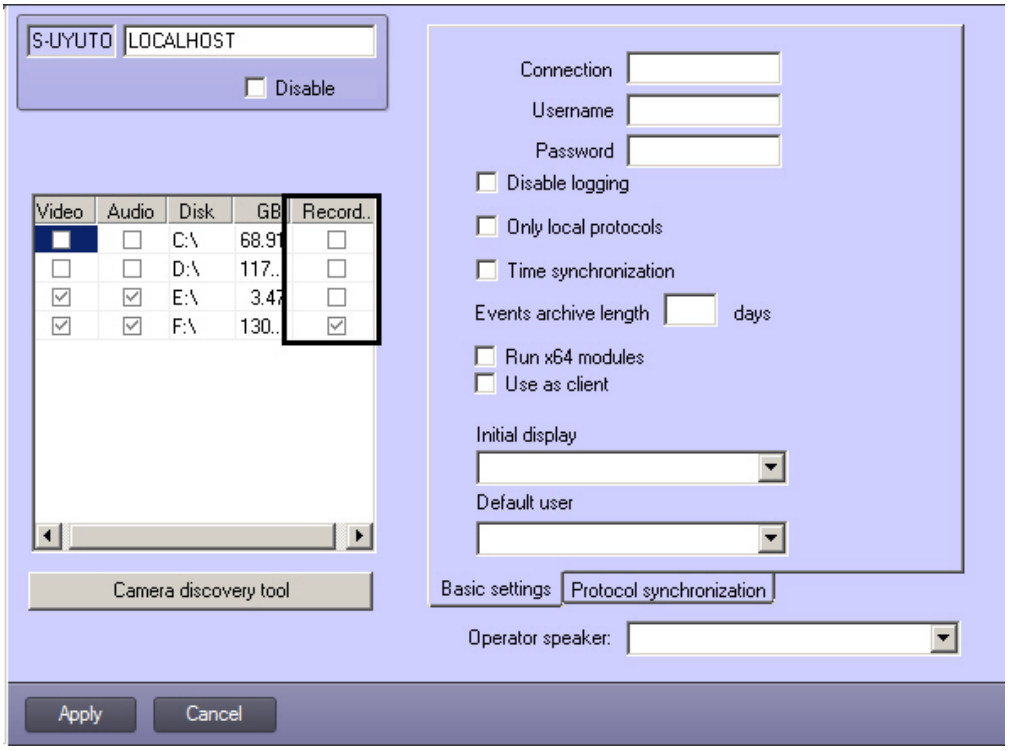
As a result the archive is stored on the selected disk. Further the loop recording continues (see General information on video archiving).

Note.

m_nCurVolume and m_dwTime registry parameters change when the current drive for recording is changed – see Registry keys reference guide.

10.3.2.5.12 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.



10.3.2.5.13 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 **Keep no longer than** and **Keep no less than** parameters:

- The **Keep 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 **Keep 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). 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 **Keep no longer 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 **Keep no longer 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.

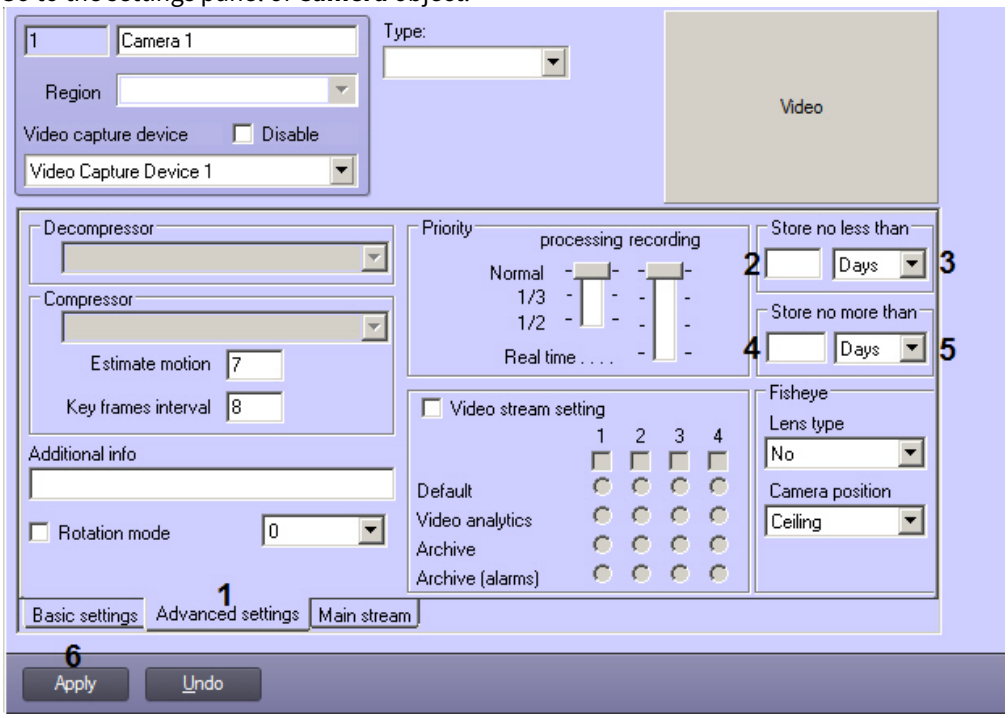
Note.

The **Keep no less than** and **Keep no longer than** parameters refer to calendar time, e.g. if you set **Keep no longer 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 **Keep 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 **Keep no less than** dropdown list select the units used to set the time period in the **Keep no less than** field: days or hours (3).
5. In the **Keep no longer 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 **Keep no longer than** dropdown list select the units used to set the time period in the **Keep no longer than** field: days or hours (5).
7. Click the **Apply** button (6).

The video camera archive depth is now configured.

10.3.2.5.14 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).

10.3.2.6 Additional information on camera

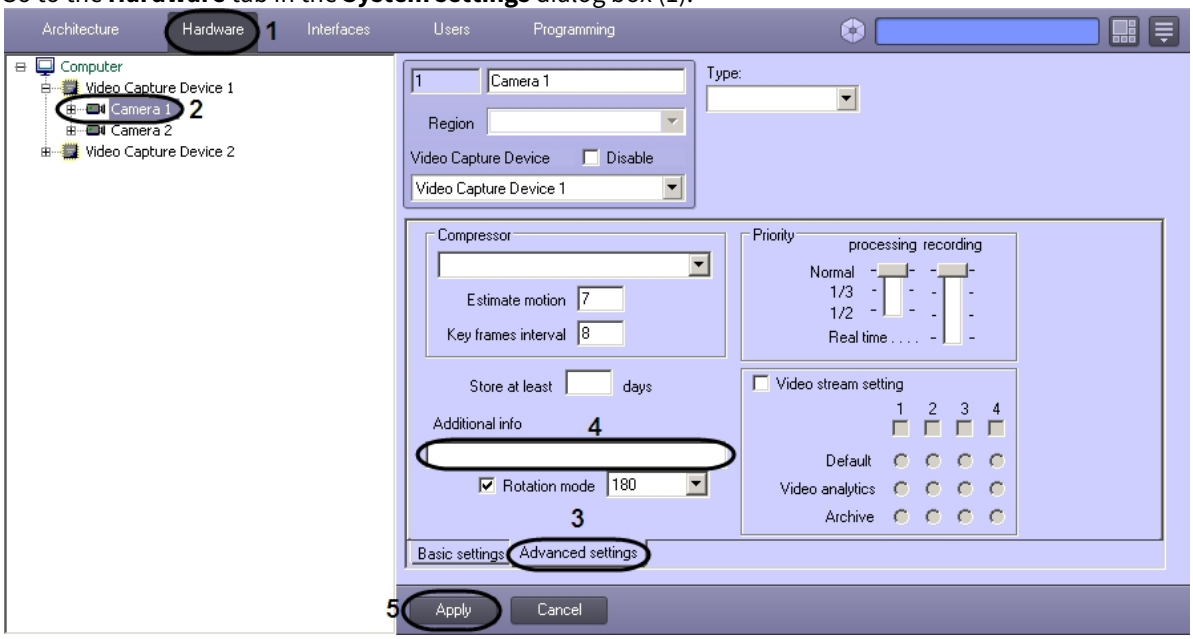
Additional information on the camera is:

1. Displayed on the video surveillance monitor over the camera name (disabled by default in order to reduce GPU load, see Selecting 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).
5. To save the changes, click the **Apply** button (5).

Additional information is now set.

Event control via event log

Viewing video sequences from surveillance cameras

Export and print out

10.3.2.7 Configuring video detection tools

10.3.2.7.1 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.

10.3.2.7.2 Enabling, configuring and disabling basic video detection tools

10.3.2.7.2.1 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 decimation for the H264 codec (key frames only).

Requirements to video parameters while working with detection tools and Tracker

Camera arming and disarming

Use of video detection tools

10.3.2.7.2.2 Requirements to video parameters while working with detection tools and Tracker

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

1. Camera requirements:
   a. Resolution:
      i. at least 640x480 but no more than 800x600 pixels for smart video detection tools.
      ii. at leasr 320x240 pixels for other video detection tools.
   b. Framerate:
      i. at least 6 frames per second for smart video detection tools.
      ii. at least 1 frame per second for other video detection tools.
   c. Video analytics works with both black-and-white and color images.
   d. Camera shaking must not cause image shifting of more than 1% of the frame size.
2. Lighting requirements:
   a. Moderate lighting. Lighting that is too little (night) or too much (bright sunlight) may impact the quality of video analytics.
   b. No major fluctuations in lighting levels.
3. Scene and camera angle requirements:

a. Moving objects must be visually separable from each other in the video.
b. The background must be primarily static and not undergo sudden changes.
c. Minimal obscuration of moving objects by static objects (columns, trees, etc.).
d. Reflective surfaces and harsh shadows from moving objects can affect the quality of analytics.
e. Long single-color objects may not be tracked properly.

4. Object requirements for smart video detection tools:
   a. An object must be visible on the image.
   b. There is no noise on the video image and there are no artifacts caused by the compression algorithm.
   c. 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).
   d. The width and height of objects in the video should not be more than 75% of the frame size.
   e. It is recommended that the linear measurements of objects in the frame do not exceed 75% of the frame size.
   f. The speed of objects in the frame must be at least 1 pixel per second.
   g. The object is to be visible at not less than 8 frames.
   h. Within two adjacent frames the object cannot move in the movement direction for the distance that is longer than its size.
   i. Quantity of simultaneously tracked objects on a frame – not more than 25.

10.3.2.7.2.3 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.

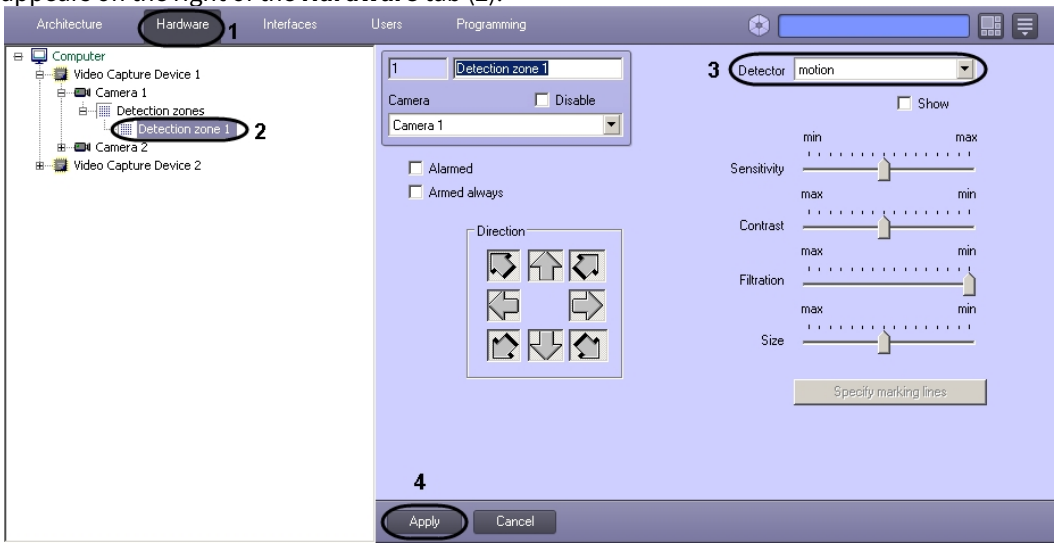
10.3.2.7.2.4 Connecting basic detection tools

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 video detection tools

10.3.2.7.2.5 Configuring basic detection tools

Configuring Main motion detection tool
The main motion detection tool is used to detect motion on the guarded location 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.

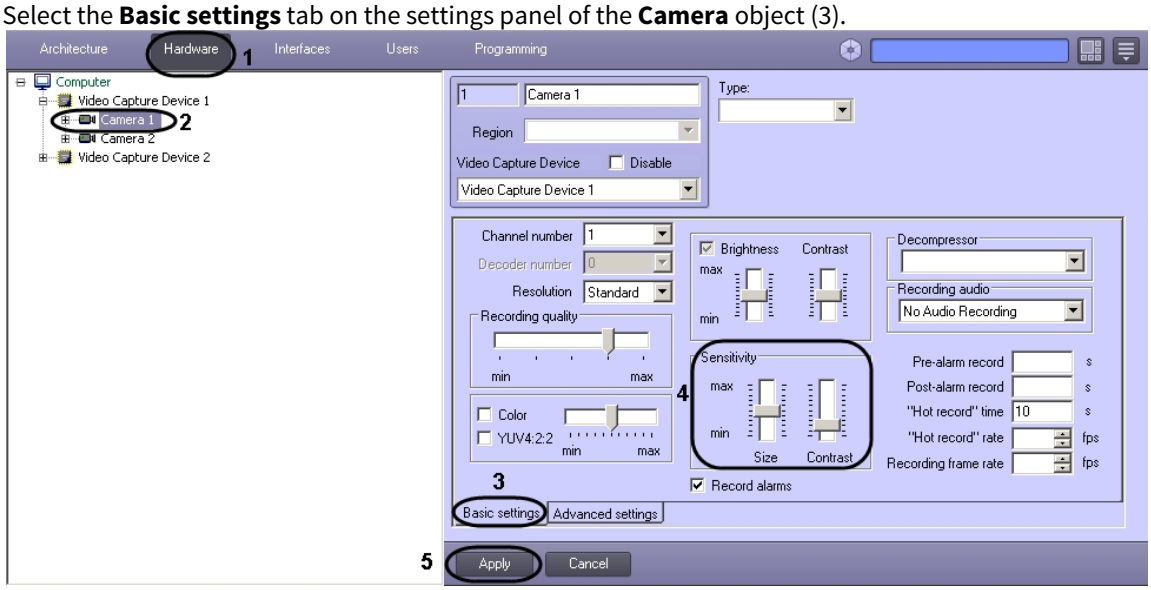
To configure Main motion detection tool, do the following:

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.

Main motion detection tool is now configured.

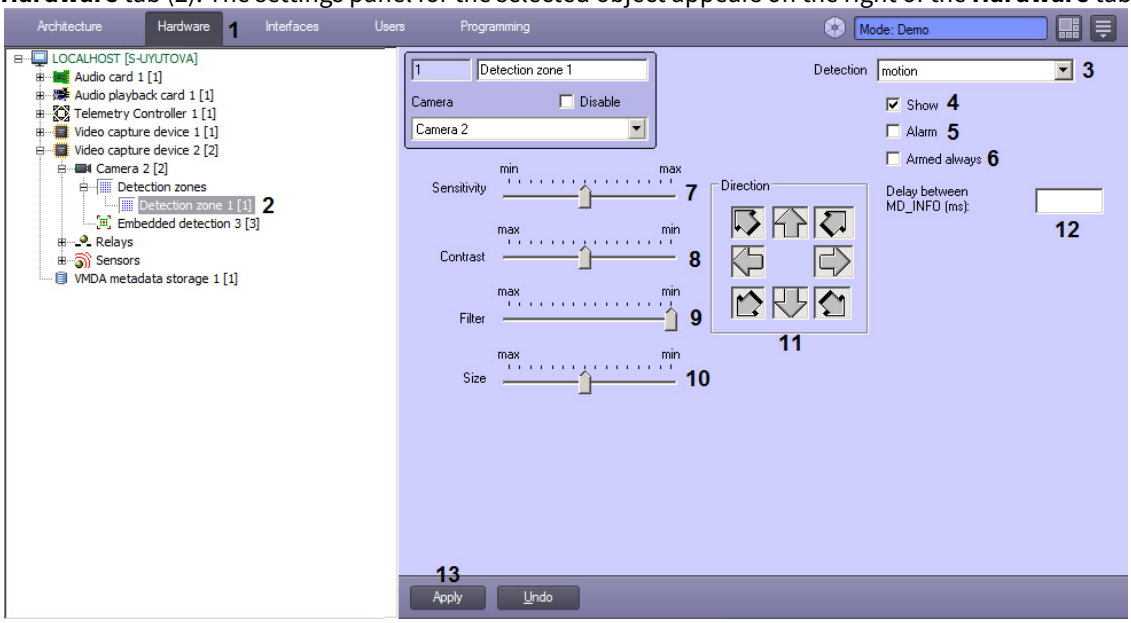
Configuring Motion detection tool
The Motion detection tool discovers moving objects in the zone under control. When a moving object is detected, it is dynamically framed. The motion is detected by calculating the gradient between sequential frames to time.

> **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 dynamically framed with its motion direction is marked with an arrow. If the moving object does not need to be framed, set the **Show** checkbox unchecked (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.

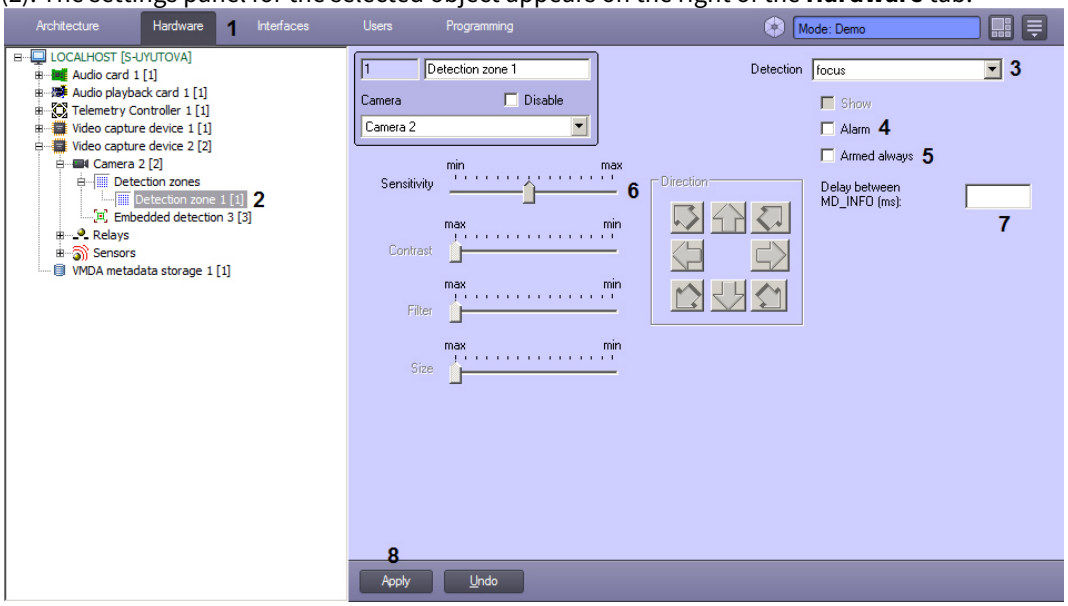
Configuring Focus detection tool

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).

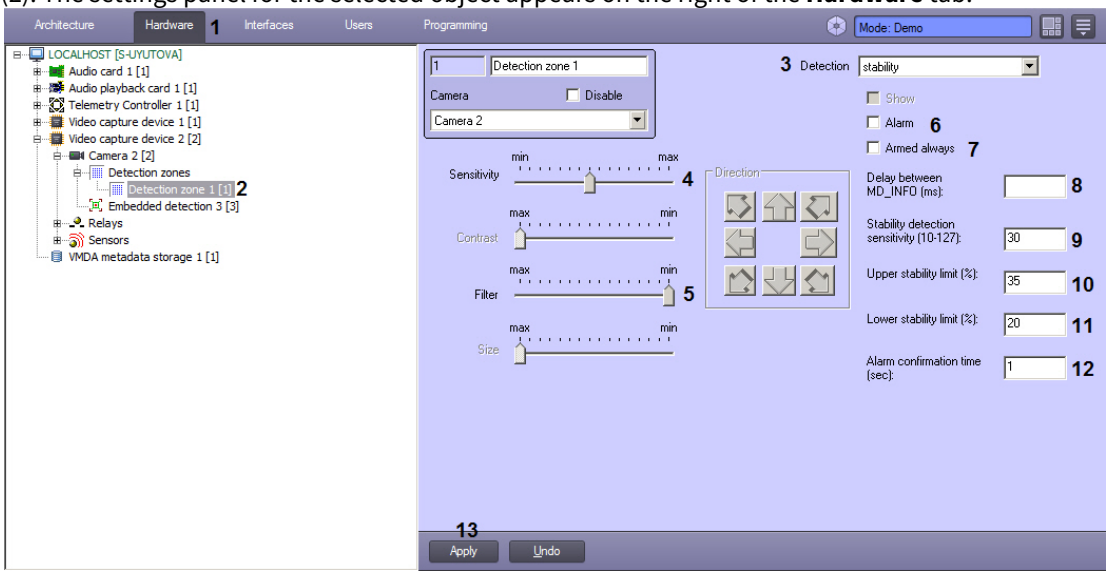
Focus detection tool is now configured.

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).

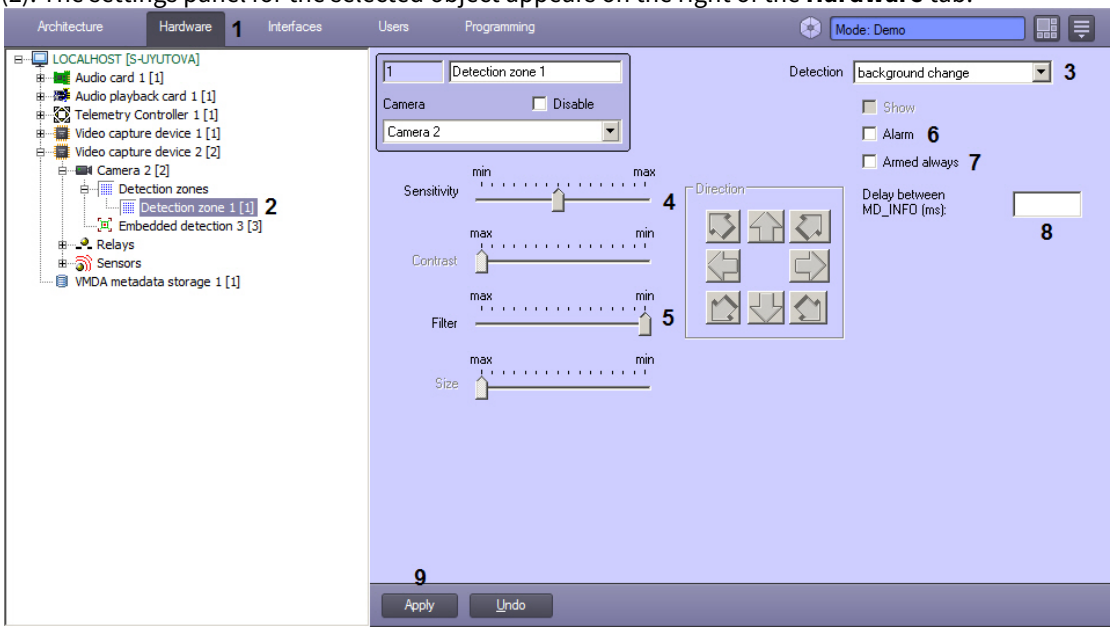
Stability detection tool is now configured.

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.

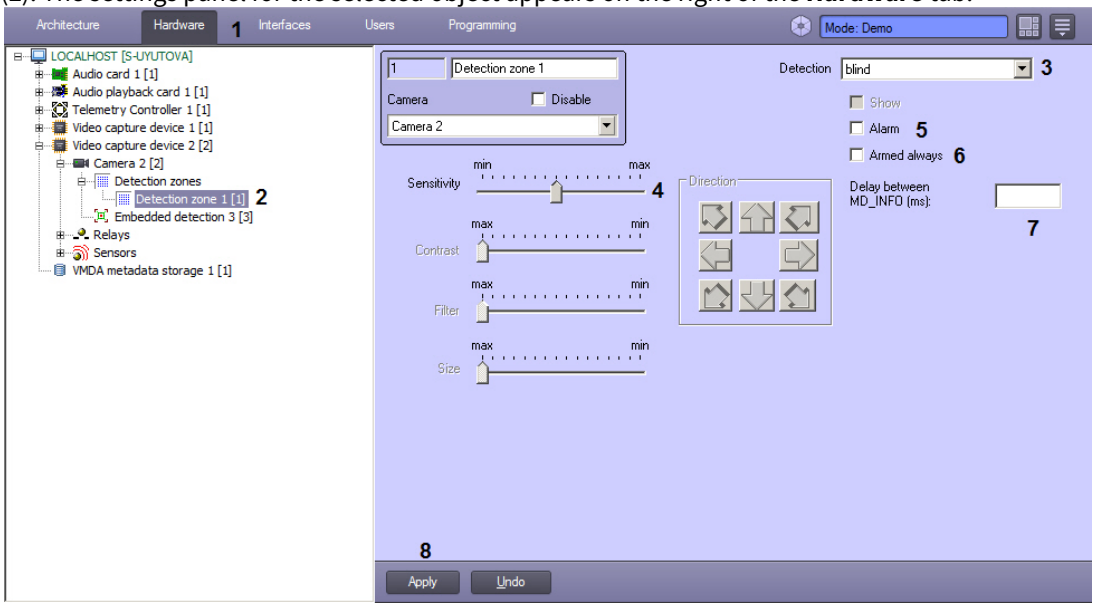
Configuring Blind detection tool

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).

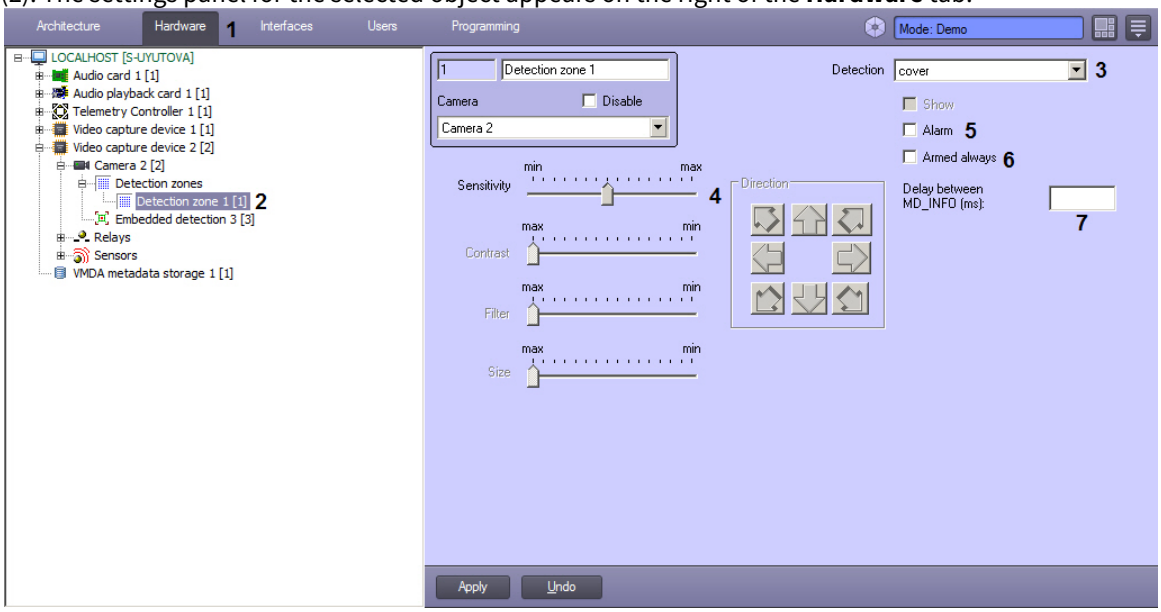
Note.

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.

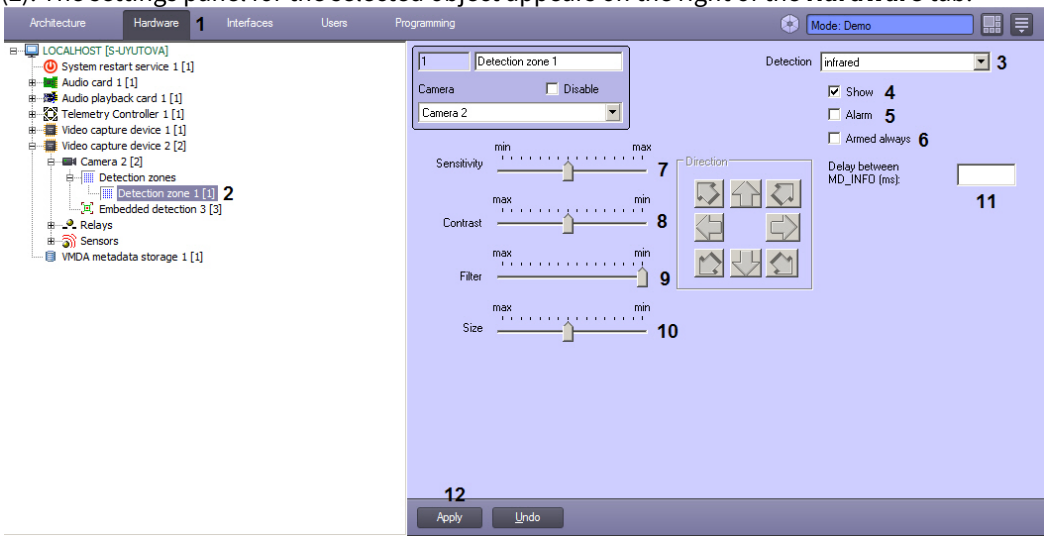
The video signal from the thermal imager is treated as a standard video signal, but the size of a detected object may be very small (as small as 3 pixels), so the detection tool needs fine tuning.

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.

10.3.2.7.3 Configuring smart video detection tools

10.3.2.7.3.1 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 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 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

10.3.2.7.3.2 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 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. .

10.3.2.7.3.3 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.

Important!

The neural analytic functions are not available for AArch64 (ARM) architecture processors.

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

10.3.2.7.3.4 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.

If these requirements are met, the following performance indicators of the abandoned object detection tool are guaranteed:

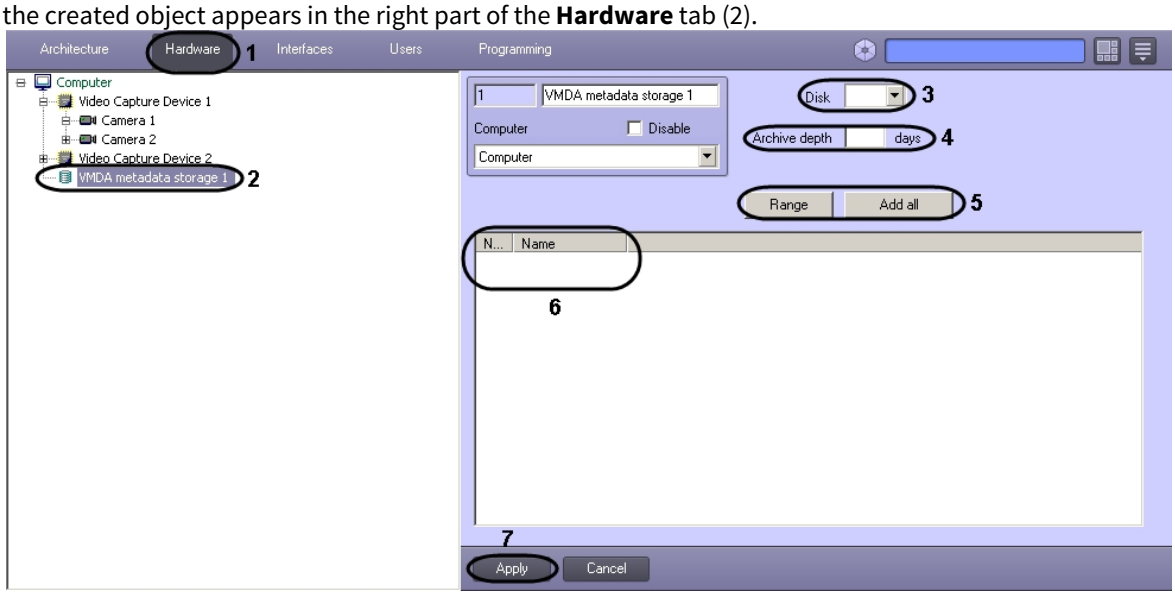
- 92 of 100 abandoned objects are detected.
- Out of 100 detection tool triggerings, 80 will be caused by real abandoned objects, and 20 - by other changes in the scene under surveillance.

10.3.2.7.3.5 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 select all cameras registered in the system click the **Add all** button or click the **Range** button to go to the **Add/Edit Camera objects** window (5).
   As a result all selected cameras are displayed in the table (6). One can edit the list of selected cameras in the table.
6. To save the changes, click the **Apply** button (7).

The VMDA metadata is now created and configured.

10.3.2.7.3.6 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 false alarms:

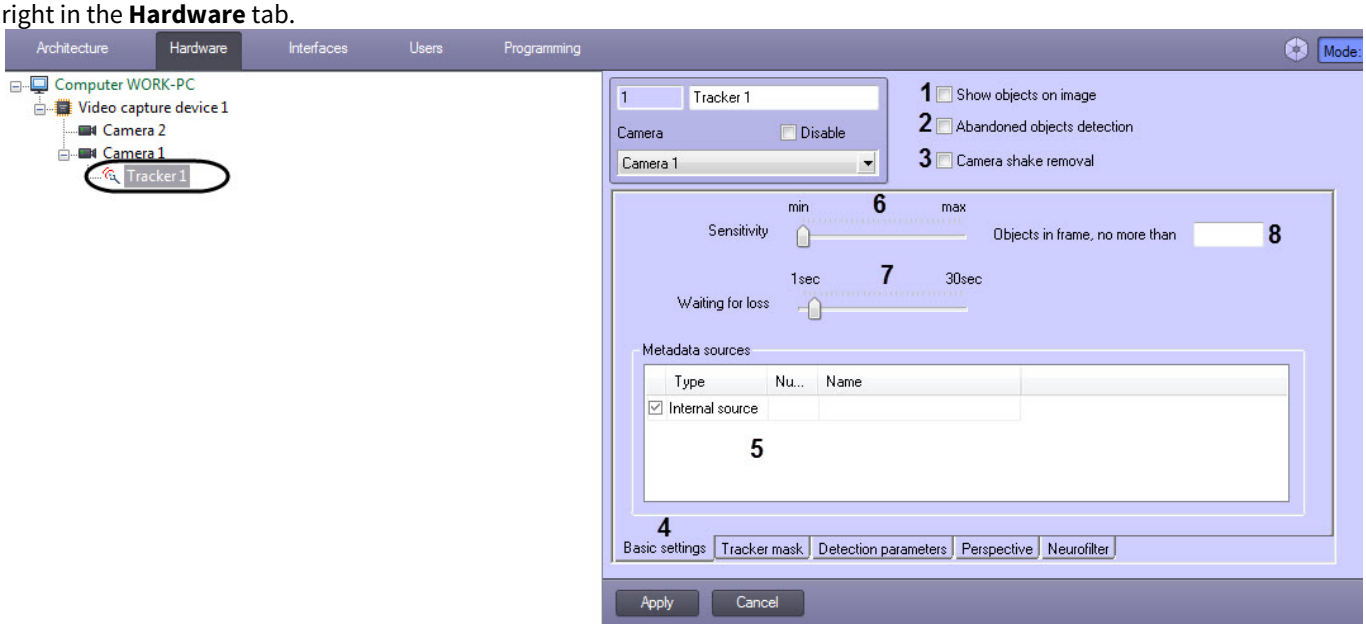
1. Configure the **Tracker** object iteratively and check its operation quality at each iteration.
2. The parameters that affect the **Tracker** object operation quality the most are: **Minimum size**, **Maximum size**, and **Sensitivity**.
3. It is recommended to set **Sensitivity** to zero (left end 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** value 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 is to be selected so that it is a little less than typical object size on the image.
6. Maximum size is to be selected so that it is a little greater than typical object size on the image, considering that the object can be joined with its shadow.
7. Lowering the **Waiting for loss parameter** allows excluding triggering of false static objects, while setting it to a higher value could allow not breaking off alarms for overlapping or temporarily disappearing objects in some cases.
8. To increase the VMDA detection tools accuracy, use an advanced object classifier, which is configured using the scripts and registry keys — see also CAM_VMDA_DETECTOR section of the Programming Guide.
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).

10.3.2.7.3.7 Creating and configuring the Tracker object

The **Tracker** object is designed for motion detection and saving video recordings to VMDA metadata storage.

To configure the **Tracker** object, do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box.
2. Select the **Camera** object in the objects tree of the **Hardware** tab.
3. Create the **Tracker** object on the base of the **Camera** object. The settings panel for the created object appears on the right in the **Hardware** tab.



4. Set the **Show objects on image** checkbox (1), if the objects are to be framed in the Video surveillance window.

Note.

To enable displaying tracker ID, set 1 value for the DrawDetectorNumbers line parameter in the HKEY_LOCAL_MACHINE\SOFTWARE\ITV\INTELLECT\Video (HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\INTELLECT\Video for 64-bit system) registry. Frame color is adjusted by the DrawDetectorColors parameter in the same registry:

a. When value is 1, then the frame color is the average one in the area
b. When value is 0, then the frame color is white.

5. To allow VMDA detectors monitoring abandoned objects in area covered by the camera set the **Abandoned objects detection** checkbox (2). See the video requirements for this feature to operate in the Video requirements to be met for abandoned object detection tool of the Tracker object operation section.

Note.

If there is no need to monitor abandoned objects in area covered by the camera, disable the **Abandoned objects detection** option to reduce Server load. Disabling this option you disable detectors configured to monitor abandoned objects.

By default, if the **Abandoned objects detection** feature is enabled, then when viewing the live video and archive video, only the abandoned objects will be framed on a video image. In order for the VMDA detector to detect only the disappeared objects, or both the abandoned and the disappeared objects at the same time, it is necessary to change the value of the **VMDA.filterGivenOrTaken** registry key (for details, see Registry keys reference guide, for more information about working with the registry, see Working with Windows OS registry).

Note

The function of framing the abandoned and disappeared objects on the video is available for both standard and converted fisheye video



6. If the camera is installed on the moving object, then set the **Camera shake removal** checkbox to stabilize the image and reduce detector's errors (3).

Attention!

When the Camera shake removal option is active, the Server load increases.

7. Go to the **Basic settings** tab (4).
8. In the **Metadata sources** table, set checkboxes next to objects used for metadata creation (5):
   a. Internal source. The resources of the **Tracker** object itself are used as metadata source.

b. Embedded detector. Metadata goes from detectors embedded in the camera (see Embedded detectors section).

> **Note.**
>
> Functionality of recording tracks from the embedded detectors must be supported by the device. Furthermore, this functionality has to be integrated in the *Intellect* software.

9. Set the value of the **Sensitivity** parameter by moving the slider to the required position (6). The parameter value corresponds to minimal value of moving object's averaged brightness on which the detector will trigger only to its motion, not to video signal noise (including snow, rain, etc.).

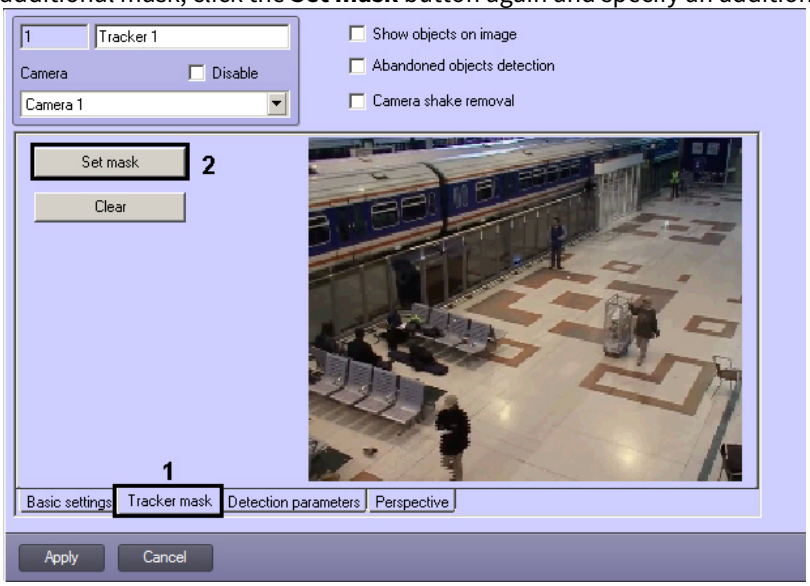
> **Note.**
>
> If the slider is in the left end position, then the value of the **Sensitivity** parameter is selected automatically.

10. 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 (7). If the object is motionless for a longer period than the value which has been set, then the object is considered to be lost.

> **Note.**
>
> If the lost object starts moving it is considered as a new one.

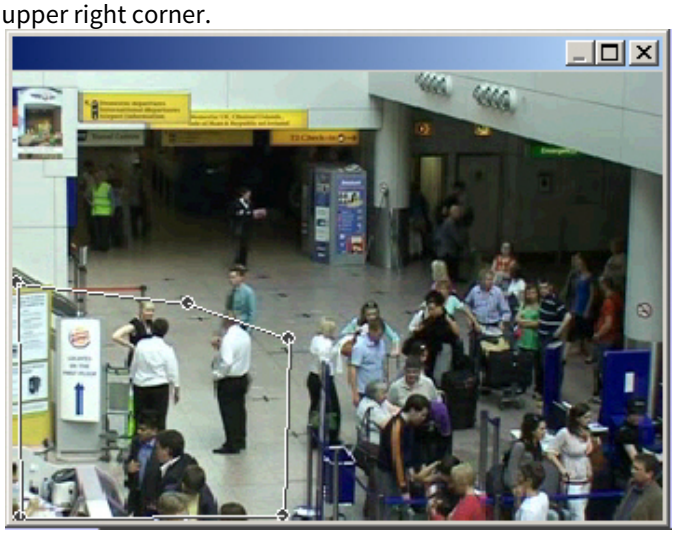
> **Note.**
>
> More sophisticated configuration of abandoned objects detection tool is performed using registry keys – see Registry keys reference guide.

11. In the **Objects in frame, not more than** field specify maximum number of objects in the frame that are detected (8). If the number of objects exceeds the specified value, then MD_LIMIT event is generated (see CAM section of Programming Guide). If the parameter is not set or equal to 0, then this event is not generated.
12. To disable analysis in the area covered by the camera click the **Set mask** button (2) in the **Tracker mask** tab (1) and specify the area in the preview field. 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 field.



To zoom in on the video preview field for more precise selection of the masked area, right-click the video preview while holding 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

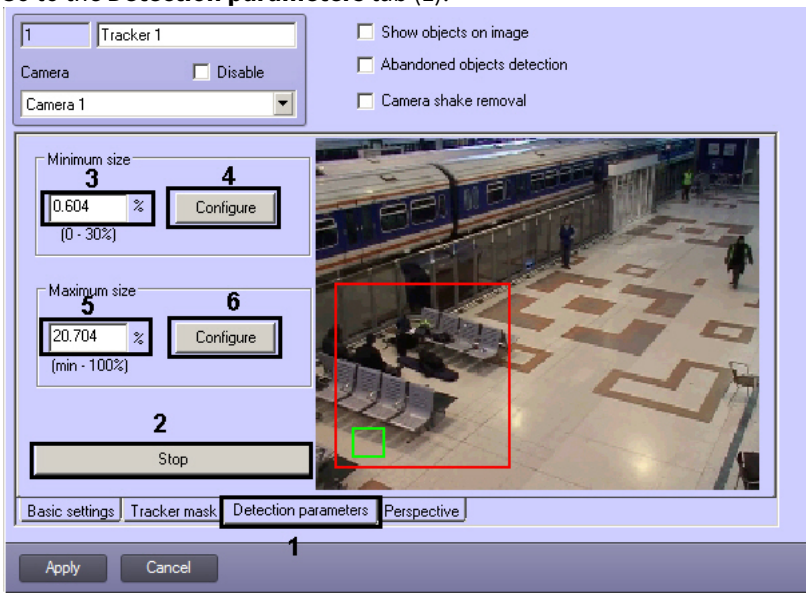
upper right corner.



13. To set the minimal and maximal sizes of detected object do the following:

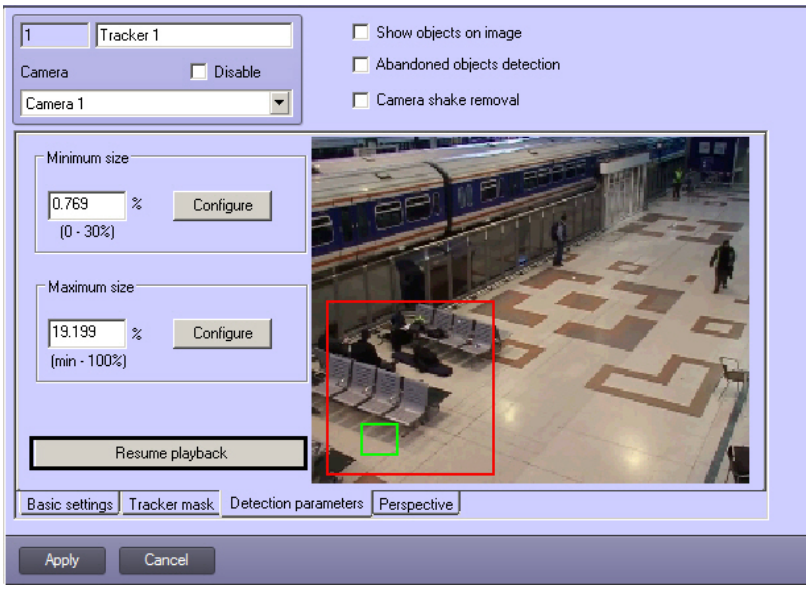
> **Note.**
>
> If the perspective configuration is enabled, maximum and minimum object size for detection parameters are ignored. **Width, m and Height, m parameters** in the **Perspective tab** (see Configuring perspective) are considered instead.

a. Go to the **Detection parameters** tab (1).



b. To stop playback in the preview, click the **Stop** button (2).

> **Note.**
>
> To resume playback, click the **Resume playback** button.



c. In the **Minimal size** group specify the minimal size of detected object as a percentage of total image area (3) or click the **Configure** button and specify the size in the preview area (4).

> **Note.**
>
> Range of values of the **Minimal size** parameter varies from 0 to 30% relatively the frame size.

d. In the **Maximal size** group, specify the maximal size of detected object as a percentage of total image area (5) or click the **Configure** button and specify the size in the preview area (6).

> **Note.**
>
> **Maximal size** is to be bigger than the minimal one and not more than 100%. If the maximal size is the same as the minimal, then there is no detection.

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

The **Tracker** object is now created and configured. During video signal recording in VMDA metadata storage the information about all objects in camera coverage will be recorded.

Configuring perspective

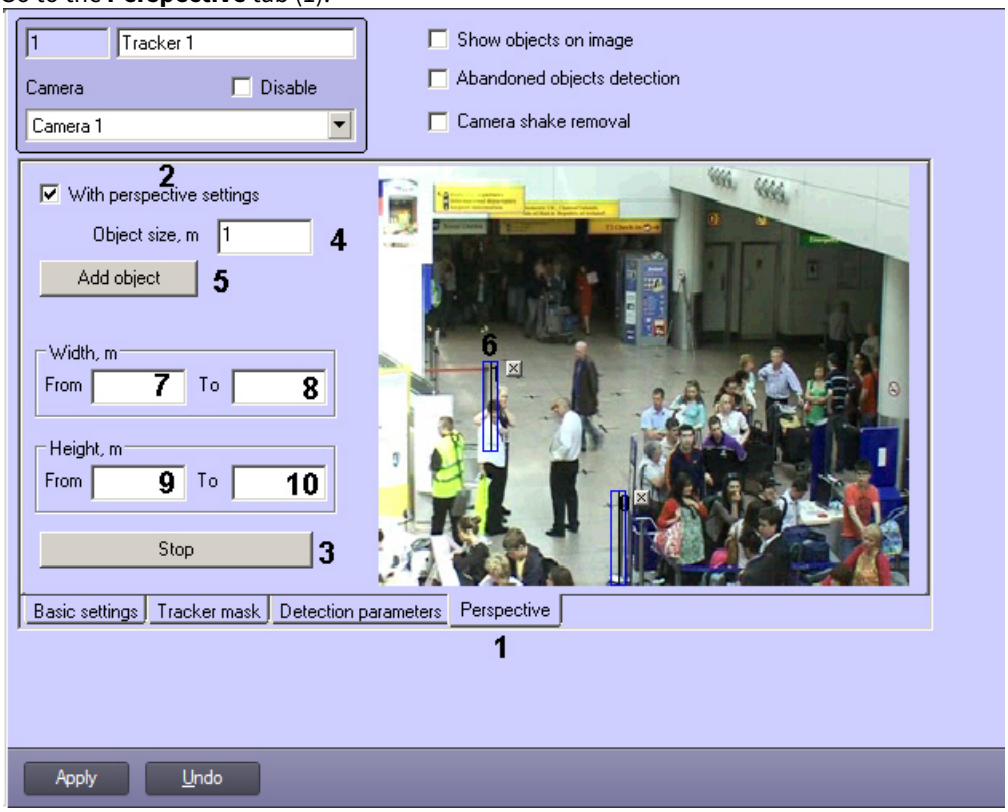
Perspective in the **Tracker** object is configured in order to set maximum and minimum object size (in meters) for these sizes to be considered correctly regardless of the fact that small objects can look bigger than big objects in the background. Perspective calibration allow better performance of 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.

10.3.2.7.3.8 Configuring object classification

There are 3 types of object classification by the smart detectors in *Intellect*.

1. Standard. The following objects can be classified: a human, a vehicle, an other object (see Cross line detector configuration and Motion in the Area detector configuration).
2. Advanced. The following objects can be classified: a human, a group of humans, a vehicle, noise, an object carried into the area, an object carried out of the area, an other object (see the CAM_VMDA_DETECTOR section of the Programming Guide).
3. Neural filter — 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:

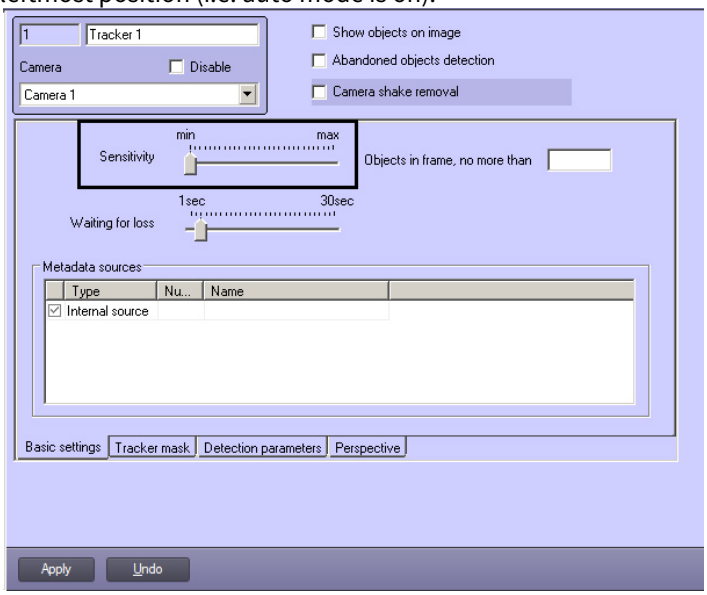
- if there are different classification tasks: for example, for some cameras the human/vehicle object classification is required, and for other cameras, the vehicle type (passenger car/freight vehicle) classification is required;
- if different conditions apply to different cameras, and the tracker will 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.

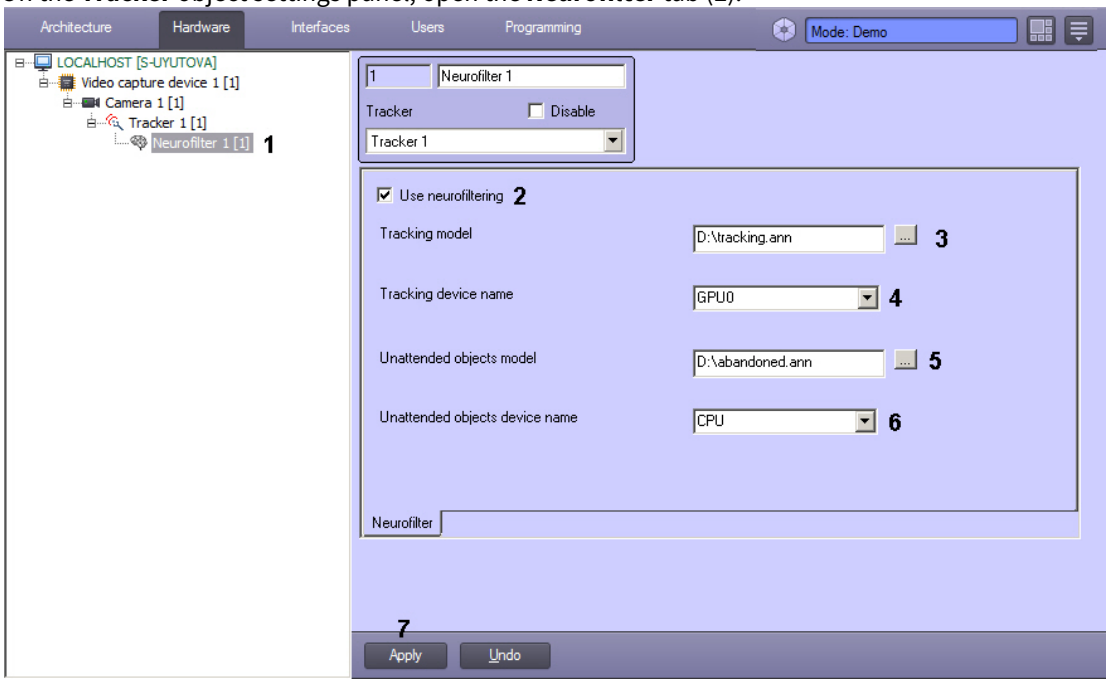
The neural filter is configured in the following way:

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**).

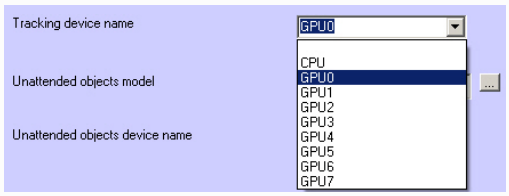


6. Set the **Use neurofiltering** (**2**) checkbox.
7. In the **Tracking model** field (**3**), enter the full path to the tracker model file received from the AxxonSoft technical support, or click the **...** button and select the file in the standard Windows dialog box.
8. In the **Tracking device name** field (**4**), enter 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, th CPU resources should be used. GPUs from other manufacturers are not supported.

Note

In the 64-bit version of Intellect (Intellect64.exe), the the tracking device name is selected from the drop-down list of the processors and GPUs available on the computer.



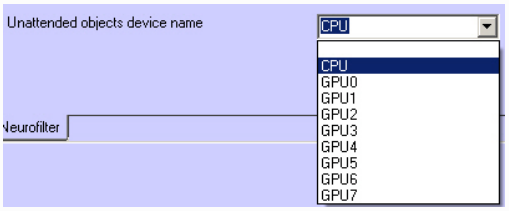
9. In the **Unattended objects model** field (**5**), enter the full path to the abandoned objects detection model file received from the AxxonSoft technical support, or click the **...** button and select the file in the standard Windows dialog box.
10. In the **Unattended objects device name** field (**6**), enter 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).

Note

In the 64-bit version of *Intellect* (Intellect64.exe), the unattended objects device name is selected from the drop-down list of the processors and GPUs available on the computer.



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 VMDA detection
VMDA detection are detection tools due to triggering of which some actions can be performed in the system.

For instance, when the detection tool with corresponding settings triggers, the alarm on camera is generated and recording to the archive starts. Thus VMDA detection tools allow recording to the archive and, therefore, the recording of object trajectories, not steadily, but in the required situations.

If it is necessary to initiate a camera alarm when the VMDA detection tool is triggered, select the **Generate alarm on camera** check box.

Detections arming and disarming is performed using macros or scripts which are to be created manually (detailed information about macros see in the Creating and using macros section). The initial state of detection is defined by **Generate alarm on camera** checkbox – detection armed if the checkbox is set, otherwise – disarmed.

The table below describes the cases and reactions on detection tool triggering (e.g. on line crossing or motion in the area).

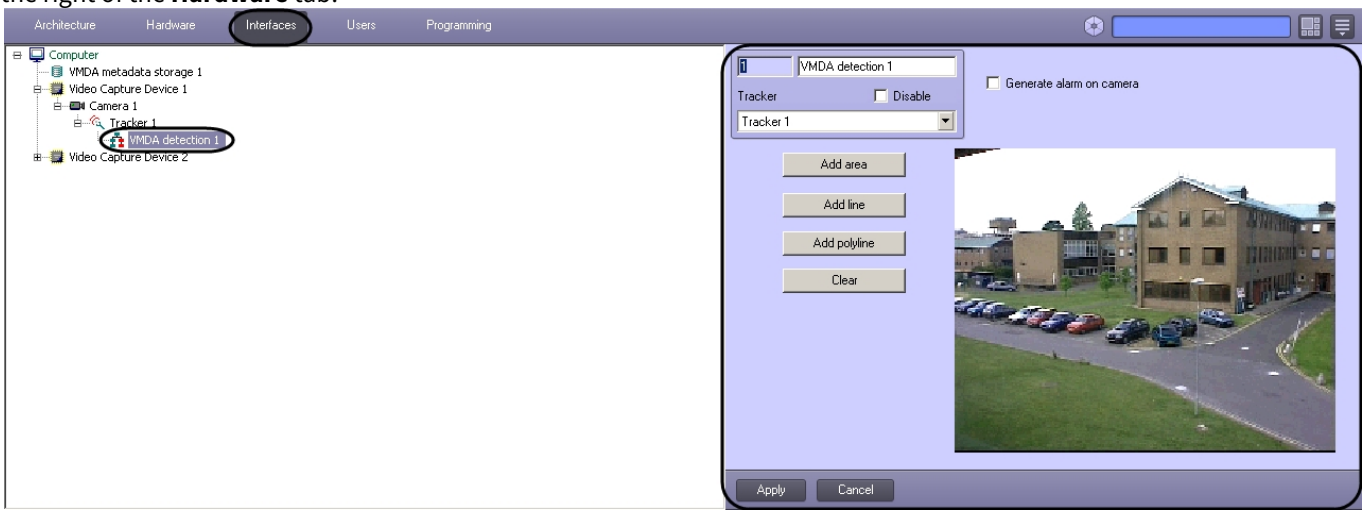
	Detection tool is armed	**Detection tool is disarmed**
Generate alarm on camera check box is set	Alarm on camera + alarm on detection tool	nothing happens
Generate alarm on camera check box is not set	Alarm on detection tool	nothing happens

Note.

The **Disappearance in the area** detection tool is triggered **immediately** after an object in the area disappears. By default, the alarm is reset 15 seconds after the alarm is triggered. To change the length of time after which an alarm is reset, edit the DisappearedAlarmDuration registry key in the HKEY_LOCAL_MACHINE\SOFTWARE\ITV\INTELLECT\Video section for 32-bit systems (HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ITV\INTELLECT\Video for 64-bit systems).

To create a **VMDA detector,** do the following:

1. Go to the **Hardware** tab in the **System settings** dialog box.
2. Select the **Tracker** object in the objects tree of the **Hardware** tab.
3. Create the **VMDA detection** object on the base of the **Tracker** object. The settings panel for the created object appears on the right of the **Hardware** tab.



Note.

Video from the camera on the baase of which the VMDA detection object is created is displayed in the **Video** field.

The **VMDA detection** is now created. Information only about the objects that triggered detector action is recorded to the VMDA metadata storage.

Attention!

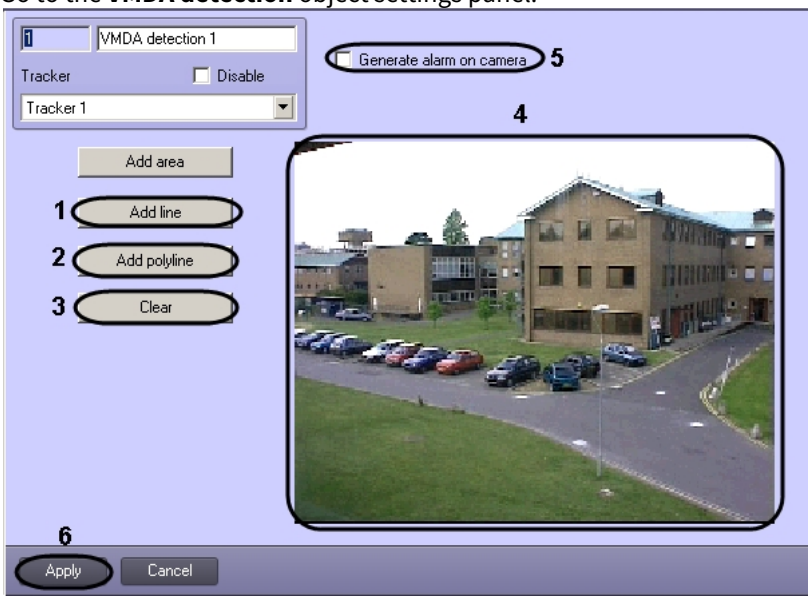
Creating VMDA detection on IP cameras, do not forget about information in the Requirements for IP devices of audio and video input section.

Cross line detection tool configuration

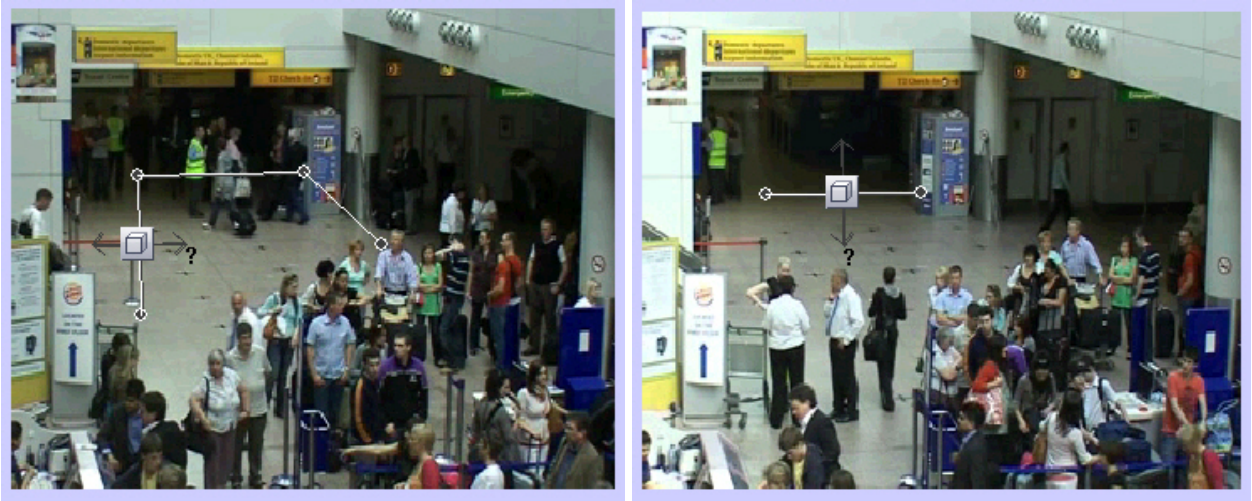
A cross line detection tool is a VMDA detection tool that triggers when the object trajectory in the camera FOV crosses a virtual line.

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 a human

c. Vehicle. Detector triggers when the line is crossed by a vehicle

> **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 section of the Programming Guide.
>
> 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.

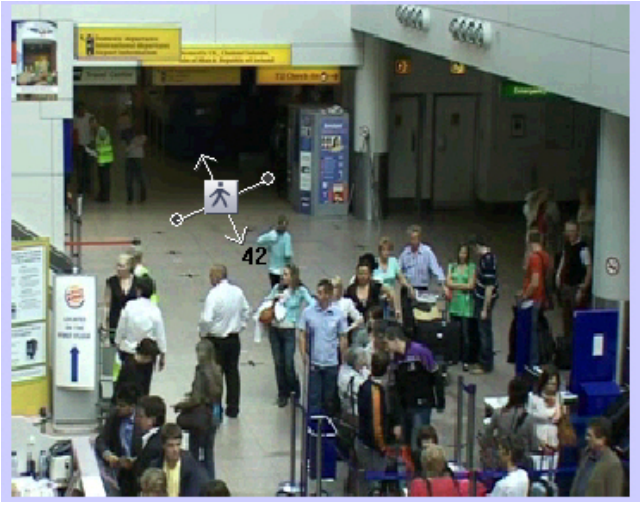
7. By default, the detection tool triggers on line crossing in both directions. Click the left mouse button upon one of the arrows to ignore crossing in one of the directions. The arrow will be colored gray.

> **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 save the changes, click the **Apply** button (**6**).

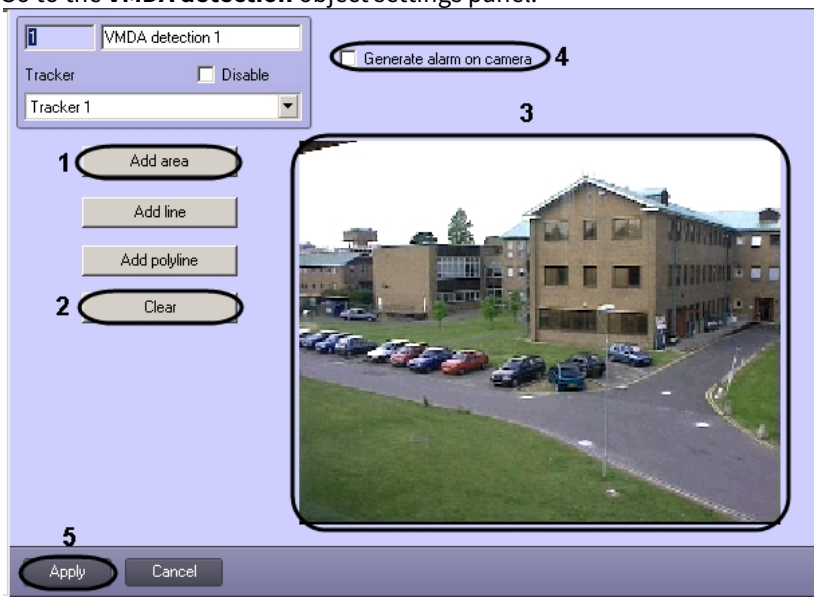
> **Note**
>
> To clear the preview field from a visual element (a line), click the **Clear** button (**3**).

A cross line detector is configured.

Motion in the Area detection tool configuration
A motion in the area detector is a VMDA detectoion 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. The operations are shown in the table.

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 while dealing with any object.
   b.  A human. Detector triggers while dealing with a human.
   c.  A vehicle. Detector triggers while dealing with a vehicle.

> **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 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 given below.
   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 precense in the area for more than 10 sec. This period can be confgured with LongInZoneTimeout registry key (see Registry keys reference guide).
   h. An abandoned object. Detector triggers due to the item abandoned in the area
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 save the changes, click the **Apply** button (**5**).

> **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 a Moving from one area to another detection, do the following:

1. Configure the Motion in the Area detection, do not select the detection tool type – see Motion in the Area detection tool configuration.
2. Add the second area similar to the first. The ability to select the type of Motion in the Area detection tool for the first zone is disabled when the second zone is added. The second zone is not configurable.



3. Click **Apply**.

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.

The setup of the Moving from one area to another detection tool is now complete.

10.3.2.7.4 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 tracking 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.

10.3.2.7.4.1 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.

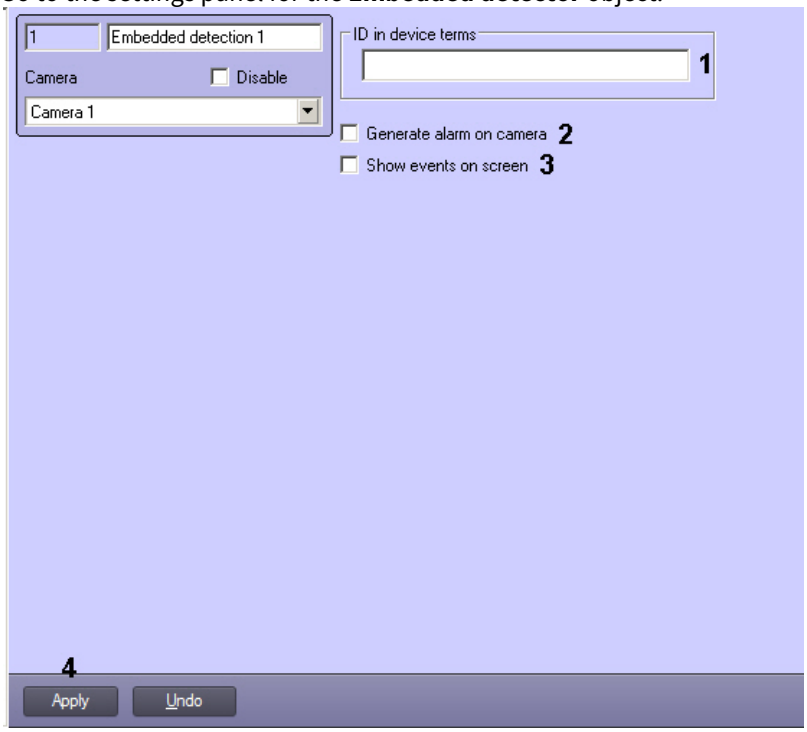


Build-in detectors creation is completed.

10.3.2.7.4.2 Configuring embedded detectors

To configure embedded detectors, do the following:

1. Go to the settings panel for the **Embedded detector** 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 detector.
3. Set the **Generate alarm** on the 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 tracking in Axis devices.

> **Note.**
>
> See also Creating and configuring the Tracker object.

5. Click the **Apply** button to save the changes (4).

Embedded detectors are now configured.

10.3.2.7.4.3 AxxonSoft tracking in Axis devices

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.

> **Note.**
>
> In order to perform forensic search in the archive while using this method of 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, follow these steps:

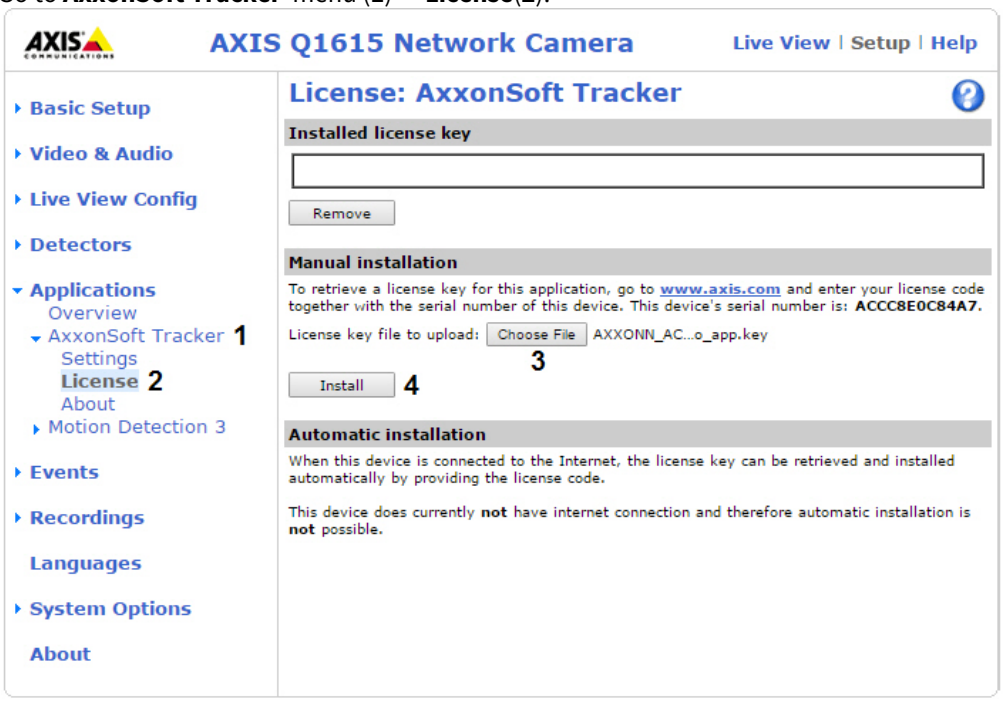
1. Go to the device's web interface.
2. Select the **Setup** menu (**1**) -> **Applications** (**2**).



3. Select the ACAP application (**3**) and click **Upload the Package** (**4**).

> **Important!**
>
> The application can be downloaded from AxxonSoft web site here.

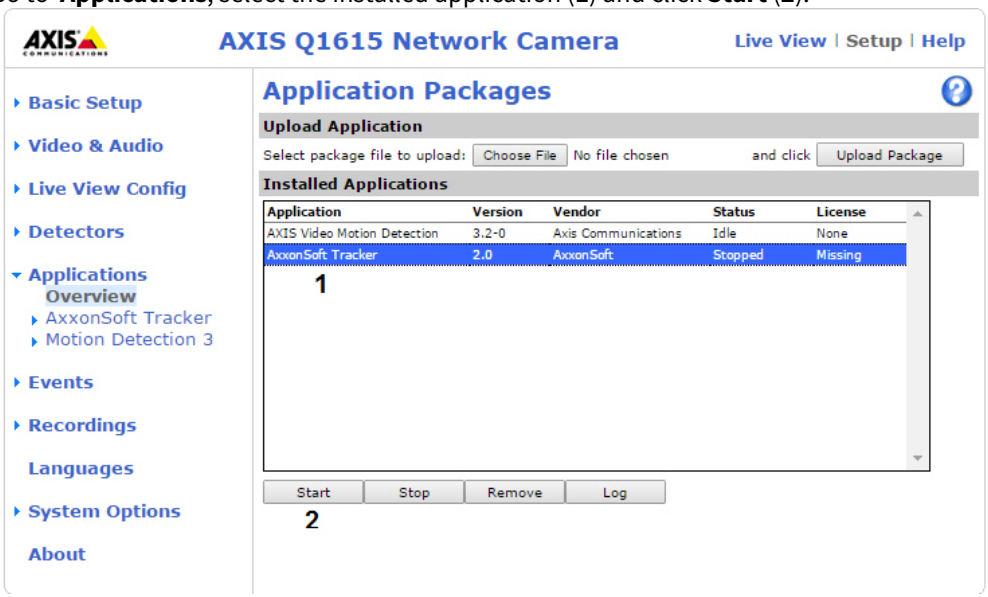
4. Go to **AxxonSoft Tracker** menu (**1**) -> **License**(**2**).



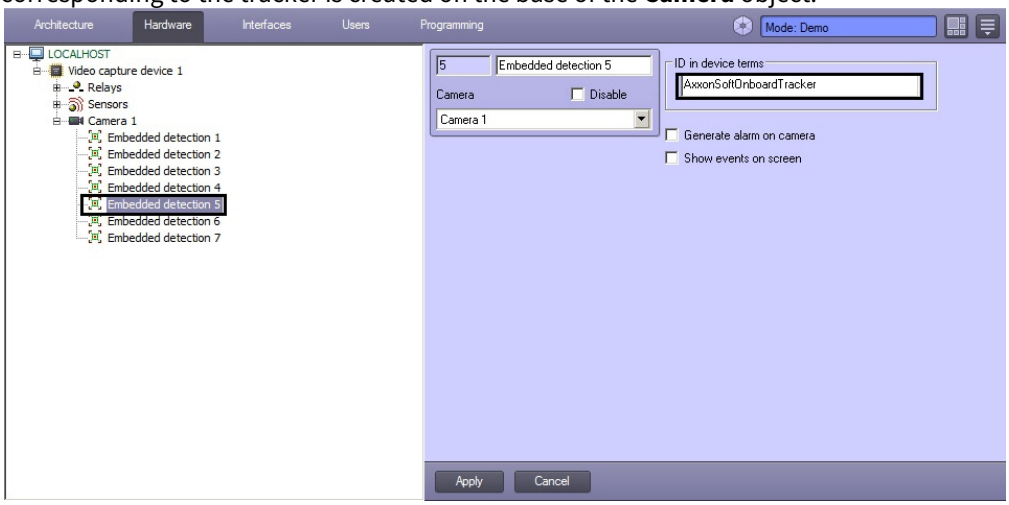
5. Select the license file (**3**) and click **Install** (**4**).

> **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 **Start** (**2**).



7. Add the Axis device to the *Intellect* software using the Camera discovery tool. An **Embedded detection tool** object corresponding to the tracker is created on the base of the **Camera** object.



8. Configure this object in the Intellect software according to the Configuring embedded detectors section.

> **Note.**
>
> The tracker parameters are configured in the **Setup** -> **Applications** -> **AxxonSoft Tracker** -> **Settings** section of the Axis device web-interface similar to the **Tracker** object in the Intellect software (see Creating and configuring the Tracker object).

Axxonsoft tracker is now configured to be used in Axis devices.

10.3.2.7.4.4 Example of setting up and using the embedded detectors on Bosch FLEXIDOME IP dynamic 7000 VR IP camera

On the page:

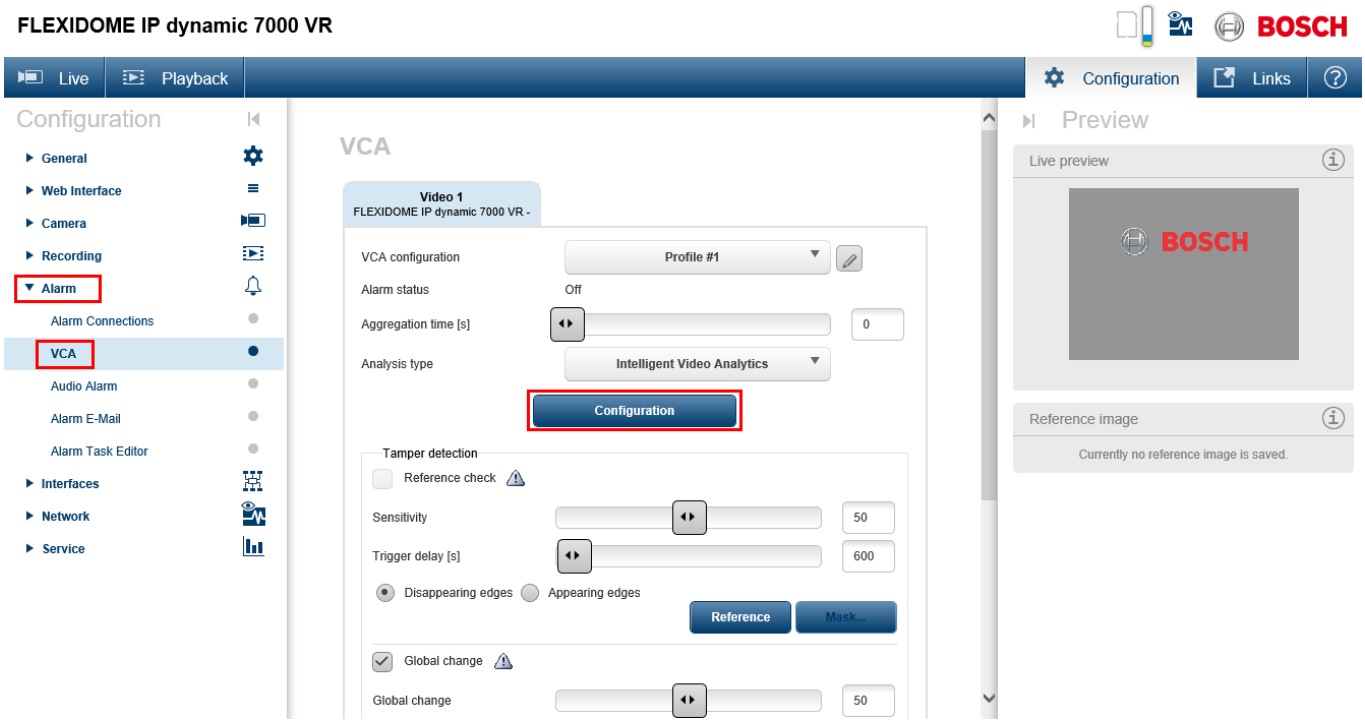
- Configuring the visitors counter using the camera web interface
- Configuring Intellect to receive the events from the Bosch camera's visitors counter
- Using the Bosch camera visitors counter in Intellect

Configuring the visitors counter using the camera web interface

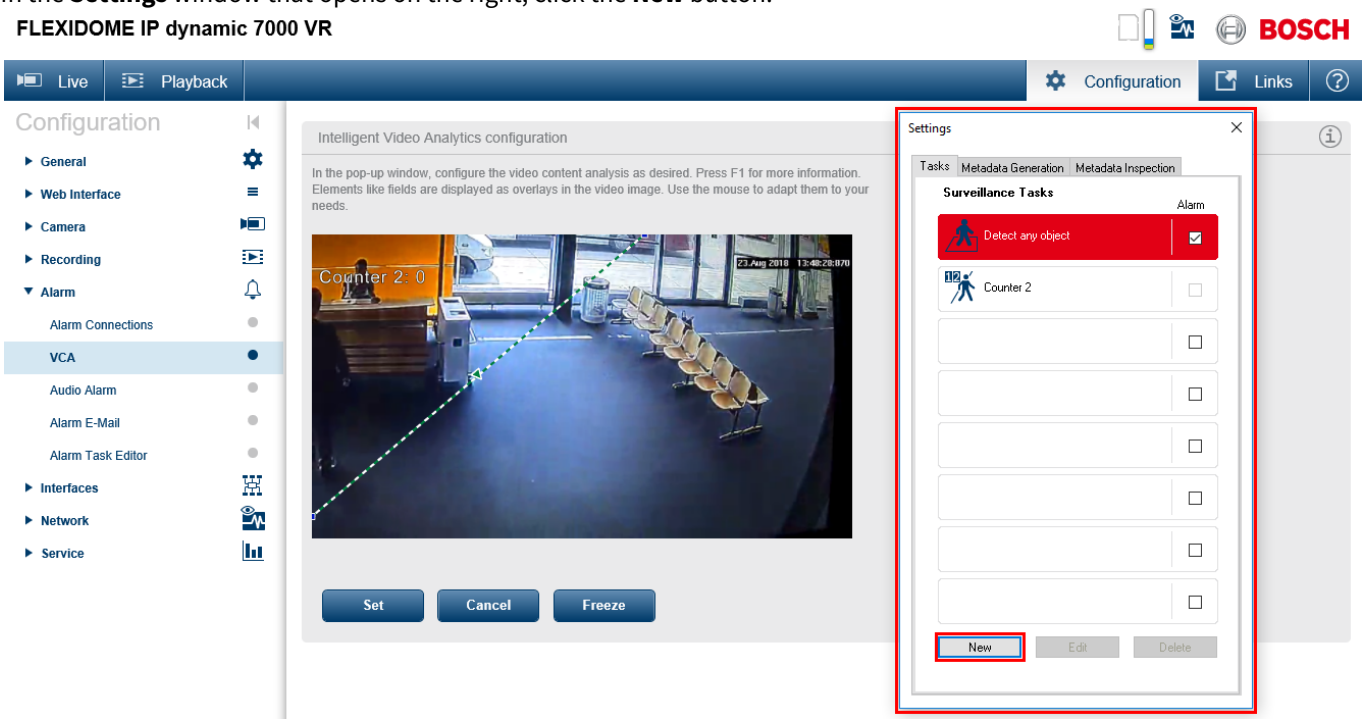
To configure the visitors counter using the camera web interface, do the following:

1. Open the camera web interface in the browser (see How to call the Web Server home page of IP device).

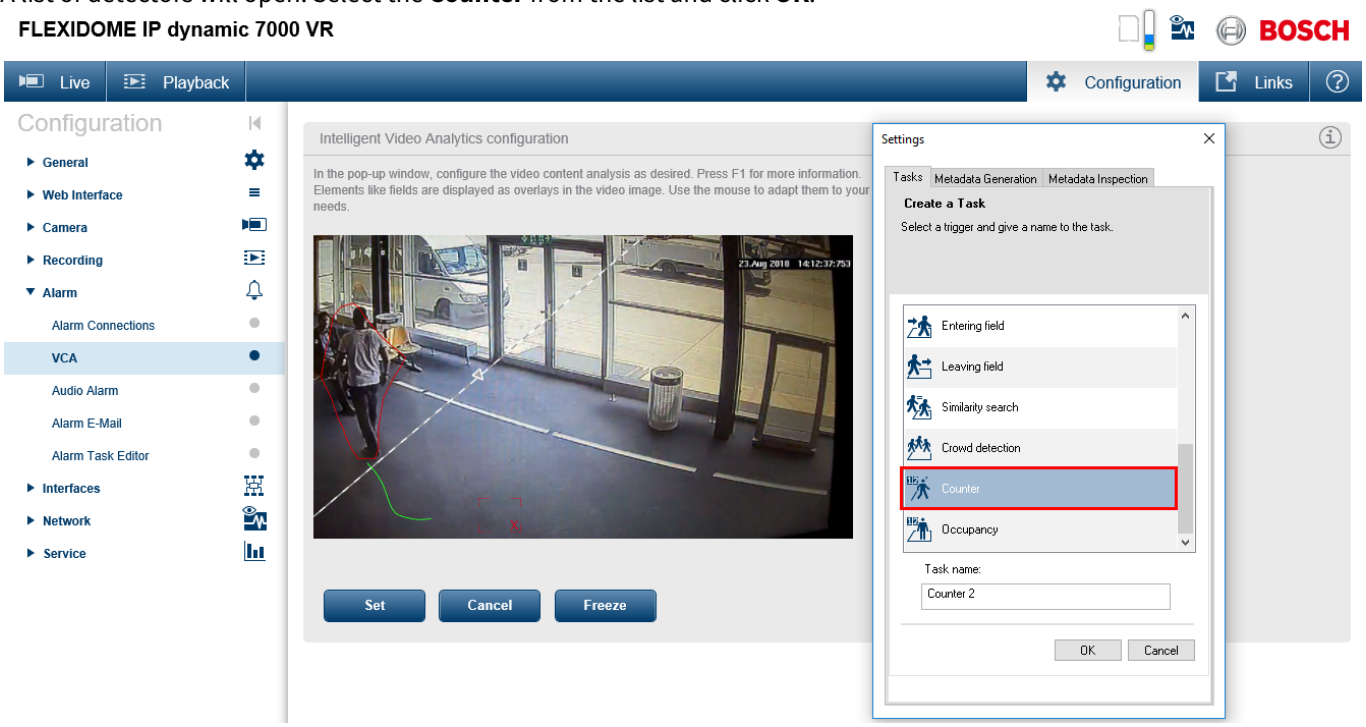
2. Go to **Settings** → **Alarm** → **VCA**, and then click on the **Configuration** button.



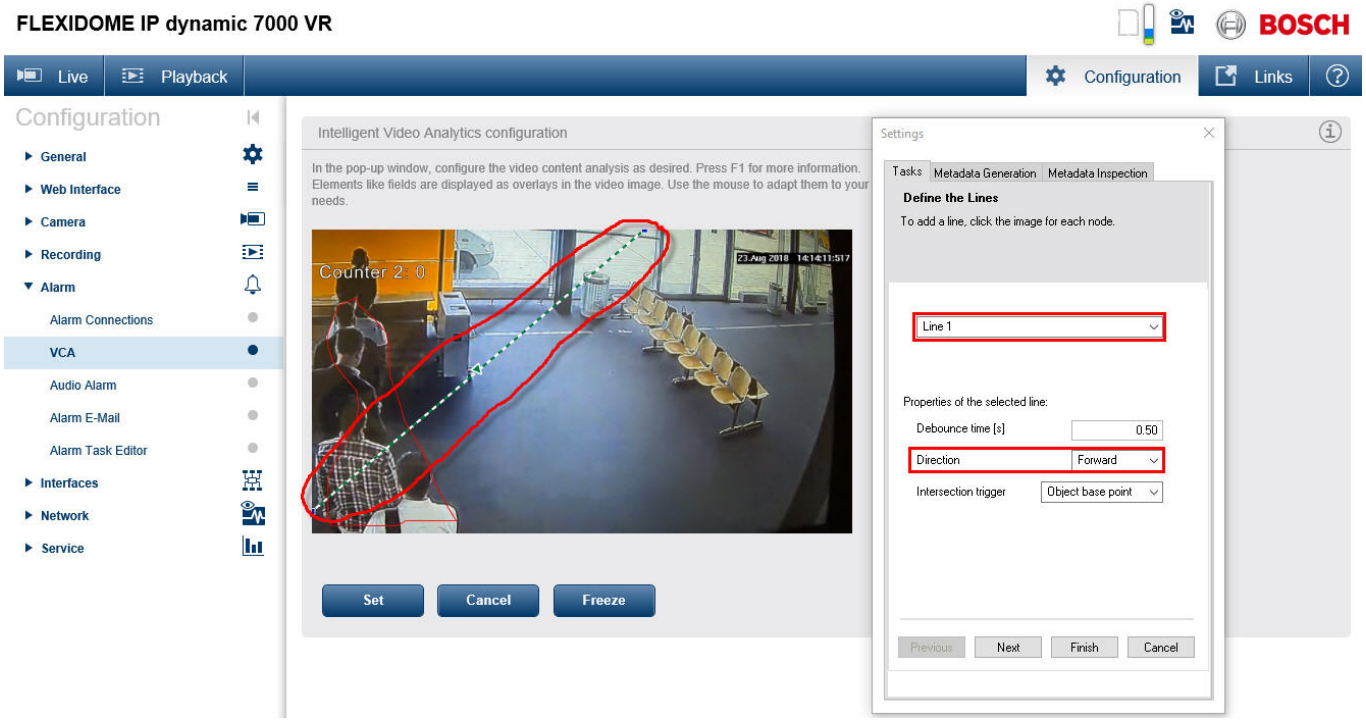
3. In the **Settings** window that opens on the right, click the **New** button.



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**.

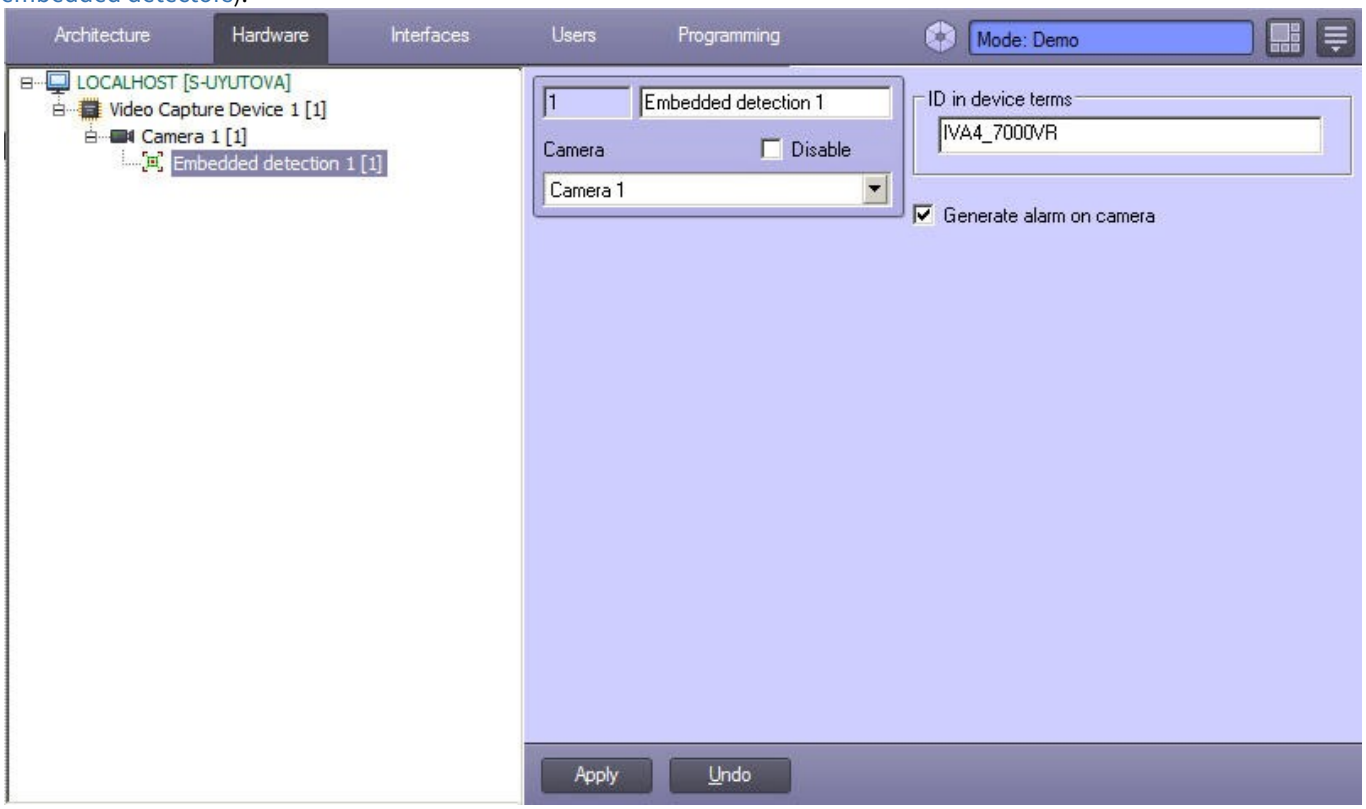


Configuring the visitors counter using the camera web interface is complete.

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

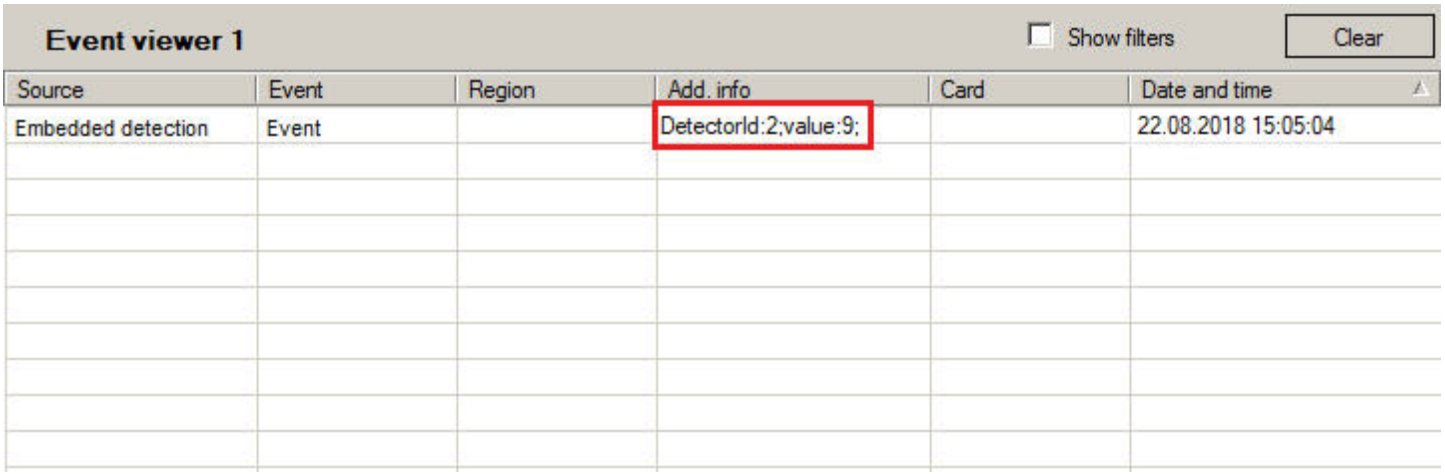
embedded detectors).



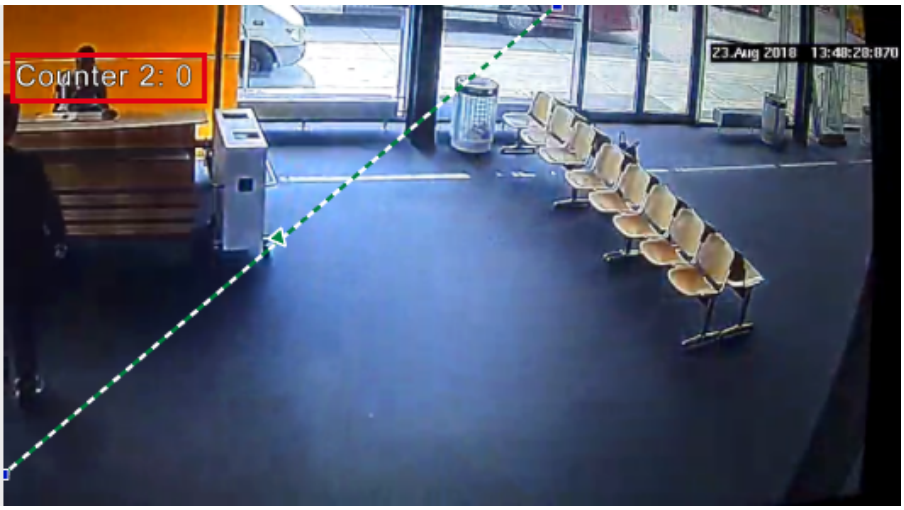
2. Create and configure the **Event viewer** object based on the **Display** object on the **Hardware** tab of the **System settings** dialog box (see Configuring the Event Viewer interface object).

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) 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.

10.3.2.7.5 Face detection tool

10.3.2.7.5.1 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.

10.3.2.7.5.2 Requirements to video parameters while using face detection tool

When a face detection tool is in use, the following requirements must be met:

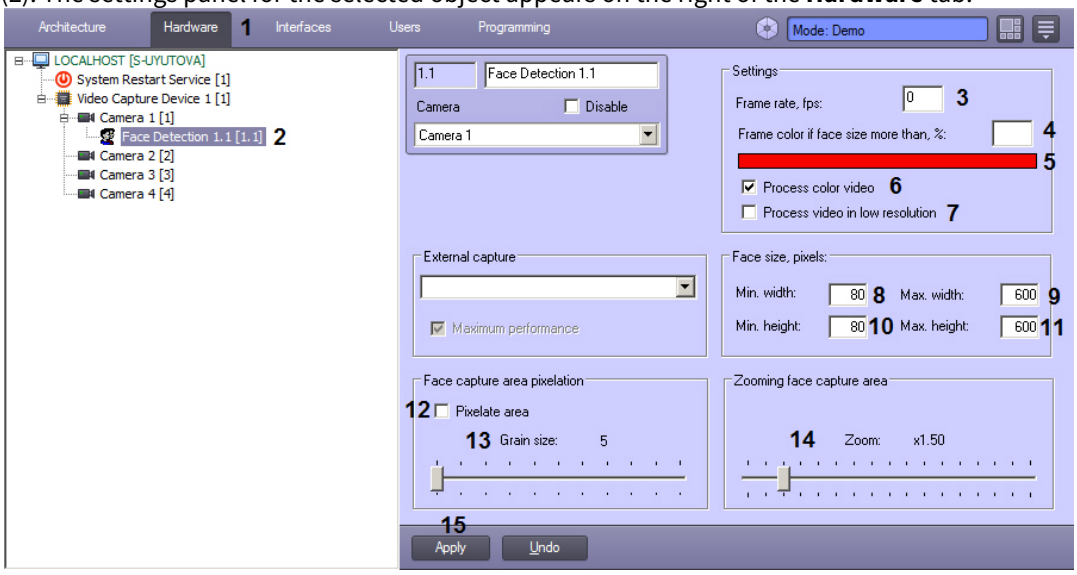
1. Minimum linear dimensions of a face to be detected are 24 pixels.
2. Maximum speed of a face to be detected is not to be more than a half of linear dimensions in pixels per frame (i.e. face overlapping between two adjacent frames must be not less than half-width and half-height of face).
3. A detection tool needs 8 frames to confirm face detection – otherwise, a face detection message won't be sent.

10.3.2.7.5.3 Configuring Face detection tool

To configure Face detection tool, do the following:

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

2. Select the **Face detection** 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. 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 (3).
4. Specify the size of a face in percent relatively to the sizes of camera's video surveillance window when the face is required to be dynamically framed (4).
5. If the color of a dynamic frame is to be changed, then left click the **Color** field (5). Select the required color in the standard **Color** dialog box and click **OK.**
6. Disabling of **Process color video** function (6) is only feasible if *Face Intellect* is installed. It is not recommended to disable it.

> **Note.**
>
> If the **Process color video** checkbox is unset, the color video image will be converted to black and white image to generate the vectors by the black-and-white frames. This function is supported by Tevian 2.3.0 face recognition module only. It reduces the CPU load, insignificantly affecting face capture and recognition quality (see Face Intellect Administrator's Guide for details).

7. 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 (7).

> **Note.**
>
> Enabling this option reduces the load of the Server's processor, but the probability of face detection 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.

8. Set approximate width of face on the video image in pixels;
   a. In the **From** field enter minimally allowable width of face on the video image (8).
   b. In the **To** field enter maximally allowable width of face on the video image (9).
9. Set approximate height of face on the video image in pixels;
   a. In the **From** field enter minimally allowable height of face on the video image (10).
   b. In the **To** field enter maximally allowable height of face on the video image (11).

Note.

Faces won't be detected if specified minimal sizes highly differ from actual sizes.
For example, if there are big faces (15-30%) on the video and minimal size is 5% and maximal size is 80%, then faces won't be detected. But if minimal size is 12% and maximal size is 80%, then faces will be detected.

So, detection won't detect big faces if it is configured for detection of small faces, 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 being part of the *Face Intellect* software.

10. To pixelate the part of video image in which the face was recognized, do the following:
    a. To enable the pixelate function set the **Pixelate area** checkbox (12).
    b. Set the **Grain size** cursor in position corresponding to the pixilation grain size in pixels (13).
11. Set the **Face capture area's scaling** slider to the position corresponding to the required scaling of a face in the frame for recording (14). The current scale value is displayed in the field above the slider and ranges from 1 (only the face is recorded) to 5 (the whole frame is recorded).

    Note.

    This setting is relevant in case of installed *Face-Intellect* system. A frame with a face is recorded to the < Face-Intellect>\ Bmp\ person\ folder.
12. Click the **Apply** button (15).

Face detection tool is now configured.

10.3.2.8 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.

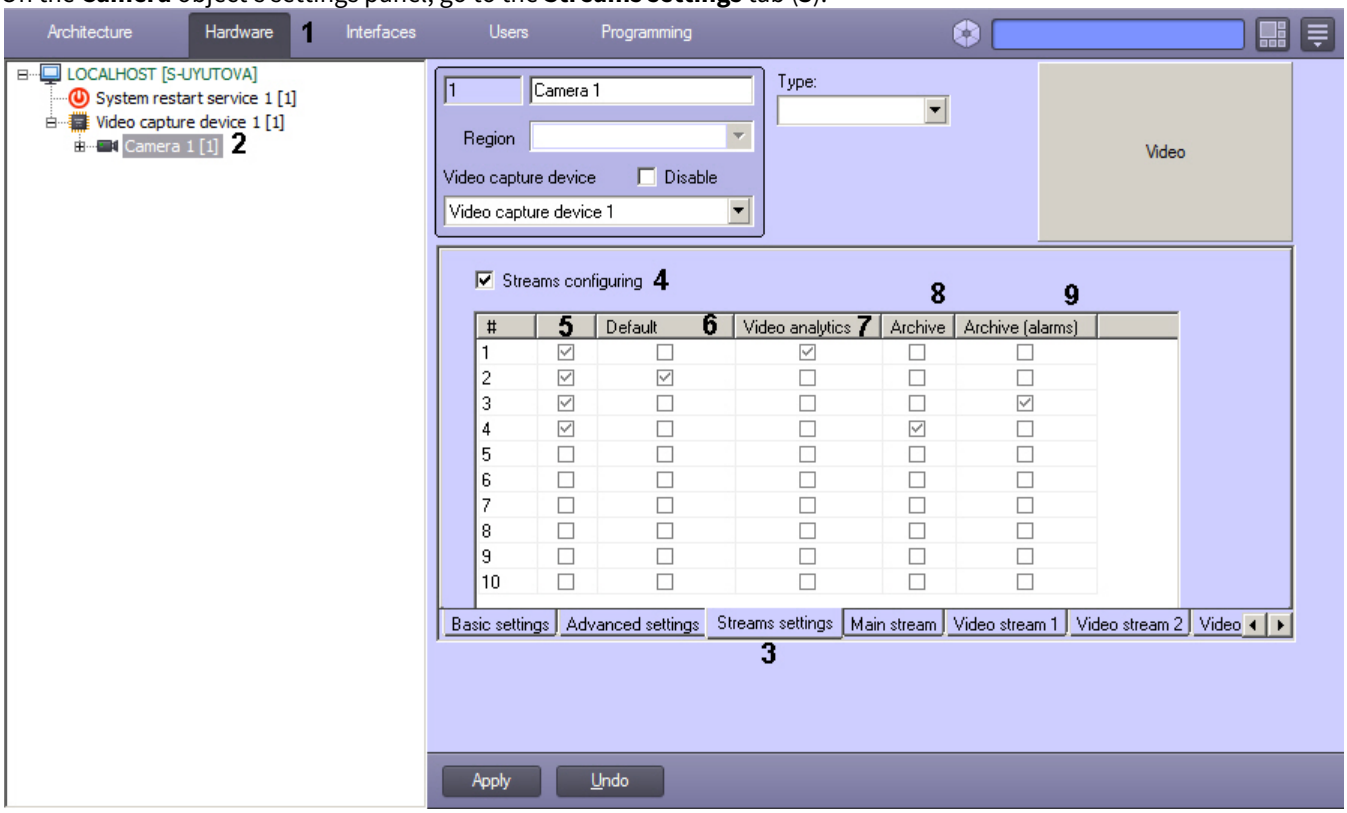
Note.

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.

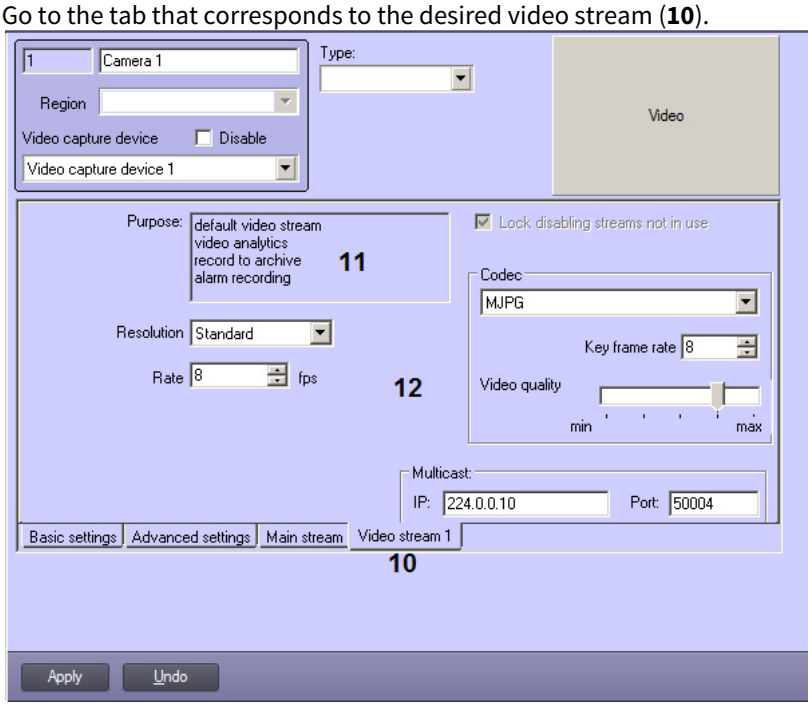
If different streams are selected for recording to the archive upon alarms and continuous recording, recording is performed non-stop and detection tools are enabled, then upon alarm recording of the current archive fragment is stopped in the continuous recording stream and recording of a new fragment 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.

10.3.2.9 Video record from computer monitor

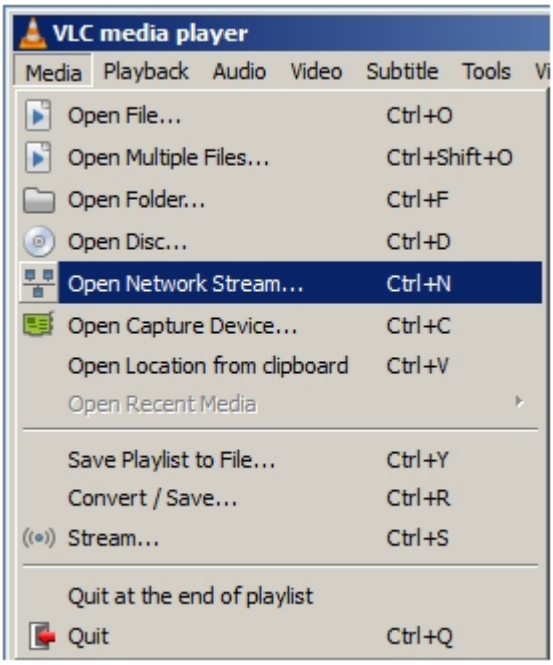
Record of video from computer monitor is performed to control operator actions. Video from computer monitor can be transmitted to the Intellect software package by general protocols using external programs, for example:

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.

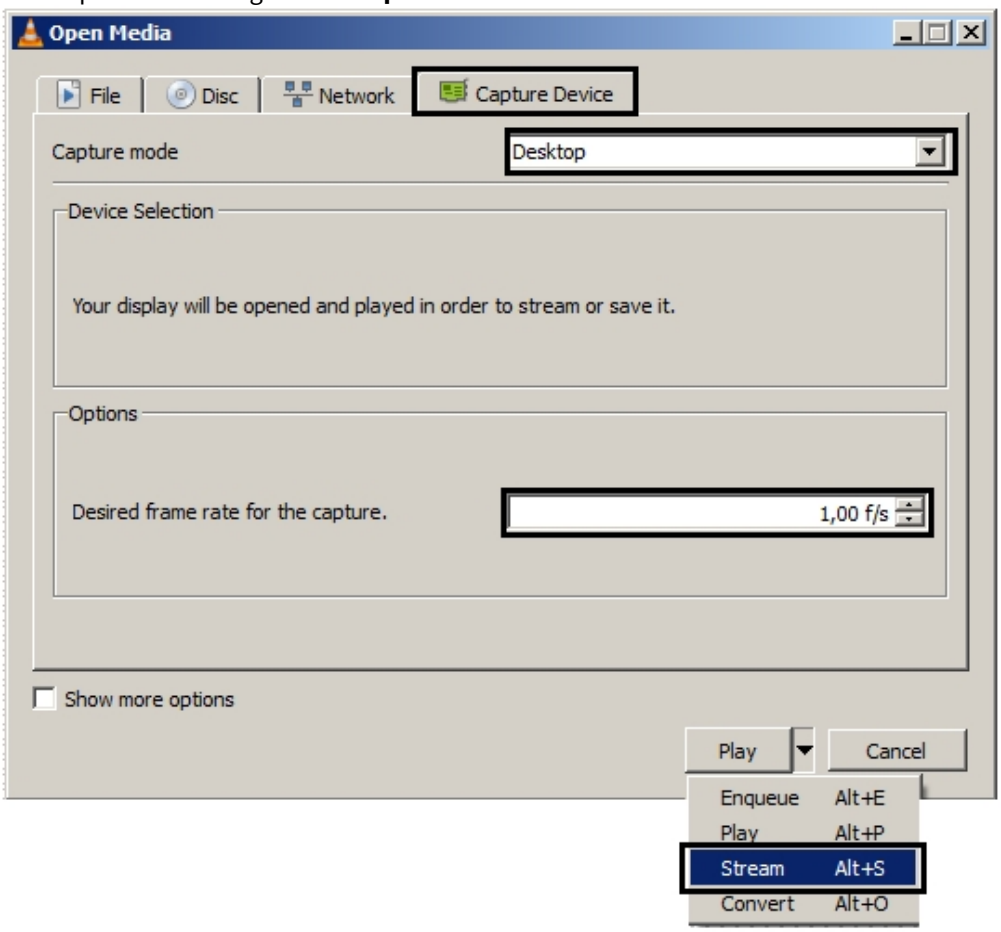
Example of the VLC Media Player configuring for transmitting video from computer monitor to the *Intellect* by the RTSP protocol is presented in this section. Configuring of the Intellect software package to receive and record this video stream is performed by standard means as described in the Configuring 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:

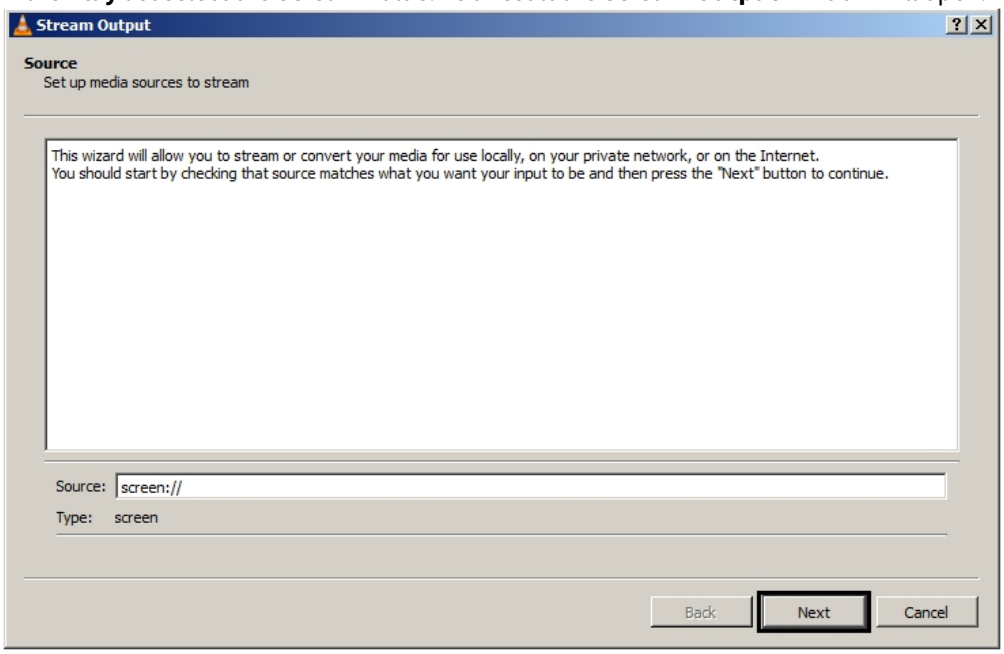
1. Run the VLC Media Player.
2. Select the **Open Network Stream item...** in the **Media** menu.



3. In the opened window go to the **Capture Device** tab.

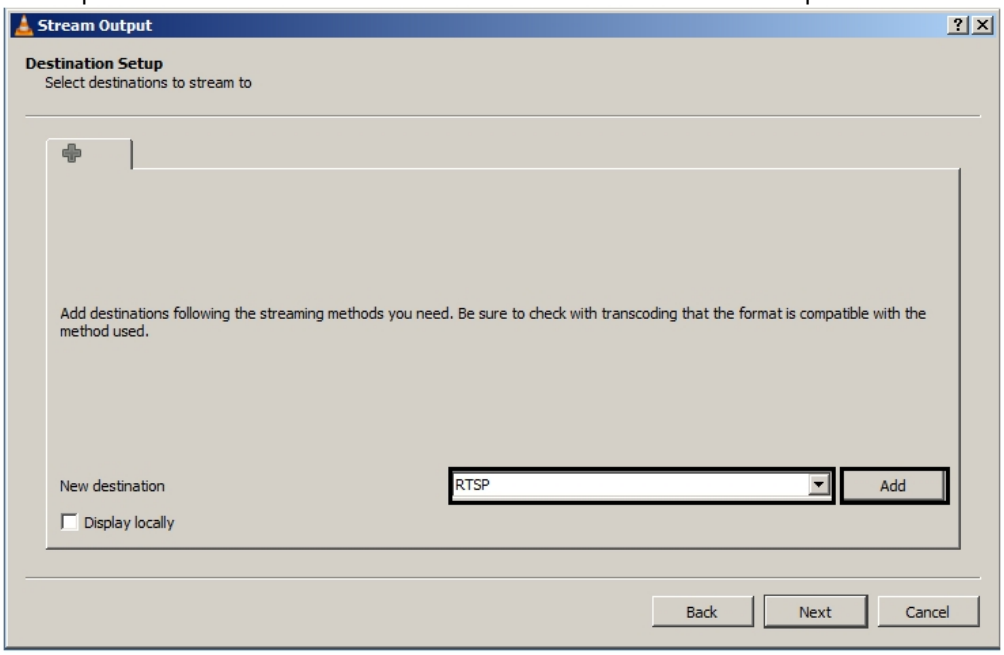


4. In the **Capture mode** drop-down list select the **Desktop** value.
5. Set the desired frame rate for the capture in the corresponding field.
6. In the **Play** list select the **Stream** value. As a result the **Stream Output** window will open.

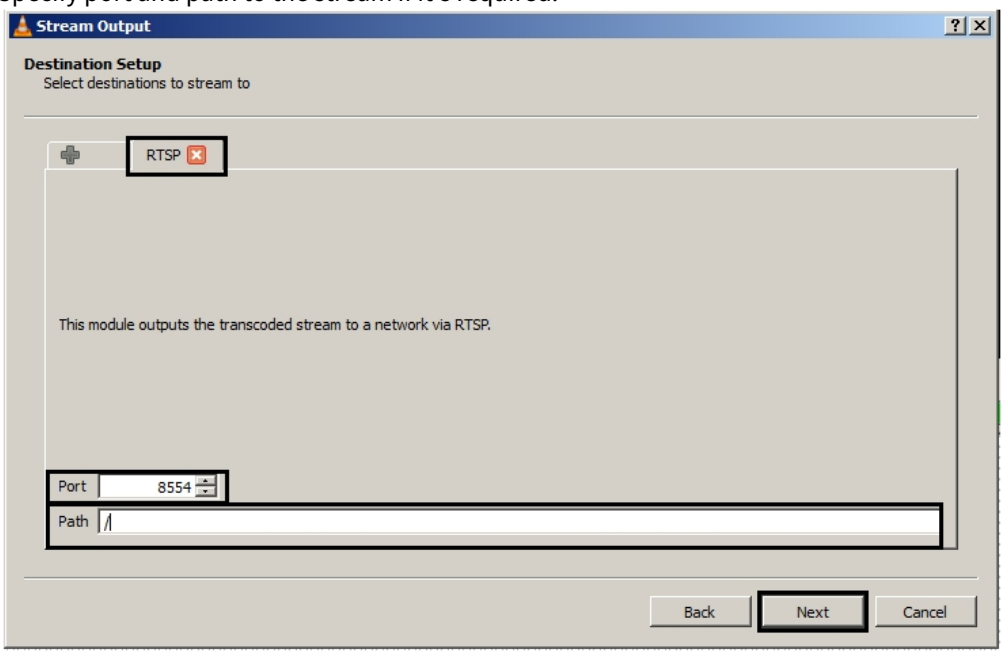


7. Click the **Next** button.

8. In the opened window select the **RTSP** value in the **New destination** drop-down list and click **Add** button.

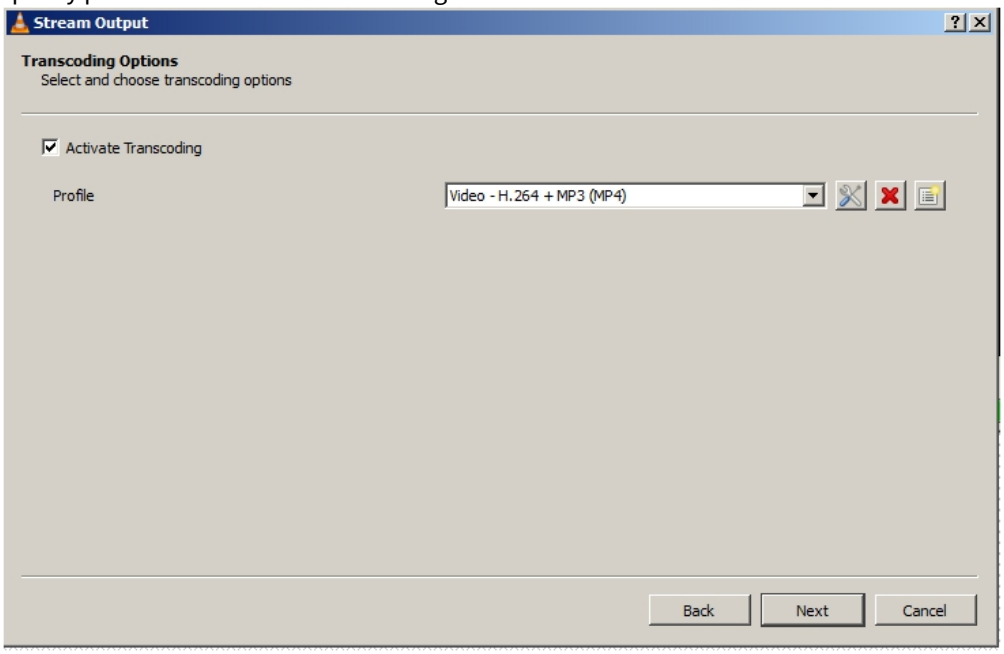


9. Go to the **RTSP** tab.
10. Specify port and path to the stream if it's required.

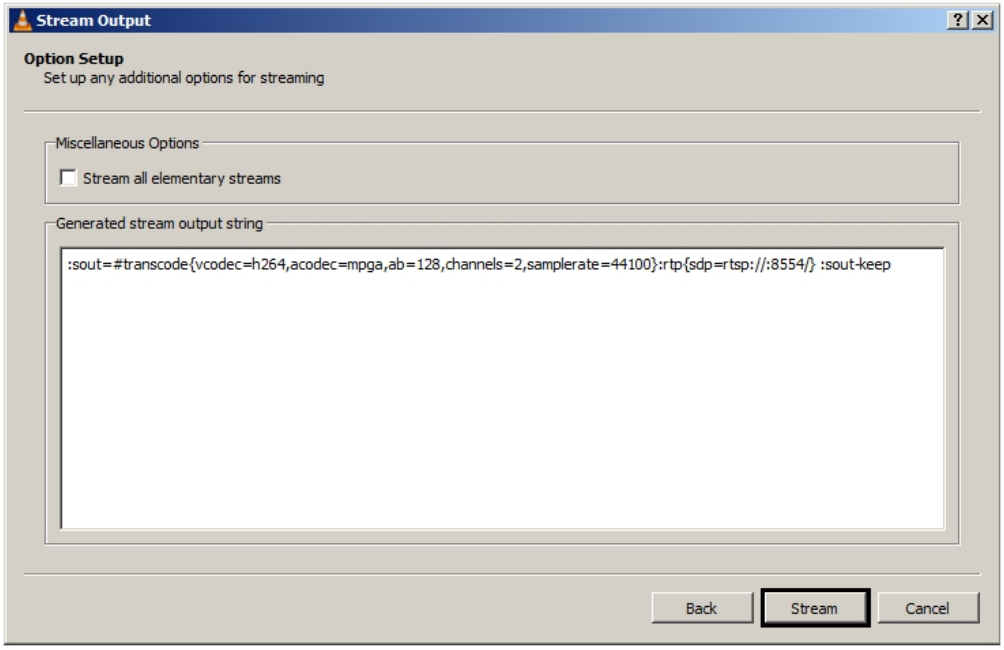


11. Click **Next** button.

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.

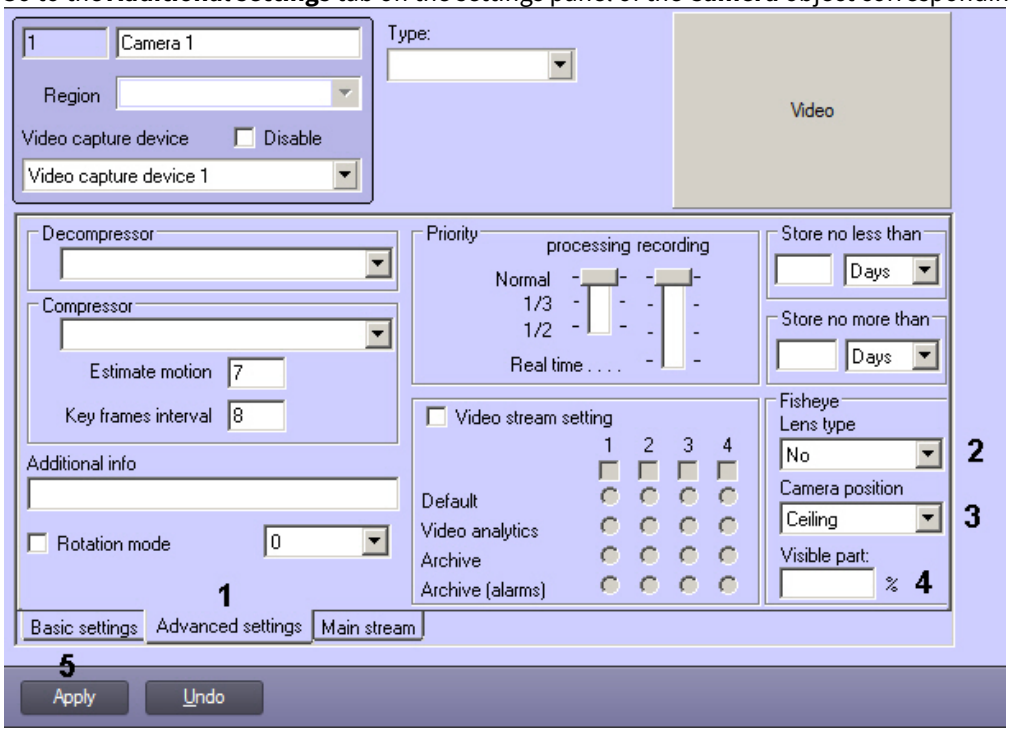
10.3.2.10 Configuring fisheye cameras

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 log),
- 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.

10.3.3 Configuring audio subsystem

10.3.3.1 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

10.3.3.1.1 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.

10.3.3.1.1.1 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.

10.3.3.1.1.2 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.

10.3.3.1.1.3 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.

10.3.3.1.1.4 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

10.3.3.1.2 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

10.3.3.1.3 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

10.3.3.1.4 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.

Both real-time and archive audio signals may be transmitted to Remote Workstations.

10.3.3.1.5 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

10.3.3.2 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).

Eavesdropping on the audio signal through microphones

10.3.3.3 Configuring audio signals digitization and processing

10.3.3.3.1 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.

10.3.3.3.2 Setting up the audio signal volume amplification

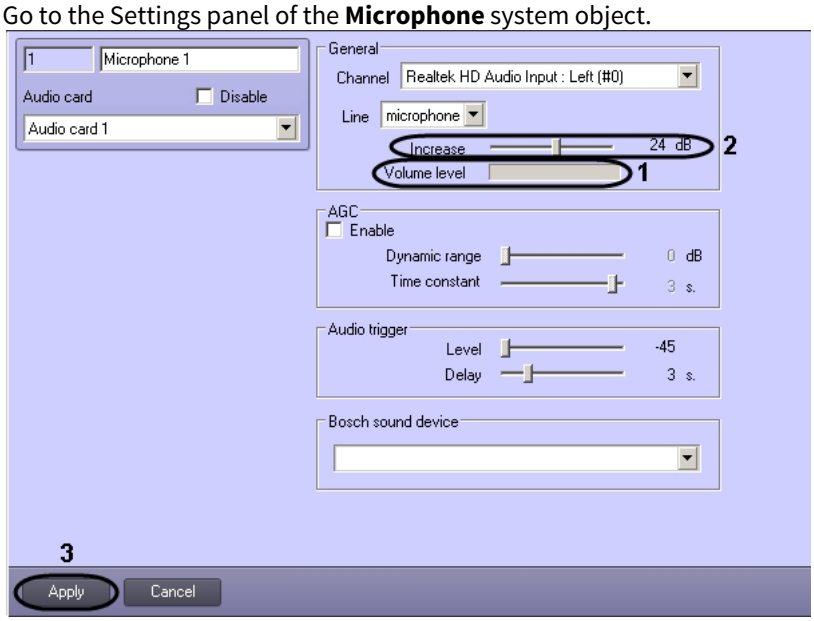
It is possible to amplify incoming audio signals with the help of software.

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.

10.3.3.3.3 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.

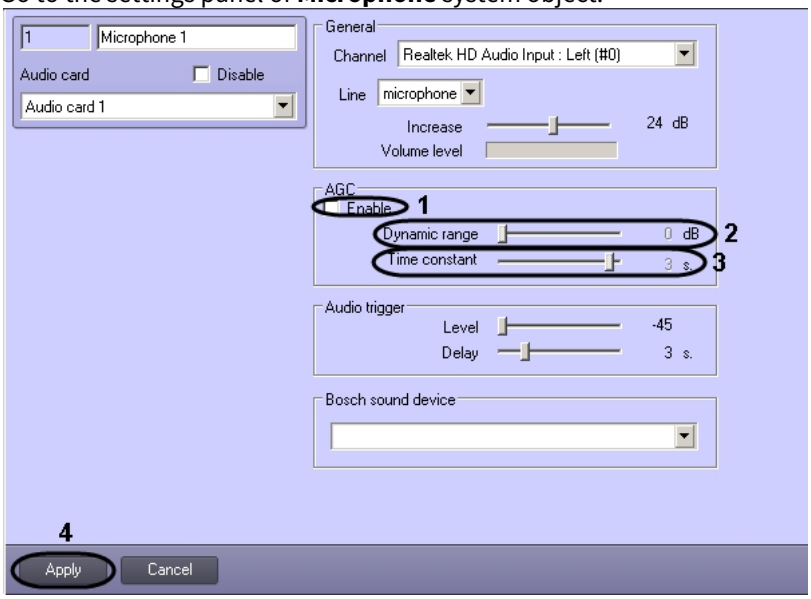
INTELLECT™ software has an AGC adjust option. AGC has two adjustable parameters: a target power level, to which AGC brings different audio signals, and the adjustment time of bringing the signal to the target power level. The second parameter has certain restrictions: the less time it takes to bring 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.

10.3.3.4 Configuring audio signals recording

10.3.3.4.1 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

10.3.3.4.2 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.

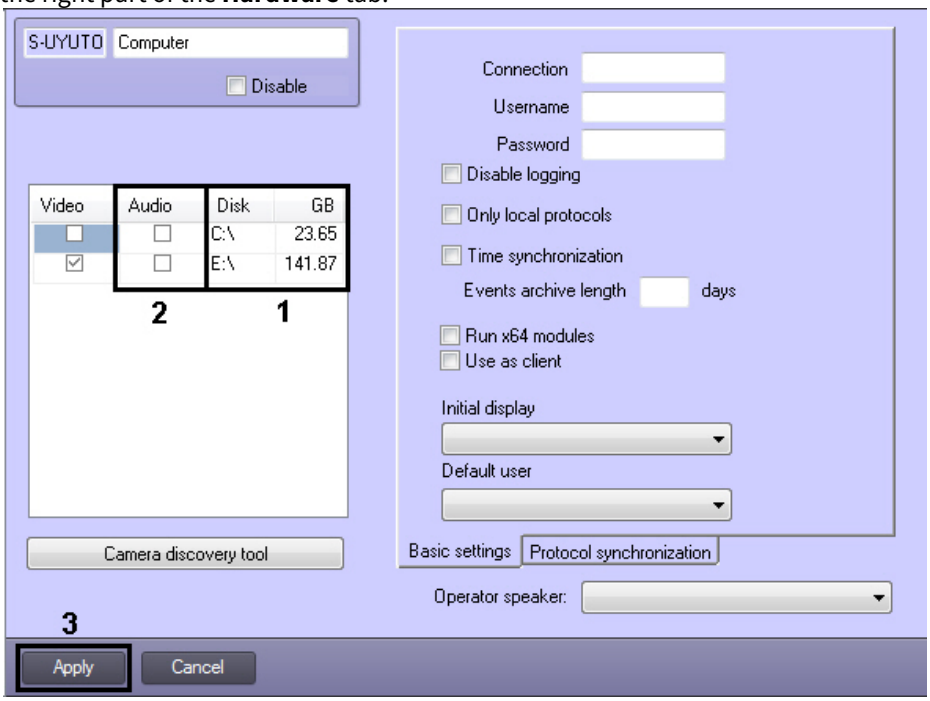
Note.

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.

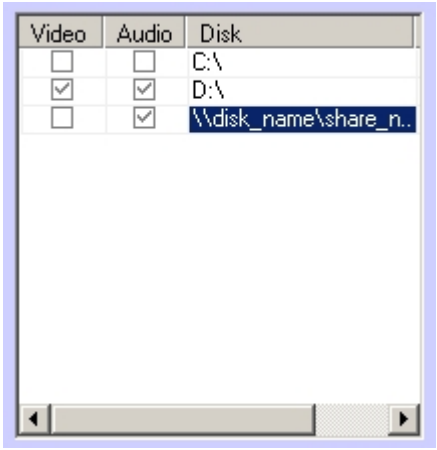
Disk(s) selection is done in one of the following ways:

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.

10.3.3.4.3 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:

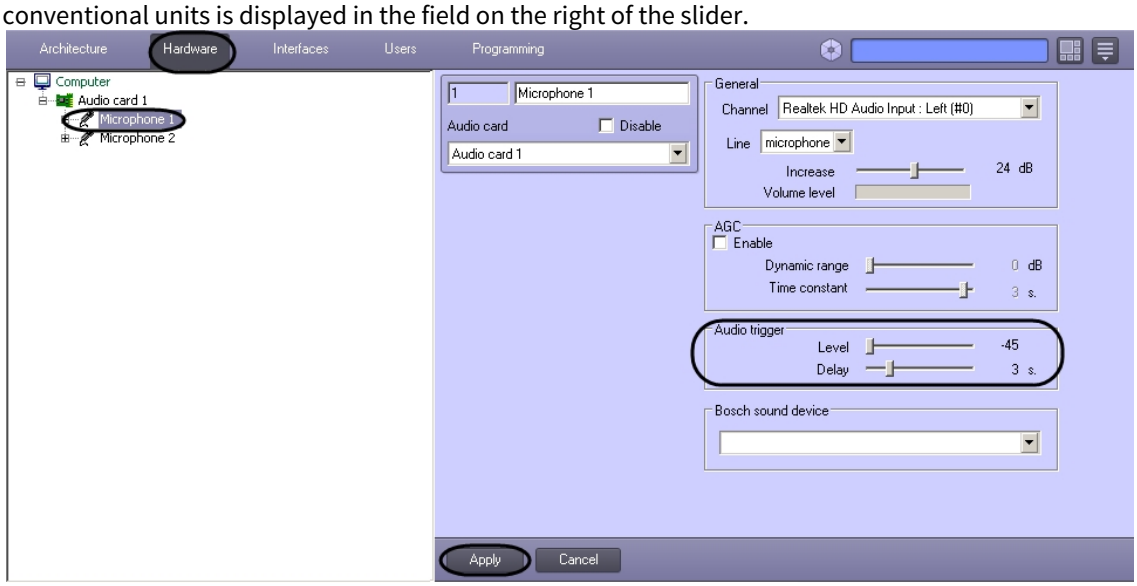
1. **Level** - When audio signal power exceeds a threshold value (Level setting) during a preset interval (Delay), audio signal recording starts automatically(alarm's registration).
2. The **Delay** setting defines the time interval, during which audio signal is prerecorded after the end of alarm.

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

10.3.3.4.4 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.

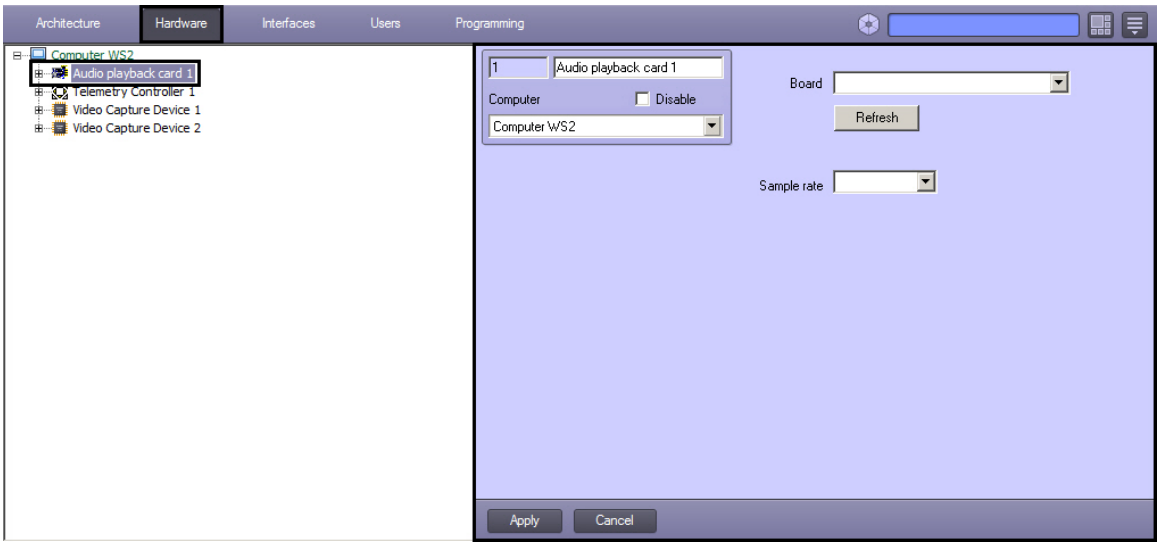
Synchro audio and video recordings

10.3.3.5 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.

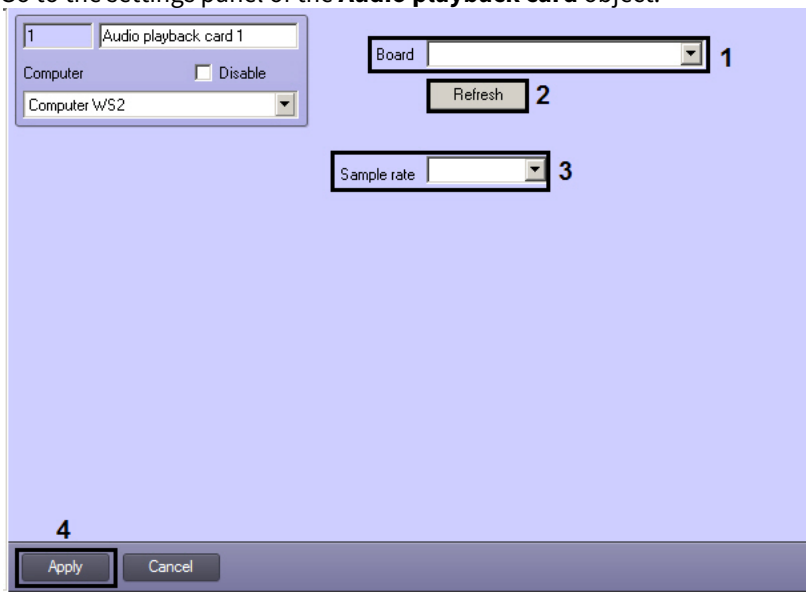
10.3.3.5.1 Creating and configuring the Audio playback card object

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).

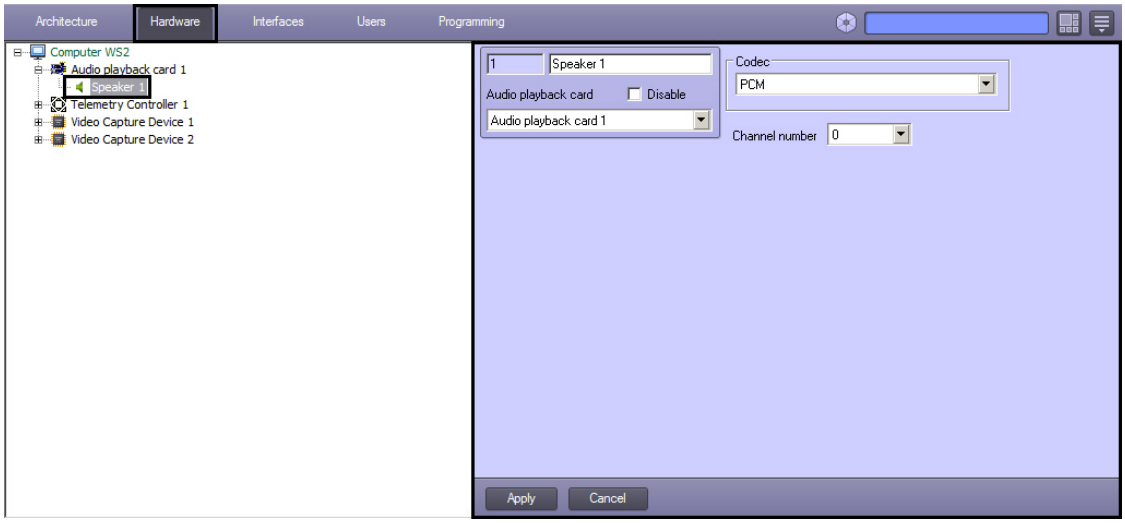
> **Note.**
>
> The **Refresh** button is for returning to previous settings of audio digitization device if new settings were not saved (2).

The **Audio playback card** object is now configured.

10.3.3.5.2 Creating and configuring the Speaker object

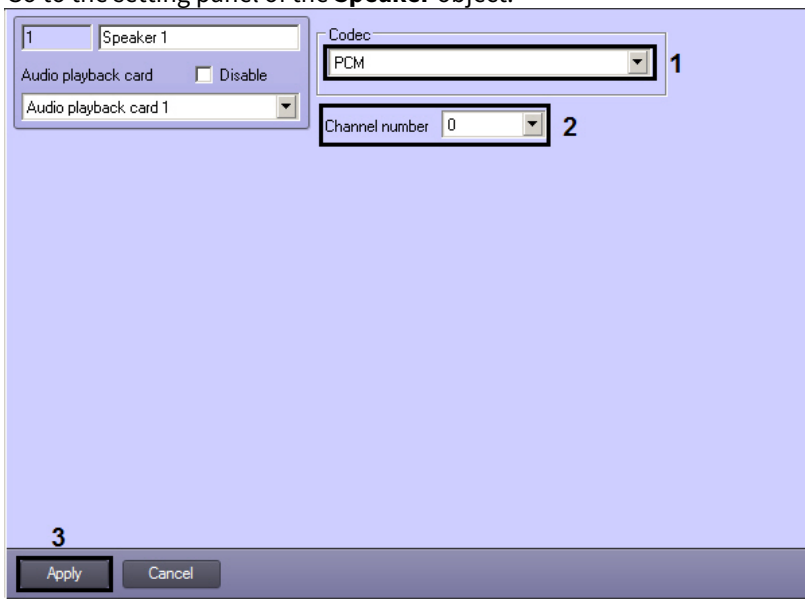
The **Speaker** object is an audio playback device.

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.

10.3.3.6 Features of standard sound card use

10.3.3.6.1 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.

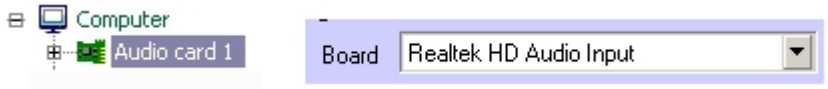
The audio signal sampling rate range depends on the audio card type. The INTELLECT™ software system sampling rate range, available to the installed card, is bounded by the 48 kHz maximum value.

10.3.3.6.2 Features of standard sound card setup

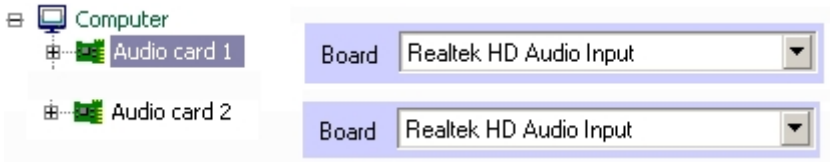
As a rule a standard sound card digitizes no more than 2 audio signals.

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

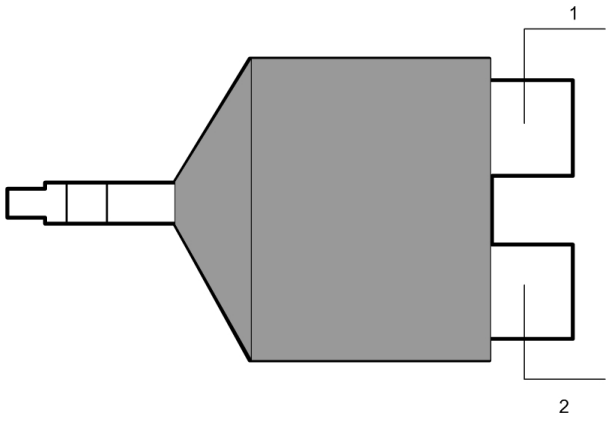
To register the microphones, connected to the standard sound card input audio channels, create **Microphone** objects on the base of the **Audio card** object. Up to 2 **Microphone** objects may be placedn the base of a single **Audio card** object. The relevant hardware tree segment during the registration 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.

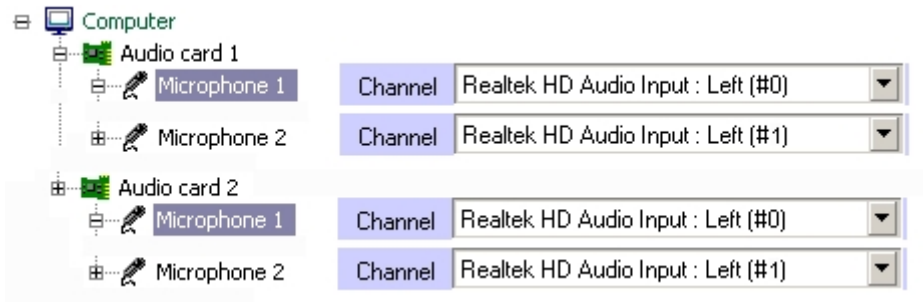
To connect more than one microphone to a standard sound card, the mini jack 2xRCA adapter is used. The mini jack 2xRCA adapter numbering layout is shown in Figure 8.8 31. Examples of **Microphone** object settings with one and two FS-5 video capture cards, registered in the INTELLECT™ system, are shown 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

10.3.3.7 Using multi-channel audio capture devices

10.3.3.7.1 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.

10.3.3.7.2 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.

10.3.3.8 Using IP-devices

10.3.3.8.1 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.

10.3.3.8.2 Setting up the transmission of video signals to IP-devices

INTELLECT™ software has the facility to transmit audio signals from microphones to IP-devices and to play them back with loudspeakers or headphones, connected to IP-devices.

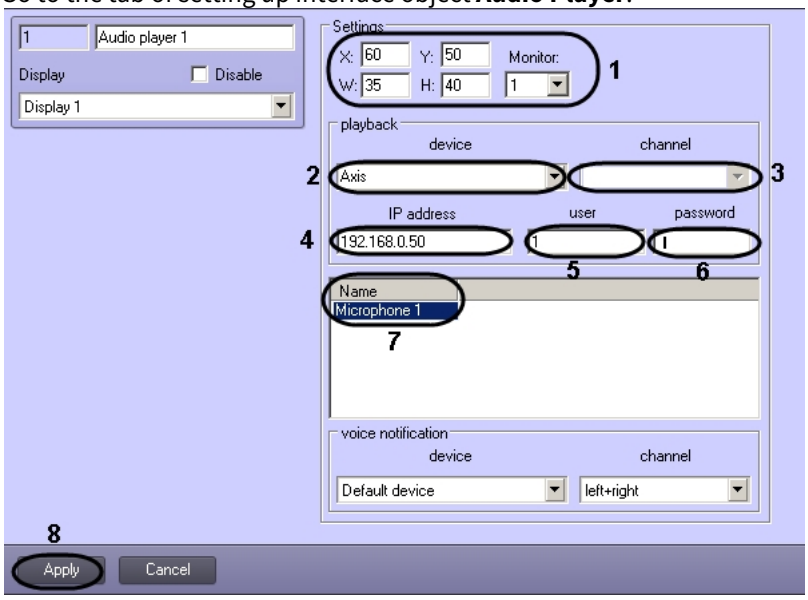
Audio signal transmission to IP-devices can be performed in two ways:

1. with the help of interface object the **Audio player**;
2. with the help of system object the voice notification service.

The object **Audio player** is used to transmit audio signals from the selected microphones on the supported IP-devices.

To set up the transmition of audio signals with the help of the **Audio player** object do the following:

1. Go to the tab of setting up interface object **Audio Player**.



2. Enter the settings of the **Audio player** interface box (1).
3. Select the required IP-device from the dropdown list **Device** (2).

> **Note.**
>
> Select the value **Virtual Cable** to transmit audio signals to IP-device Bosch (see Setting up the transmission of audio signals to IP-device Bosch)

4. From the dropdown list **Channel**, select the required audio signals'playback channel (3).
5. In the field **IP address** enter the IP address of the selected IP-device (4).
6. If necessary enter user name and password in the fields **User** and **Password** to connect to the selected IP-camera (5-6).
7. From the dropdown list in the colomn **Name** select the object's name **Microphone**, from which audio signal has to be transmitted to the selected IP-device (7).
8. Repeat step 7 for each selected microphone object.
9. Click the **Apply** button to save all the changes. (8).

Setup of the audio signal's transmition with the help of **Audio player** object is completed.

> **Note.**
>
> To activate audio signals'transmition from the microphone to the IP-device click the  button (**Interception from microphone**) in the **Audio player** interface box.

Voice notification object is used to transmit files of WAV format to the supported IP-devices. Set up order of the object **Voice notification service**is described in the Setting up the voice notification.

> **Note.**
>
> With joint use of the Audio player and voice notification service, bear in mind, that the sampling rate of audio signals, fed from microphones via the **Audio player** (**Sample rate** setting of **Audio card** object) and that of the audio files, transmitted with the voice notification service, must be the same.

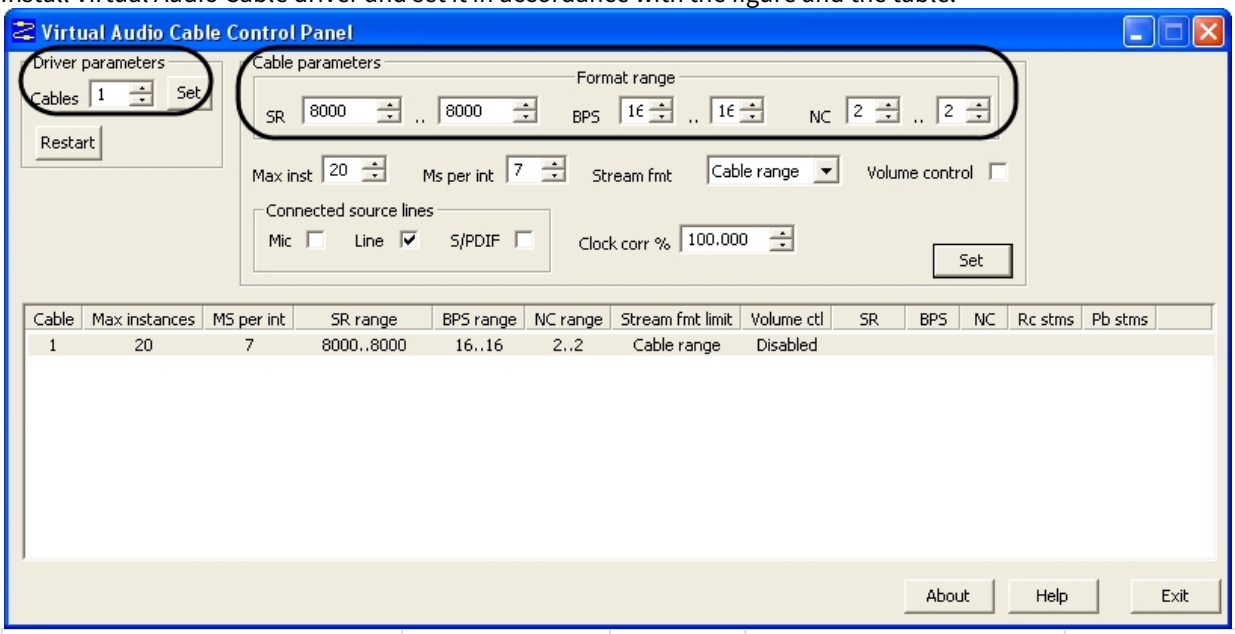
10.3.3.8.3 Setting up the transmission of audio signals to IP-device Bosch

Transmission of audio signals to IP-device Bosch is performed with the use of Virtual Audio Cable driver.

> **Note.**
>
> Information about program Virtual Audio Cable one can find in official reference manual of this program. The program is not a part of the Intellect™ software.

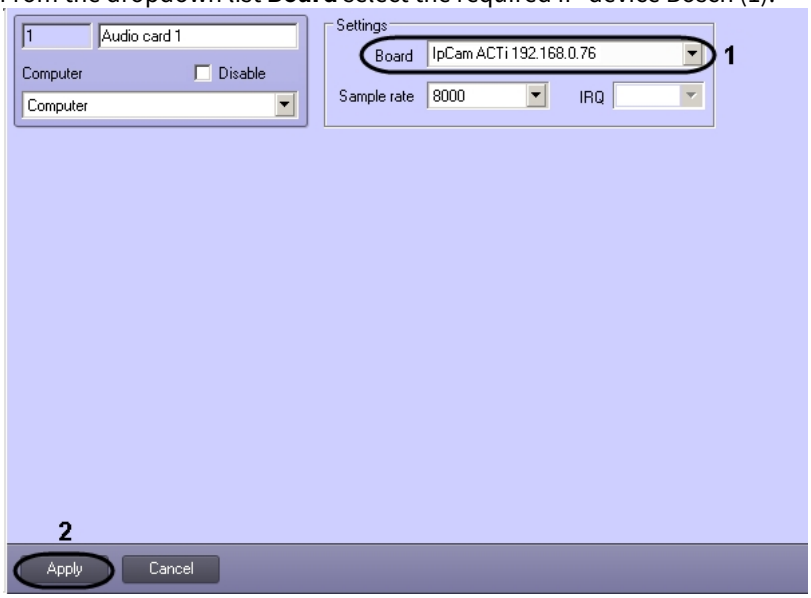
To set up the transmission of audio signals to IP-device Bosch do the following:

1. Install Virtual Audio Cable driver and set it in accordance with the figure and the table.



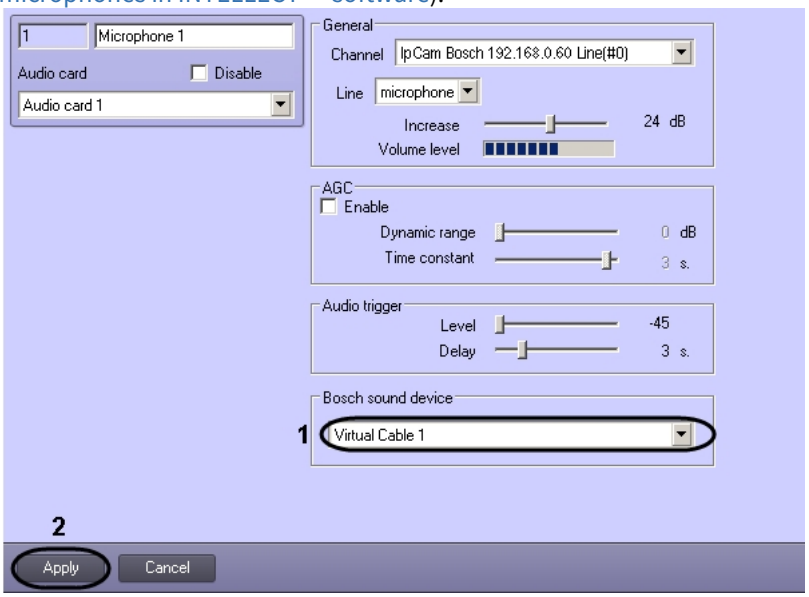
Driver set up utility	Group	Parameter	Description of parameter	Range of parameter's value
Start -> All programs -> Virtual Audio Cable -> Control Panel	Driver parameters	**Cable**	Number of virtual audio cables	1
	Cable parameters -> Format range	**SR**	Sampling rate of audio signals	8000..8000
		BPS	Depth of audio signals sampling	16..16
		NC	Number of channels of virtual audio cable	2..2

2. Start *Intellect* program complex.
3. Go to the settings panel of system object **Audio card** (see Registration of audio cards and microphones in INTELLECT™ software).
4. From the dropdown list **Board** select the required IP-device Bosch (1).

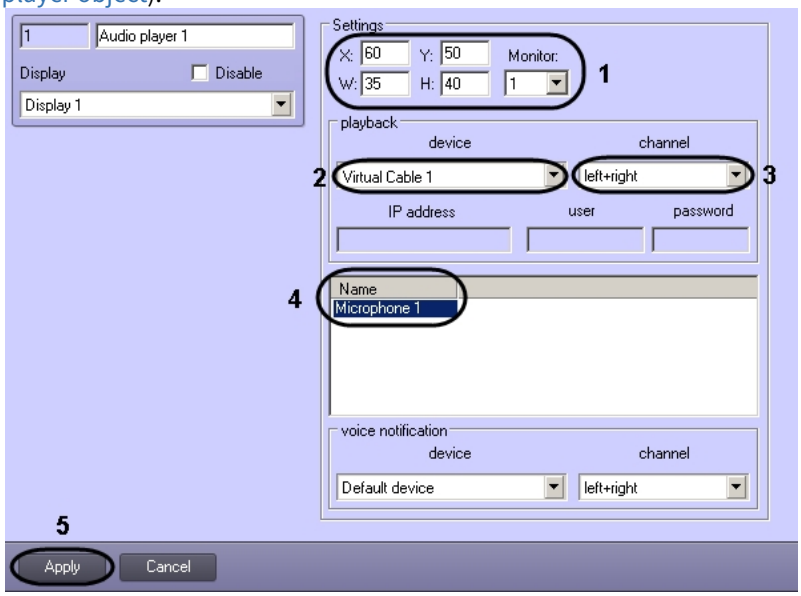


5. To save the changes click **Apply** button (2).

6. Create **Microphone** object on the base of this object and go to its settings panel (see Registration of audio cards and microphones in INTELLECT™ software).



7. From the dropdown list **Bosh sound device** select the value **Virtual Cable** (1).
8. To save the changes click **Apply** button (2).
9. Go to the settings panel of the **Audio player** interface object(see Configuring audio signals playback using the Audio player object).



10. Set the coordinates and size of the **Audio player** interface box (1).
11. From the dropdown list **Device** select the value **Virtual Cable** (2).
12. From the dropdown list **Channel** select the required chanal of audio signals playback (3).
13. From the dropdown list in the column **Name** select the name of **Microphone** object which audio signal has to be transmitted to IP-device Bosch (4).
14. Repeat step for all the required **Microphone** objects.
15. To save the changes click **Apply** button (5).
16. Restart *Intellect* program complex.
17. Setting up the transmission of audio signals to IP-device Bosch is completed.

Note.

To enable the transmission of audio signals from the microphone to IP-device Bosh click the  button (**Interception from microphone**) in the **Audio player** interface box.

10.3.3.8.4 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).

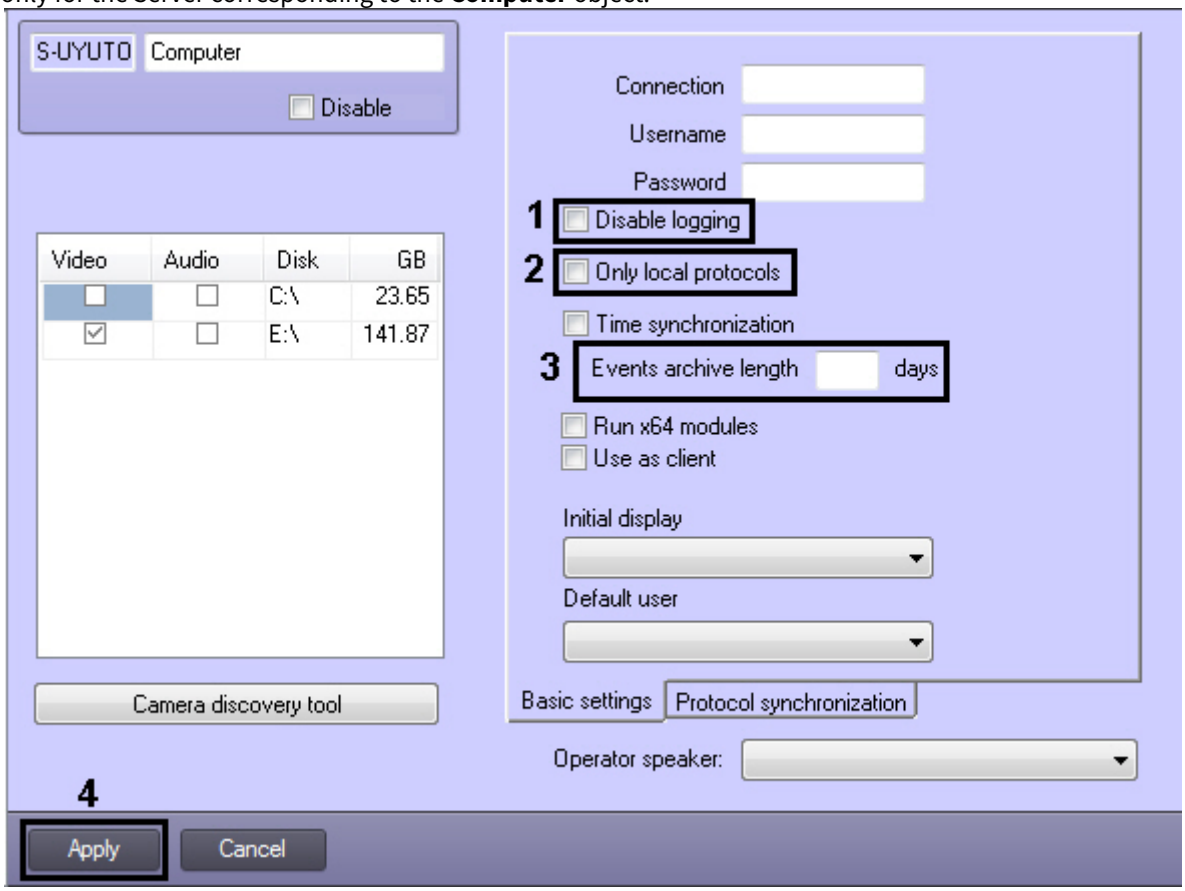
10.3.4 Configuring events logging

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. Set the **Only local protocols** checkbox in case when only events registered on this computer are to be logged to the database (2). This setting is relevant only for the Server corresponding to the **Computer** object.
   If this checkbox is set checked, then the event log database synchronization is to be started manually using the SyncProtocol.exe utility or 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 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 section). The value of the **Events archive length** parameter on the settings panel of the **Computer** object has the higher priority.

   Note

   If no value is specified in the **Events archive length** field on the configuration panel of the **Computer** object, the value specified in the configuration panel of the **Security zone** object is used.

4. Click the **Apply** button to save all the changes (4).

Note

Steps 1 and 3 are for configuring events viewing in the system with distributed configuration.

The Event Viewer database is now configured.

Note

The tweaki.exe utility can also be used to configure events viewing (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 log
Event processing using the Operator protocol

10.3.5 Configuring the Event Viewer databases synchronization

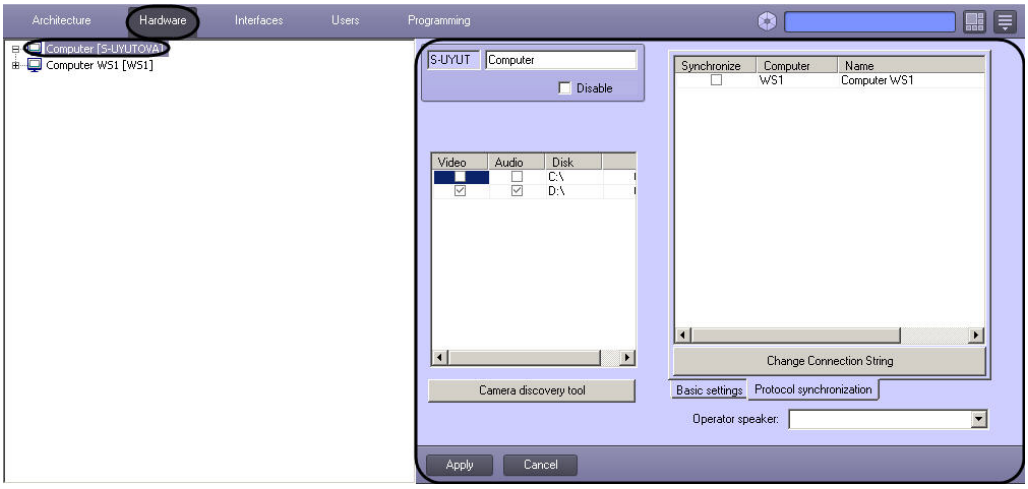
10.3.5.1 General information on the Event Viewer databases synchronization

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.

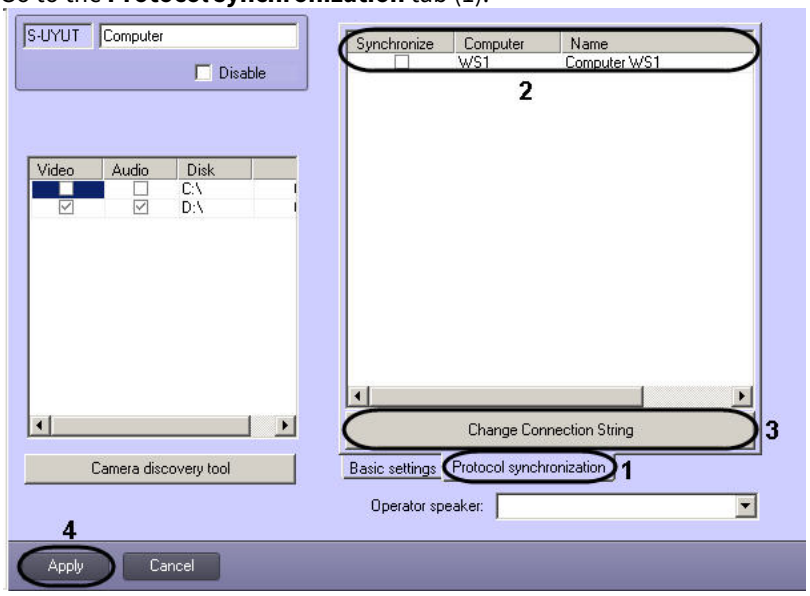
10.3.5.2 Configuring the Event Viewer database synchronization

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).

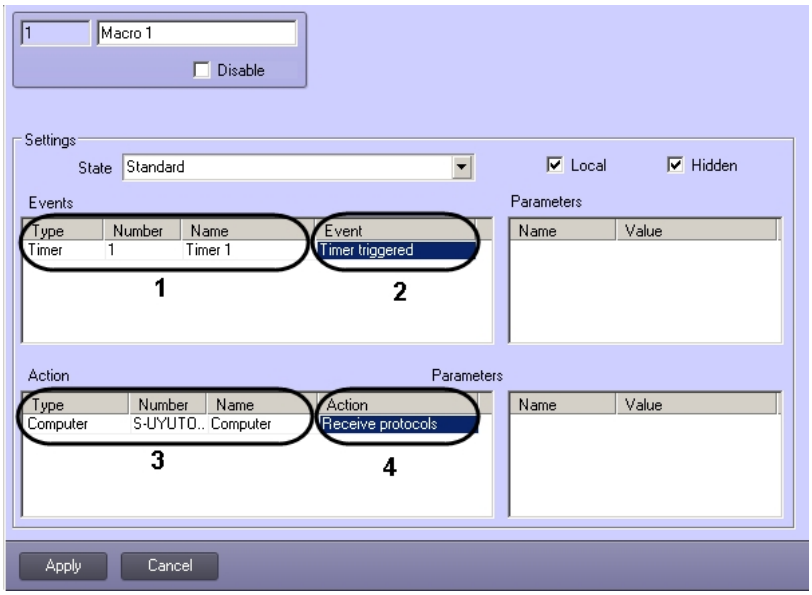
Synchronization of the Event Viewer databases is now configured.

10.3.5.3 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)



10.3.6 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

10.3.7 Configuring operation of distributed architecture in the failover mode

10.3.7.1 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

10.3.7.1.1 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 transfering 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 section). 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 so as the update is performed sequentially once in 3 seconds. Video is displayed as usual after update. If more than 64 cameras is added no 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 JScript language section of Programming Guide (JScript).

The configuration transfer time after losing communication 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 that the key be set to 1.
4. The system objects tree (the more subsystems and modules, 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 verca):

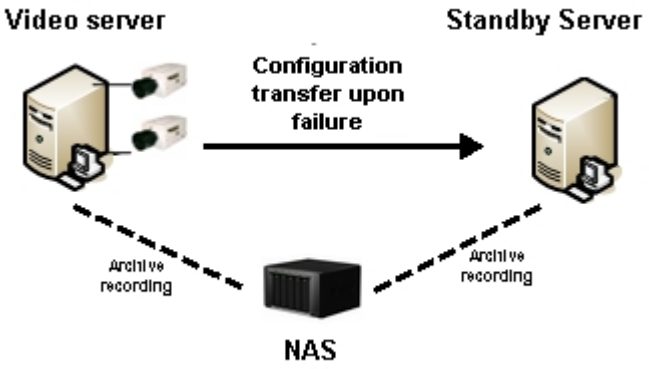
1. 100 cameras are transferred in less than 20 seconds;
2. 200 cameras are transferred in less than 30 seconds.

The archive size tested was more than 5TB and the Servers hardware as follows:
Main Server: Intel Core i5-8500, 16 GB RAM.
Standby Server: Intel Core i5-8400, 16 GB RAM.

10.3.7.1.2 Examples of Failover system organization

10.3.7.1.2.1 1 main Server + standby Server

If the main Server + standby Server flowchart is in use, it is possible to configure both main and standby Servers for recording on the same network resource or several resources (see Using network disks section). In this case the archive is always available no matter what Server operates with cameras.

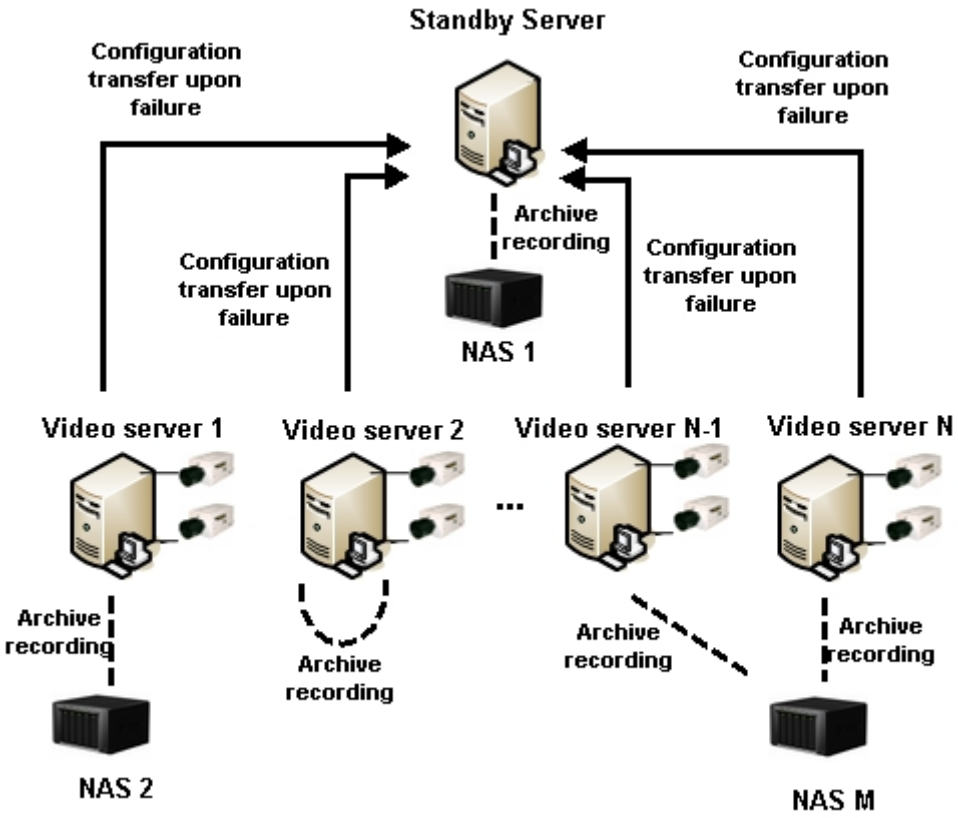


10.3.7.1.2.2 N main Servers + standby server

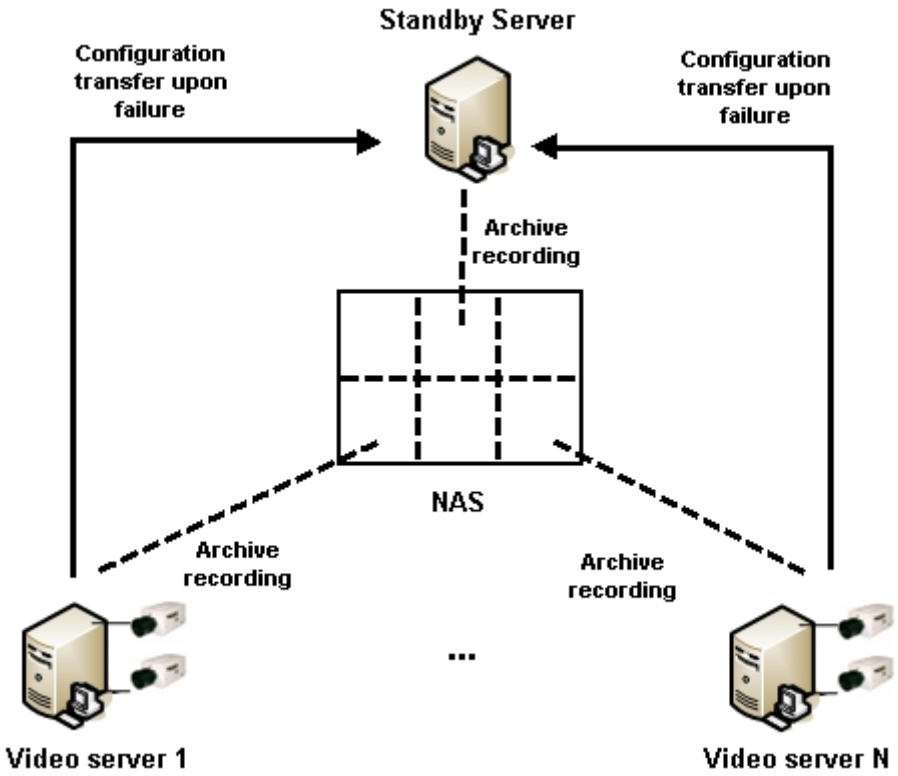
If the N main Servers + standby server flowchart is in use, it is impossible to create a unified archive. In this case main Servers perform recording on different logical drives (sections, partitions), local or network. If these drives for archive recording are specified on a standby Server, then archives from different main Servers will mix.

The AxxonPlayer.exe utility can be used to access the archive created by a standby Server on NAS or local drive (see The Axxon Player utility for viewing and converting the video archive). Alternatively, main and backup server archives can be synchronized through the *Backup archive* module (see Configuring archive synchronization of main and backup Servers).

The N main Servers + standby server flowchart:



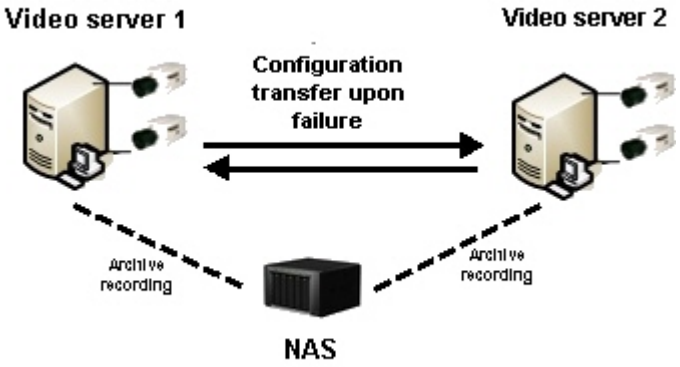
The N main Servers + standby server flowchart when archive is recorded to one NAS:



If configuration from several main Servers is transferred to one standby Server, then provide enough processor resources, RAM and LAN on a standby Server in case when all main Servers become disabled.

10.3.7.1.2.3 Two Servers being standby for each other

Any Server can act both as a primary 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 write the archive to the network storage, access to the archive is available when the configuration is transferred. If the Servers write 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 a standby Server on NAS or local drive.

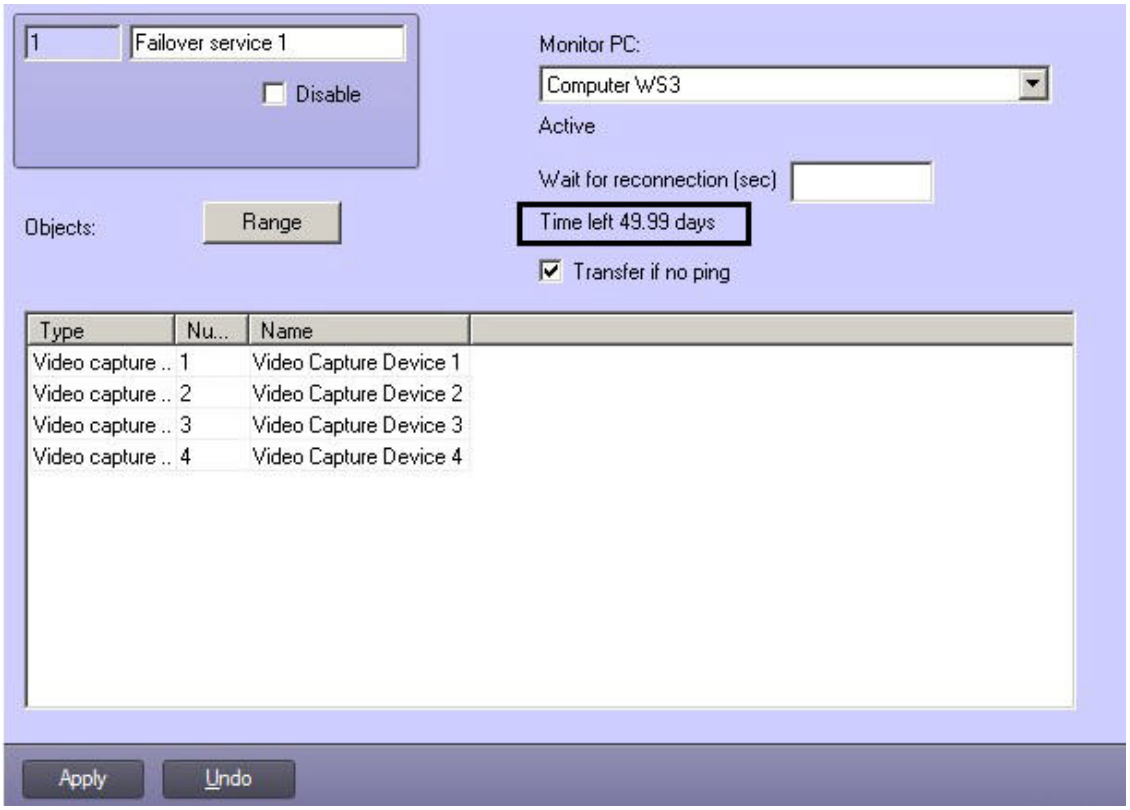


10.3.7.1.3 Limitations of the Failover mode

The Failover mode is configured using the **Failover service** objects created under the **Computer** objects corresponding to backup servers in the **Hardware** tab of the **System settings** dialog box.

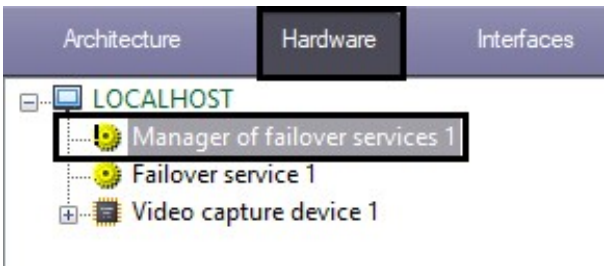


If the quantity of cameras is bound to specific Servers in the license key, then the license becomes invalid when cameras are moved to the backup Server. In this case the system gives 50 days to restore the faulty Server in order to move the cameras back and the license to become valid again. Otherwise, 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 section). Time (in days) remaining for restoring the main Server is shown on the settings panel of the **Failover service** object:



When you log off INTELLECT™, configuration is not transferred from main Server to a standby server.

The number of failovers running on a backup Server simultaneously can be limited. For this the **Manager of Failover services** object is used. It is created under the **Computer** object (that is not a Client) (see Role-assignment in distributed system section).

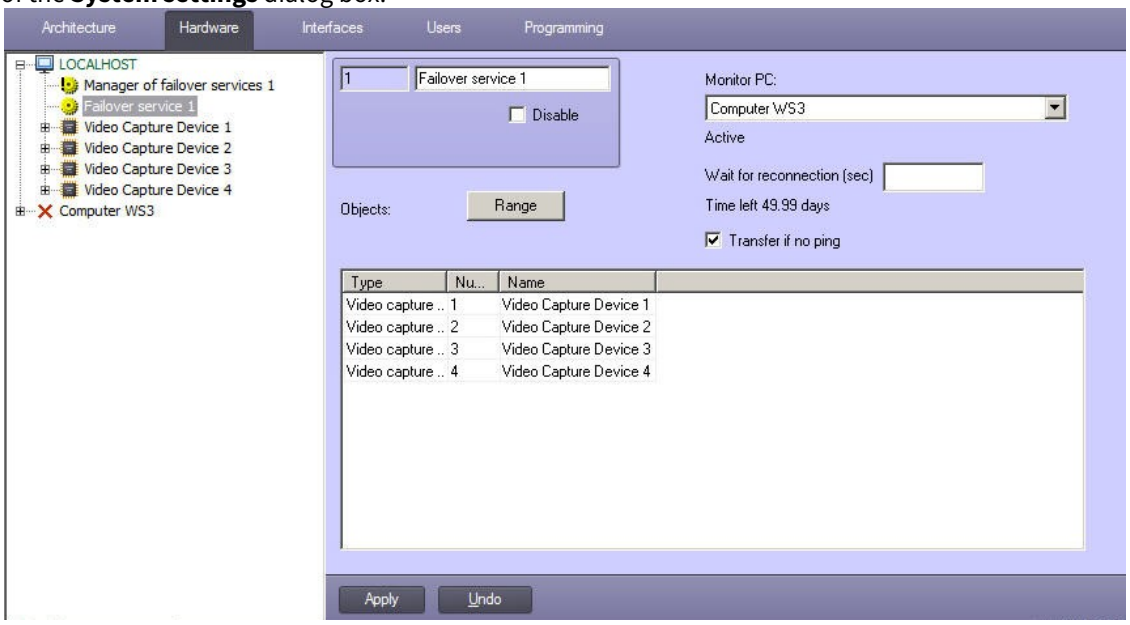


If the number of dead servers exceeds the limit specified for the backup Server, configuration from new dead servers will be transferred to the corresponding backup Server as previously dead servers restore.

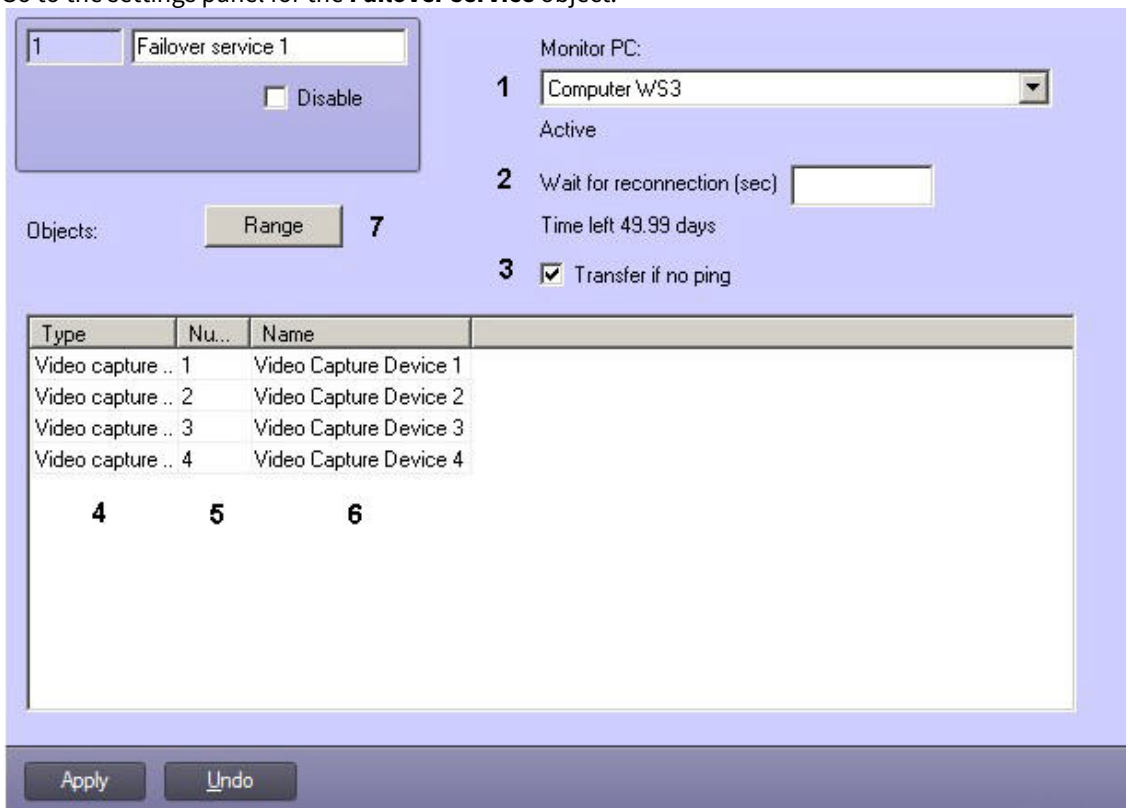
10.3.7.2 Configuring Failover mode

To configure the failover mode, 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** dropdown 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** dropdown list, select the object type (4).

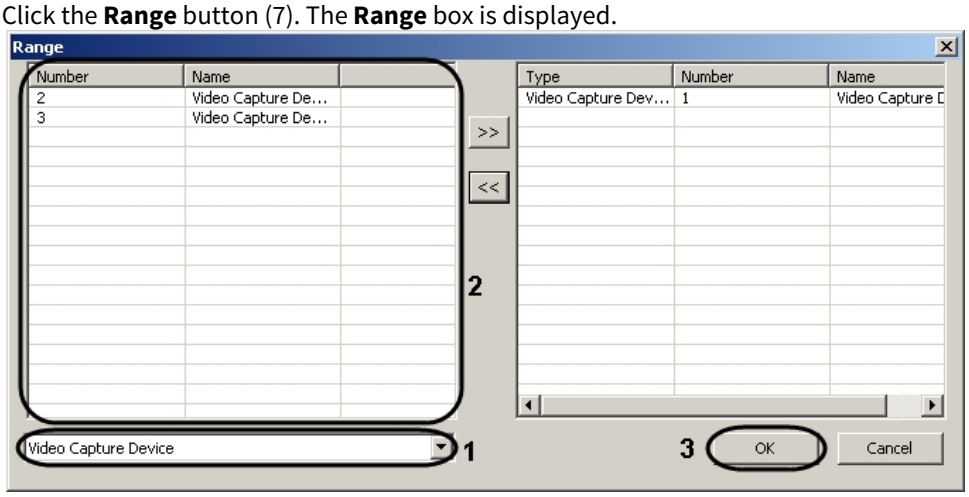
> **Note.**
>
> The **Manager of failover services** type is not available. Such objects are not transferred to the backup Servers as each backup Server has to have its own **Manager of failover services**.

   ii. In the **Number** dropdown 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 dropdown 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.

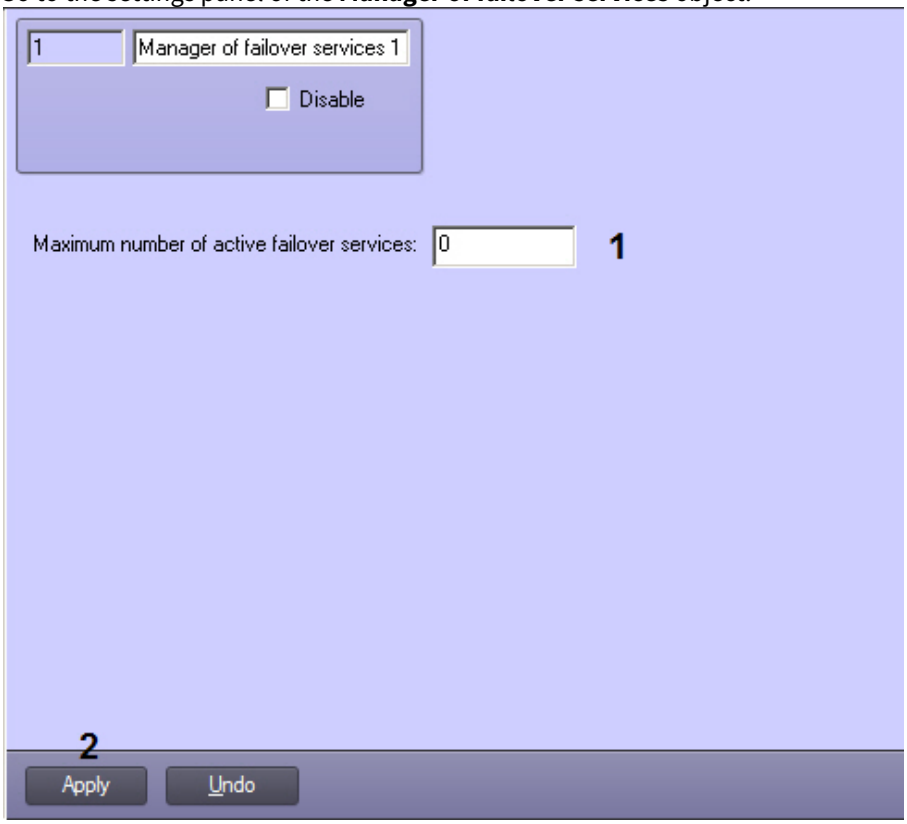
The failover mode is now configured.

10.3.7.3 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).

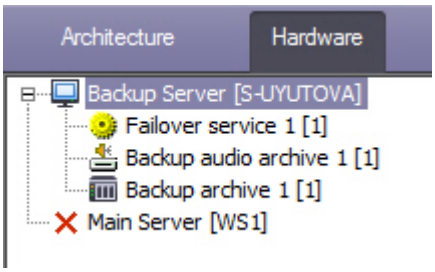
Limit to the number of failovers running simultaneously is now set.

10.3.7.4 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.

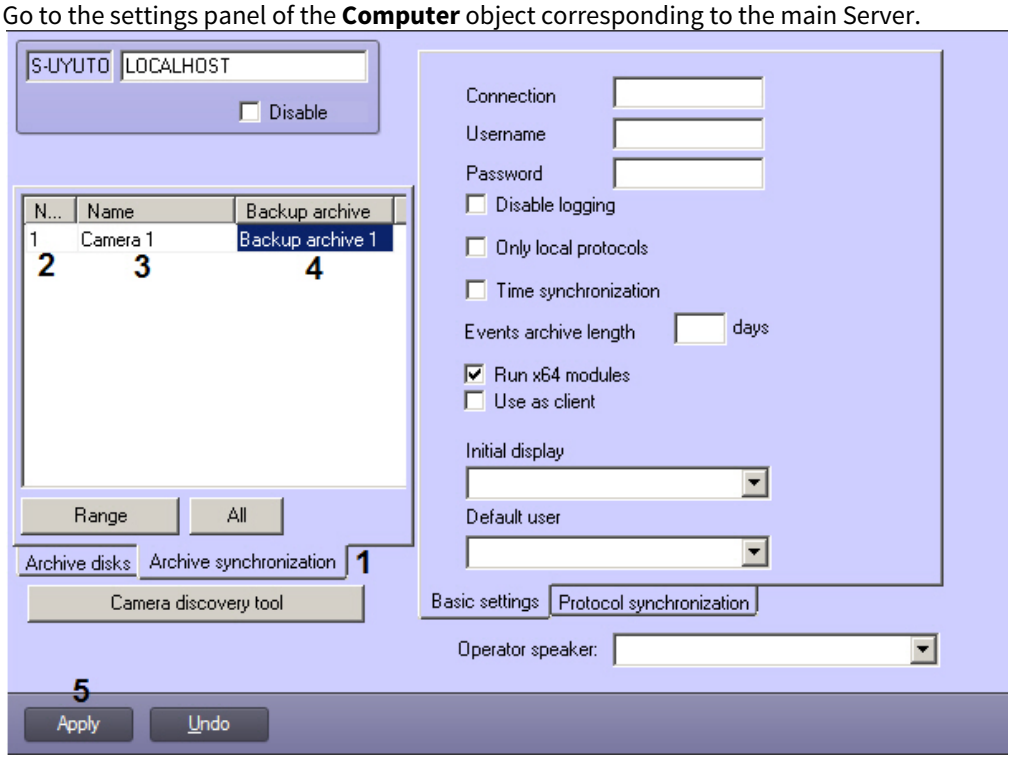
> **Important!**
>
> Only video records without sound are moved from backup Server to main Server at synchronization. If synchronous recording of video and audio is configured, sound will be eliminated at transmission files from backup Server to main Server, and only video files will get to the main 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.

10.3.8 Configuring the SNMP-service

10.3.8.1 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:

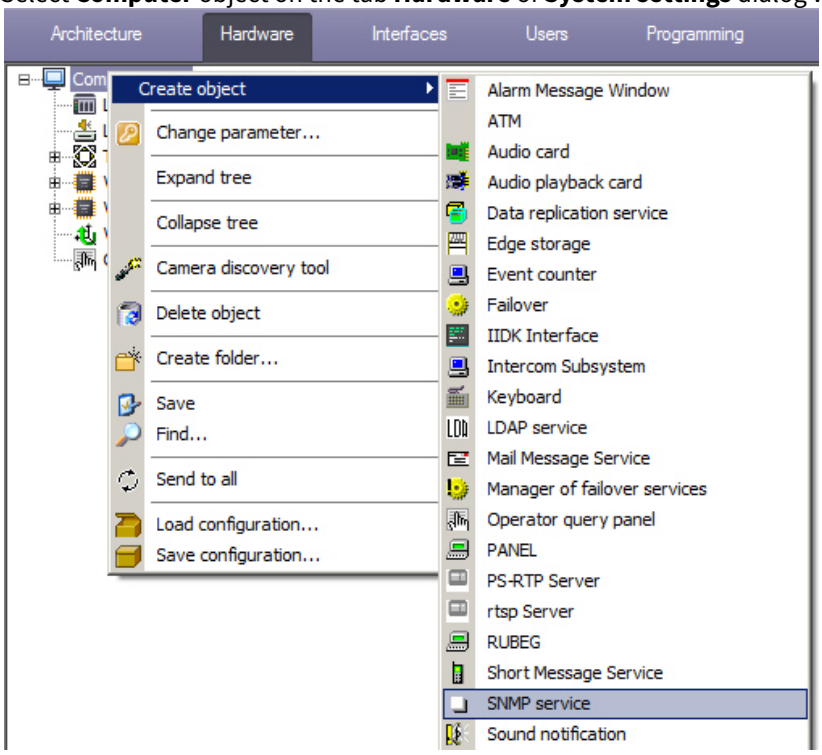
1. Create **SNMP trap** object on the basis of **SNMP service** system objects (see Creating the SNMP trap object).
2. Select the events, which messages should be transferred to SNMP-manager (see Events selection for transmitting to SNMP manager).
3. Set the message conversion to SNMP format (see Configuring 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.

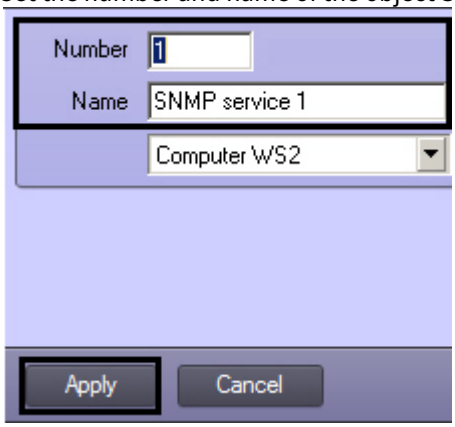
10.3.8.2 Creating the SNMP trap object

Creating the **SNMP trap** object is done in the following way:

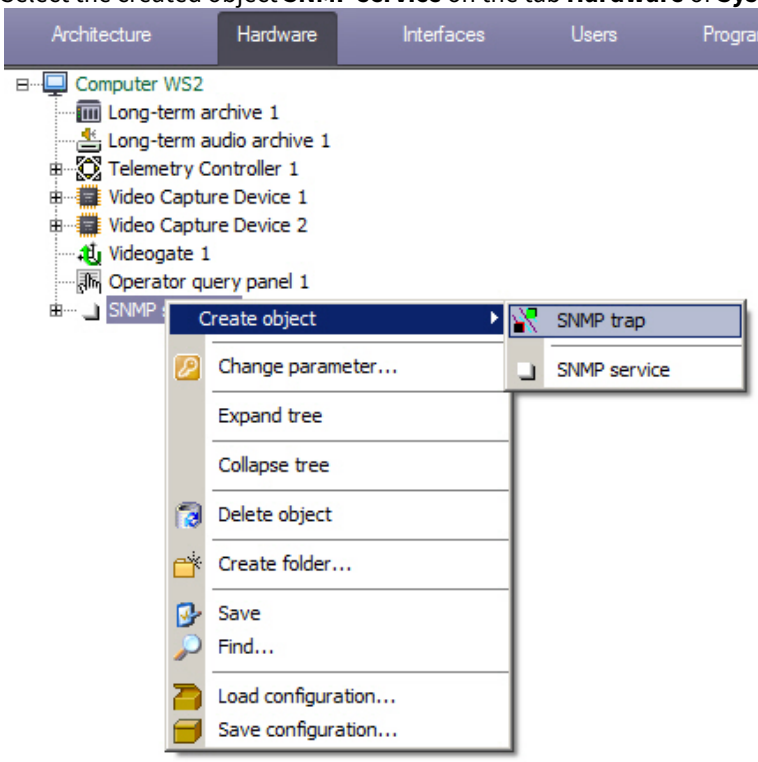
1. Select **Computer** object on the tab **Hardware** of **System settings** dialog window.



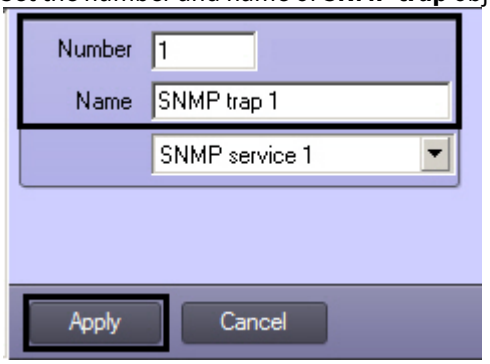
2. Make a right mouse click upon the selected **Computer** object and select **Create object -> SNMP service** in the contextual window.
3. Set the number and name of the object **SNMP service** and then click **Apply**.



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.



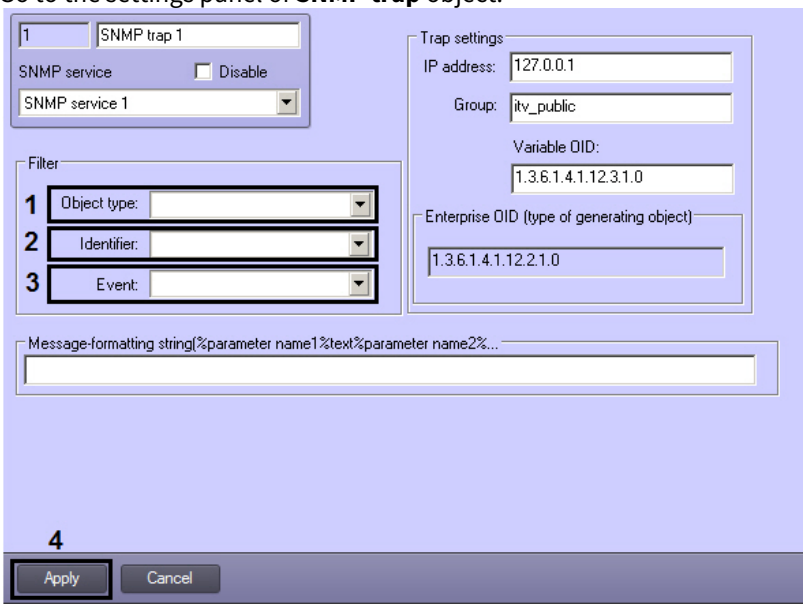
> **Note.**
>
> Settings panel of **SNMP trap** object will appear in result.

Creating the **SNMP trap** object is over.

10.3.8.3 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.



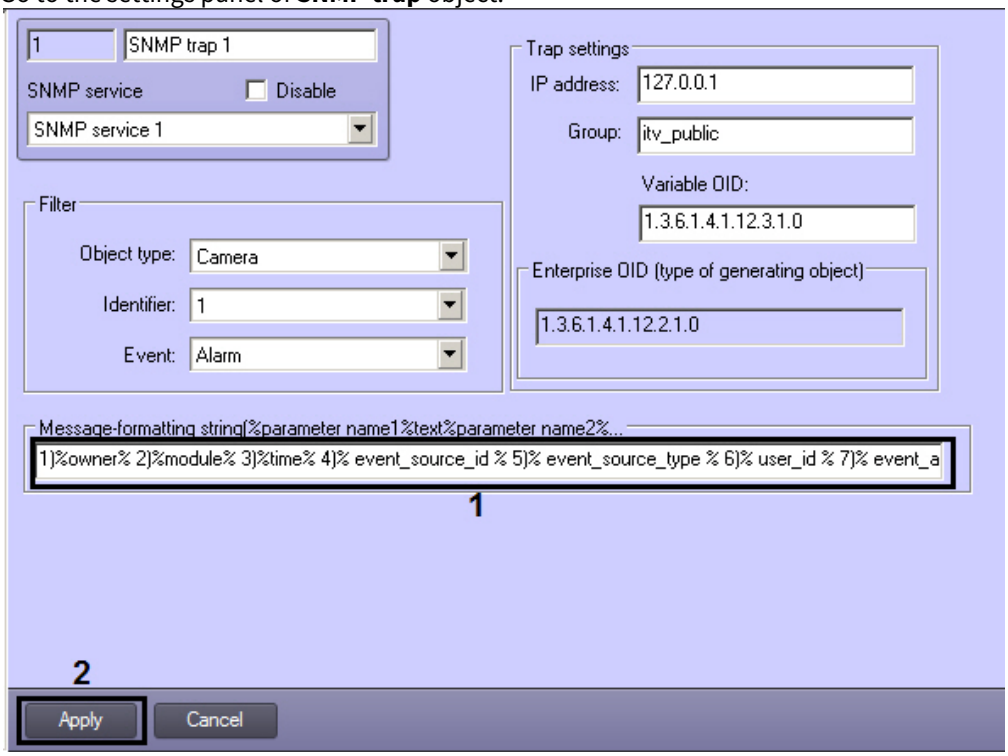
2. From the dropdown list **Object's type** of **filter** group select the object's type for which the required event may be registered (1). If no object's type is selected, all the events concerning all the system objects will be transferred to SNMP-manager.
3. From the dropdown list **Identifier** 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.

10.3.8.4 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	

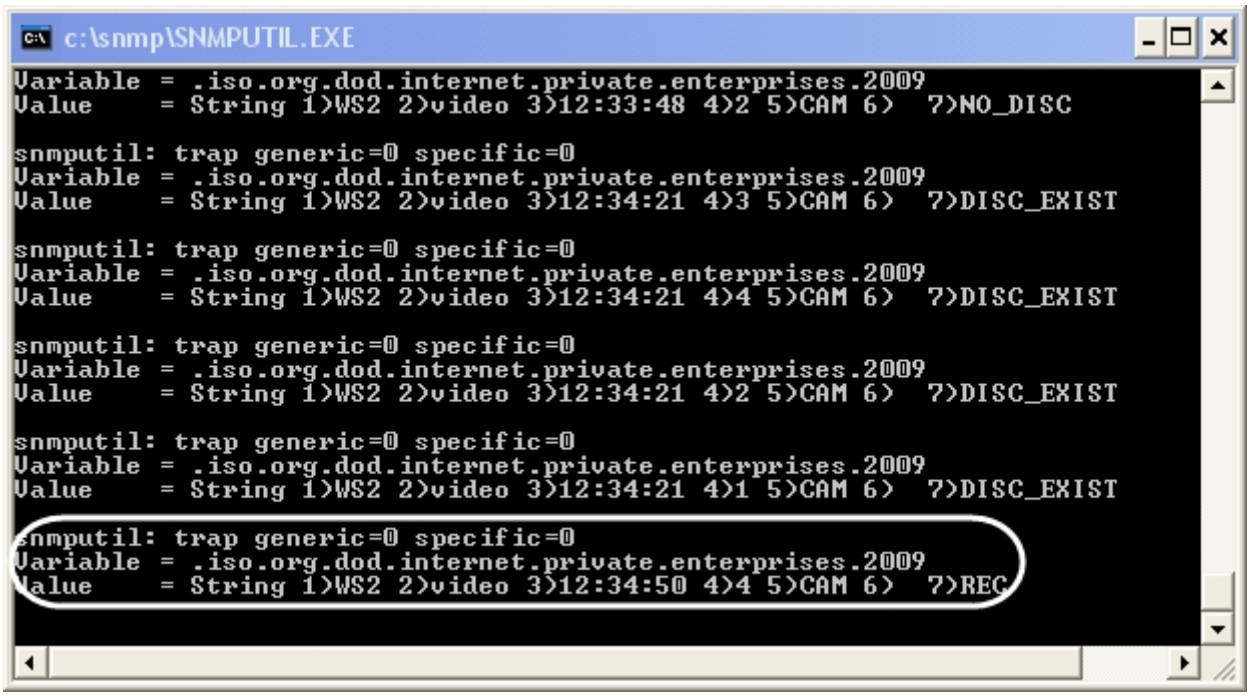
Note.

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.

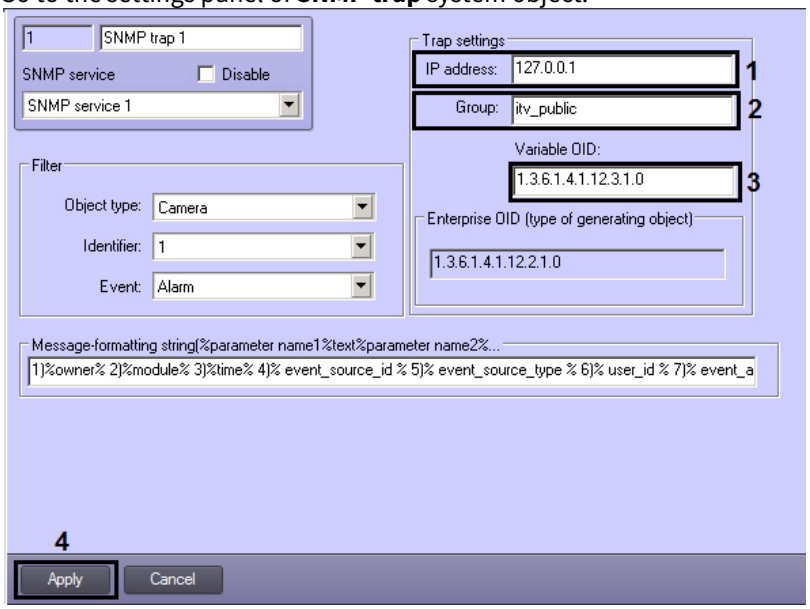
Example of SNMP-message, formed in accordance with the pattern 1)%owner% 2)%module% 3)%time% 4)% event_source_id % 5)% event_source_type % 6)% user_id % 7)% event_action % is exemplified in the figure below.



10.3.8.5 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.

10.3.8.6 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.

10.3.9 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.

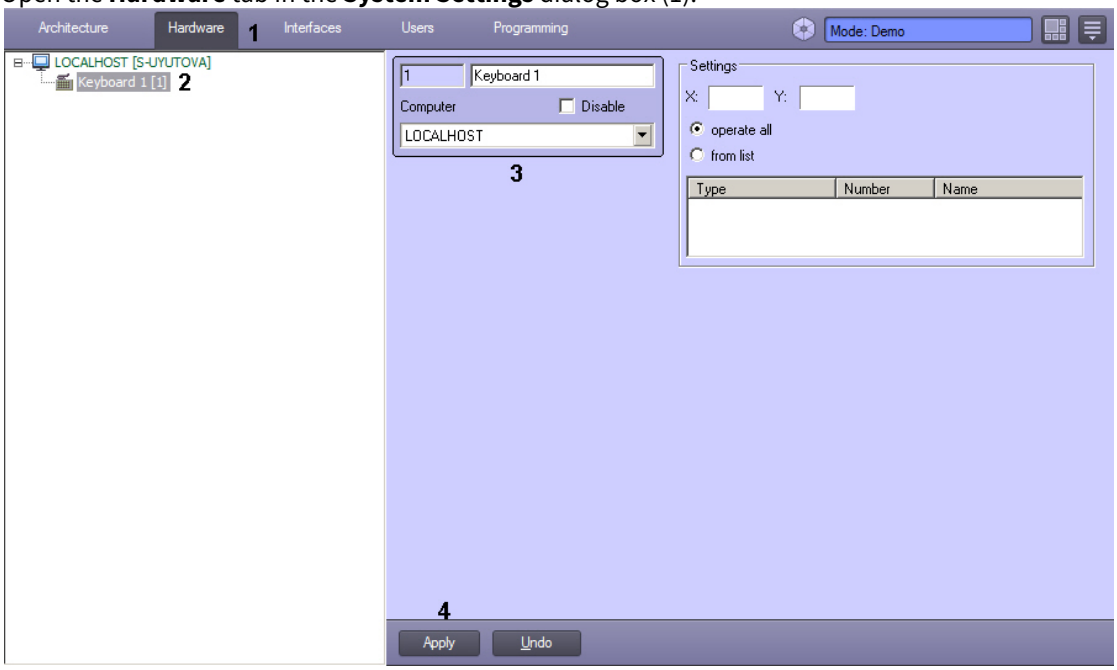
> **Note.**
>
> The process of connecting and setting up the PROMAG KB-950A model is the same as for PROMAG KB-840. PROMAG KB-950A setup is described in the documentation for INTELLECT™ version 4.7.4, PROMAG KB-840 – version 4.9.8 (see AxxonSoft documentation repository).

> Use of the specialized keyboard

10.3.9.1 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.

10.3.9.2 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 Programming Guide (JScript)).

10.3.10 Configuring the System restart service

10.3.10.1 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.

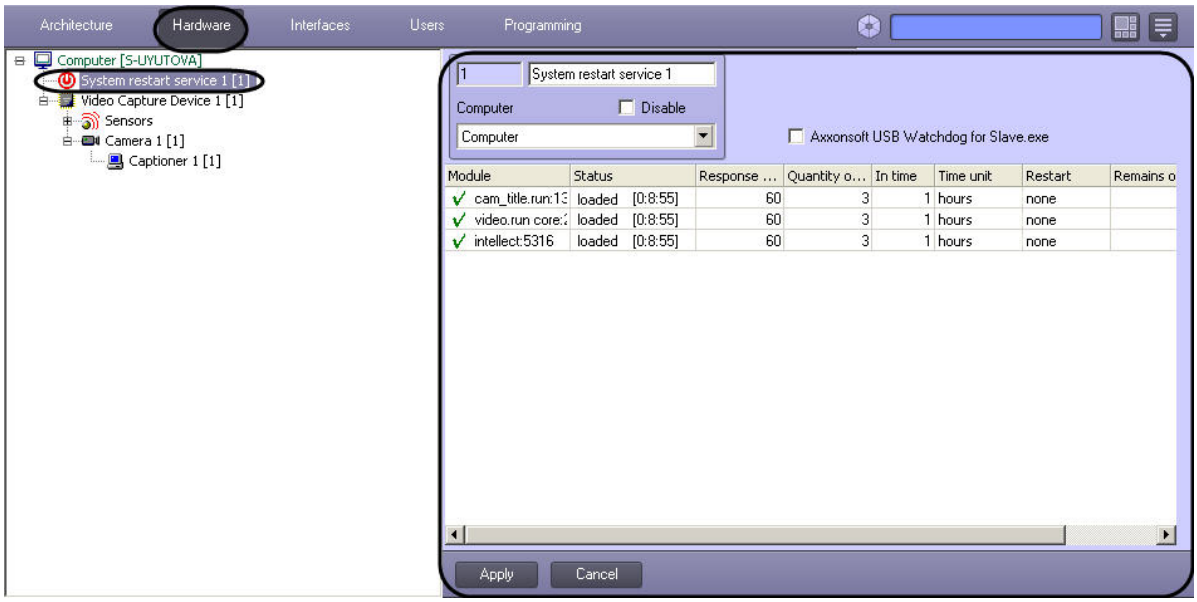
> **Important!**
>
> Only those *Intellect* modules the processes of which are created under Slave.exe process (run under Intellect.exe process) are displayed in the system restart service.

> **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.

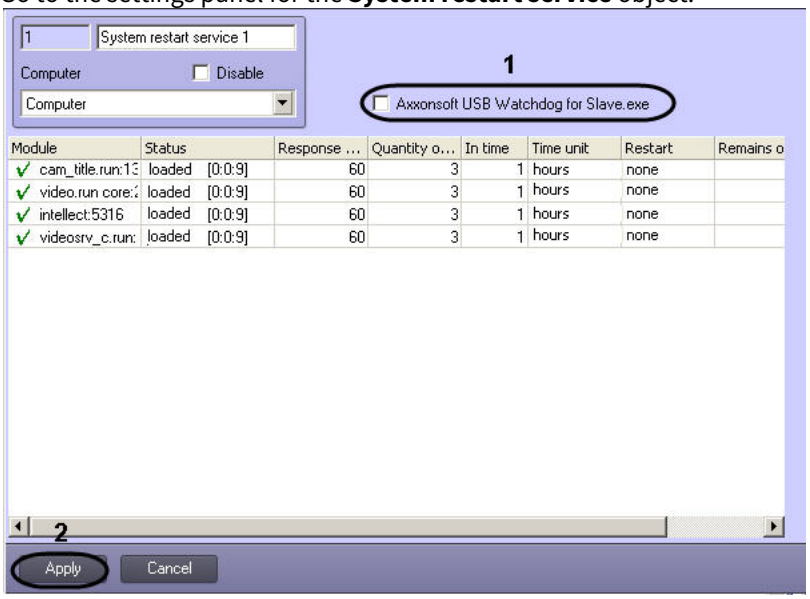


10.3.10.2 Activating the hardware control of workability

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).

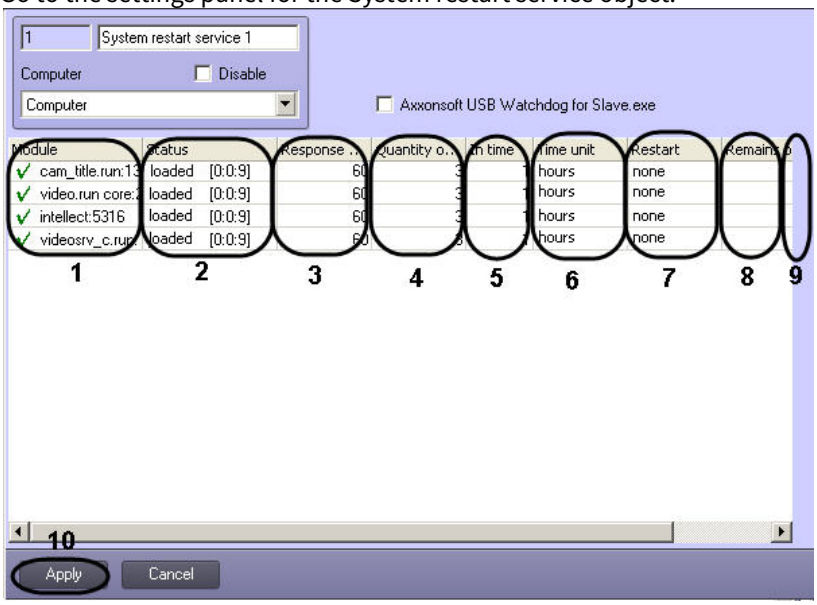
Hardware control of workability is now activated.

10.3.10.3 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.

10.3.10.4 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.

10.3.11 Configuring backup archiving

10.3.11.1 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 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

10.3.11.2 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 Workplace (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.

10.3.11.2.1 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 scaling when it is copied to the *Backup archive* (see Configuring the scaling 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.

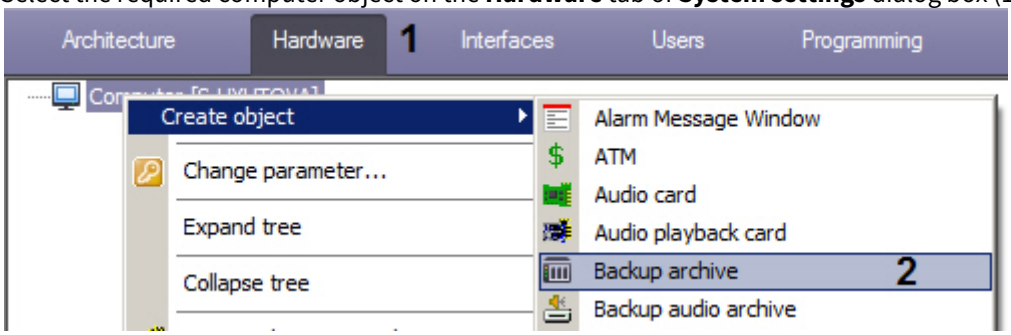
   It is recommended to restart the *Intellect* software after performing actions described above for correct using of **Backup archive** object settings.

7. Configure the **Panel of Backup archive** interface object (see Configuring the Panel of Backup archive object).

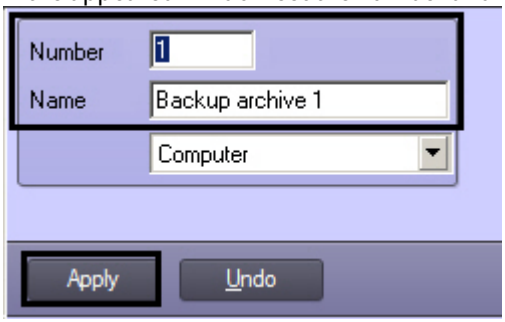
10.3.11.2.2 Creating the Backup archive object

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.

10.3.11.2.3 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*:

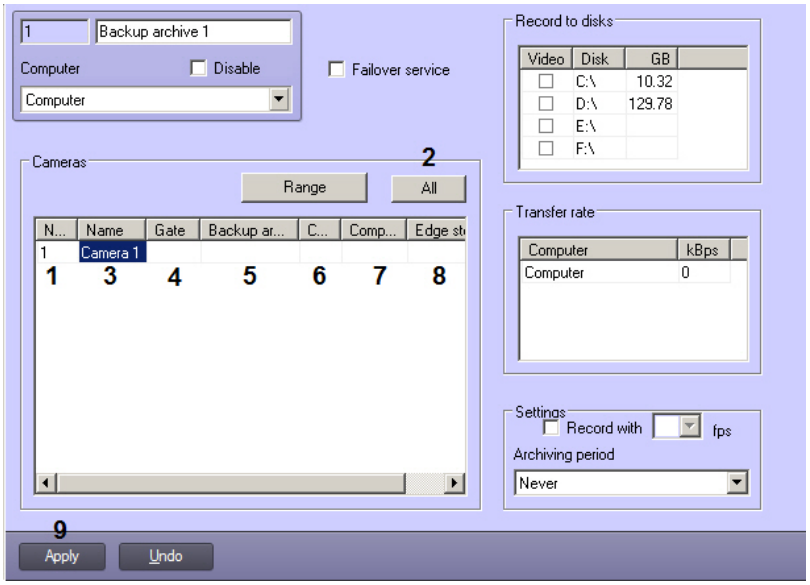
1. Separately. The settings panel for the **Backup archive** object is in use.
2. Integrated selection. The **Add/Edit cameras** dialog box is in use.

> **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. Repeat steps 2-8 for all the cameras.
10. To save all the changes, click the **Apply** button (9)

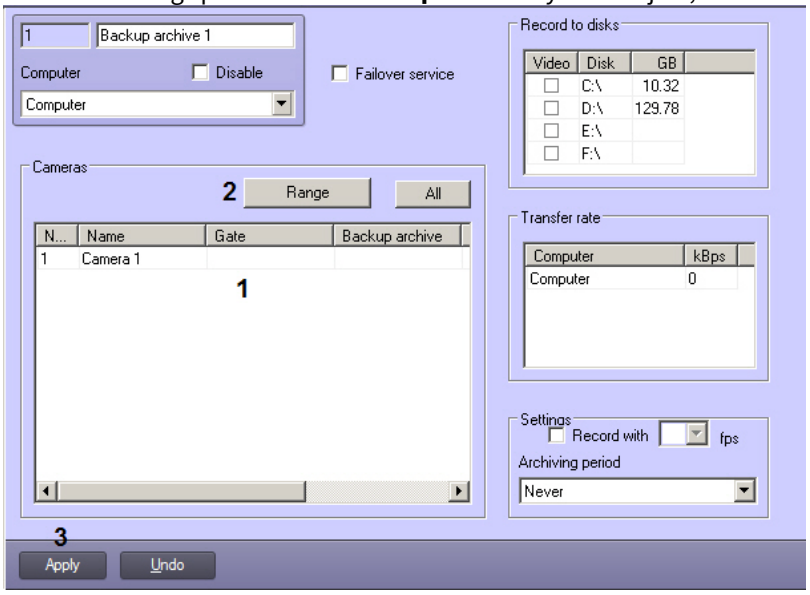
The cameras on the settings panel of the **Backup archive** object are now selected.

10.3.11.2.4 Selecting cameras as a group for the Backup archive

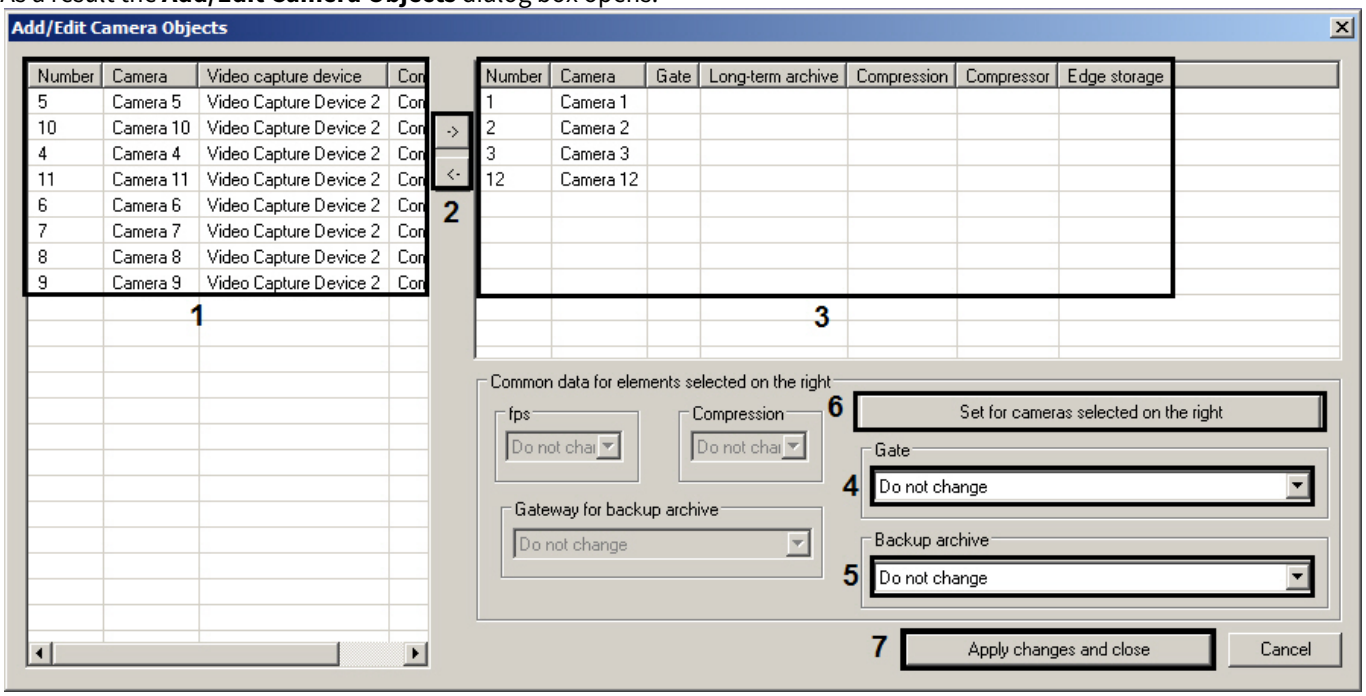
There is an opportunity of integrated selection and editing of cameras' parameters for copying the video archive to the *Backup archive*.

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** and **Backup archive** settings belong to the **Common data for the elements selected in the list 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. To save the parameters, click the **Set for the cameras selected in the list on the right** button (6).
10. As a result the set parameters are shown in the list on the right of the **Add/Edit Camera Objects** box (3).
11. Repeat steps 6-9 for complex editing of all the required cameras.
12. To save the changes and close the **Add/Edit Camera Objects** box, click the **Apply** changes and close button (7).
13. Camera settings are shown in the **Cameras** table on the settings panel of the **Backup archive** object (2).
14. To save all the changes, click the **Apply** button (3).

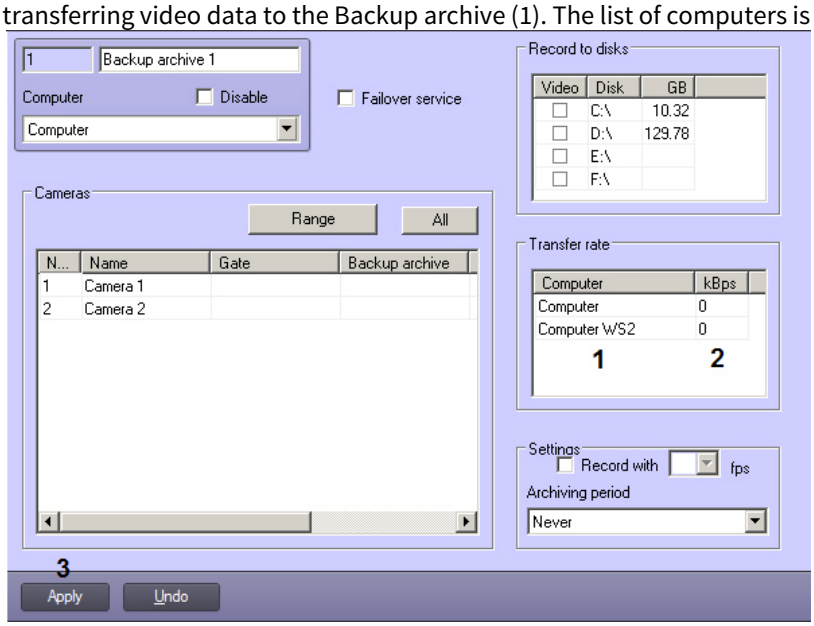
Integrated selection of video cameras is now over.

10.3.11.2.5 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.

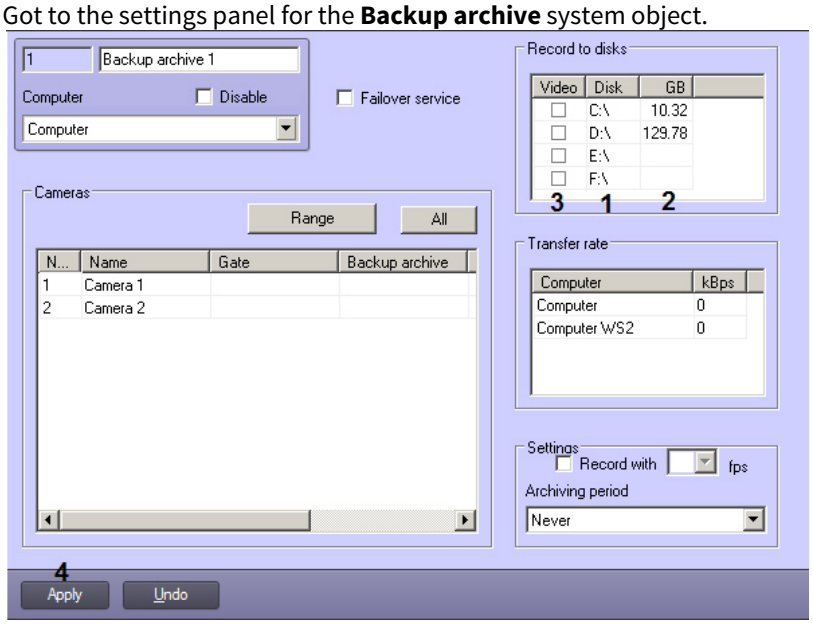
10.3.11.2.6 Selecting disks to store the archive of the Backup archive module

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 diskes to store the archive of the *Backup archive* module, do the following:

1. Got to the settings panel for the **Backup archive** system object.



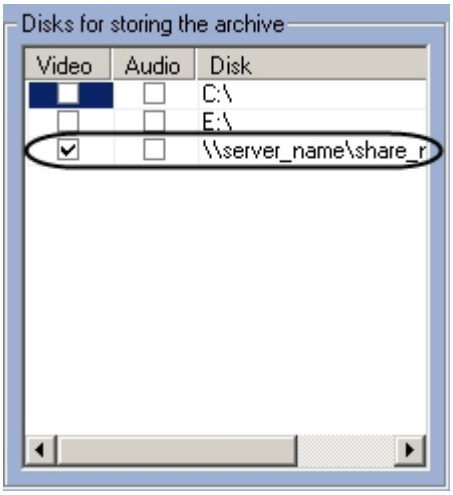
2. Names of local (net, USB) disks available for storing the archive of the *Backup archive* module are given in the **Disk** column of the **Record to disks** table (1).

> **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.

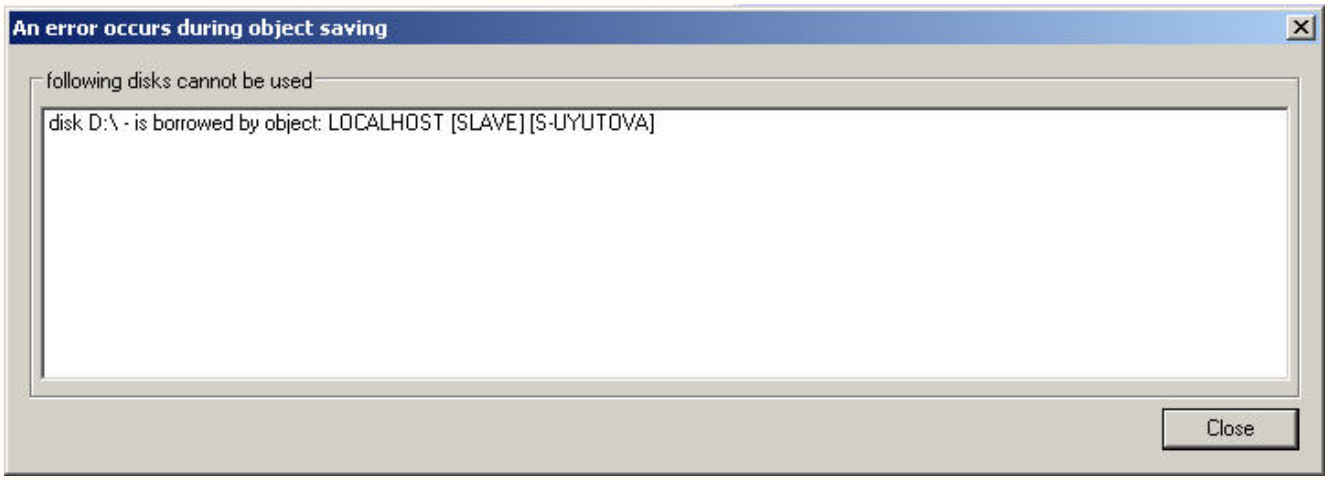


b. Specify the path to a net file in the appeared line in the **Disk** column. The UNC path is set in the "\ \server_name\share_name" format, where the "server_name" is the name of file server and the share_name is the net name of general folder.
c. In the **Video** column, set the checkbox for the created 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.

10.3.11.2.7 Configuring the scaling of the video archive

Video signals can be scaled before they are copied to a backup archive of the *Backup archive* module. Scaling is performed at the Server from which the video signal is transmitted to the Backup archive.

Note.

Scaling in the Backup archive may be performed with such codecs as MJPEG, Motion Wavelet, MPEG, H264 and MxPeg.

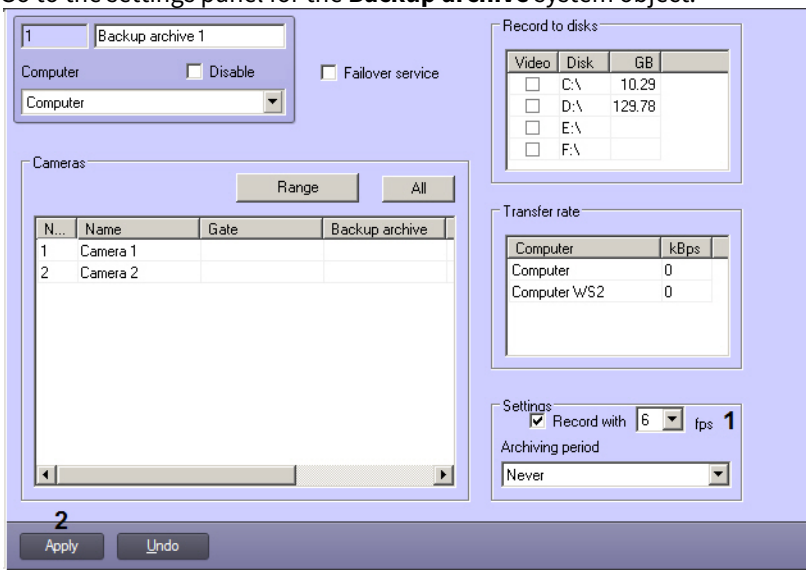
If the scaling rate is 25 fps, the videois processed at a lower rate for the first minute (~12 fps).

The maximum allowable scaling rate for MxPeg codec is 12 fps.

By default, a signal is copied from the server to the Backup archive without scaling.

To configure the scaling 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 scaling, 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* (1).

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 framerate value of the video archive that is to be transferred to the *Backup archive* is an average value. A real value of framerate may be different from that one, indicated in the **Record with ___ fps** drop-down list.

4. To save the changes, click the **Apply** button (2)

Video scaling is now configured.

10.3.11.2.8 Configuring the schedule of the video archive copying

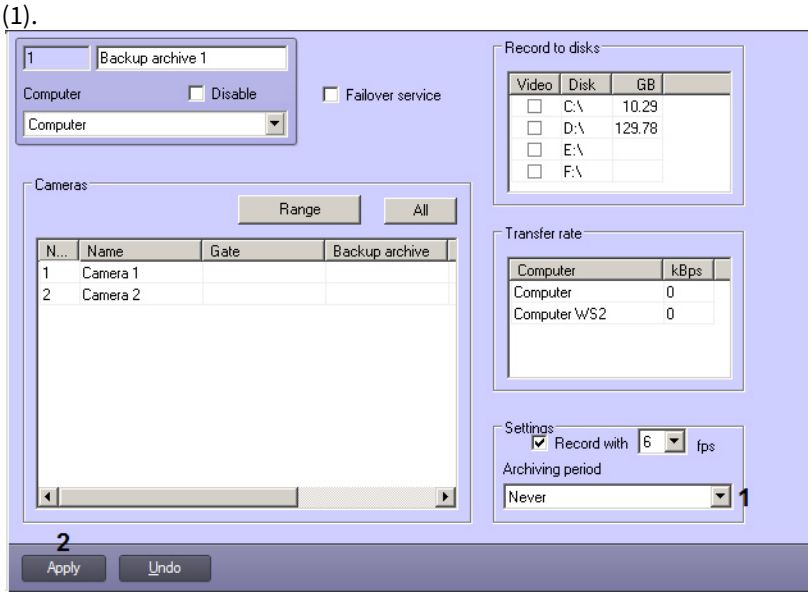
The *Backup archive* module can be started in two ways:

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.

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:

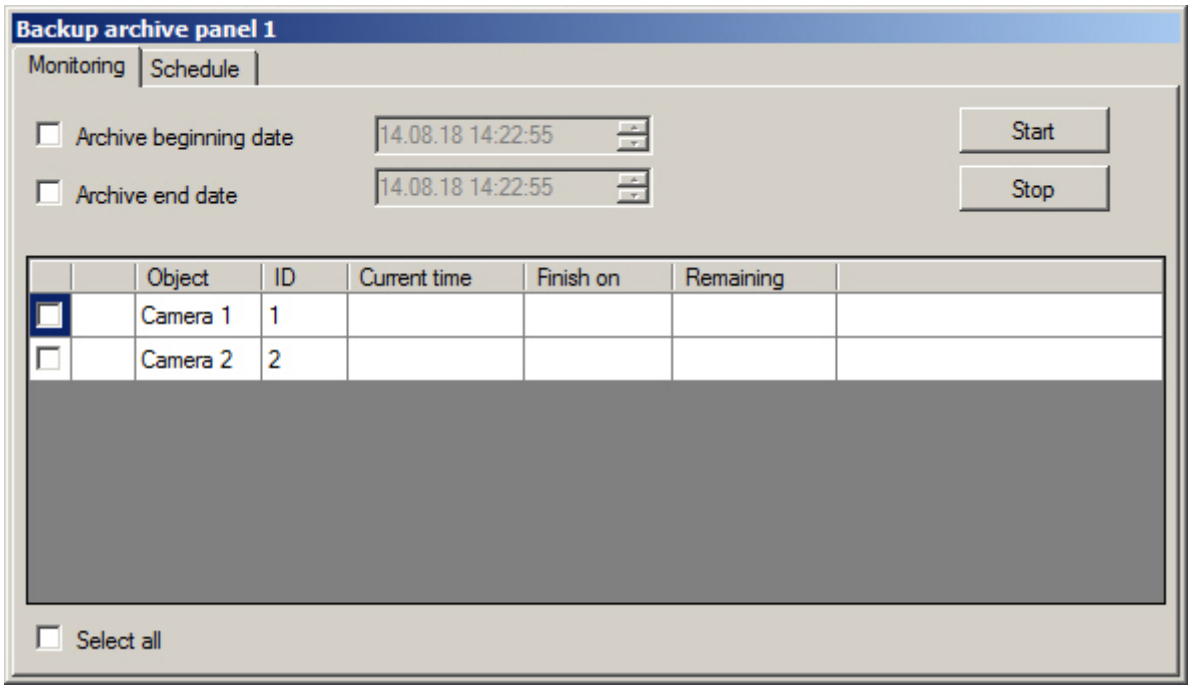
1. Go to the settings panel for the **Backup archive** system object.
2. In the **Archiving period** drop-down list, select the required time zone (time period) of the *Backup archive* module start (1).



3. To save the changes, click the **Apply** button (2).

The schedule of video archive copying to the *Backup archive* is now configured.

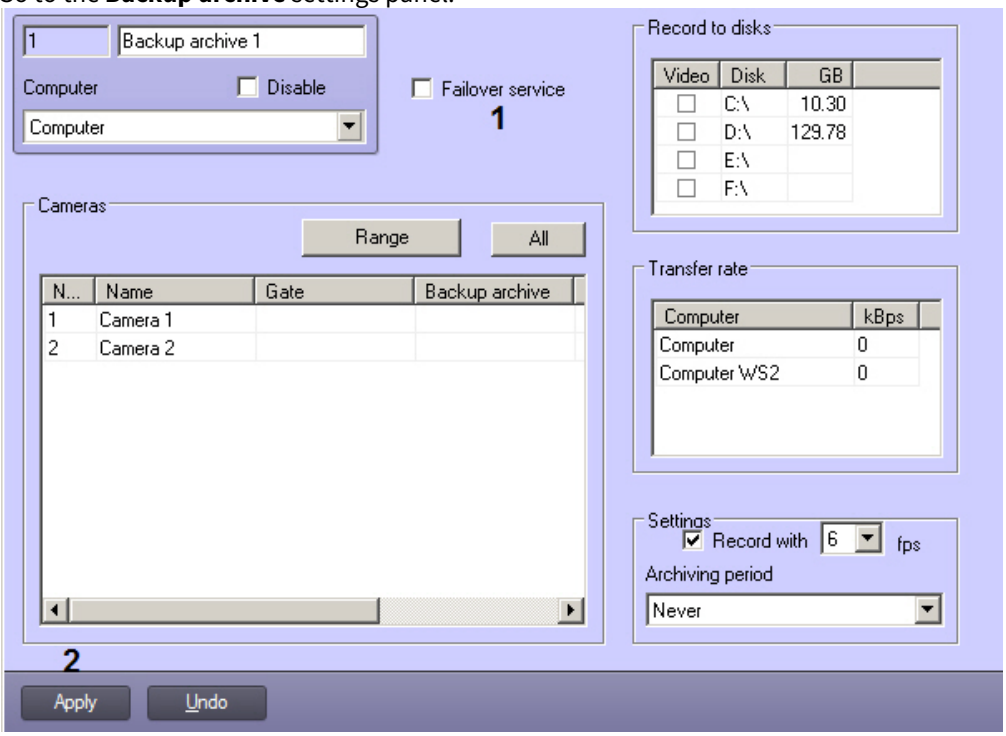
To start the archive backup manually, set the beginning and the ending dates of the archive to be copied and click the **Start** button.



10.3.11.2.9 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).

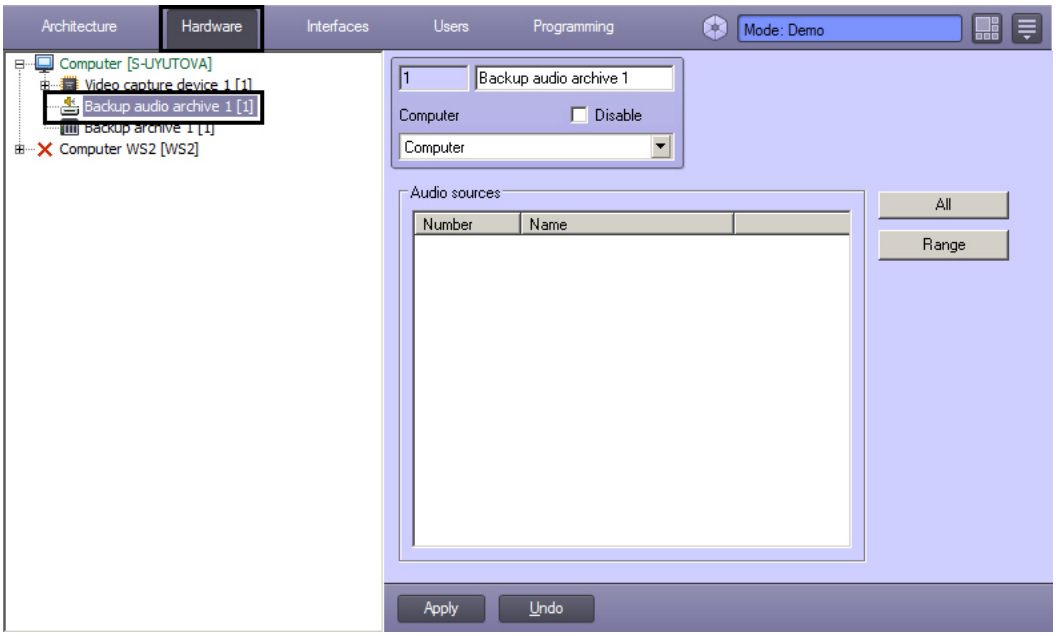
Cooperation of the Backup archive and the Failover service is now enabled.

10.3.11.3 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.

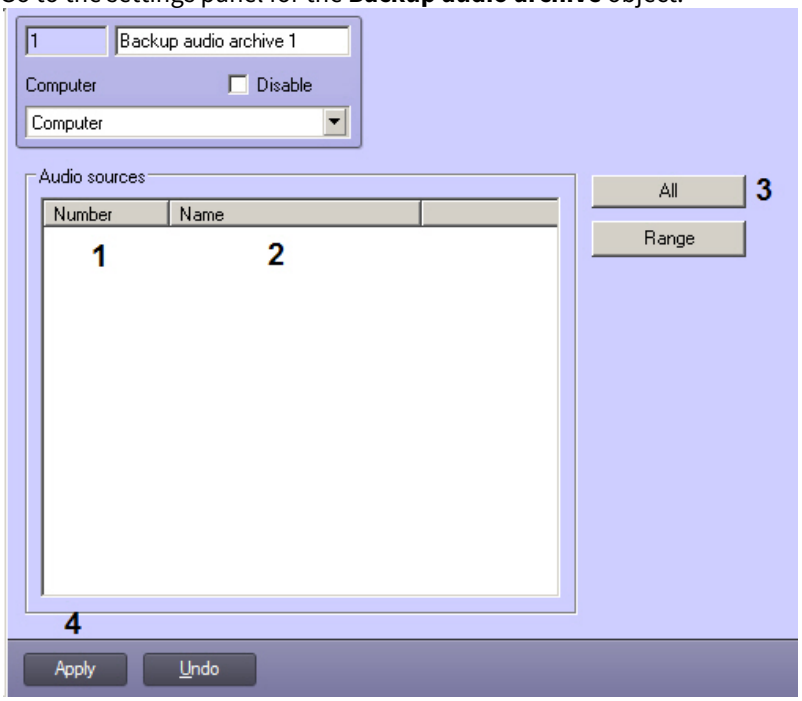
Configuration of the *Backup audio archive* is performed using the **Backup audio archive** system object. The **Backup audio archive** object is created automatically while creating the **Backup archive** object.

> **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.



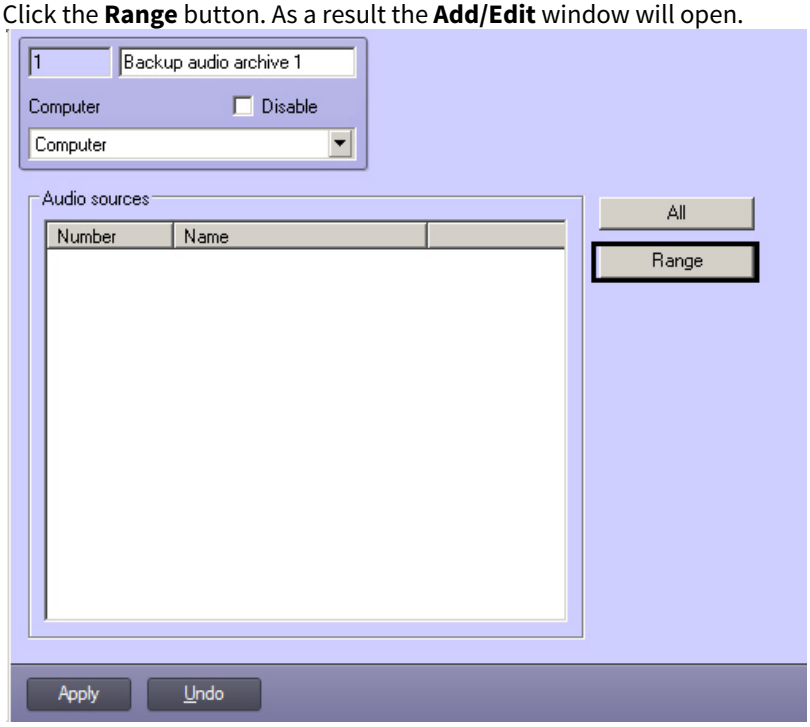
2. In the **Number** drop-downlist, select the id of a microphone related to the camera the archive from which is to be moved to the backup archive (1).
3. Left-click in the **Name** field. It will be automatically filled with the name of selected microphone (2).

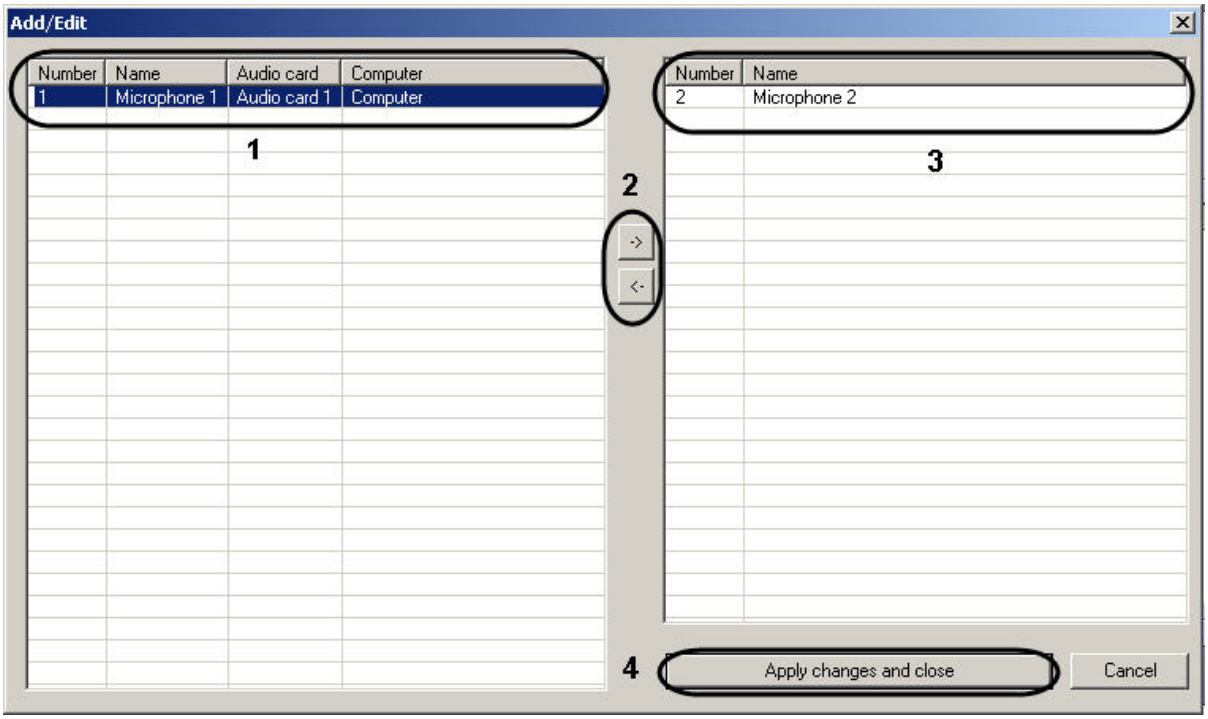
> **Note.**
>
> To add all **Microphone** objects created in the system to the list click the **All** button (3).

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** button. 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.

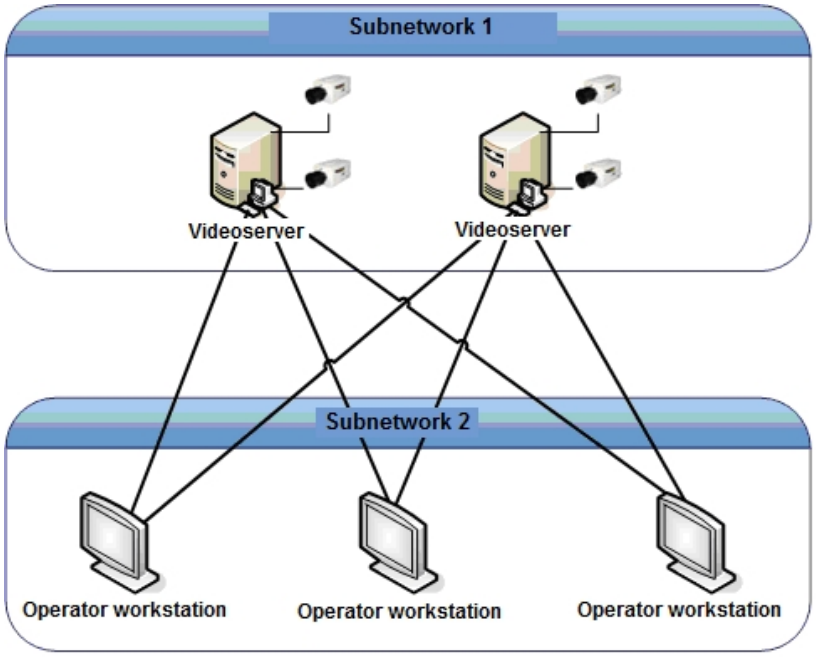
10.3.12 Configuring the Videogate module

10.3.12.1 General information on the videogate

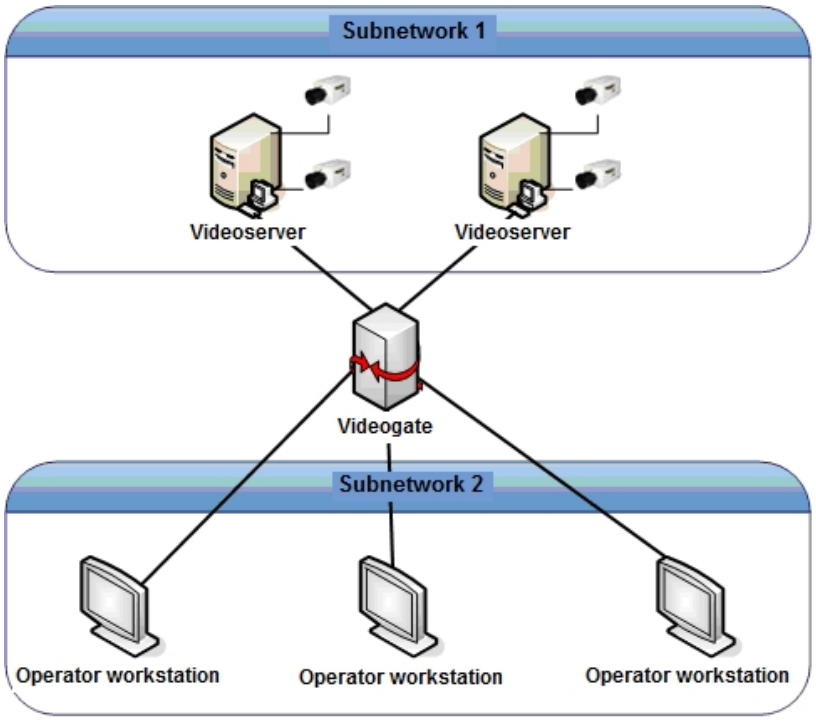
Videogate is used in large distributed video surveillance systems for routing the video signals among servers and clients (or administrator workstations used as operator workstations) located in different subnetworks. Servers and remote workstations are grouped into different subnetworks due to the following 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.

10.3.12.2 Order of setting up the Videogate object

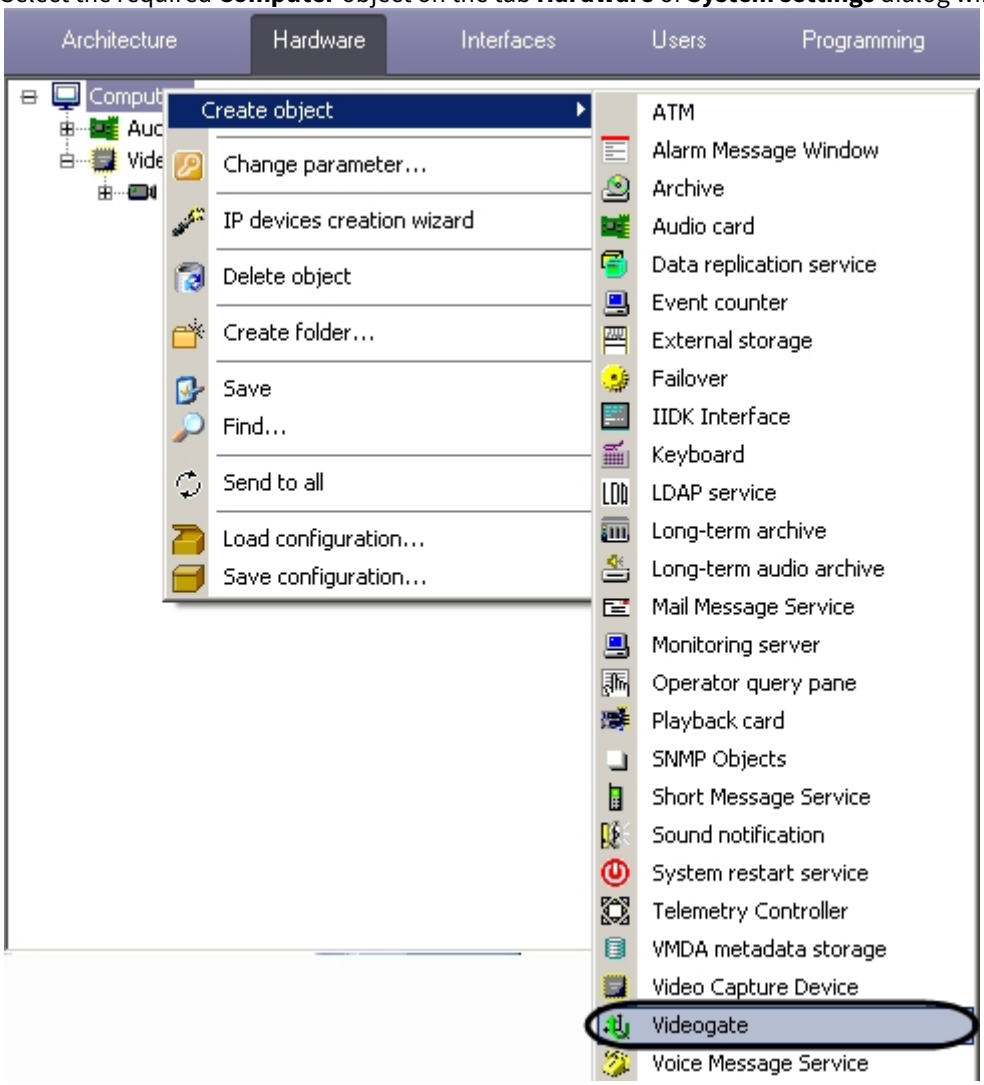
To set the **Videogate** object do the following:

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 as a group 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).

10.3.12.3 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.

10.3.12.4 Selecting and configuring the cameras for the Videogate module

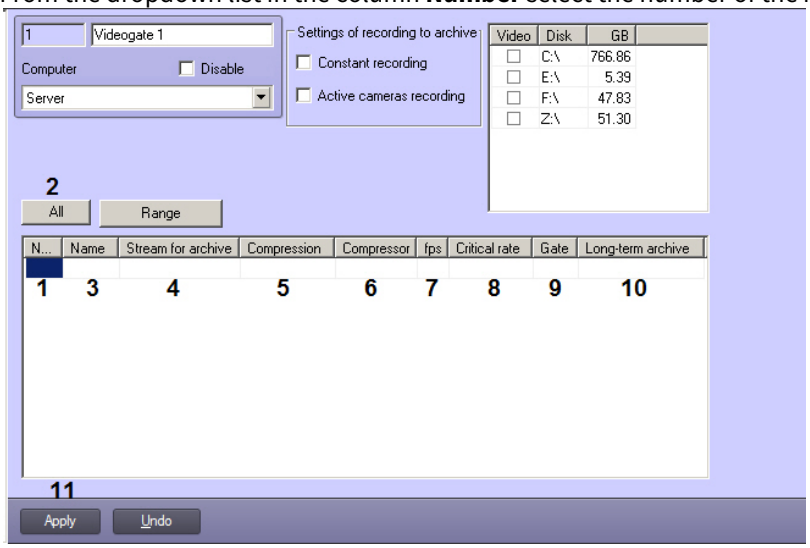
One can set and select cameras for transmitting the video signals through Videogate in two ways:

1. Separately. Use the settings panel of **Videogate** object.
2. Complex. Use the **Add/edit cameras** dialog box.

> **Note.**
>
> Order of complex selection of video cameras for transmitting video signals through the Videogate is described in Selecting video cameras as a group 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 Videogate system object.
2. From the dropdown list in the column **Number** select the number of the required video camera (1).



> **Note.**
>
> To select all cameras, registered in the system, click the **ALL** button (2).

3. In result in the column **Name** the name of the selected camera will be displayed (3).
4. In the **Stream for archive** dropdown 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, when compression level of the video signal for transmitting through the Videogate, select from the dropdown list in the column **Compression** the required compression level of video signal (5). Compression level of the video signal rises from «0» (compression is absent) to «5» (maximum compression).

> **Note.**
>
> In case of setting the compression level video signal on the Server has to be preliminary decompressed, that leads to great load on CP of the Server.

6. To change the procedure of video signal compression during transtission through the Videogate, select the required procedure of compression from the **Compressor** drop-down list (6).The value in the **Compression** list is to be selected if the compressor is specified (5). If **Compression** is selected but **Compressor** is not set, the Motion Wavelet compressor if used.

> **Note.**
>
> Recompression is performed on the Server side.

7. In case, when video signal has to be thinned out for its transmitting through the Videogate, enter in the field in the column **fps** the required frame rate of the video signal (7).

> **Note.**
>
> The given **fps** value must be less than the frame rate of video signal's digitizing by video input device. Otherwise frame rate of video signal will be equal to the frame rate of digitizing.
> The given **fps** value must not be less than 0.01 which corresponds to transmission of one frame in 100 seconds.

> **Note.**
>
> For correct thinning 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).

8. In case, when transmission of video signals through the local net or from the Server to the Videogate has to be controlled, enter in the field in the column **Critical rate** minimal available value of frame rate of video signals, transmitted to the Videogate (8).

> **Note.**
>
> The given value Critical rate should not be more 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 **Alarm messages window** system object (see. Setting up the Alarm Message window). In this case with the reduction of rate of inputting signals below the given value **Alarm messages window** will be displayed with the message "Reduced input rate".

9. In case, when video signal from the selected video camera is to be received from the other **Videogate** object, then select the name of this object from the dropdown list in the **Gate** column (9).
10. In case, when the video archive for the selected camera has to be received from the **Backup archive** object, select the name of this object from the dropdown list in the **Backup archive** (10).

> **Attention!**
>
> Selected value is to be coincide with value which is specified while configuring video cameras for displaying for this Camera – see the Selecting and configuring video cameras section.

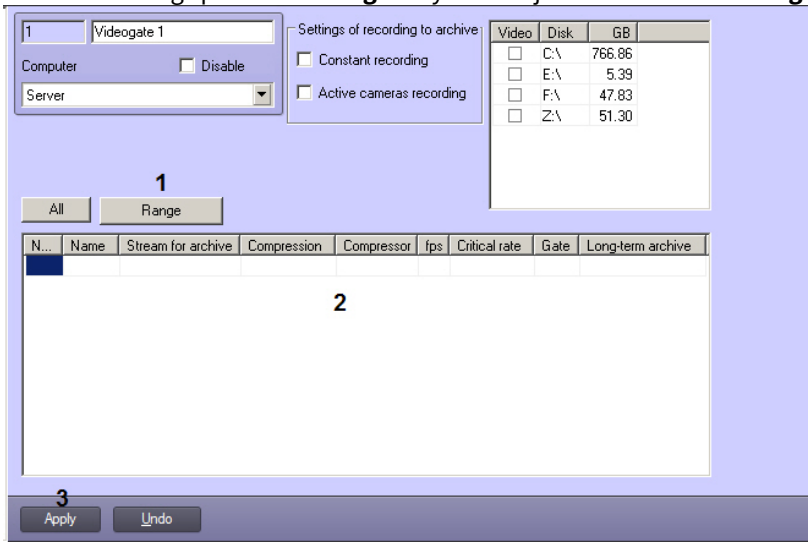
11. Repeat steps 2-8 for all the required cameras.
12. To save all the changes click **Apply** button (11).

Selection of cameras on the settings panel of the **Videogate** object is completed.

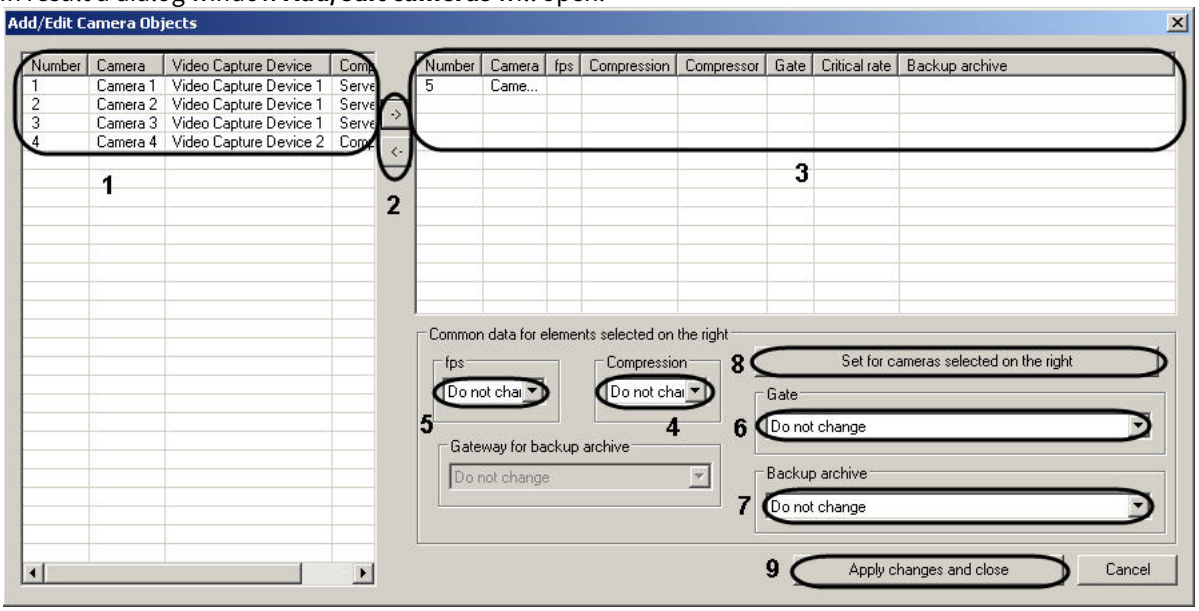
10.3.12.5 Selecting video cameras as a group for the Videogate module

There is opportunity of complex selection and editing parameters of video cameras for transmitting video signal through Videogate. Complex selection of cameras is performed in the following way:

1. Go to the settings panel of **Videogate** system object and then click **Range** button (1).



2. In result a dialog window **Add/edit cameras** will open.



3. Select the required objects in the left list of **Add/edit cameras** window (1).
4. Remove the selected cameras to the right list, clicking the -> button (2).

> **Note.**
>
> Right list contains a list of cameras, selected for transmitting the video signals through the Videogate.
>
> Button <- is used for back action, for removing the selected cameras from the right list to the left (2).

5. In result the selected video cameras will be displayed in the right list of **Add/edit cameras** window (3).
6. When necessary select in the right list the names of the required cameras for complex editing of parameters (3).

> **Attention!**
>
> For all the selected cameras the same value of parameters will be set.

> **Note.**
>
> There is no possibility to edit **Critical rate** parameter with the help of **Add/edit cameras**.

7. In case, when compression level of video signal has to be changed for transmitting through the Videogate, select from the **Compression** dropdown list the required compression level (4).**Compression** level rises from «0» (no compression) till «5» (maximum compression).

> **Note.**
>
> In case of setting the compression level video signal must be preliminary decompressed on the Server that leads to great loading on the CP of the Server.
> Settings **Compression**, **fps**, **Gate**, **Backup archive** belong to the group **Set for the selected in right list of cameras**(6).

8. In case, when video signal has to be thinned out for transmitting through Videogate select from the **fps** dropdown list the required frame rate of video signals (5).

> **Note.**
>
> The given **fps** value must be less the frame rate of video signal's digitizing by video capture card. Otherwise frame rate of video signal will be equal to the frame rate of digitizing.

9. In case, if video signal form the selected cameras is to be received from the other **Videogate** object, then select the name of this objet from the **Gate** dropdown list (6).
10. In case when video signal has to be transmitted from the selected cameras from the **Backup archive** object, select from the **Backup archive** dropdown list the name of this object (7).
11. To save the set parameters click **Set for the selected in right list of cameras** button (8).
12. In result the set parameters will be displayed in the right list of **Add/edit cameras** window (3).
13. Repeat steps 6-11 for complex editing of all the required cameras.
14. To save all the changes and close **Add/edit cameras** window click **Apply** changes and close button (9).
15. The given settings will be displayed on the settings panel of the **Videogate** object (2).
16. To save the given changes click **Apply** button (3).

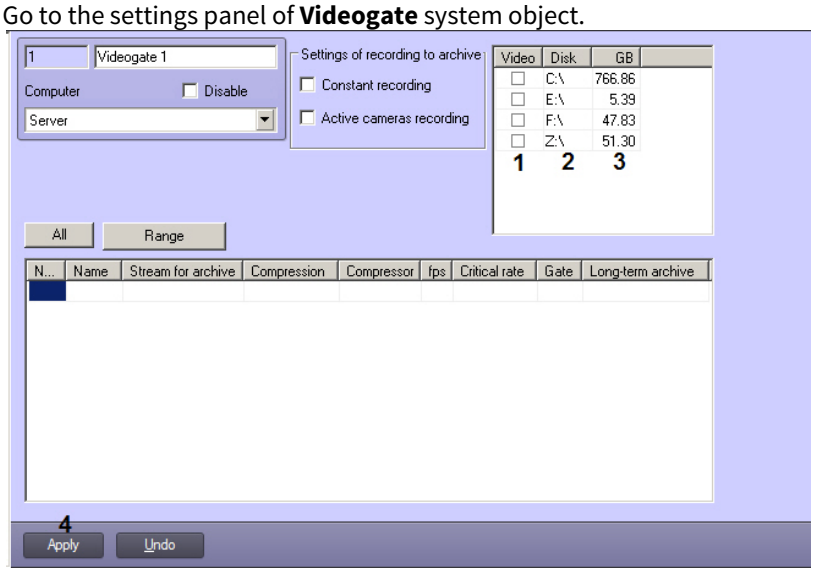
Complex selection of cameras is completed.

10.3.12.6 Selecting disks for storing the archive of the Videogate module

To enable video signals archiving, going through the Videogate, it is necessary to select the disks for archive storing.

To select the disks do the following:

1. Go to the settings panel of **Videogate** system object.



2. Names of local (net, USB) disks, accessible for archive of *Videogate* module are given in the column **Disk** (1).

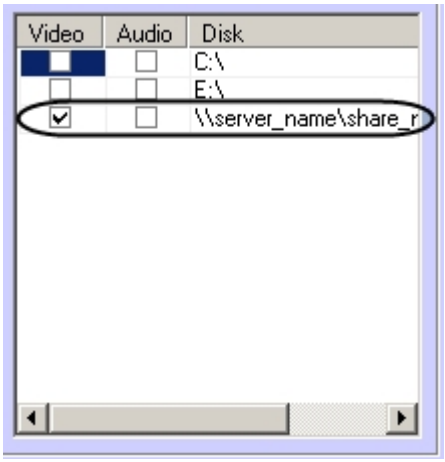
Attention!

For Windows Vista and Windows 7 OS with connected UAC it's necessary to connect net disks through command prompt with Administrator's rights. The way of connection is described in Connecting network disks in Windows Vista and Windows 7 OS part.

Note.

To use net disks as an archive, set UNC paths to them in Intellect software. Details of working with net disks in Intellect software that is installed a s a Service are described in Working with Windows OS services for operating Intellect™ installed as a Service.

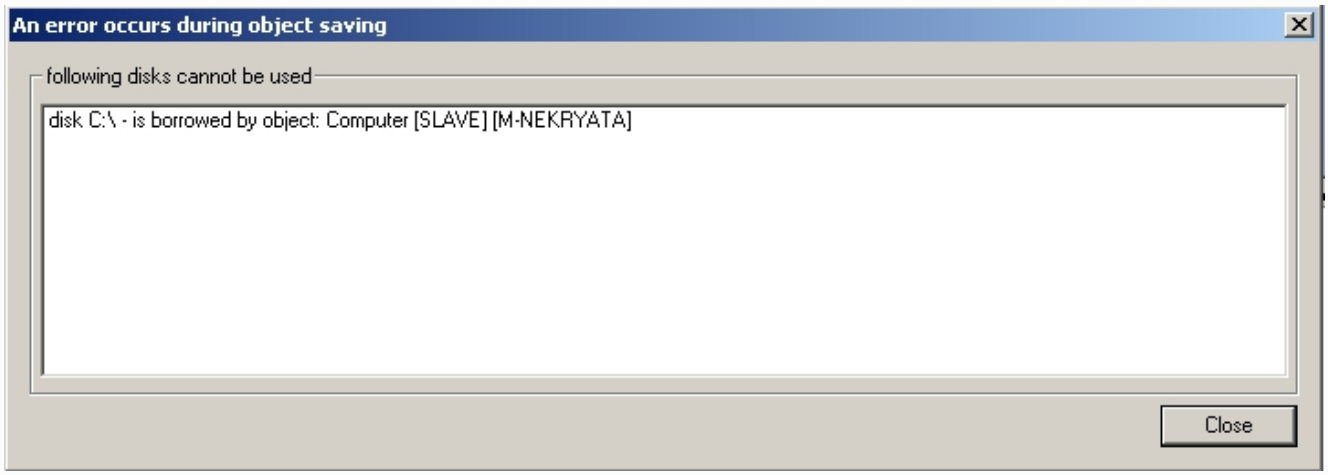
3. In the column **GB** there is a size of free space on disk in GB (2).
4. In the column **Video** put the check mark for disks, selected for storing archive of *Videogate* module (3).
5. To add a net disk via entering the UNC path, do the following:
   a. Go to the last line in the **Disk** list and click **Down** key.



   b. Enter the path to a net file in the appeared line in **Disk** column. UNC path is set in format «\\server_name\share_name», where «server_name» is file server's name and «share_name» is net name of generalfolder.
   c. Set the checkbox for created disk in **Video** column.
6. To save the set changes click **Apply** button (4).

Note.

For storing the archive of *Videogate* module 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 there will appear **Error in the process of saving the Videogate object** window.



Note.

In case, when no one disk is selected for storing video recordings, there is no recording of video signals to the archive of *Videogate* module.

Selection of disks for storing the archive of *Videogate* module is completed.

Free disk space (video archive size) required

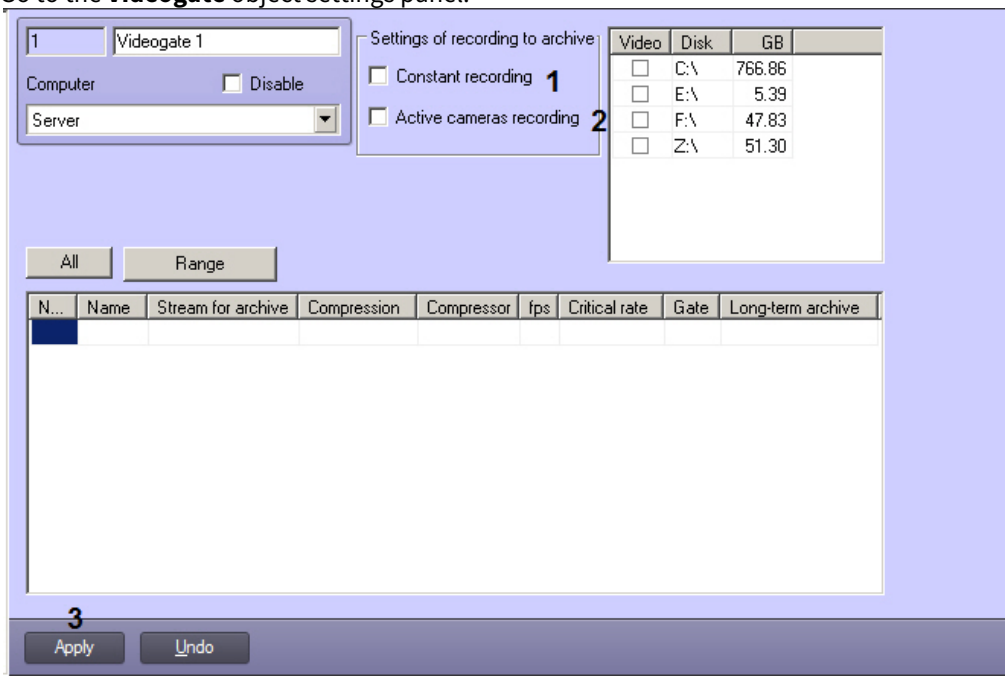
Video gateway archive playback

10.3.12.7 Configuring the record of the Videogate module archive

By default, if disks are selected for storing the archive of the Videogate module (see Selecting disks for storing the archive of the Videogate module), then Videogate requests video streams for all selected cameras (see Selecting and configuring the cameras for the Videogate module) from Server and only records the Videogate module archive if recording is configured for these cameras on the Server. Continuous Videogate archive record by all added cameras regardless of Server configuration, as well as record only on cameras requested on clients can be enabled.

To configure the record of the Videogate module archive do the following:

1. Go to the **Videogate** object settings panel.



2. If continuous record on all cameras added to the Videogate is required regardless of whether the Server records its archive or not, set the **Constant recording** checkbox (1).
3. If only cameras requested on clients (i.e. displayed in the Video surveillance monitor) are to be recorded to the Videogate module archive, set the **Active cameras recording** checkbox (2).
4. Click **Apply** (3).

Configuring the record of the Videogate module archive is completed.

10.3.13 Notification services

10.3.13.1 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

10.3.13.1.1 General description and usage details of the Alarm Message window

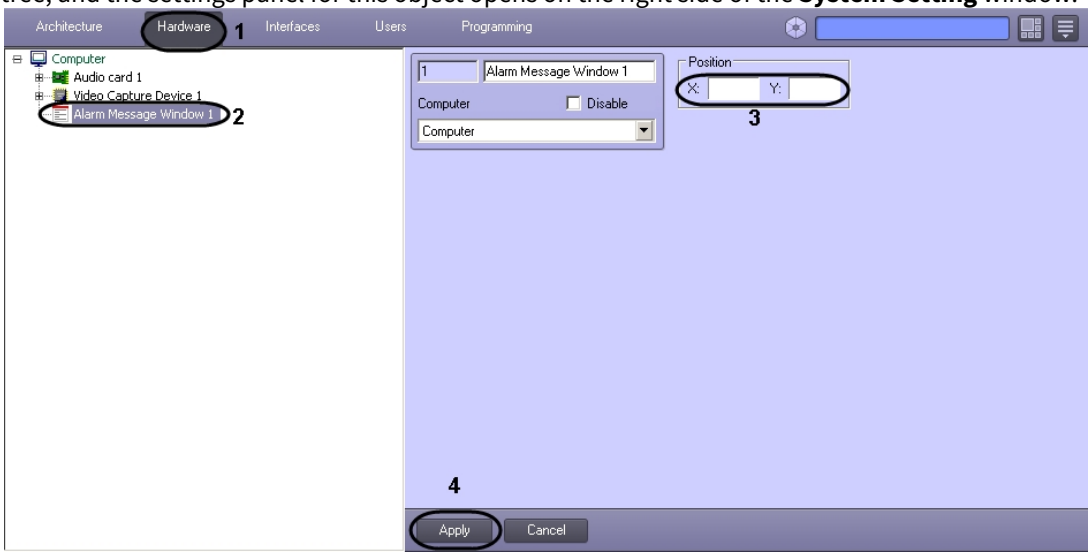
The **Alarm Message window** notifies the operator about alarms and opens above all other windows in case of an alarm event on a set device.

10.3.13.1.2 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.

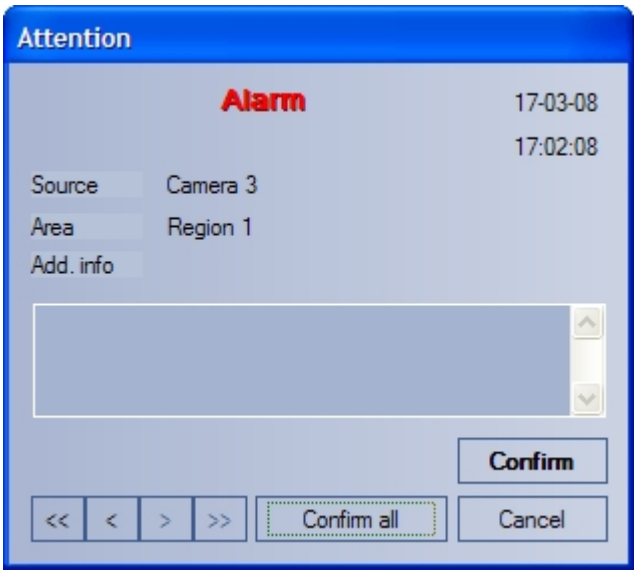


3. Set the coordinates (**X, Y**), in percent, for the position of the **Alarm Message window**.

> **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.

10.3.13.2 Setting up the Short Message Service (SMS)

10.3.13.2.1 General description and usage details of the Short Message Service

The Short Message Service (SMS) is used for sending short messages to mobile phones about alarm events registered by Intellect software. A short message is sent automatically upon registration of any of the events specified in the corresponding macro.

Actions with *Intellect* objects can be performed when a SMS is received. Macros, programs in the language embedded in Intellect or Jscript scripts are used for this. When the sms is received the SMS object sends the RECEIVE event in *Intellect.*

The short messages are transferred using the services of the GSM mobile providers. To send the short messages, dedicated devices are used: GSM modems, GSM adapters and mobile phones.

Note.

When using a device with Android OS incoming messages are transliterated in *Intellect*.

Note.

When using Intellect software SMS service a certain fee should usually be paid to the mobile providers.

To be able to send the short messages, a GSM modem, a GSM adapter or a mobile phone supporting ETSI GSM 07.07 or ETSI GSM 07.05 should be installed on the computer (see also Android-based Axxon SMS-sender Mobile Application. User Guide).

The following modem models are currently integrated into *Intellect* software:

1. 3G -modem Huawei E160, is identified as HUAWEI Mobile Connect -3G Modem in OS Windows. Modem control program is not required to be run to work with this device.
2. 3G-modem ZTE MF626 is identified as ZTE Proprietary HS-USB Modem in OS Windows.To use this device it is necessary to install the hardware, which installation will be run automatically after the modem is connected.
3. Huawei E173 3G modem. The RECEIVE event is supported if the ProcessFromSim registry key is in use (see Registry keys reference guide).

Note.

Most mobile operators protect their USB-modems from using them in mobile networks of other operators. Launch the utility installed with the device simultaneously with the *Intellect* software to activate sms-notifications when the modem protected by operator is in use. Any other actions (connect to 3G, etc.) with the utility are not required.

To create and send a short 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.

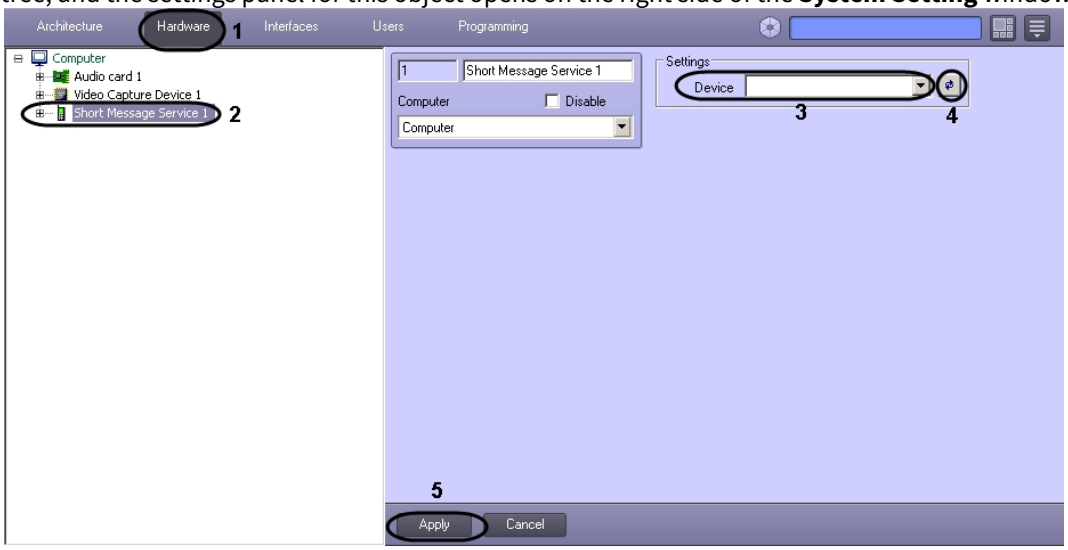
Requirements for GSM Equipment

10.3.13.2.2 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.

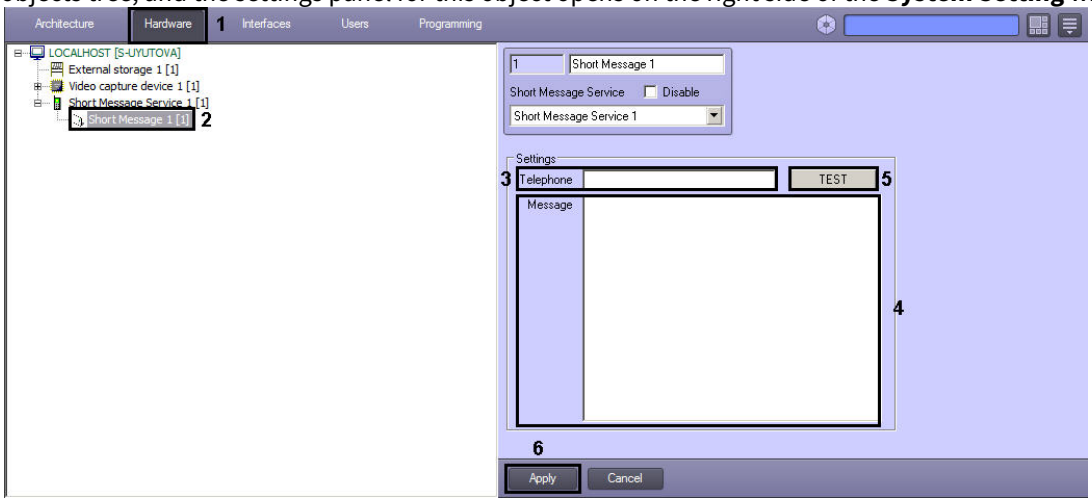


3. Select the GSM-device to be used for sending SMS, in the **Device** drop-down list.
4. Press the refresh button for the system to update the list if the device was not listed.
5. Press the **Apply** button to save the settings for the **Short Messages Service** object.

10.3.13.2.3 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.



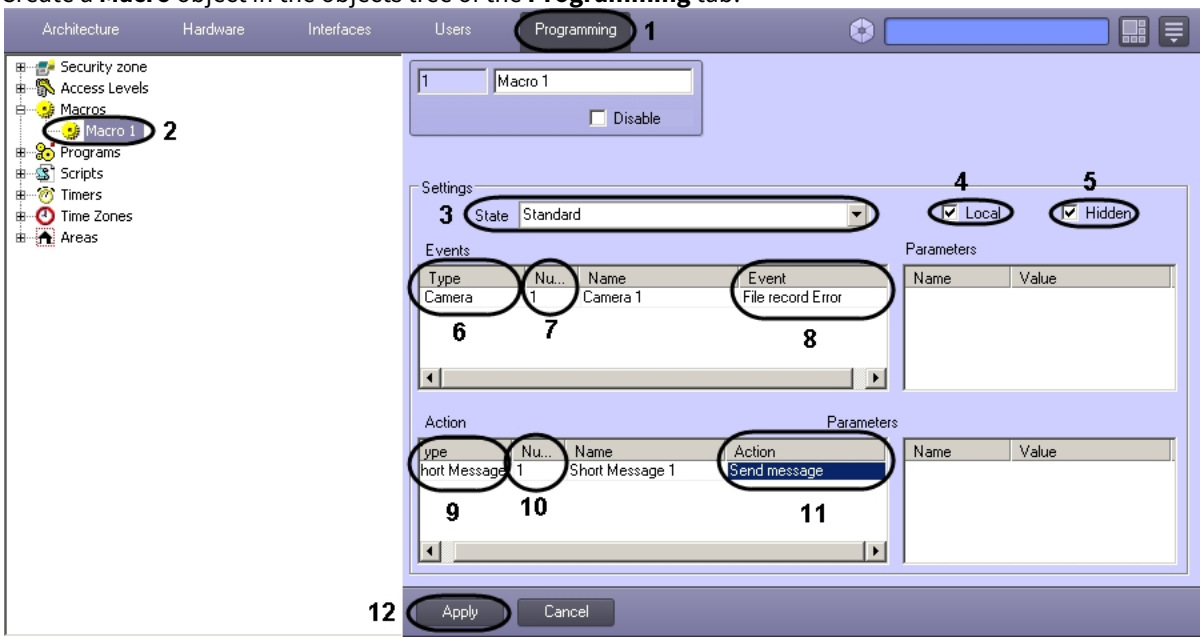
3. Enter the telephone number into the **Phone** field in the following format: [prefix "+"] [country code] [city/provider code] [phone number] with no spaces or other delimiters (3).
4. Enter the message text into the **Message** field (4).
5. If a short message is to be force sent, click the **TEST** 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).

10.3.13.2.4 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.

10.3.13.3 Setting up the Mail Message Service (E-mail)

10.3.13.3.1 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:

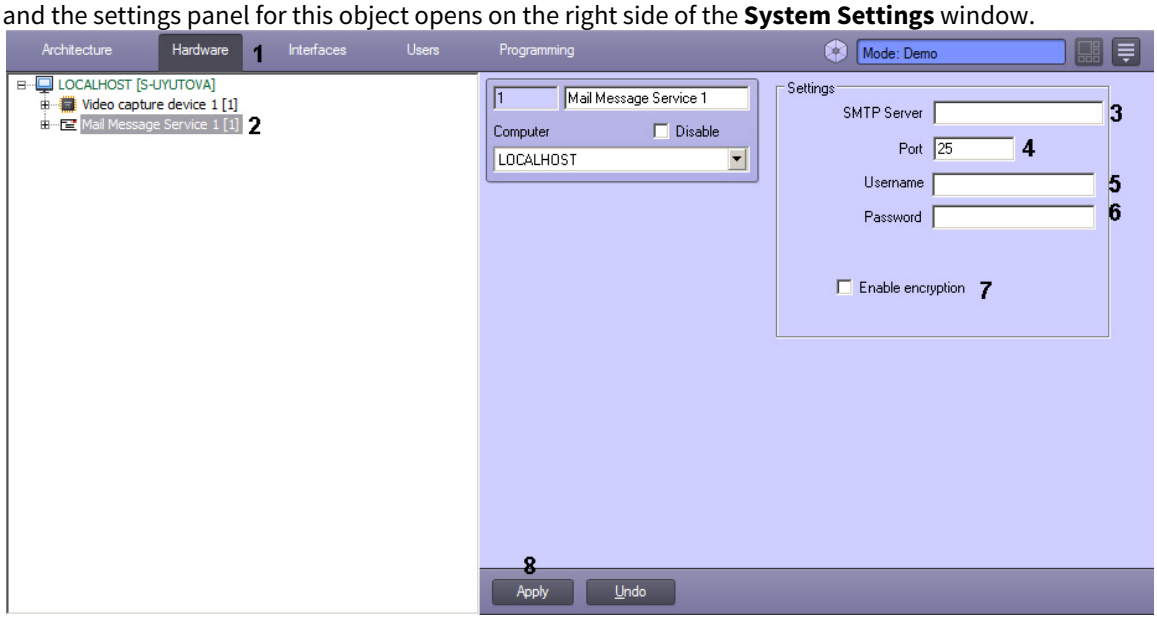
1. Create and set up the **Mail Message Service** object.

2. Create and set up the **Mail Message** object.
3. Create a macro for sending the e-mail message.

10.3.13.3.2 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.
2. Create the **Mail 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 Settings** window.



3. Enter the URL address of the SMTP server.
4. Enter the port number for outgoing messages.
5. Enter the username for authorization on the SMTP-server.
6. Enter the password for authorization on the SMTP-server.
7. Enable encryption if necessary.
8. Press the **Apply** button to save the settings for the **Mail Messages Service** object.

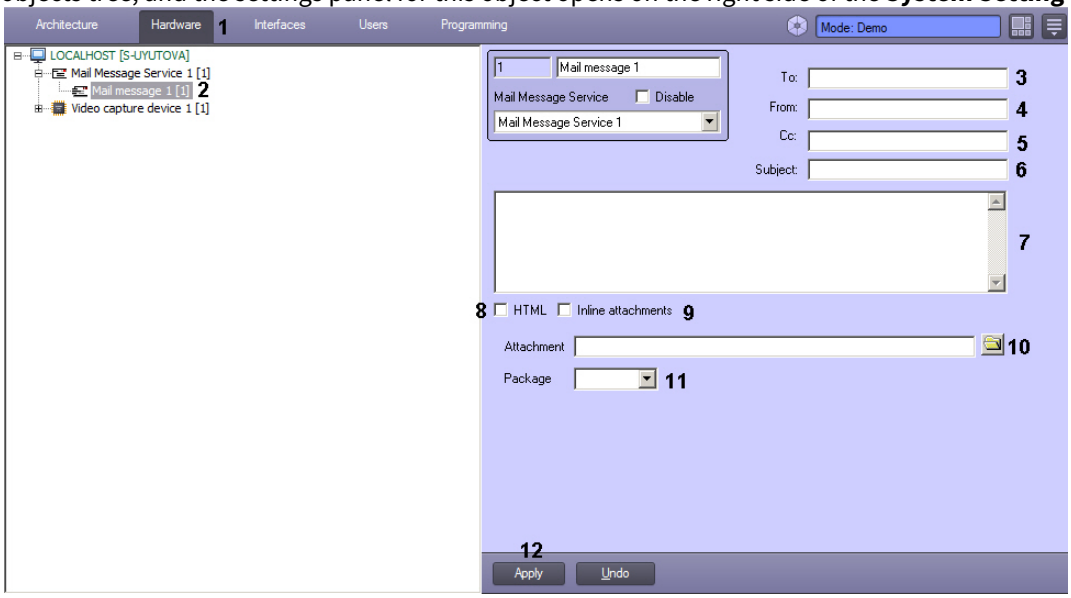
Find information on how to set up mail servers in the table.

	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	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 your account in Yahoo settings.	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 secure apps access your account in Gmail settings.
Encryption	Yes	Yes	Yes	Yes

10.3.13.3.3 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

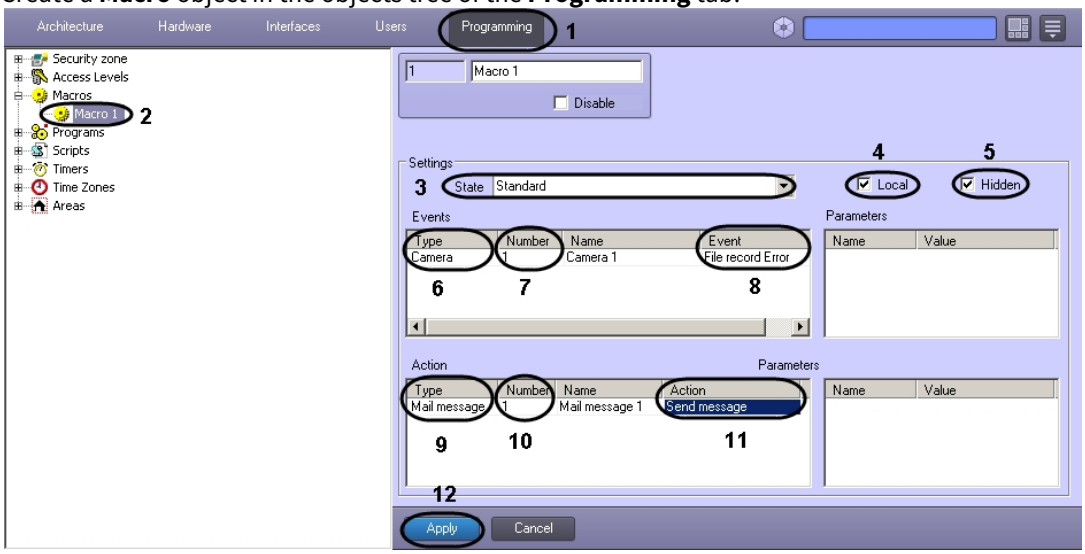
10. Attach a file to the alarm message (report, audio, image), if necessary (10). If several files are attached, their addresses are semicolon separated.
11. Specify if the attachment should be packaged (archived) (11).
12. Press the **Apply** button to save the settings for the **Mail Message** object (12).

10.3.13.3.4 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.

10.3.13.4 Setting up the Voice Message Service (V-dial)

10.3.13.4.1 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:

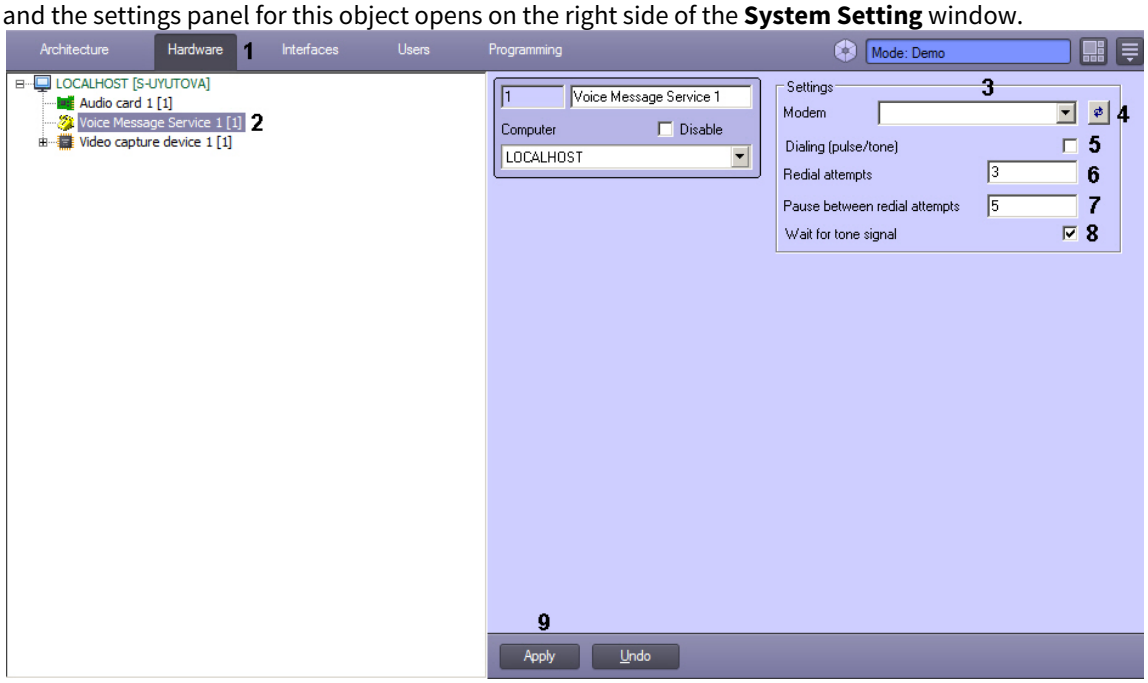
1. Create and configure the **Voice Message Service** object.
2. Create and configure the **Voice Message** object.
3. Create a macro for sending the voice message.

> Requirements for voice modems

10.3.13.4.2 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.

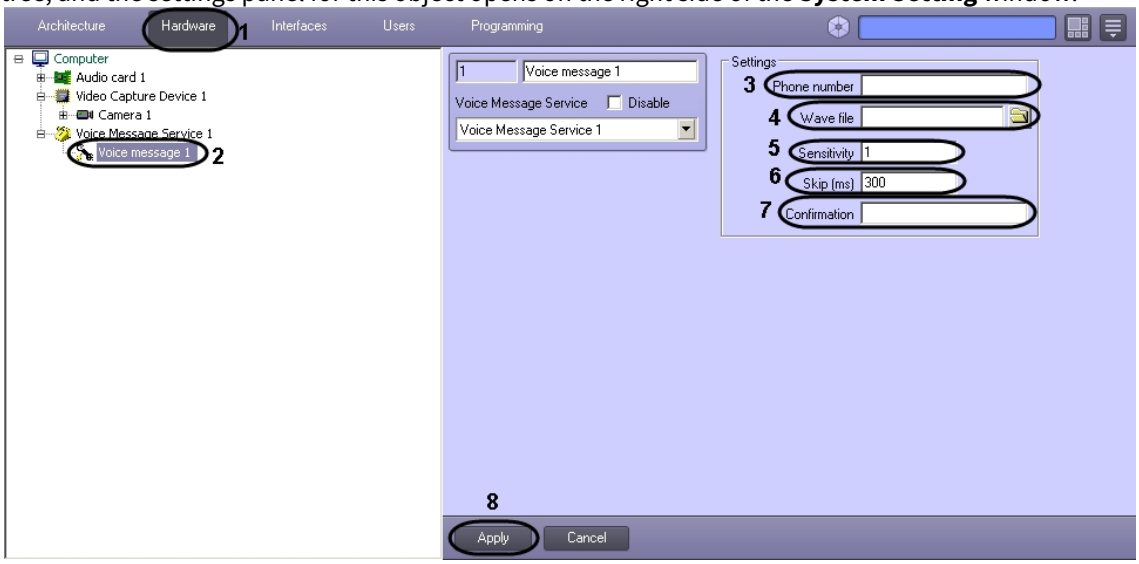


3. Choose a modem in the list of all modems available in the system.
4. If the modem is not in the list or there are no modems in the list, press the modem search button.
5. Check/uncheck the checkbox to choose the dialing mode.
6. Enter the number of dialing attempts.
7. Enter the delay between dialing 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.

10.3.13.4.3 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.



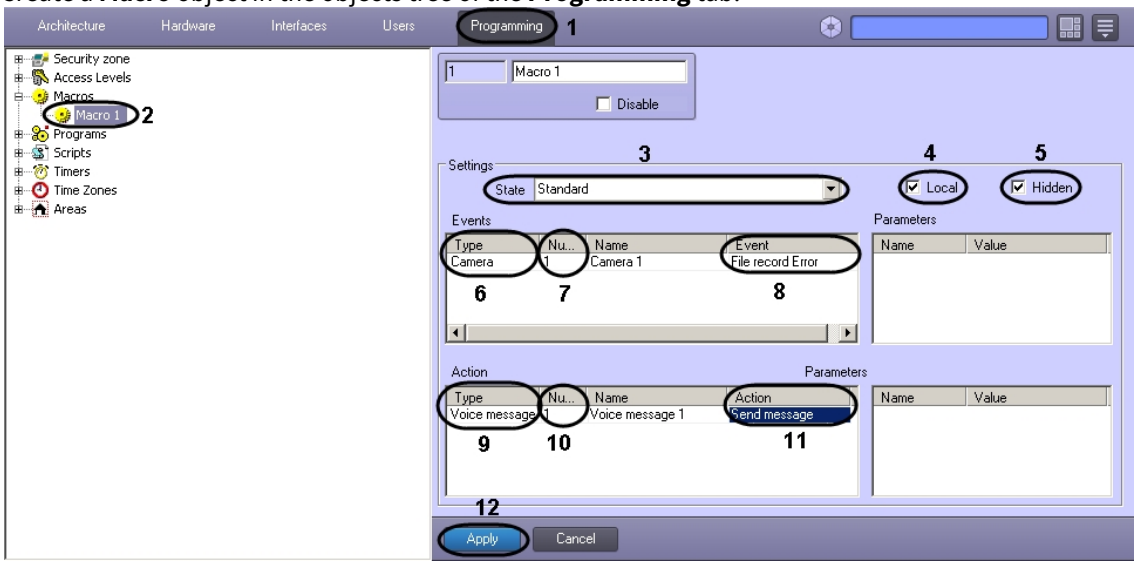
3. Enter the telephone number into the **Phone** field in the following format: [prefix “+”] [country code] [city/provider code] [phone number] with no spaces or other delimiters.
4. Load the wave file to be sent as a voice message.

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.

10.3.13.4.4 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.

10.3.13.5 Setting up the Voice Notification Service

10.3.13.5.1 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.

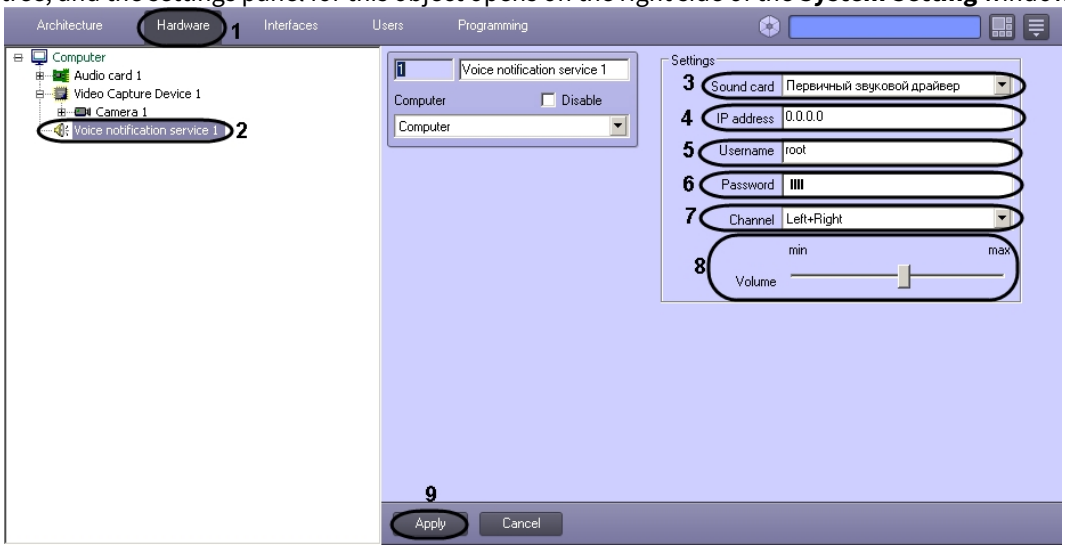
To create and send the voice notification:

1. Create and set up the **Voice Notification Service** object.
2. Create a macro for sending the voice notification.

10.3.13.5.2 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.



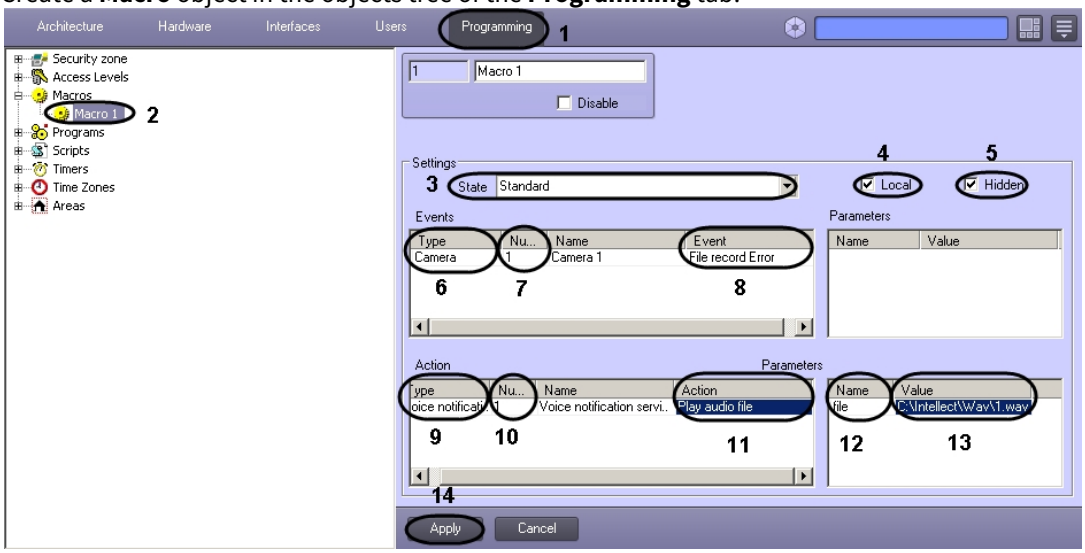
3. Choose the device in the **Sound card** list to send the notification to.
4. Specify the IP address of the network device (sound card, IP camera or Linux Hub), used to access this device over the network. If the sound card of the local computer is selected, this field is disabled.
5. Specify the username 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.

10.3.13.5.3 Creating and setting up the macro for sending 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.



3. Specify the **State** parameter.
4. Check the **Local** checkbox to send the voice notifications 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 voice notification macro to be related to.
7. Choose the event object number for the voice notification macro to be related to.
8. Choose the name of the event to trigger the sending of the voice notification.
9. Choose the **Voice Notification** object in the **Type** column.
10. Choose the number of the **Voice Notification** object.
11. Choose **Play wave file** action.
12. Click the **Name** field in the **Parameters** table. The **Value** field becomes available to specify the audio file.
13. Specify the full pathname of the wave file to be sent as the voice notification.
14. Press the **Apply** button to save the settings for the **Macro** object.

10.3.13.6 Setting up messaging via Telegram bot

On the page:

- Configuring the Intellect to Telegram messaging function
- Example macros for sending messages to Telegram

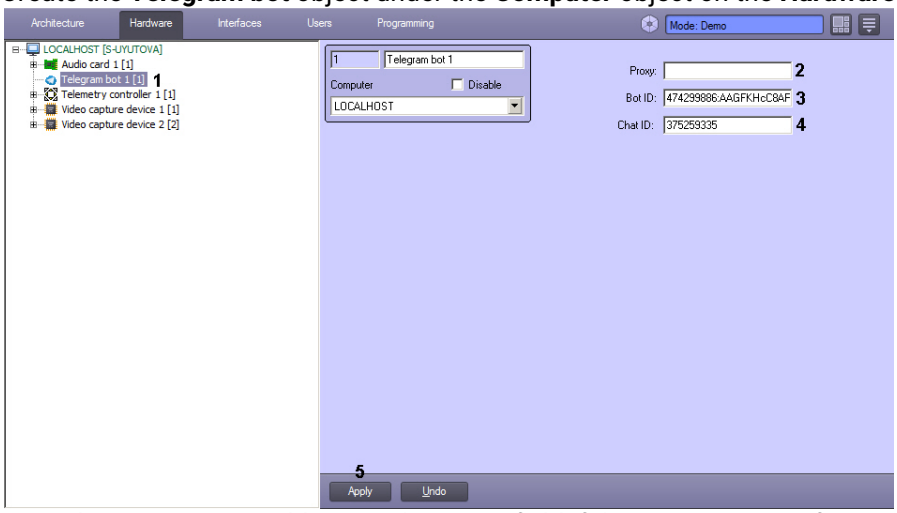
Intellect allows sending text or image to the Telegram chat on any event of any object created in the *Intellect* object tree. After configuration, sending a message is initiated by a macro or a script from *Intellect*.

Create the bot and the group chat with it in Telegram before configuring the messaging function in *Intellect*. You may use the pre-created and configured bot @IntellectNotificationsBot. Please refer to the developer's official website for installer and user guides for the Telegram messenger: telegram.org.

10.3.13.6.1 Configuring the Intellect to Telegram messaging function

Configure the Intellect to Telegram messaging as follows:

1. Create the **Telegram bot** object under the **Computer** object on the **Hardware** tab of the **System settings** dialog (1).



2. Enter the proxy server address in the **Proxy** field if the proxy is in use for connection (2).
3. In the **Bot ID** field, enter the Telegram bot identification number (3).

> **Note.**
>
> The identification number is provided when creating the bot.
> @IntellectNotificationsBot bot id is 474299886:AAGFKHcC8ARX9ziXgTlvKnwNhxnwlDhmD3M

4. In the **Chat ID** field, enter the chat identification number (4).

> **Note.**
>
> To find out the identifier of the chat, you can add @RawDataBot 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 **Apply** (5).

The Intellect to Telegram messaging is configured.

10.3.13.6.2 Example macros for sending messages to Telegram

Text message macro:

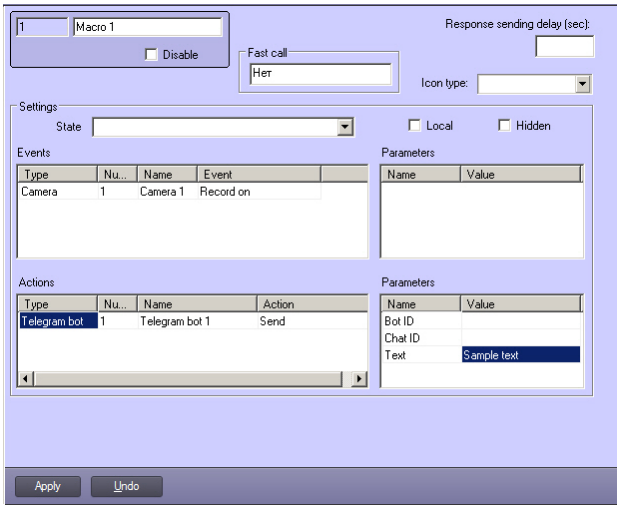
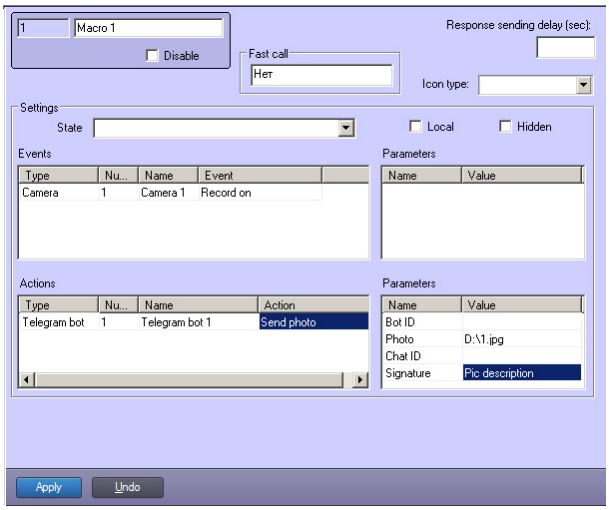


Image macro:



10.3.14 Replicating archive from unconnected servers using the removable storage

10.3.14.1 Order of archive replication from unconnected servers

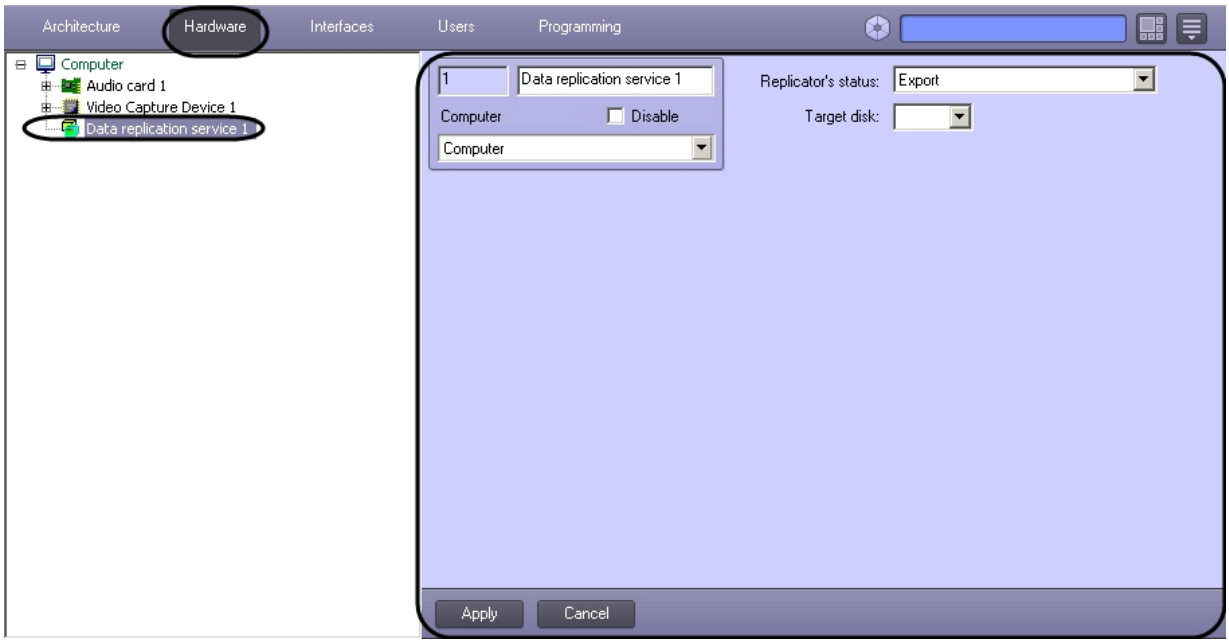
It is possible to receive video and audio archive from unconnected Servers in the *Intellect* software using the removable storage. Records over a specified period are copied from the Source-Server to the Target-Server while replicating archive.

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.

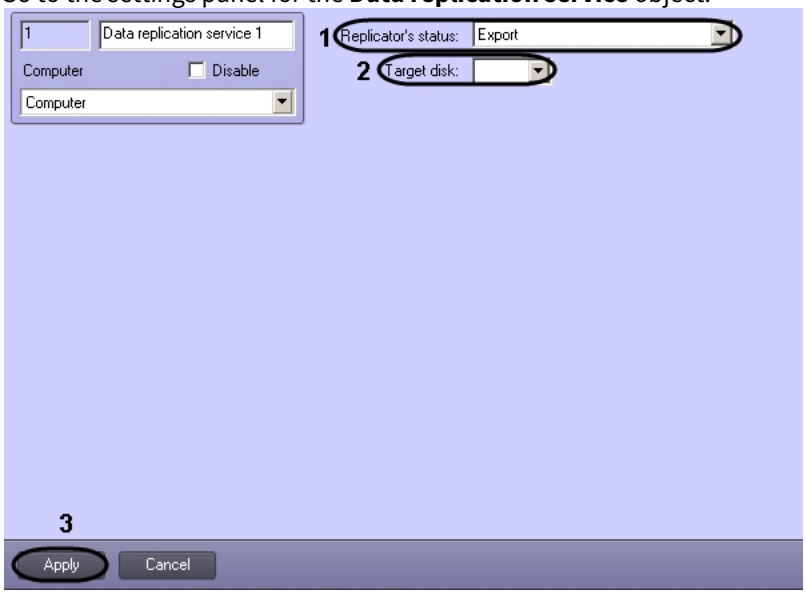
10.3.14.2 Configuring the Data replication service object

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.

10.3.14.3 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.

10.3.14.4 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**.

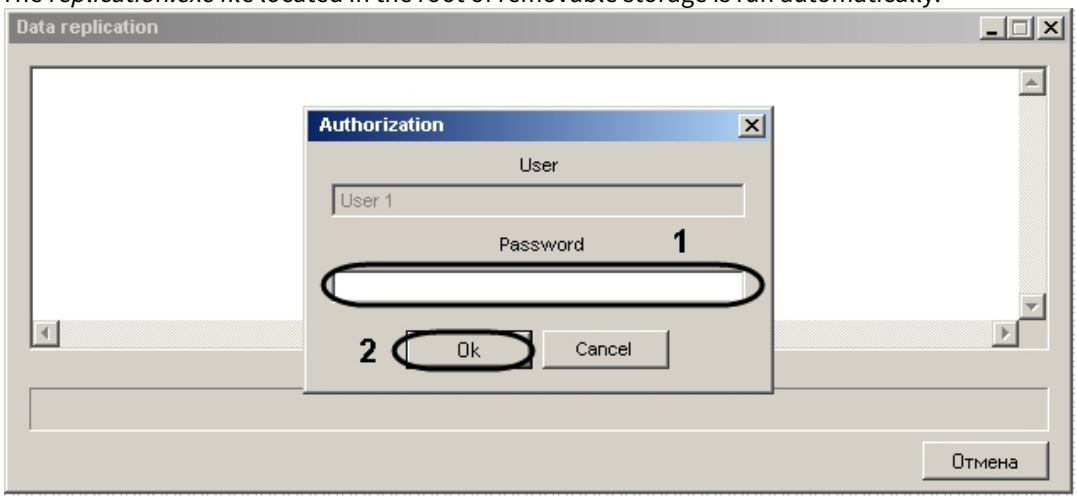
2. Corresponding rights are assigned to users (see Registration of users' rights section).
3. At least one **Camera** object is created in the Target hardware tree.

The query file is created using the *schedule.exe* utility (see The shedule.exe utility for creating a replication query file section).

10.3.14.5 Copying the archive from the Source

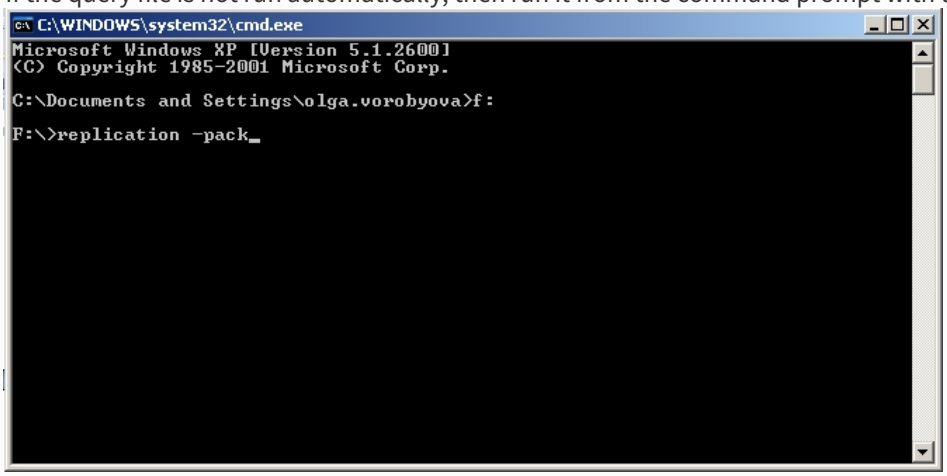
To copy the archive from the Source, do the following:

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.

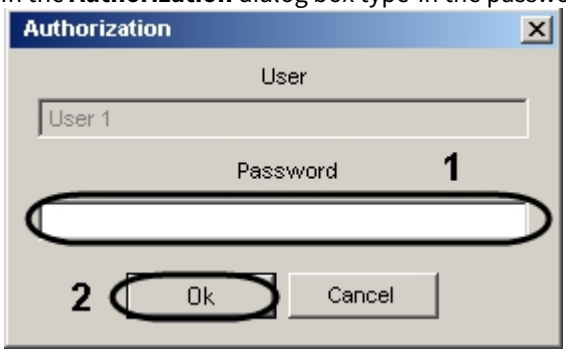


Note.

If the query file is not run automatically, then run it from the command prompt with the **-pack** parameter.

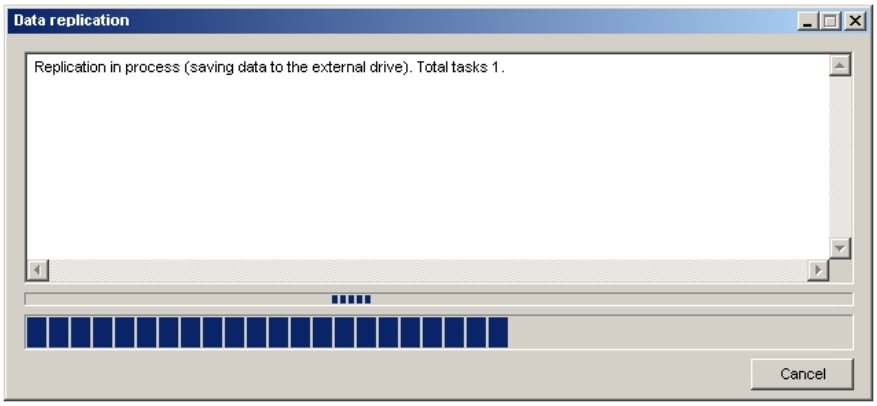


3. In the **Authorization** dialog box type-in the password of user who makes the replication (1).



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.

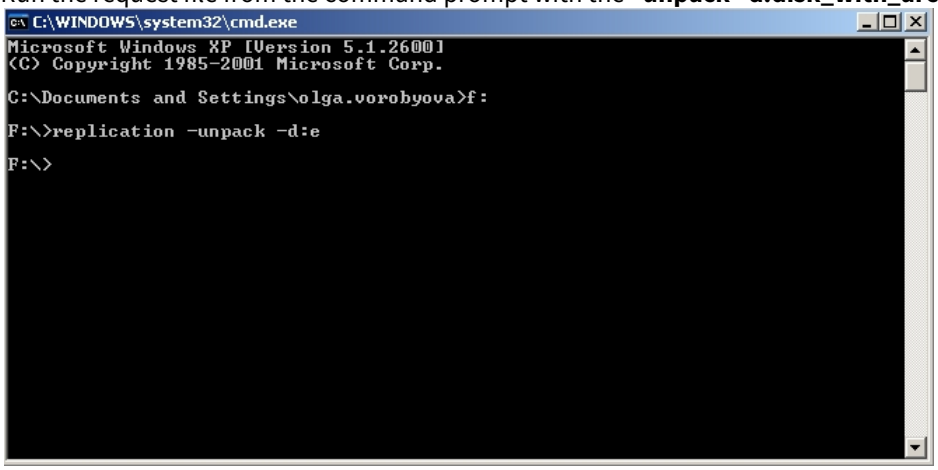
10.3.14.6 Restoring the archive on the Target

When the archive is restored data is copied from the removable storage to the Target.

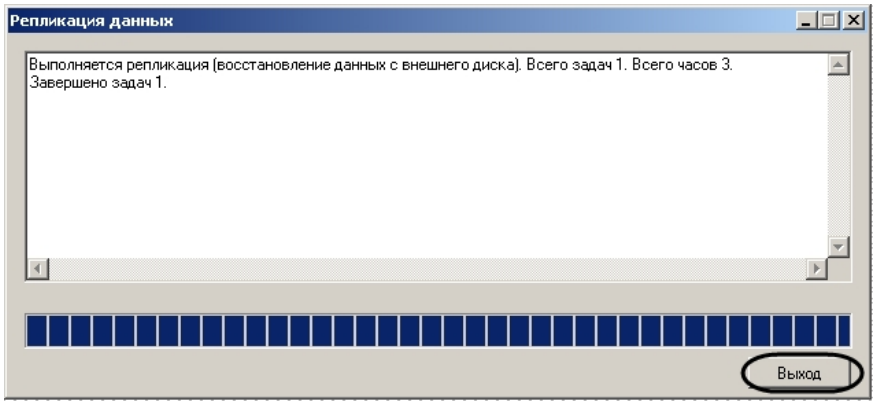
To restore the archive do the following:

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.

10.3.15 Configuring the Web-server module

10.3.15.1 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

10.3.15.2 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

10.3.15.3 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.

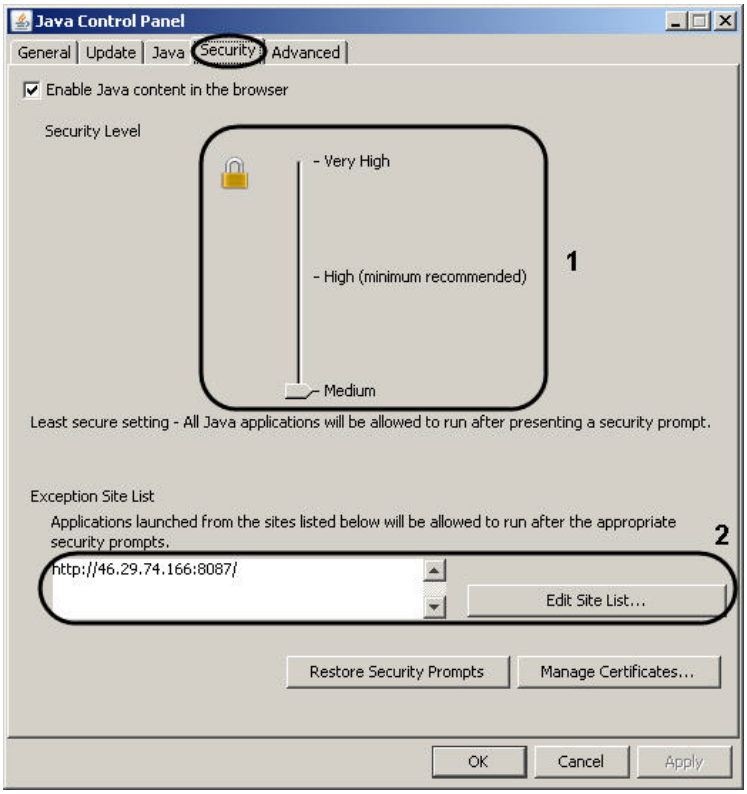
It is necessary to install Java Runtime Environment not in quiet mode. Otherwise the Intellect may not respond displaying two possible messages:

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).

10.3.15.4 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:

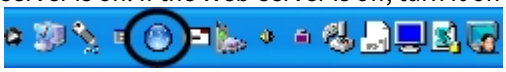
```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\
```

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

10.3.15.5 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.

10.3.15.6 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:

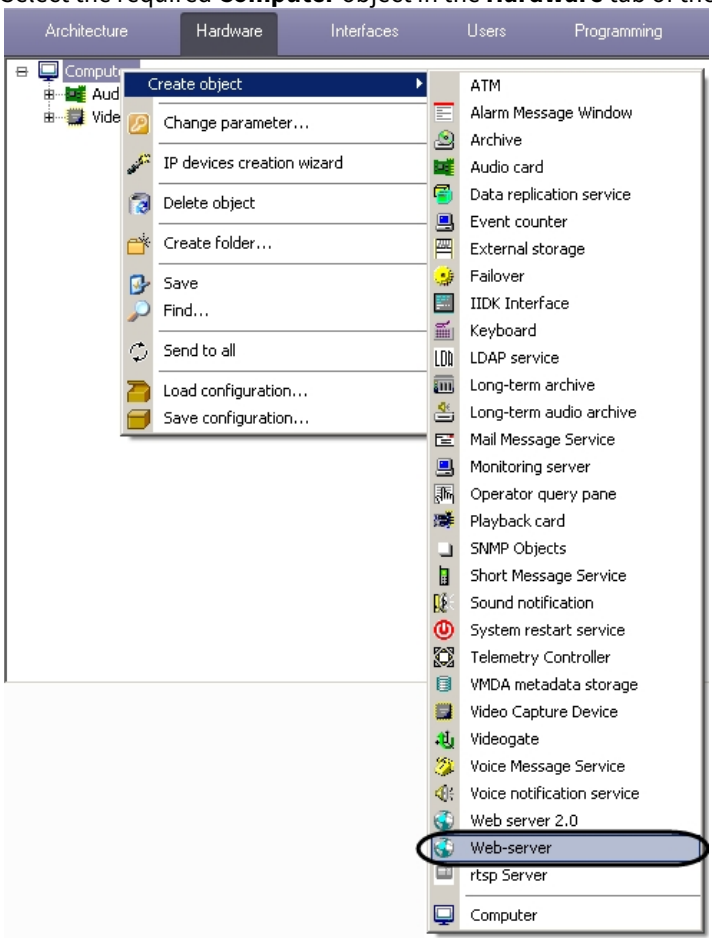
1. Create the **Web-server** object on the basis of the **Computer** system object (see Creating the Web-server object).
2. Select and configure cameras for displaying on the Web-server home page (see Selecting and configuring cameras for the Web-server module or Bulk selecting and configuring cameras 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

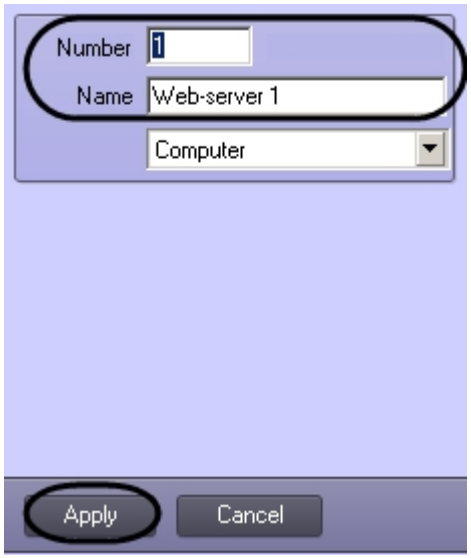
10.3.15.6.1 Creating the Web-server object

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.

10.3.15.6.2 Selecting and configuring cameras for the Web-server module

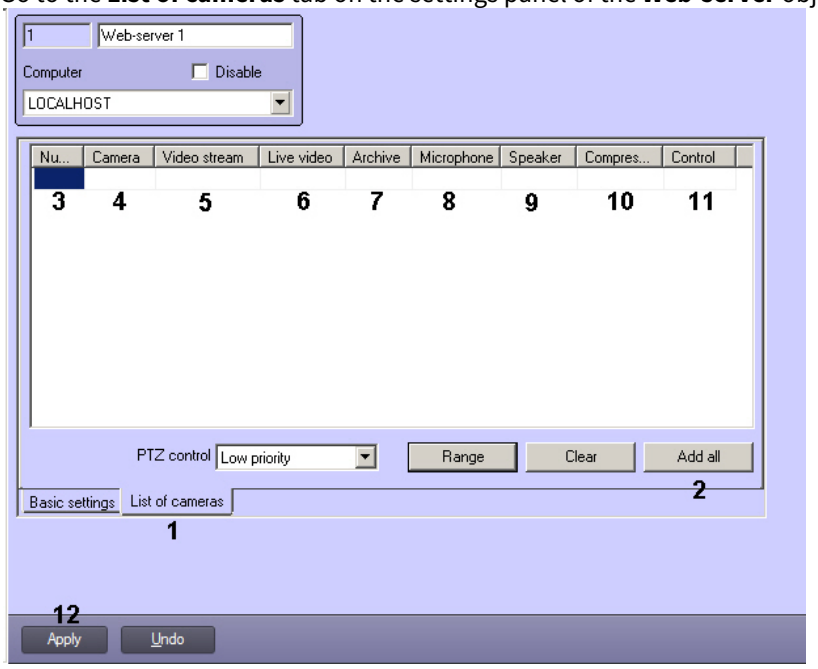
One can select and configure cameras for displaying on the **Web-server** home page in two ways:

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 for the clients connection 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.

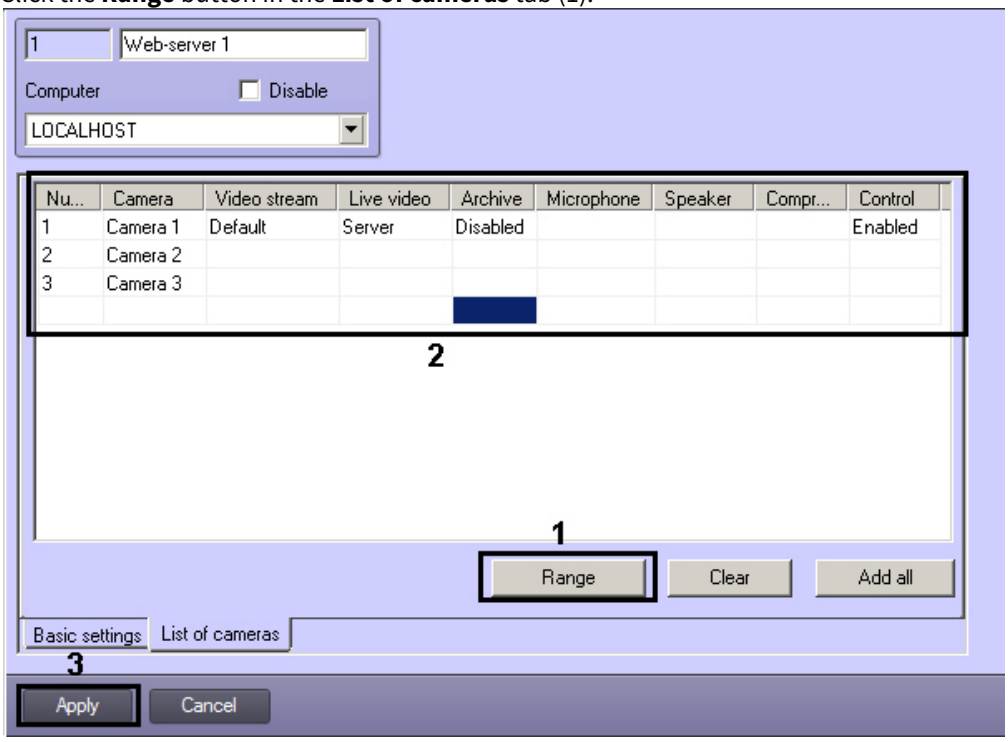
10.3.15.6.3 Bulk selecting and configuring cameras for Web-server

Parameters of cameras can be bulk selected and edited for displaying on the **Web-server** home page.

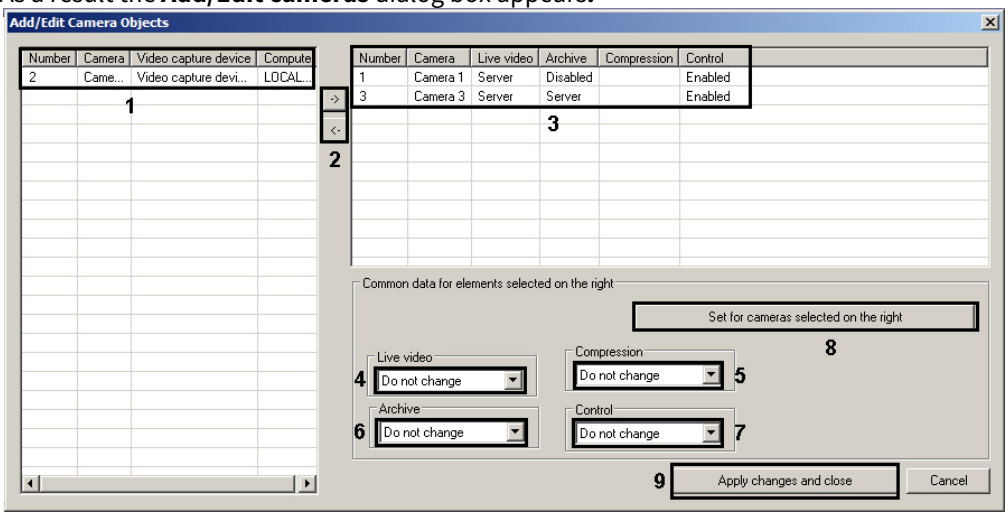
Bulk select cameras as follows:

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.

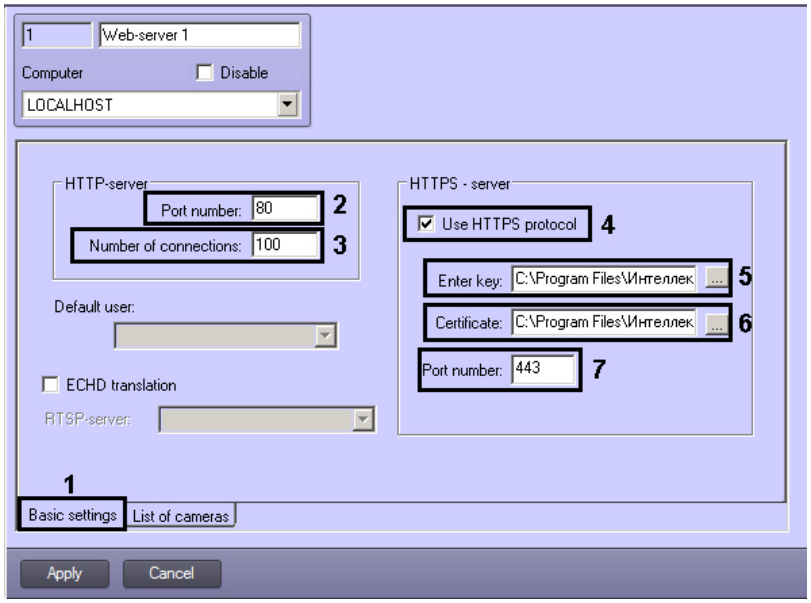
10.3.15.6.4 Setting the parameters of connecting Clients to the Web-server

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.

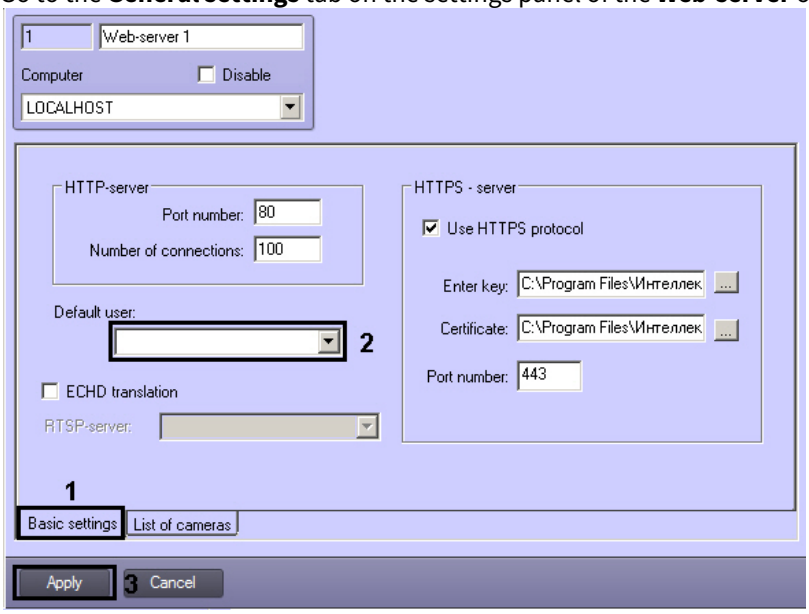
10.3.15.6.5 Configuring the authorization for the Web-server module. Default user

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.

10.3.15.6.6 Enabling the processing of SDC (ECHD) requests and selecting the RTSP server

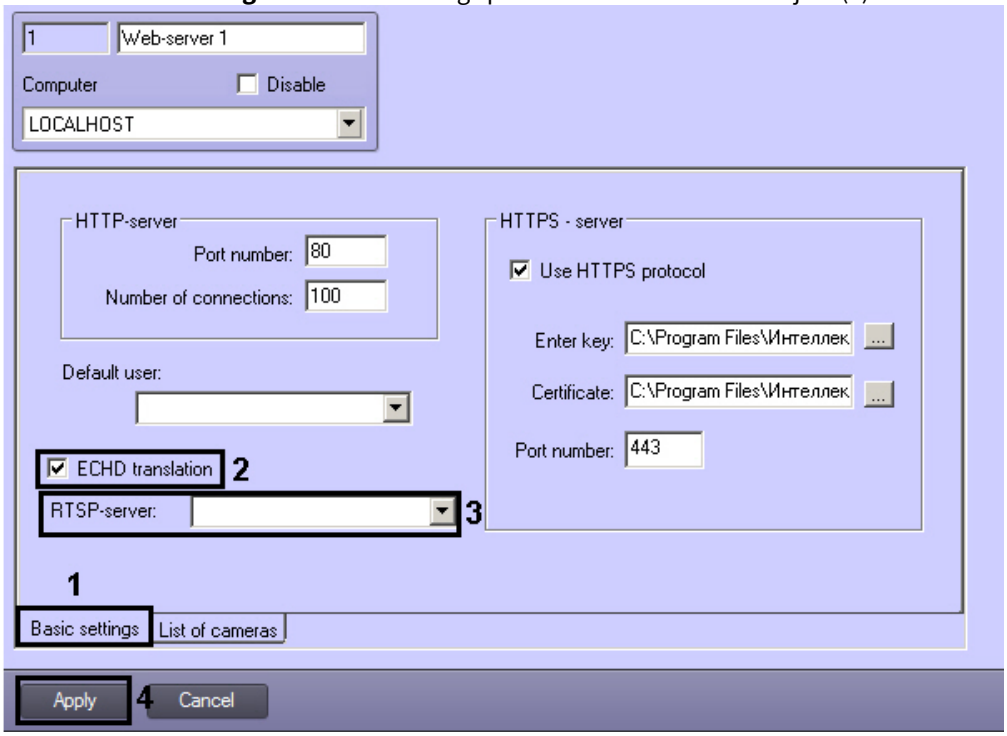
Integration with Single Data Center (ECHD) is supported in *Intellect*. Requests to *Intellect* are made in SDC using HTTP API – see Intellect HTTP API document. Some requests have http/https interface. These requests are used to get info on configuration. The **RTSP Server** bound to the **Web-server** 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 SDC 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 SDC 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 SDC, then to use the NAT address (4), set the **Use NAT address** checkbox to substitute the router address in the SDC 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.

10.3.15.6.7 Configuring PTZ control priority for Web-server

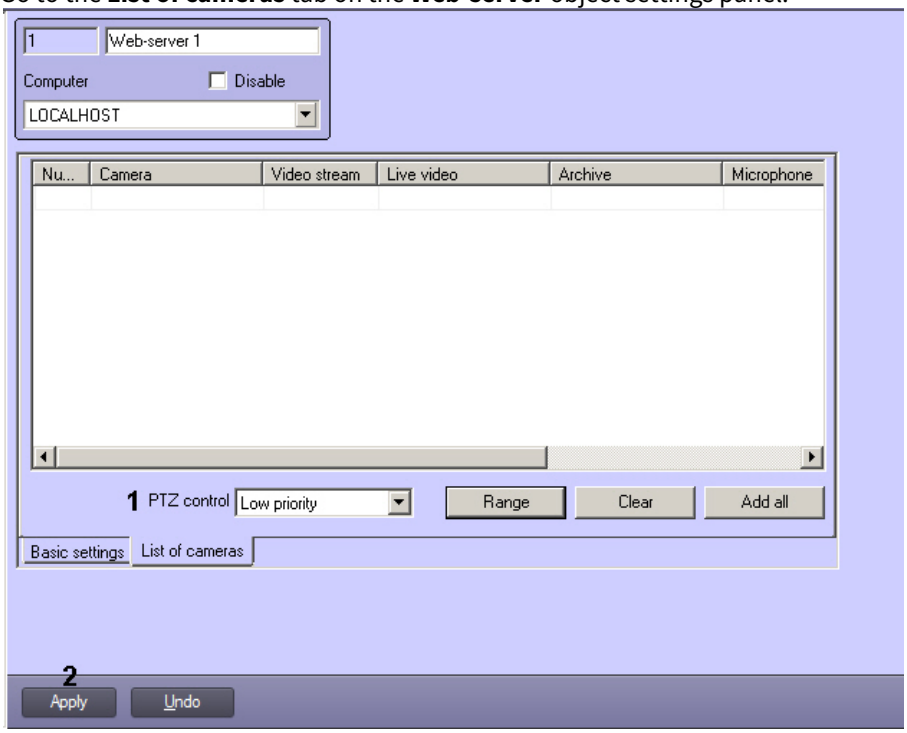
Intellect allows PTZ device control during video surveillance in web browser.

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.

10.3.15.7 Configuring the server for the clients connection via the Web-server 2.0 module

The *Web-server 2.0* module is designed 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).

The *Web-server 2.0* also provides the following functionality:

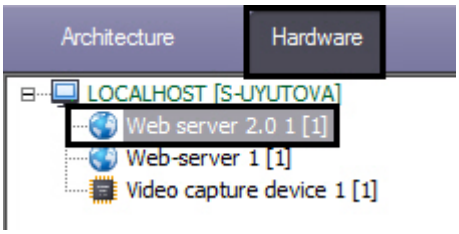
1. sending to the mobile client video and audio coming from the camera;
2. sending to the mobile client video and audio coming from the archive;
3. notification the user about the alarms;
4. execution of macros;
5. sending to the mobile client and processing alarms;
6. control of PTZ cameras;
7. working with maps;
8. sending push notifications to client.

> **Note.**
>
> Push notifications are sent to a client regardless of whether the client is connected to the Server. The Apple server is responsible for delivering notifications. The device on which the client is installed must be connected to the Internet.

The **Web-server** object are to be created and configured for correct operation of the *Web-server 2.0* module (see Configuring the videoserver to connect Clients via the Web-server module section).

10.3.15.7.1 Creating the Web-server 2.0 object

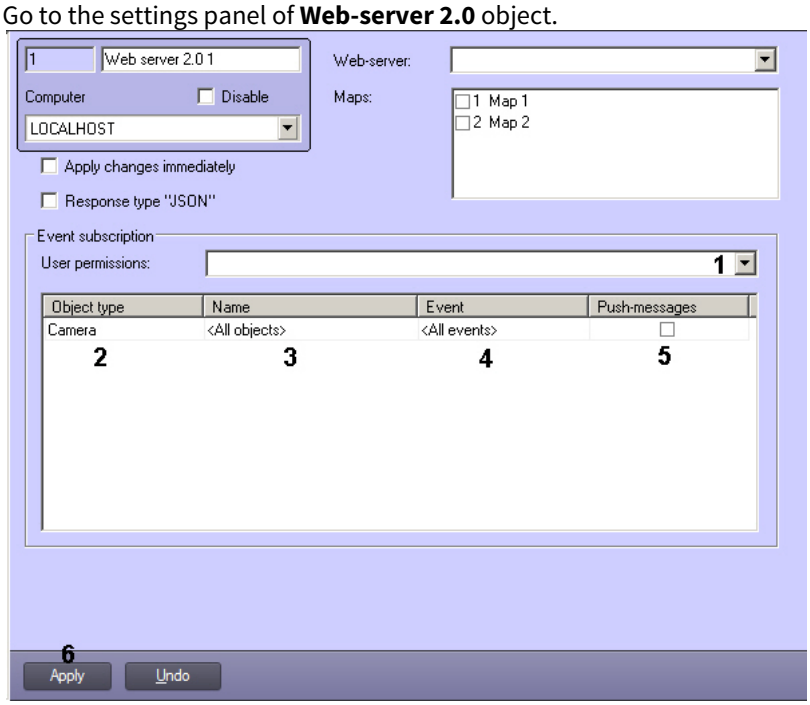
In the Intellect software the **Web-server 2.0** object is based on the **Computer** object on the **Hardware** tab of the **System settings** dialog box.



10.3.15.7.2 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 settings panel of **Web-server 2.0** object.



2. In the **User permissions** drop-down 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 the section 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 object of specified type from which the events are to be sended, if it is needed (3).
5. From the **Event** drop-down list select the type of event coming from objects of specified type which is to be sended (4).

6. If you want to authorize sending push notifications about events of the selected type to the mobile client, select the **Push notifications** check box (5). 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, notifications are not sent anywhere when a relevant event occurs.

7. Repeat steps 2 – 6 for all required objects and events.
8. Click the **Apply** button to save settings in the Intellect software (4).

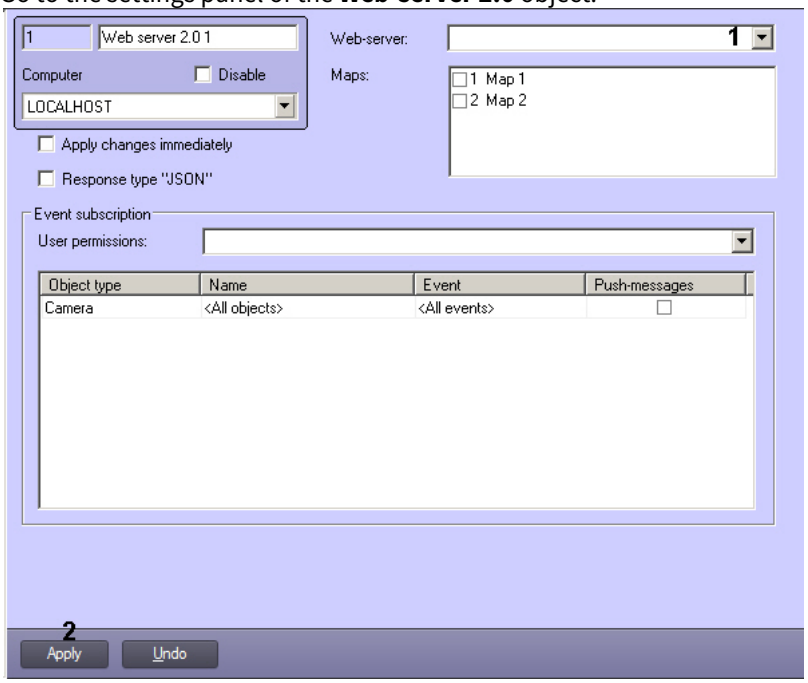
Configuration of the event filter for the Web-server 2.0 module is completed.

10.3.15.7.3 Using the Web-server settings for the Web-server 2.0 module

The **Web-server** object is to be created and configured for correct working of *Web-server 2.0* module.

Binding the **Web-server 2.0** to the **Web-server** is performed 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.

10.3.15.7.4 Selecting maps

Maps are to be selected in *Web-server 2.0* in order to function on the mobile client. Objects are to be created in the hardware tree and added to the map. If an object is added to the map after the map is selected for the *Web server 2.0* module, restart *Intellect* or *Web server 2.0* module in order to make such object available in a mobile client.

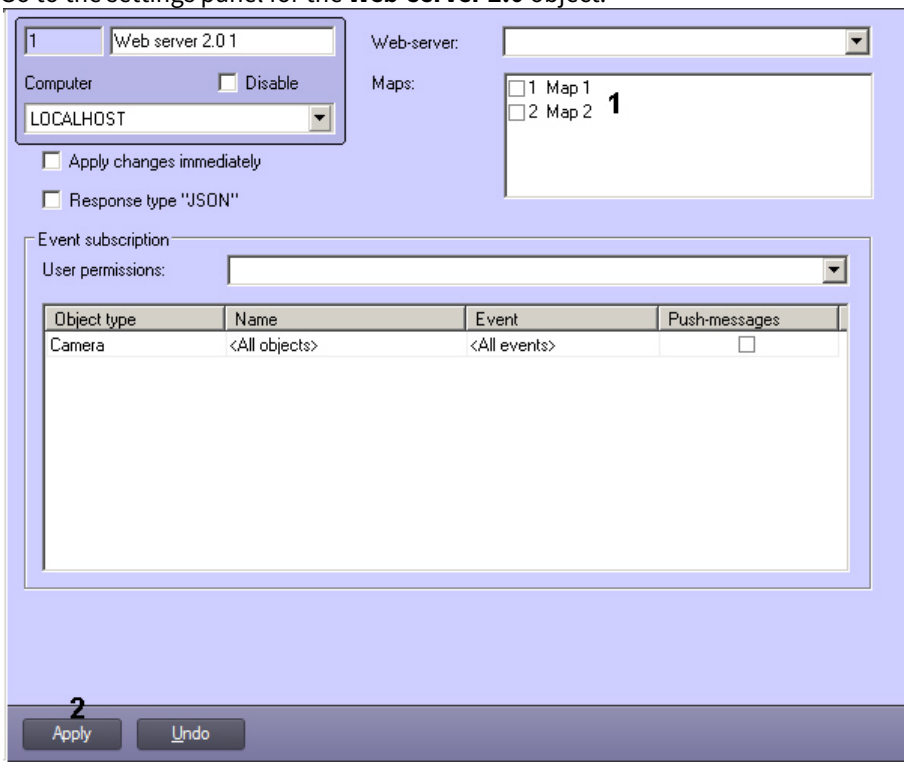
Creation and configuration of maps is described in Configuring the interactive map for object state indication and controlling the objects.

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 objects.

To select maps for *Web-server 2.0*, do the following:

1. Go to the settings panel for the **Web-server 2.0** object.



2. Set check boxes next to required **Map** objects (1).
3. Click the **Apply** button (2).

Maps are now selected.

10.3.15.7.5 Applying changes of the user rights

In *Intellect* by default when user rights are changed (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 app operates as before.

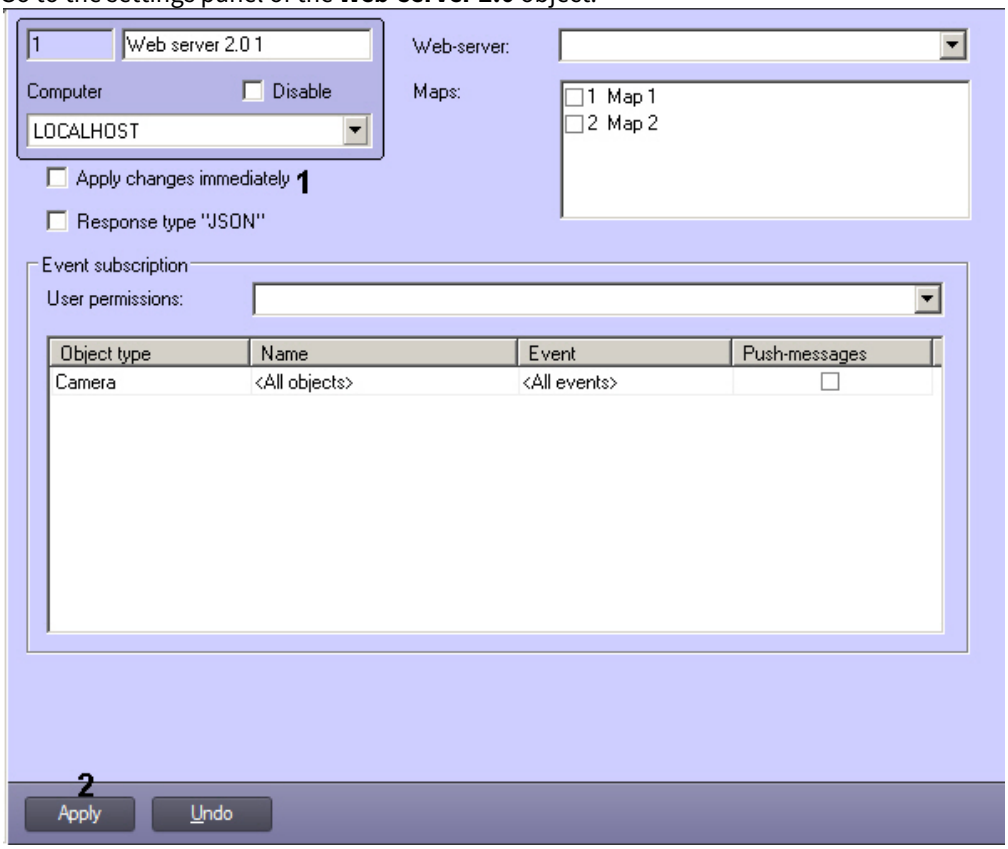
It is possible to enable the **Apply changes immediately** feature. *Web-server 2.0* module will immediately apply these changes of user rights.

Note.

This feature is not to be used in the large distributed systems.

Enable the **Apply changes immediately** feature as follows:

1. Go to the settings panel of the **Web-server 2.0** object.



2. Set the **Apply changes immediately** checkbox checked (1).
3. Click the **Apply** button (2).

The **Apply changes immediately** feature is now enabled.

10.3.15.7.6 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.

10.3.15.7.6.1 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.

10.3.15.7.6.2 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:

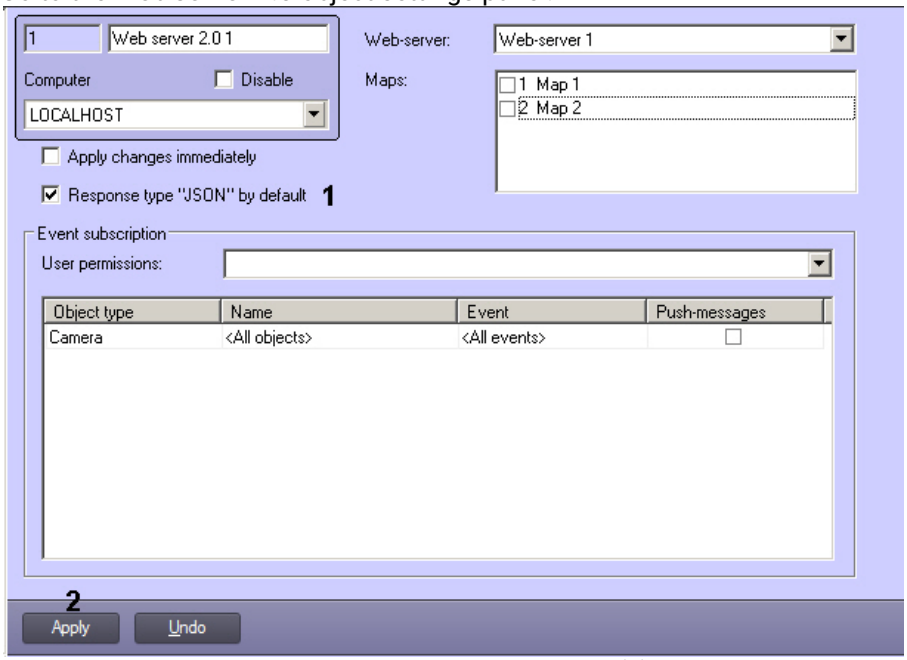
1. Open the **start_86.bat** or **start_64.bat** file.
2. Set the **jetty.port** value to the required port number.
3. Save changes to the **start_86.bat** or **start_64.bat** file.

Changing the port for the Web Server 2.0 module is complete.

10.3.15.7.7 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 XML format (see Intellect HTTP API). To enable JSON response by default, do the following:

1. Go to the **Web server 2.0** object settings panel.



2. Set the **Response type "JSON" by default** checkbox (1).
3. Click **Apply** (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.

10.3.15.8 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.

Parameter name	Possible values	Default value	Description
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.
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.

10.3.15.9 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.

10.3.15.10 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.

10.3.15.11 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.*****.ru: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.*****.ru address.
3. For Java applet to receive the signal from http://www.*****.ru: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.*****.ru: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.*****.ru/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.

10.3.15.12 Change of certificates of push-notifications for the Web-server 2.0 module

Existence of special certificate from the Apple which is given to the ITV|AxxonSoft company and valid for a year is required for working of push-notifications functional of the Web-server 2.0 module. Replace certificate if it is expired.

Updating of push-notifications certificate is performed as follows:

1. Download current web2.war file.
2. Copy this file to the \Modules\Jetty\webapps folder in the *Intellect* installation directory.

Updating of push-notifications certificate is completed.

10.3.16 Configuring RTSP Server module

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.

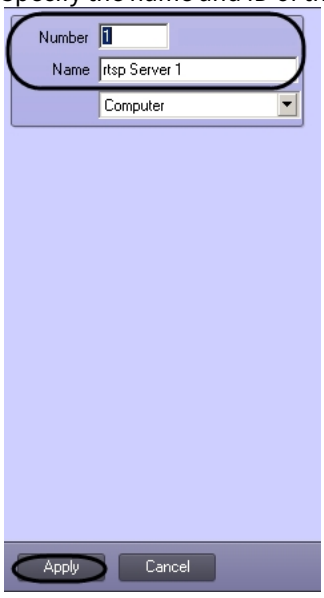
If there is sound with live video or the archive is recorded with sound, then video broadcast with sound through **RTSP Server** is supported – for this specify the ID of microphone from which the archive is recorded when requesting video (see the table with requests examples). For proper operation of 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).

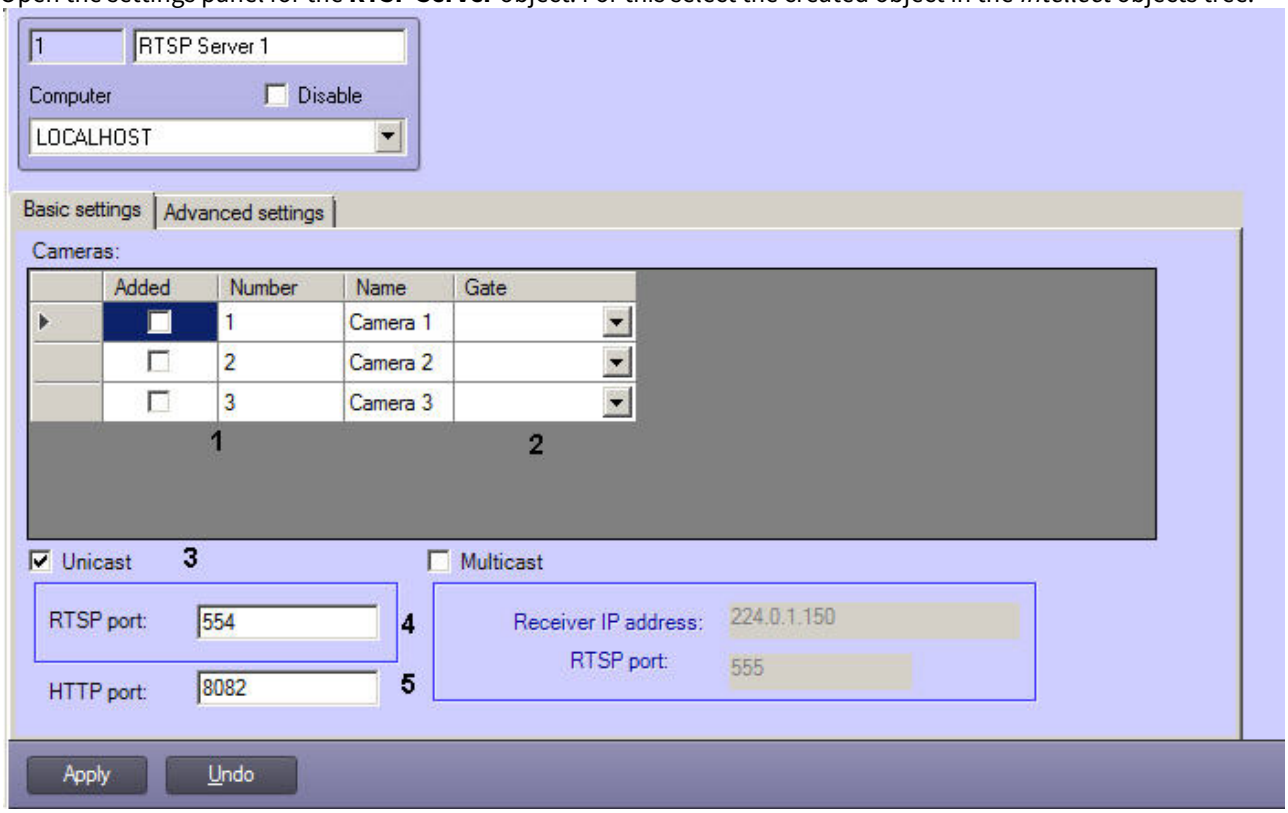
Create and configure the **RTSP Server** object as follows:

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.



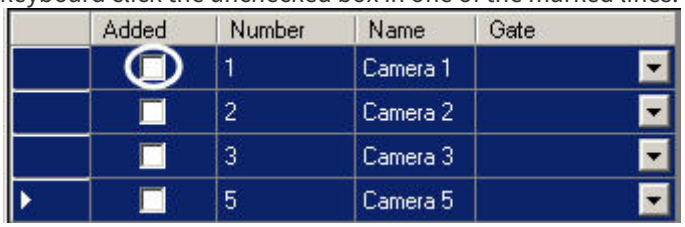
3. Click the **Apply** button to create the object.

4. Open the settings panel for the **RTSP Server** object. For this select the created object in the *Intellect* objects tree.



5. 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.

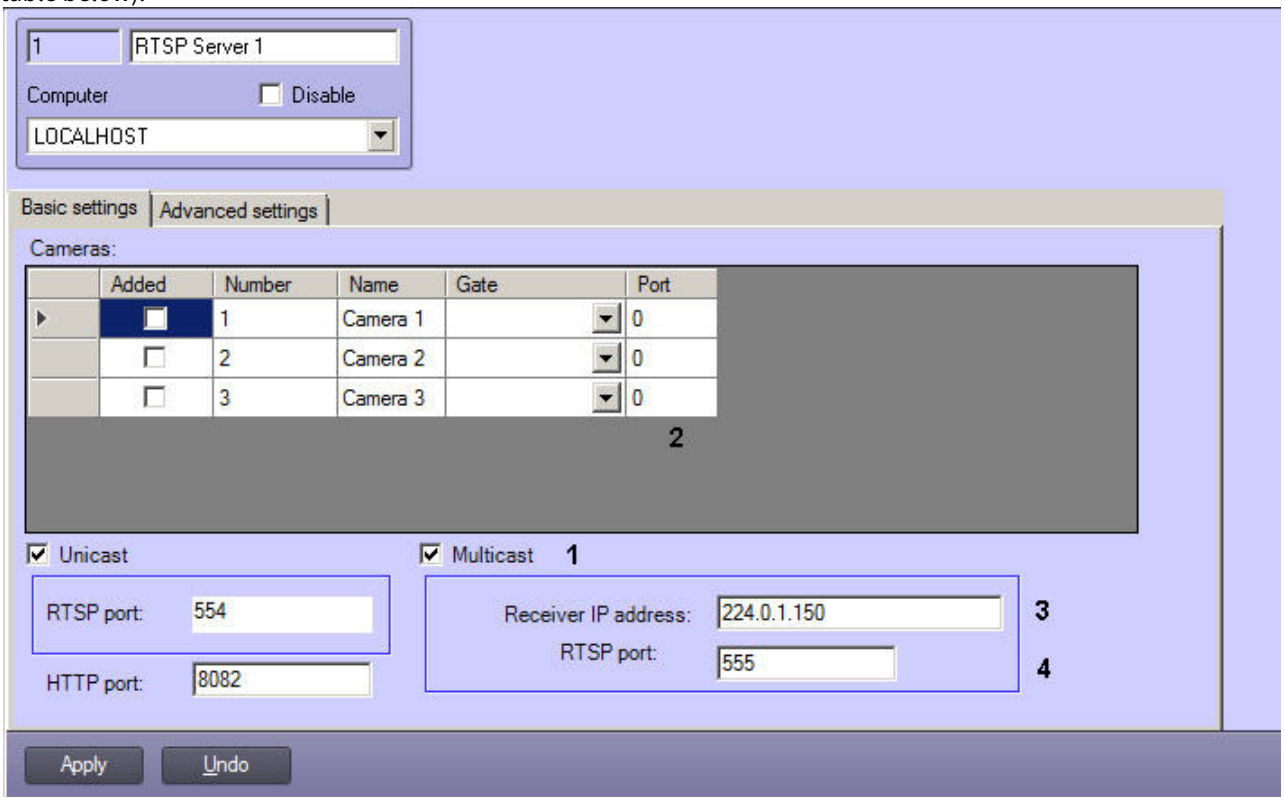
> **Note.**
>
> To select several cameras at the same time, mark lines in the table and then holding down the Ctrl key on the keyboard click the unchecked box in one of the marked lines.
>
> 
>
>
> As a result all selected lines will be set checked.
> To uncheck several boxes at the same time, do the same, but click the checked box after the selection of the lines.

6. 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).
7. Set the **Unicast** checkbox checked if signals from all cameras are to be broadcast through one port (3).
8. In the **RTSP port** field specify the port via which the video is transmitted (4).

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.

9. In the **HTTP port** field specify the port that is to be used for transmitting video via http-protocol (5).
10. To distribute transmitted signal among different RTSP-ports set the **Multicast** checkbox (1). In the **Cameras** table the **Port** column is displayed (2), in which it is necessary to specify a data transmission port for each video camera. 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).



Note.

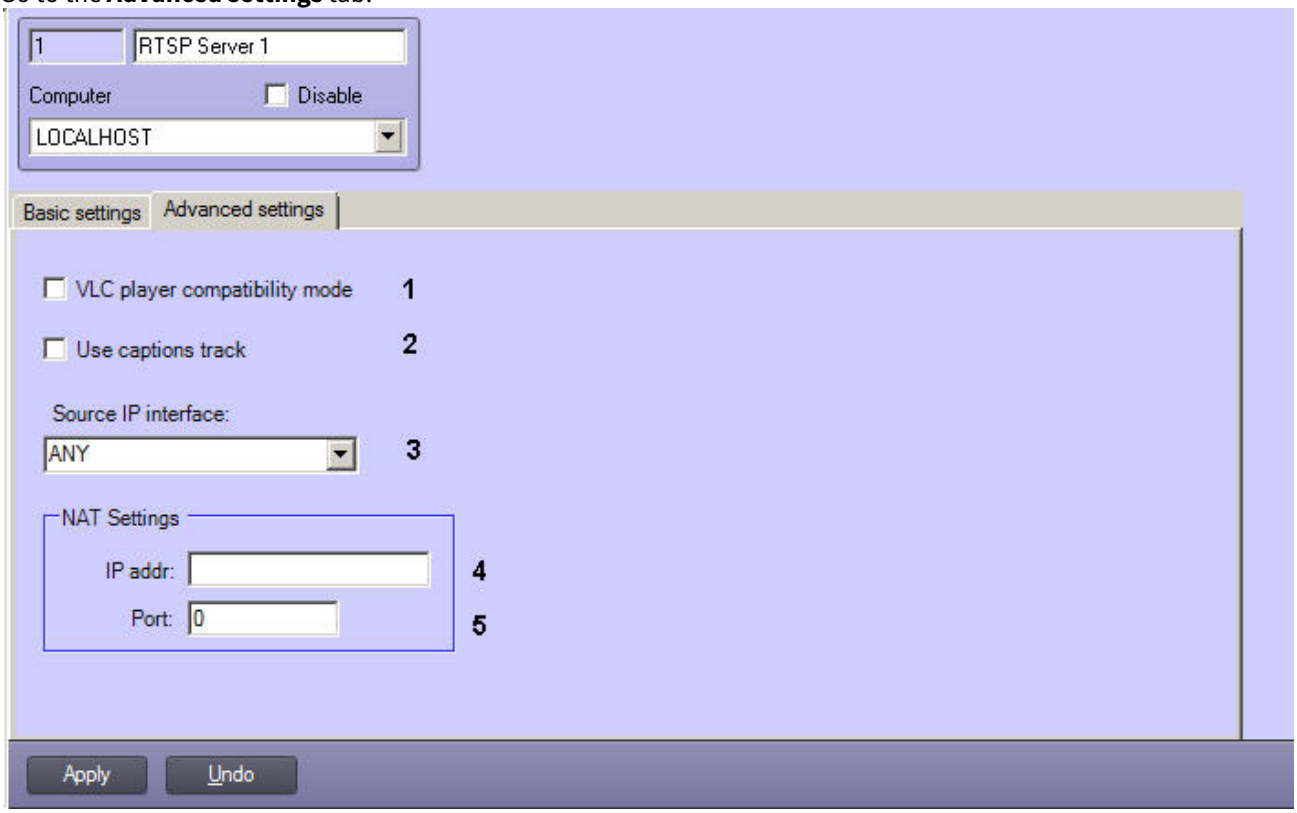
Use of the **Multicast** mode allows decreasing Server load due to reduction of transmitted data

Note.

To get such 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. Detailed information on this parameter see in Changing the transport protocol used by IP-device section.

> **Note.**
>
> **RTSP Server** can translate both in **Multicast** and **Unicast** modes simultaneously. Receiving both these streams on the *Intellect* client is impossible due to RTSP key defining the mode (see the note above). However, the VLC player allows receiving streams in both modes in the same time.

11. 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.
12. 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.
13. Go to the **Advanced settings** tab.



14. 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.
15. 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.

Important!

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.

16. 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).
17. 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 addr** 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.
18. Click the **Apply** button to save the changes.

The **RTSP Server** object is now configured.

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:

Address	Example	Description
rtsp://Server IP address[:Port]/ CameraNo[?stream_id=StreamNo]	rtsp://127.0.0.1/1	Viewing default stream from Camera 1 if default port is in use.
	rtsp://127.0.0.1:555/1	Viewing default stream from Camera 1 when broadcasting in **Multicast** mode if default port 555 is in use. *Note. Connection to the RTSP stream is performed via the broadcasting adapter IP-address, not by the destination IP which is specified in the settings panel of the **RTSP Server** and is used internally.*
	rtsp://127.0.0.1:555/7?stream_id=7.2	Viewing second stream from Camera 7.
rtsp://Login:Password@Server IP address[:Port]/CameraNo	rtsp://login:pass@127.0.0.1:554/1	Viewing video signal from Camera 1 if users and permissions are configured in *Intellect* (see Rights administration).
	rtsp://login:pass@127.0.0.1:555/1	Viewing video signal from Camera 1 in **Multicast** mode if users and permissions are configured in *Intellect.*
rtsp://Server IP address[:Port]/ CameraNo**?mic_id=**Microphone ID	rtsp://127.0.0.1:555/15?mic_id=1	Viewing video from Camera 15 with sound.
rtsp:// Server IP address[:Port]/**?mic_id=** Microphone ID	rtsp://127.0.0.1:555/?mic_id=1	Getting sound only from microphone 1 with no video from any camera.
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/archive?id=1&time_begin=2011.11.11-11:11:11&&time_end=2011.11.11-11:12:00	Viewing video archive from Camera 1 for specified time period.

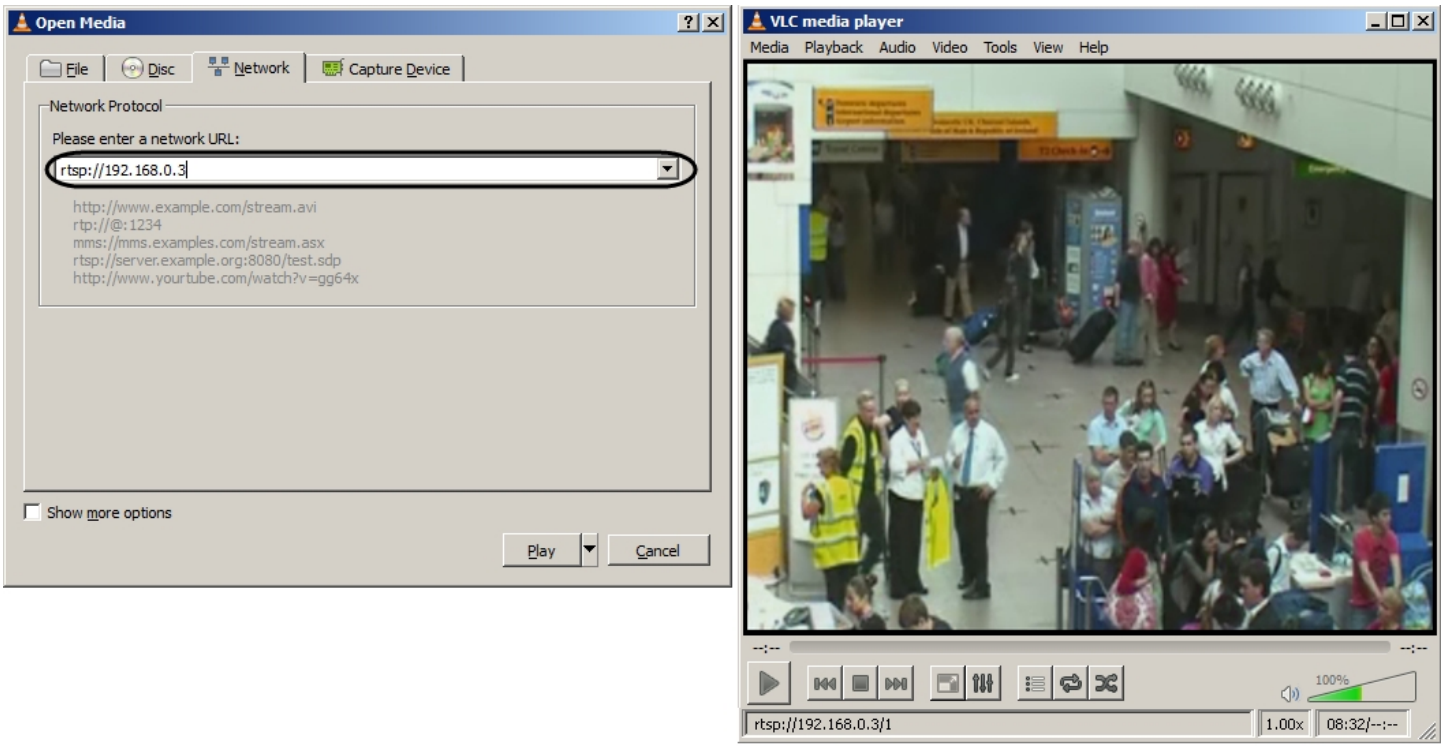
rtsp:// Server IP address[:Port]/ **archive?id=**CameraNo**&mic_id=** Microphone ID **&time_begin=**yyyy.mm.dd-hh:mm:ss**&&time_end=** yyyy.mm.dd-hh:mm:ss	rtsp://127.0.0.1:554/archive?id=1&mic_id=1&time_begin=2011.11.11-11:11:11&&time_end=2011.11.11-11:12:00	Viewing video archive from Camera 1 with sound from microphone 1 for specified time period.
rtsp://Server IP address[:Port]/ **archive?id=**CameraNo.**&time_begin=**yyyymmddThhmmssZ**&time_end=**yyyymmddThhmmssZ	rtsp://127.0.0.1:555/archive?id=1&time_begin=20160331T080000Z&time_end=20160331T080800Z	Viewing video archive from Camera 1 for specified time period.
rtsp://Server IP address[:Port]/ **archive?id=**CameraNo.**&time_begin=**yyyymmddThhmmssZ	rtsp://127.0.0.1:555/archive?id=4&time_begin=20160316T065000Z	Viewing video archive from Camera 4 from specific start time till the archive end (as the value of time_end is not specified in the address).
rtsp://Server IP address[:Port]/ **archive?id=**CameraNo	rtsp://127.0.0.1:555/archive?id=4	Viewing video archive from Camera 4 from the beginning till the end.
rtsp://Server IP address[:Port]/ **archive**?**id**=CameraNo.**&long_term_archive**=BackupArchiveNo	rtsp://127.0.0.1:559/archive?id=1&long_term_archive=2	Viewing Camera 1 video archive from Backup archive 2.
rtsp://Server IP address[:Port]/ **archive?id=**CameraNo.**&gate**=VideogateNo	rtsp://127.0.0.1:559/archive?id=1&gate=3	Viewing Camera 1 video archive from Video gate 3.
rtsp://Server IP address[:Port]/ **archive?id=**CameraNo.**&time_begin=**yyyymmddThhmmssZ**&time_end=**yyyymmddThhmmssZ**&z**=PlayBackSpeed	rtsp://127.0.0.1:554/archive?id=2&time_begin=20171120T102000Z&time_end=20171120T104000Z&z=-1	Speed-down playing back video archive of Camera 2 for the specified period of time. Value of z parameter greater than 0 (valid values are 2, 4, 6 ... 16) enables speed-up archive playback. If the parameter z is less than 0 (valid values are -1, -2, ... -16), then the archive is played back in the reverse order with the corresponding acceleration. Only key frames are played back at reverse playing.

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.



10.3.17 Counting the system events

10.3.17.1 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.

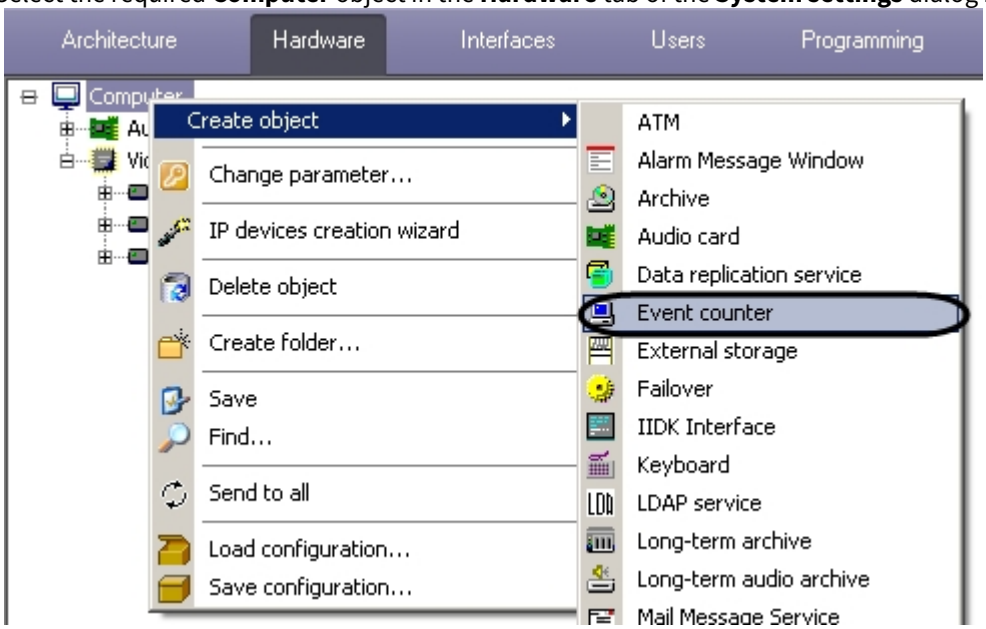
The start time for counting can be set manually, or automatically according to the last change of the **Events Counter** settings.

Besides, one **Events Counter** object allows setting a separate counter for each event.

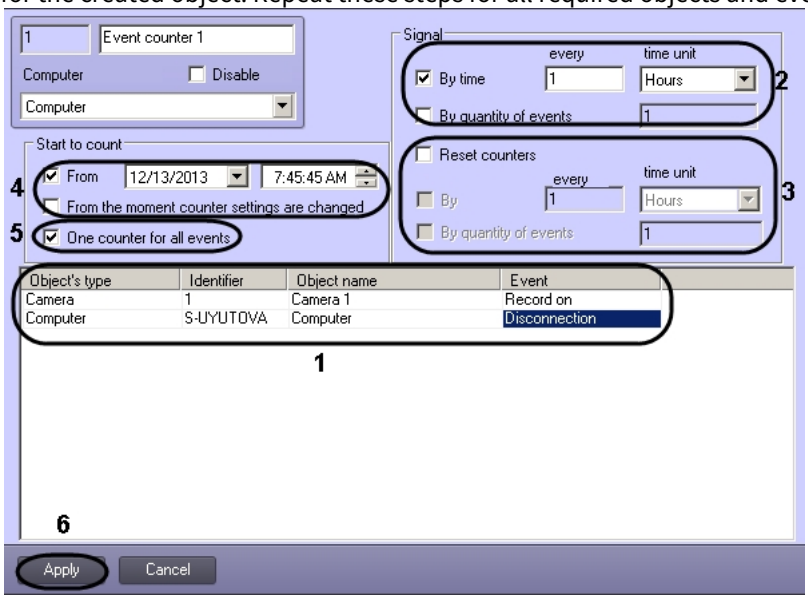
10.3.17.2 Configuring the Event Counter

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 ID column. Then, select an event in the **Event** column for the created object. Repeat these steps for all required objects and events (1).



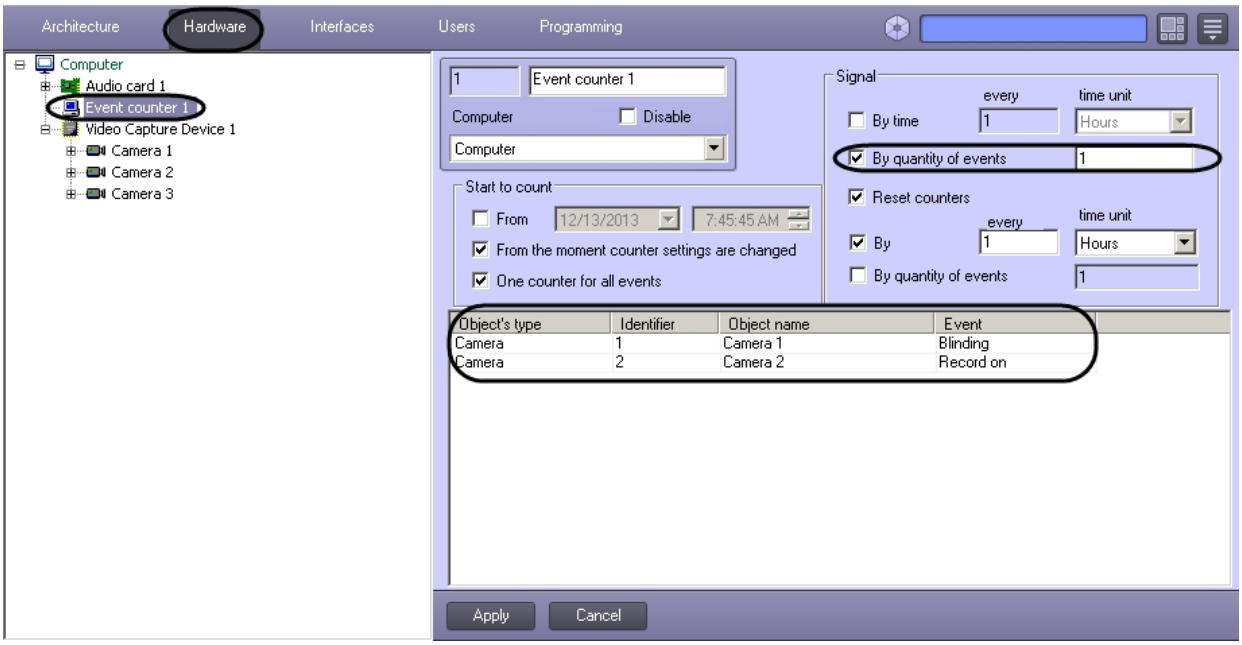
4. Select the notification mode and set the notification parameters (2).
5. Enable the counter reset option, if necessary. Select the reset mode and set the reset parameters (3).
6. Select the time setting mode and enter the date and time, if necessary (4).
7. Uncheck the option for individual events counting, if necessary (5).
8. Click **Apply** to save the settings (6).

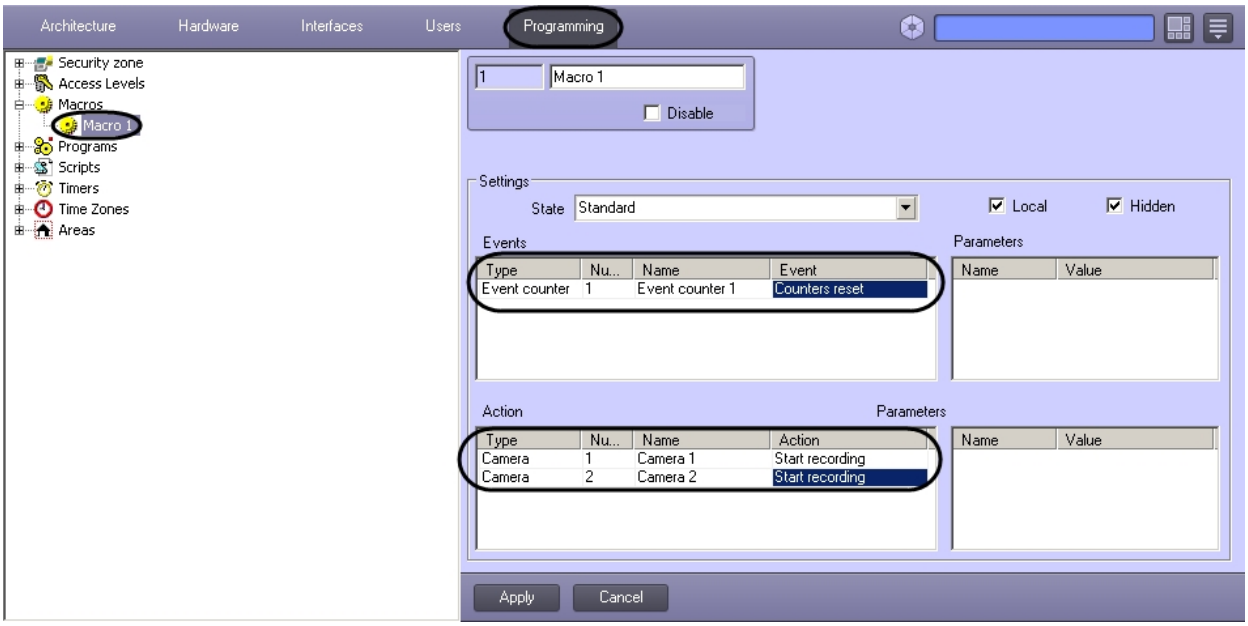
The **Event counter** is now configured.

10.3.17.3 Data output and counter control

The **Event Counter** object has no separate interface object for data input/output, thus it is used together with other objects. Usually, macros are used to control the counters.

Figures below show an example of using a counter in a macro.





The counter issues a notification (sends a “SIGNAL_POINT (Data collected)” message in any of the following cases: camera 1 blocked, camera 2 blocked, camera 1 connection lost, 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.

10.3.18 Configuring PS-RTP server

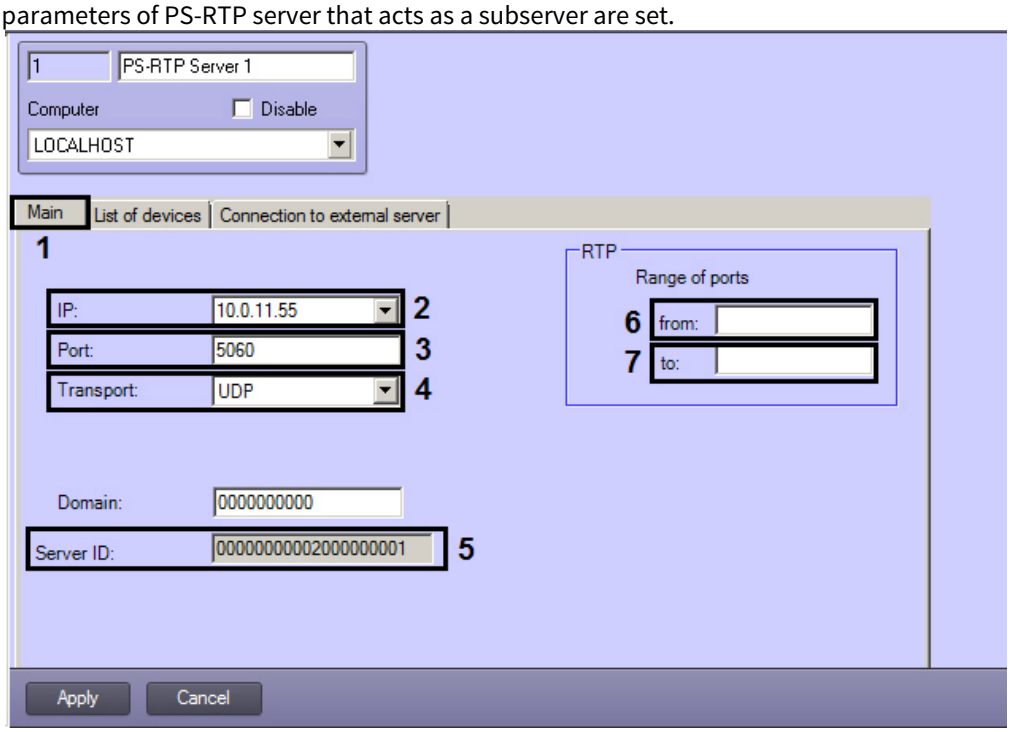
PS-RTP server enables the following functions in *Intellect*:

1. In the third-party software control cameras, PTZ, relays and sensors configured in *Intellect* using the GB28181 protocol.
2. Watch live and archived video in the third-party software.
3. According to user rights limit access to the functions listed above.

Intellect acts as a subserver in the server hierarchy. If Intellect is to act as a supserver, configure Connecting cameras via the GB/T28181 protocol.

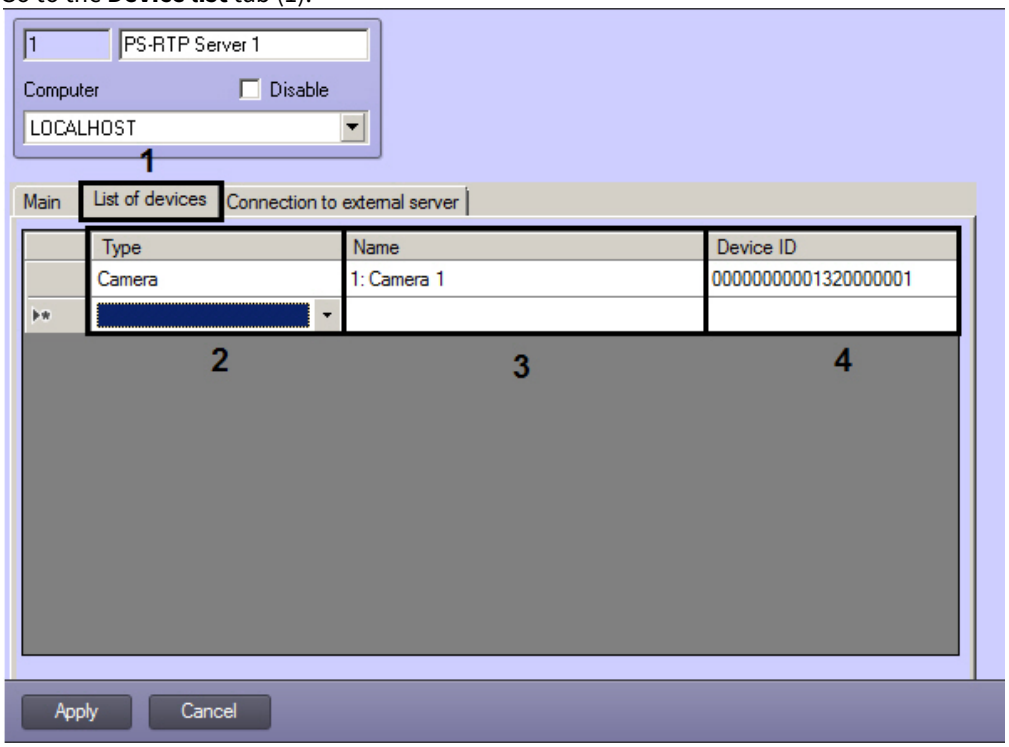
Configure PS-RTP server as follows:

1. Create a **PS-RTP server** object under the **LOCALHOST** object in the **Hardware** tab of the **System settings** dialog box.
2. The settings panel of the object is displayed in the **Main** tab on the right of the **System settings** dialog box (1). Here the parameters of PS-RTP server that acts as a subserver are set.



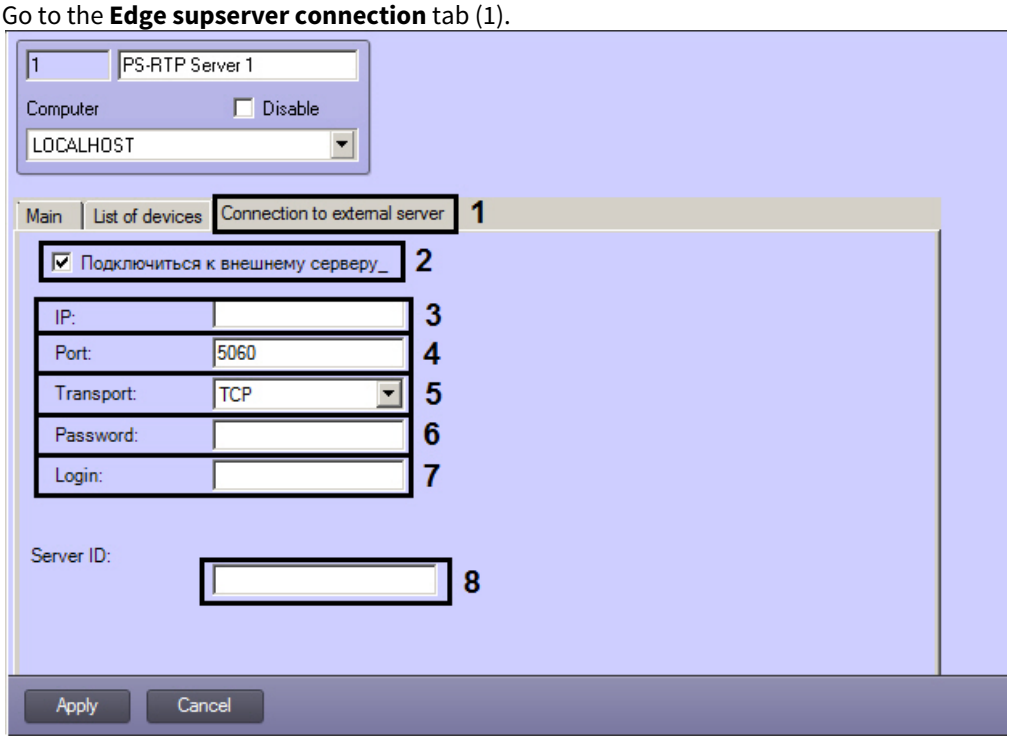
3. In the **IP:** dropdown list select the address of network interface via which the third-party software will access PS-RTP server using the GB28181 protocol (2).
4. In the **Port** field specify the number of port to which the third-party software will be connected using the GB28181 protocol (3).
5. In the **Transport** dropdown list select a data transfer protocol: UDP or TCP (4).
6. In the **Server ID** field the id of *Intellect* server is shown – it is used in the third-party software to connect to RS-RTP server via the GB28181 protocol (5).
7. In the **from:** (6) and **to:** (7) fields set the range of RTP ports used by the module.
8. Specify the list of objects the access to which is to be guaranteed by RS-RTP server as follows:

a. Go to the **Device list** tab (1).



b. In the **Type** dropdown list select the type of object created in the *Intellect* object tree (2).
c. In the **Name** dropdown list select the name of required object (3).
d. In the **Device ID** field the device id is shown – it will be used in the third-party software to control objects via the GB28181 protocol (4).
e. Repeat steps b-d for all required devices.

9. Set parameters to connect *Intellect* to edge supserver:
   a. Go to the **Edge supserver connection** tab (1).



   b. Set the **Edge server connection** checkbox checked (2). As a result edge server connection parameters are available for editing.
   c. In the **IP** field specify the edge server IP-address (2).

d. In the **Port:** field specify the edge server connection port (3).
e. In the **Transport** field select a transport protocol used for edge server connection (5).
f. In the **Login:** field specify the username for edge server connection (6).
g. In the **Password** field specify the password for edge server connection (7).
h. In the **Server ID** field specify the id of the edge server via the GB28181 protocol (8).
i. To save settings click the **Apply** button.

RS-RTP server is now configured.

10.3.19 Configuring ONVIF-Server module

10.3.19.1 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.

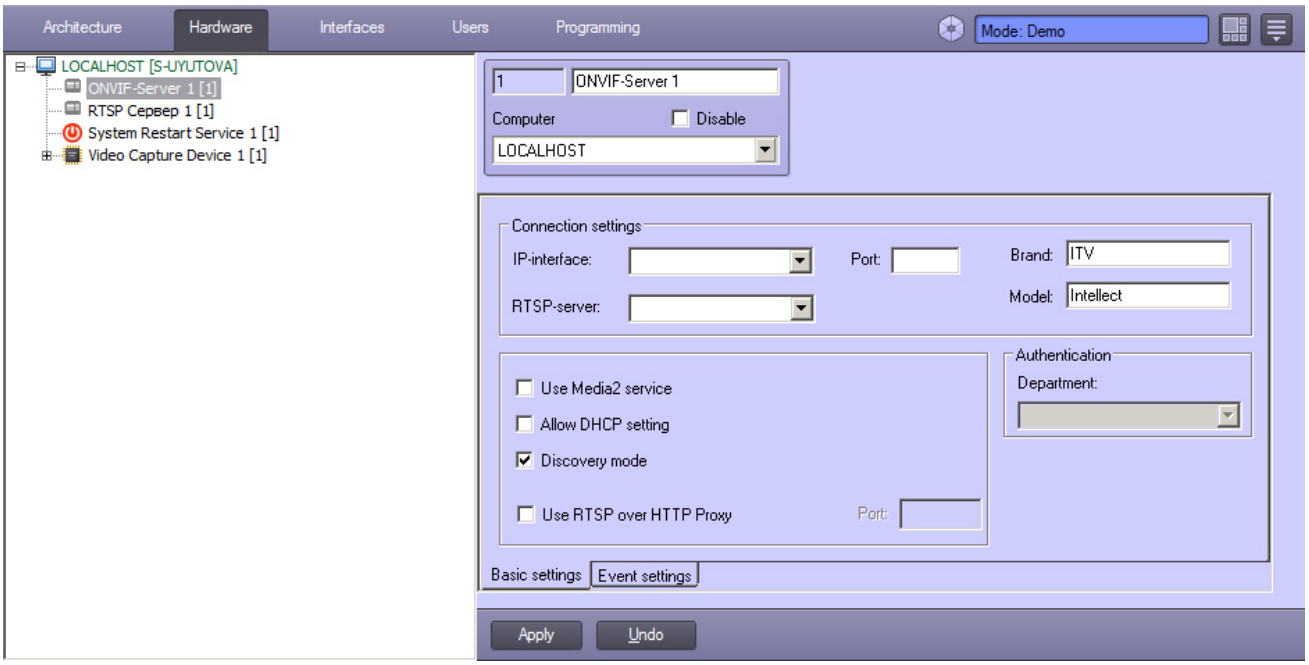
Video is also transmitted via *ONVIF Server* in the multistream mode.

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.

10.3.19.2 Configuring ONVIF-Server object

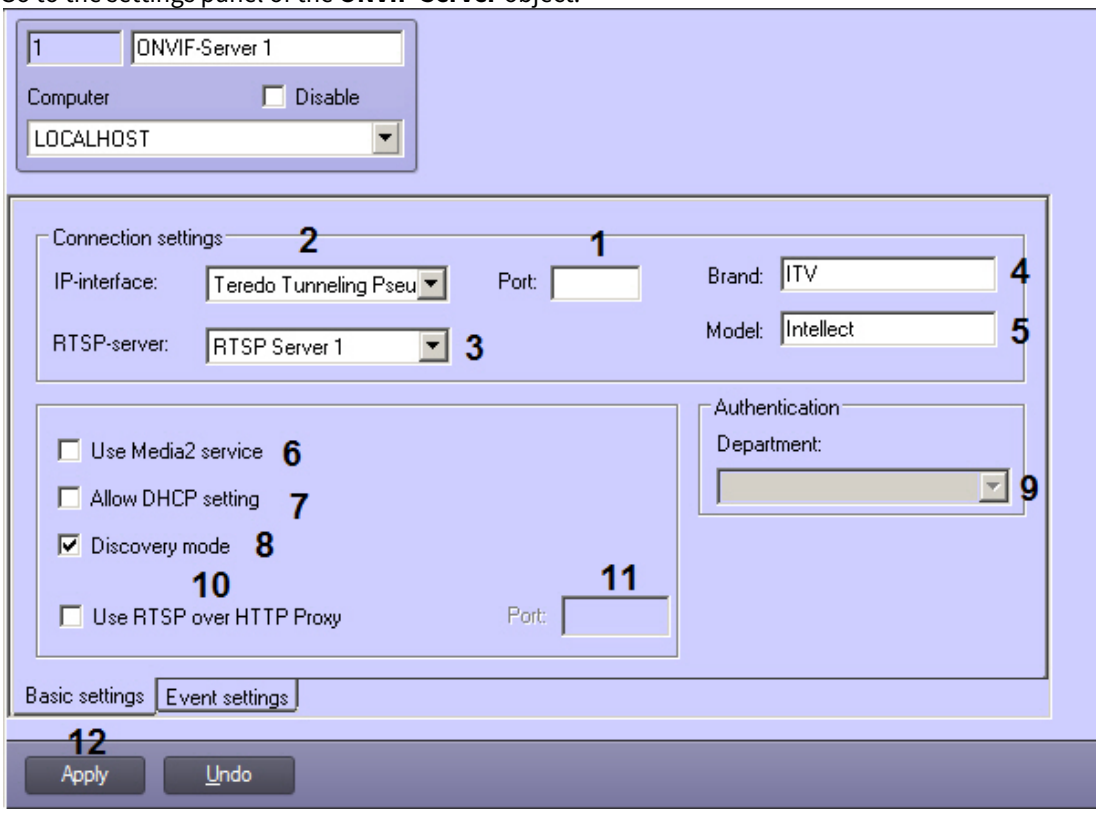
The **RTSP-Server** object is to be created and configured and all the required cameras are to be added to it before configuring the *ONVIF-Server* module - see Configuring RTSP Server module.

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** dropdown list (2).
4. In the **RTSP-Server** dropdown 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** dropdown list select the department where the users will be created when they are added via the *ONVIF-Server* interface (9).

   Note

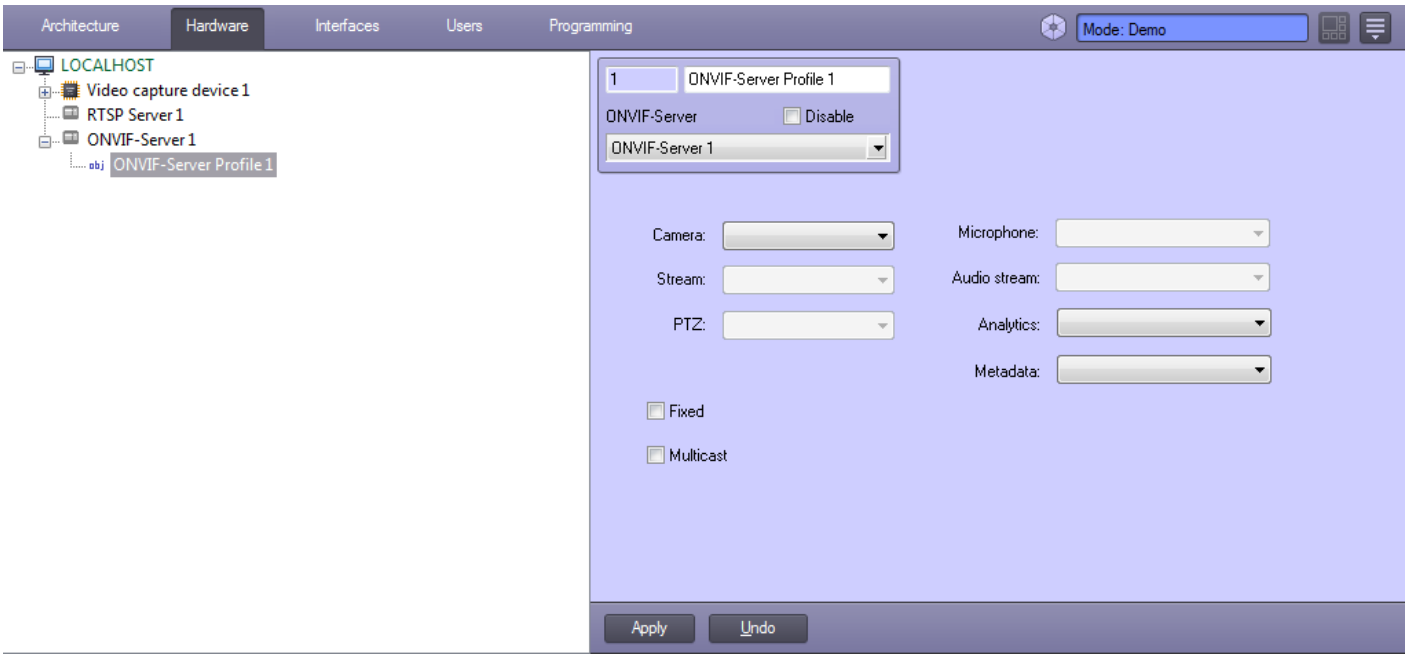
   Users are created in the *ONVIF-Server* interface using the third-party software, e.g., ONVIF Device Manager. The Administrator rights are required to create users – see Configuring rights to use ONVIF Server.

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. Click the **Apply** button (12).
    The **ONVIF-Server** object is now configured. Now it is possible to configure getting video using the *ONVIF-Server* module.

10.3.19.3 Configuring getting video using ONVIF-Server module

Getting video using *ONVIF-Server* module is configured in *Axxon Next.* Information on how to search and add IP devices to *Axxon Next* can be found in *Axxon Next.User Guide*. The latest version of this document can be found in AxxonSoft documentation repository.

After adding a camera to *Axxon Next*, 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 Next*.



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** dropdown 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 Next* the corresponding changes will be applied in *Intellect* too. For instance, if the microphone, analytics, metadata transmission and sensor/relays are enabled in *Axxon Next*, 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 Next* 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 Next* only after the *Axxon Next* Server is restarted or when the camera is deleted and added to *Axxon Next* 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.

10.3.19.4 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 Next* 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 Next* 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 Next* 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 Next* and the third-party software can be found in the corresponding documentation.

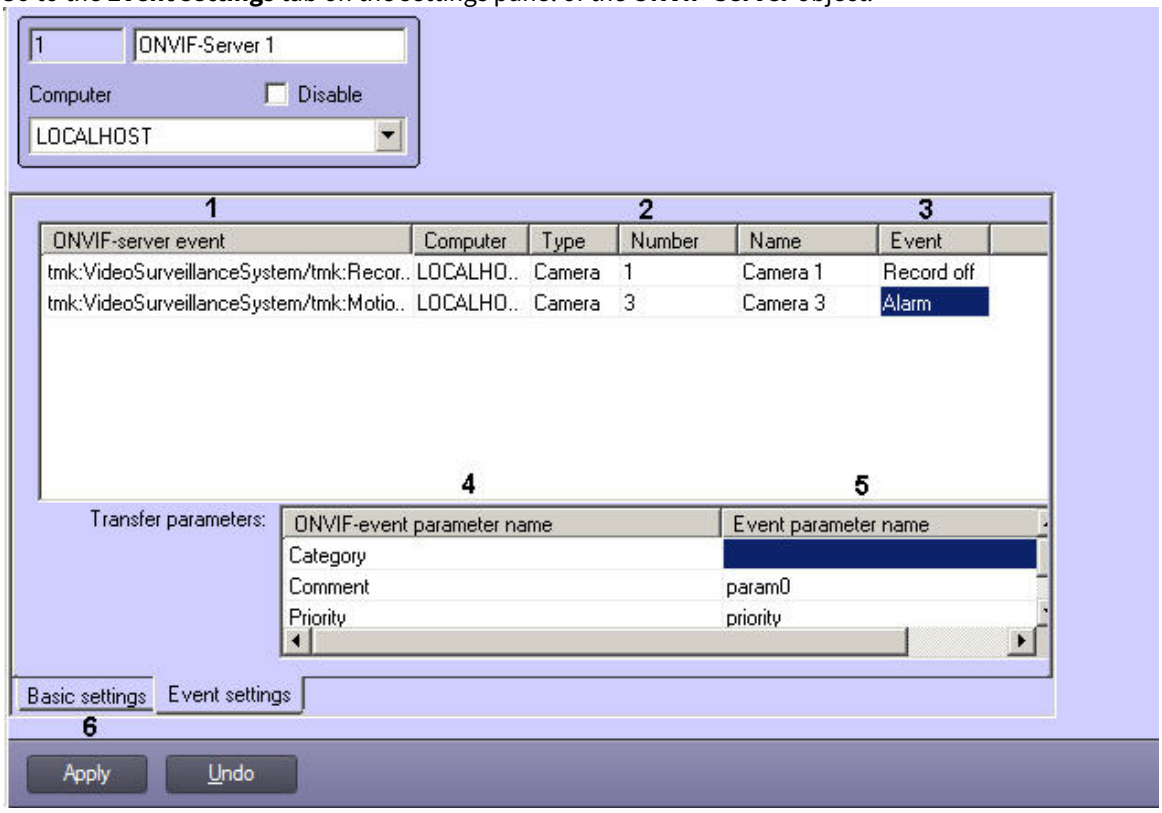
10.3.19.5 Filtering the ONVIF-Server events

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. 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.

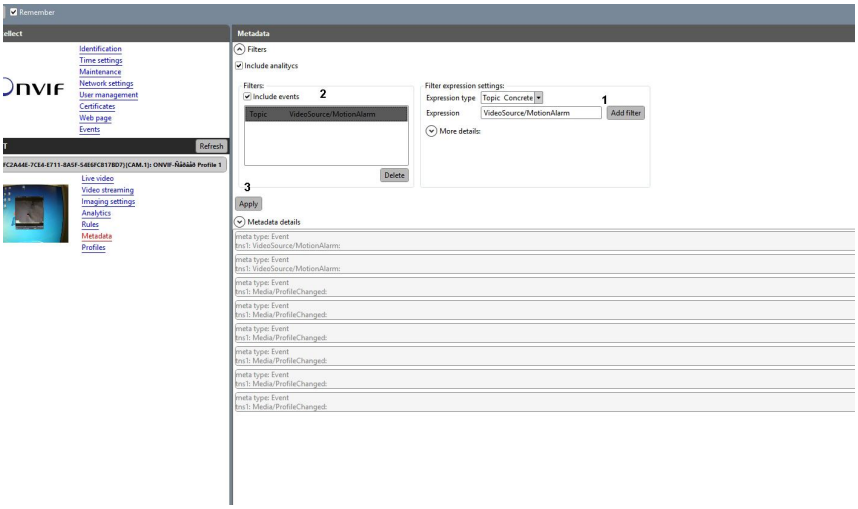
3. In the **Computer**, **Type** and **Number** columns specify the parameters of the required object, from which the corresponding event comes (**2**). The **Name** field will be filled in automatically when you left-click it. If any column parameter is empty, it means that the message will be sent 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.

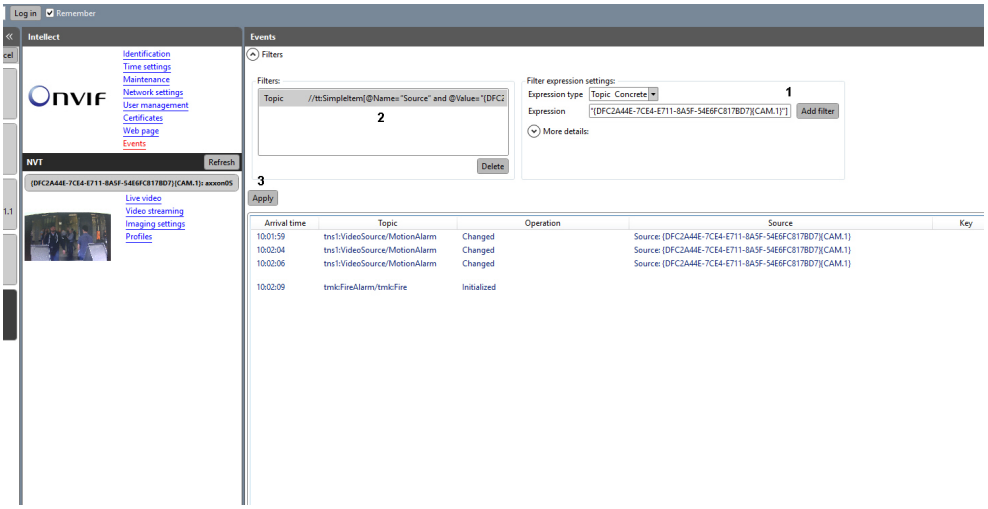
b. In the **Event parameter name** column, it is necessary to specify the parameter value or the *Intellect* event parameter names (**5**). Event parameters can be found in the Debug window, and some of them are described in the Description of system object reactions section (see Programming Guide).

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

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
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		

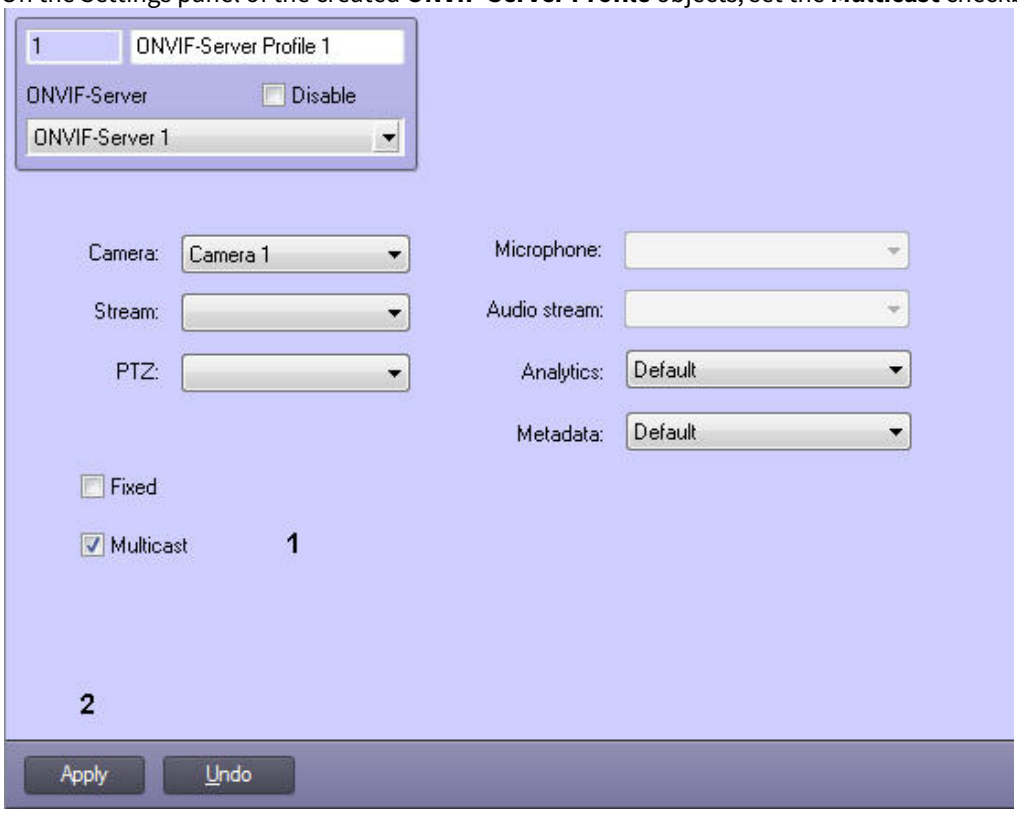
Event	Event description	Parameters	Is configuration required
tns1:Device/VideoSurveillanceSystem/ RecordTurnOff	Recording turned off		
tns1:Device/VideoSurveillanceSystem/ RecordTurnOn	Recording turned on		
tns1:Device/VideoSurveillanceSystem/ MotionDetectorTrigger	Motion detector triggering		
tns1:Device/VideoSurveillanceSystem/ 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	-	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
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

10.3.19.6 Configuring ONVIF-Server module for the Multicast mode

To configure the ONVIF-Server to operate in the Multicast mode, do the following:

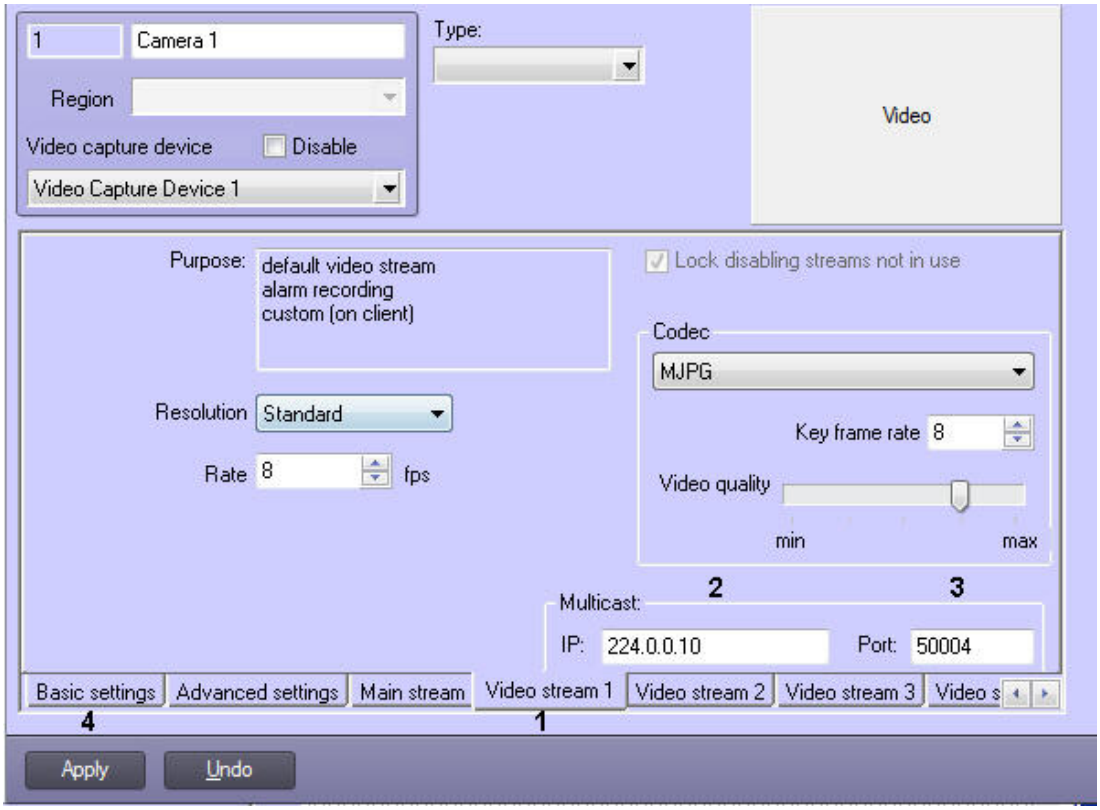
1. Configure the **ONVIF-Server** object (see Configuring ONVIF-Server object).
2. Connect to the ONVIF-Server in the software that receives the ONVIF-Server stream (the *Intellect* or *Axxon Next* Server, or the third-party software, for example, ONVIF Device Manager). For the information about setting 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 poper 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.

10.3.20 Configuring integration with third-party systems

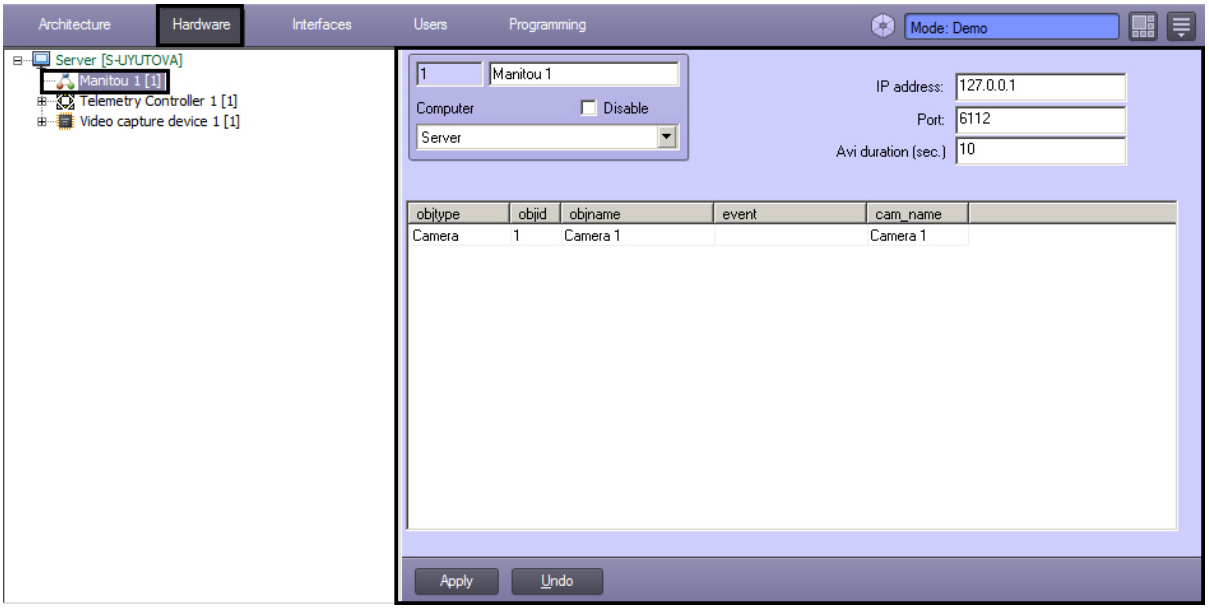
10.3.20.1 Configuring interaction with Manitou software

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 can be attached to such message.*

> **Important!**
>
> Non-stop recording is to be performed on the corresponding camera for correct operation of attaching alarm video to the message feature – see the Recording by Operator command section in Operator's Guide.

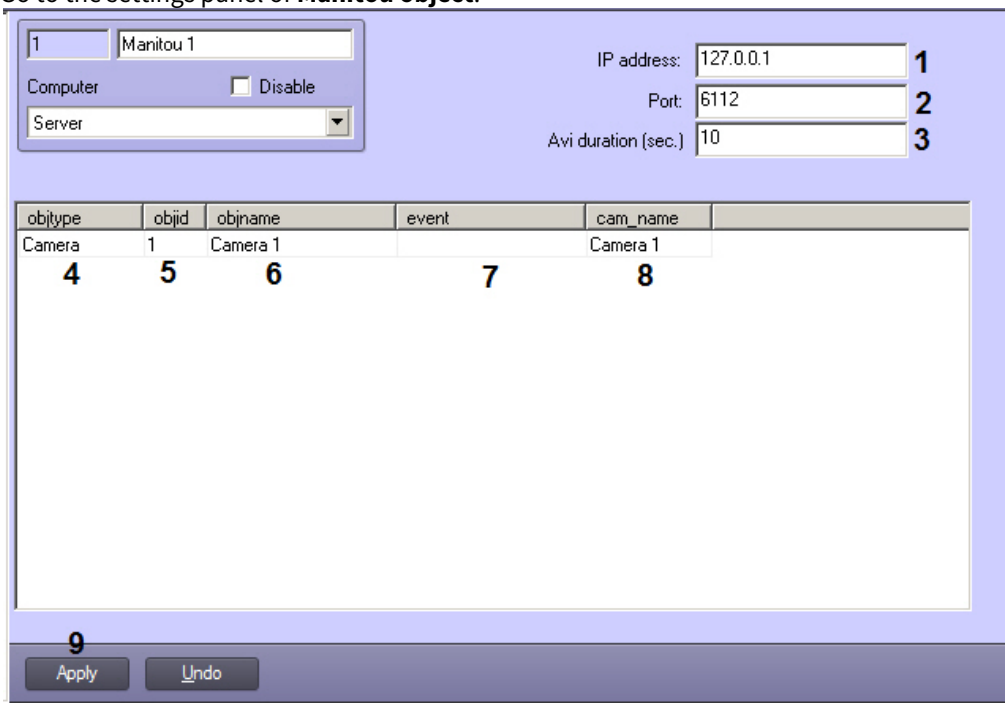
Manitou integration module stands as a client in *Intellect*.

Interaction with *Manitou* software is configured on the settings panel of the **Manitou** object created under the **Computer** object in the **Hardware** tab of the **System settings** dialog box.



Configure interaction with *Manitou* software as follows:

1. Go to the settings panel of **Manitou object**.



2. In the **IP** field specify the IP address of the Server where *Manitou software is started* and to which the connection is to 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 (sec.)** field specify the period of delay after the event happens and before sending the message with attached video (3).

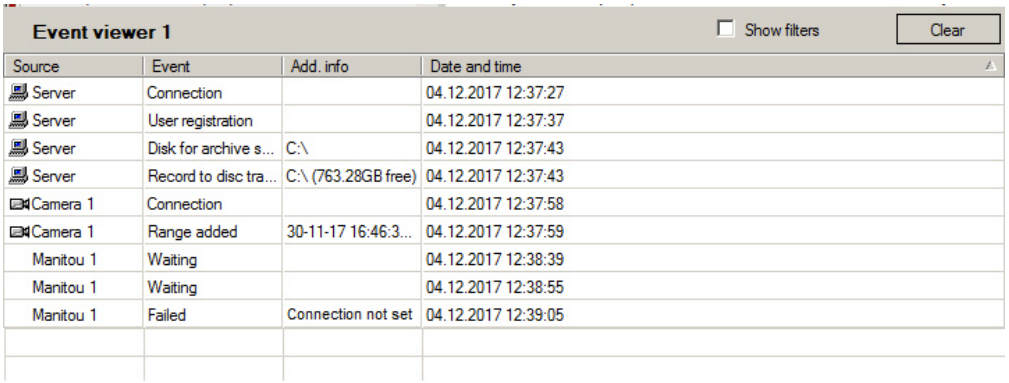
> **Note.**
>
> For correct video export, in the Tweaki.exe utility set maximum frames in one video file so the video fragment duration is shorter than the delay (for instance, 100). Otherwise it may happen that recording of the required fragment of video archive has not stopped yet when sending the message. See The Settings panel of the Video subsystem section (the **Frame count** parameter).

5. In the **objtype** dropdown list select the type of object by the event from which the message is to be sent to *Manitou* software (4).
6. In the **objid** dropdown list select the ID of object of the selected type (5).
7. Left click in the **objname** field (6). It is automatically filled with the name of corresponding object..
8. In the **event** dropdown list select the event from the object of the selected type – when this event happens the message is sent to *Manitou* software (7). If the event is not selected, then messages will be sent at any event from the selected object.
9. In the **cam_name** dropdown list select the **Camera** object the video fragment from which is to 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. Click the **Apply** button (9).

The *Manitou* connection status is displayed in the Event viewer.



Interaction with *Manitou* software is now configured.

10.3.20.2 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:

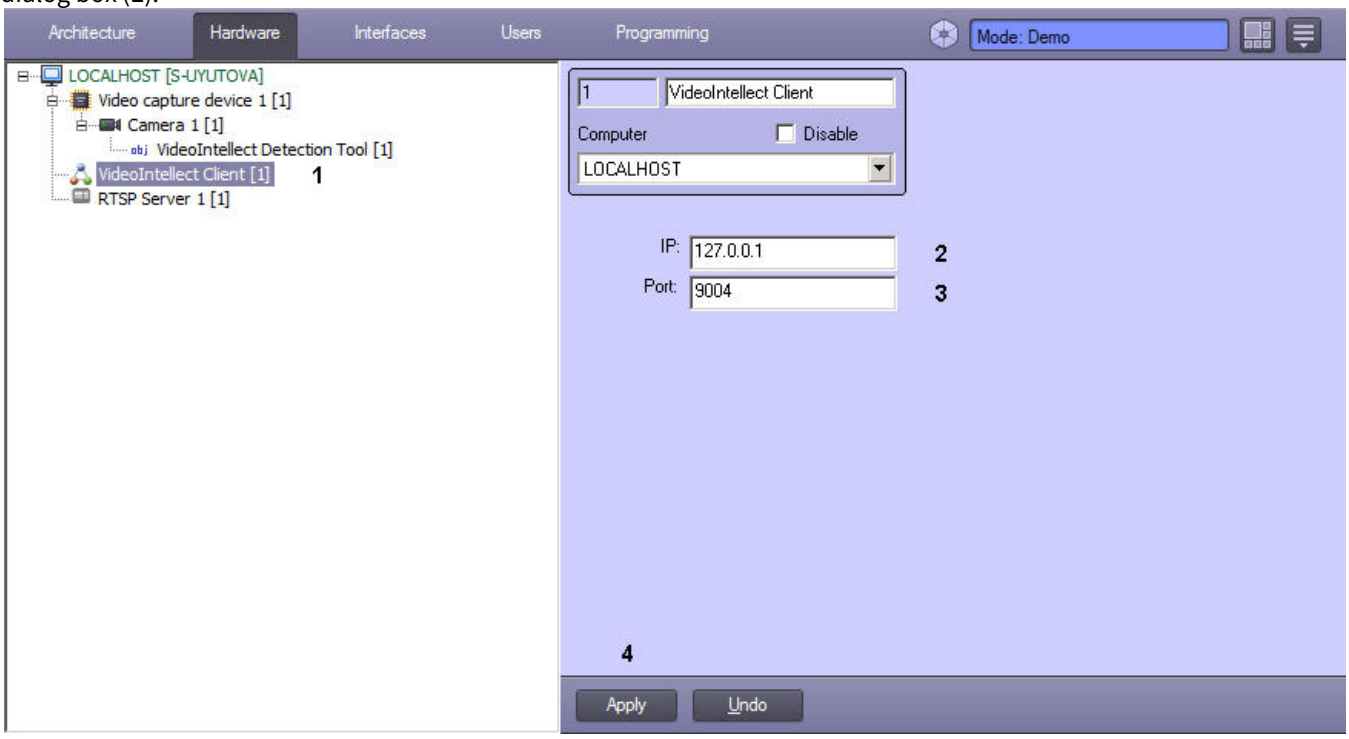
1. Transferring the video from the *Intellect* video cameras to the *VideoIntellect* server via the RTSP protocol.
2. Receiving the results of the video streams analysis (the video analytics detectors triggerings) from the *VideoIntellect* software.

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.

10.3.20.2.1 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**).



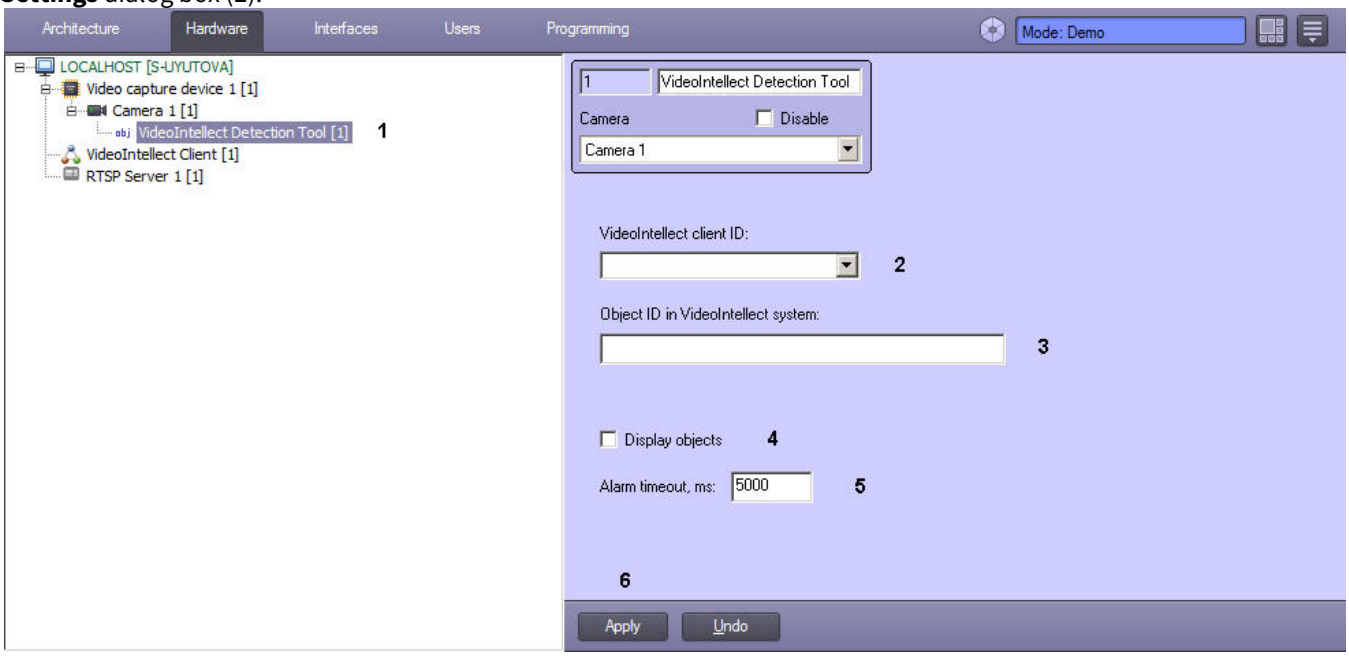
2. In the **IP** field (**2**), enter the IP address of the *VideoIntellect* server.
3. In the **Port** field (**3**), specify the connection port of the *VideoIntellect*.
4. Click **Apply** (**4**).

Setting up the connection to the *VideoIntellect* software is complete.

10.3.20.2.2 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.

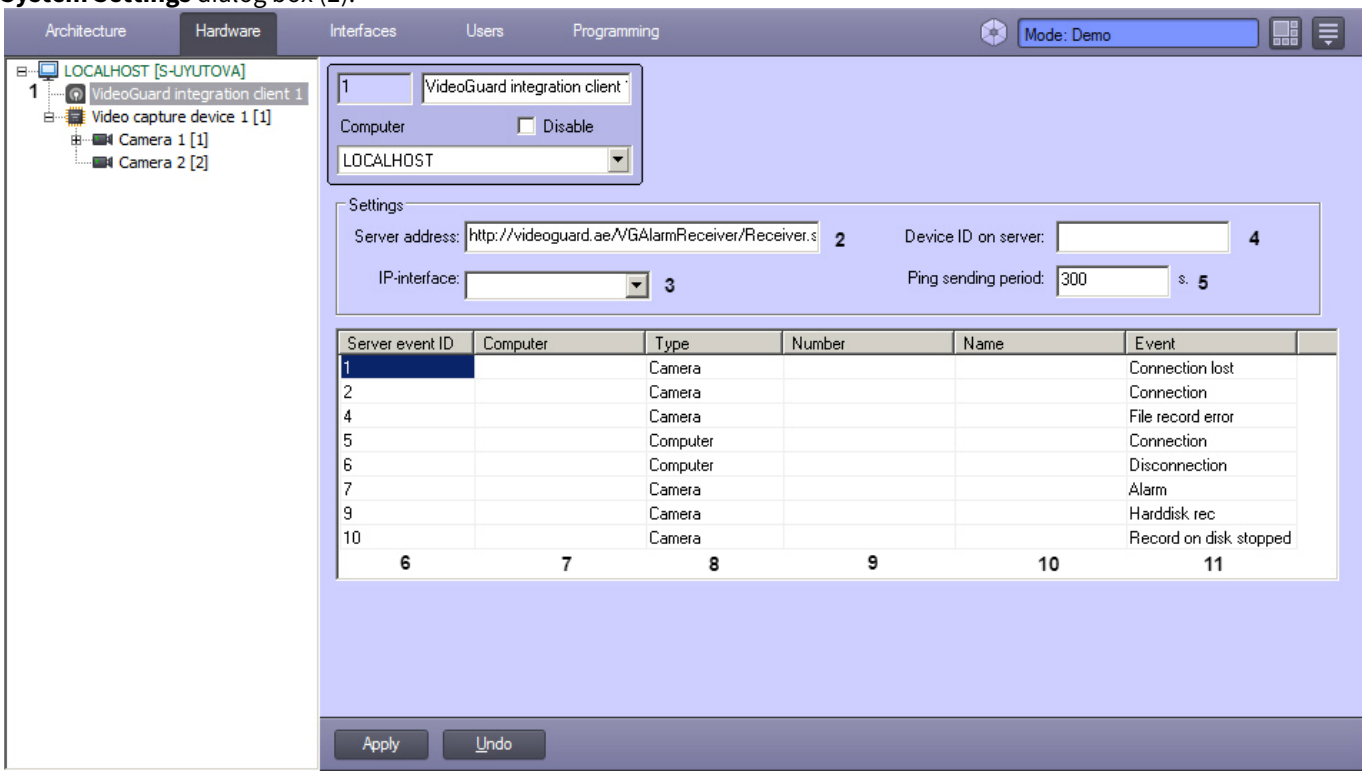
Configuring the receipt of video analytics detector triggerings from *VideoIntellect* software is completed.

10.3.20.3 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**).



2. In the **Server address** field, enter the connection address to the VideoGuard server (**2**).
3. From the **IP-interface** drop-down list, select the network adapter which is used to connect this computer to the VideoGuard server (**3**).
4. In the **Device ID on the server** field, enter the identifier which is assigned to *Intellect* on the VideoGuard server (**4**).
5. In the **Ping sending period** field, specify the Heart Beat messages sending frequency in seconds (**5**). The default value is 300 seconds.
6. 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 and add additional events:
   a. From the **Server event ID** drop-down list, select the event identifier on the VideoGuard server (**6**). 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 (**7**). If the value is not specified, the events are sent from the specified objects, regardless of which **Computer** object they are based on.
   c. From the **Type** drop-down list, select the *Intellect* object type, the events from which should be sent to the VideoGuard server (**8**).
   d. From the **Number** drop-down list, select the *Intellect* object identifier, the events from which should be sent to the VideoGuard server (**9**). 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 (**10**).
   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 (**11**).
7. Click **Apply**.

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.

The event identifiers supported on the server:

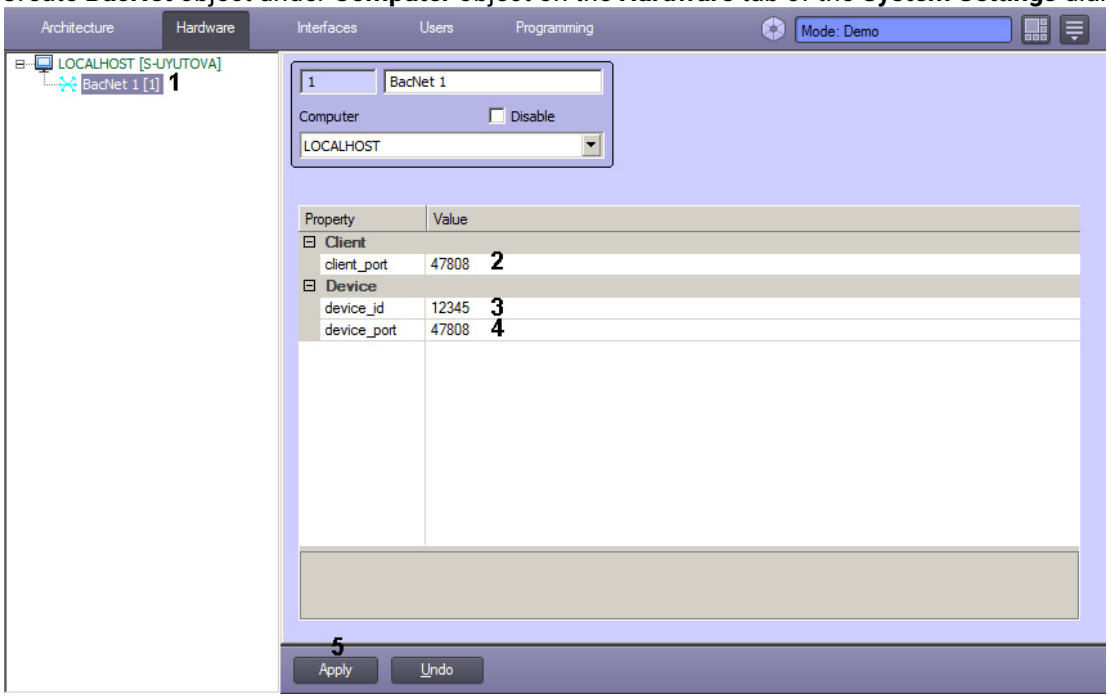
ID	Description	Corresponding Intellect event
1	No video signal	Camera: Connection lost
2	Video source connection	Camera: Connection
3	Disk overflow	-
4	Error writing to disk	Camera: File record error
5	Client connection	Computer: Connection
6	Client disconnection	Computer: Disconnection
7	Motion detection 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: Server event ID: 100; Computer: ; Type: VMDA detection; Number: 1; Name: VMDA Detection 1; Event: Alarm The event with the "101" identifier will be sent to the VideoGuard server.

10.3.20.4 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).

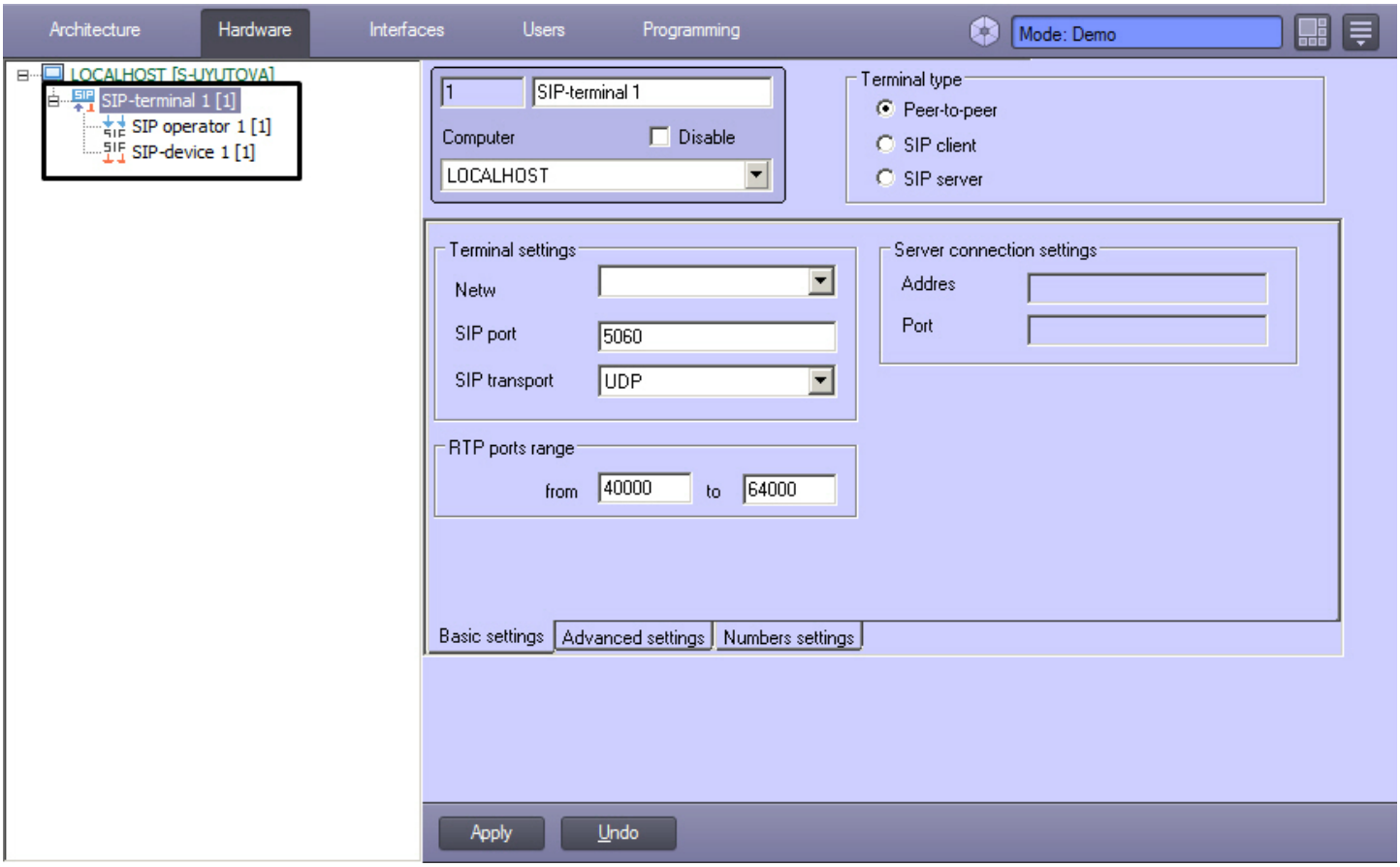
Further work with the BACnet device is carried out using scripts – see BACNET.

10.3.21 Configuring SIP-devices

SIP-devices are IP devices, mainly intercoms and call panels, connected to *Intellect* via the Session Initiation Protocol (SIP).

The *Intellect* can act both as a server and as a SIP client, and the *Intellect's* SIP client can use either third-party Asterisk software or *Intellect's* SIP server as a 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 — **SIP-operator** and **SIP-device**.



The SIP-terminal (both server and client) is configured in the following order:

1. Select the terminal type.
2. Specify the terminal network settings.
3. Create and configure the objects corresponding to the SIP-devices.
4. Create and configure the objects corresponding to the SIP-device operators.
5. Configure the special numbers of the terminal.
6. Configure the numbers of the terminal.
7. If necessary, create and configure the macros to work with the SIP-devices.
8. Configure the interface objects to work with the SIP-devices.
9. Configure the **SIP Panel** interface object to work with the SIP-devices.

Note

Despite the general configuration procedure, the steps 2-4 are different.

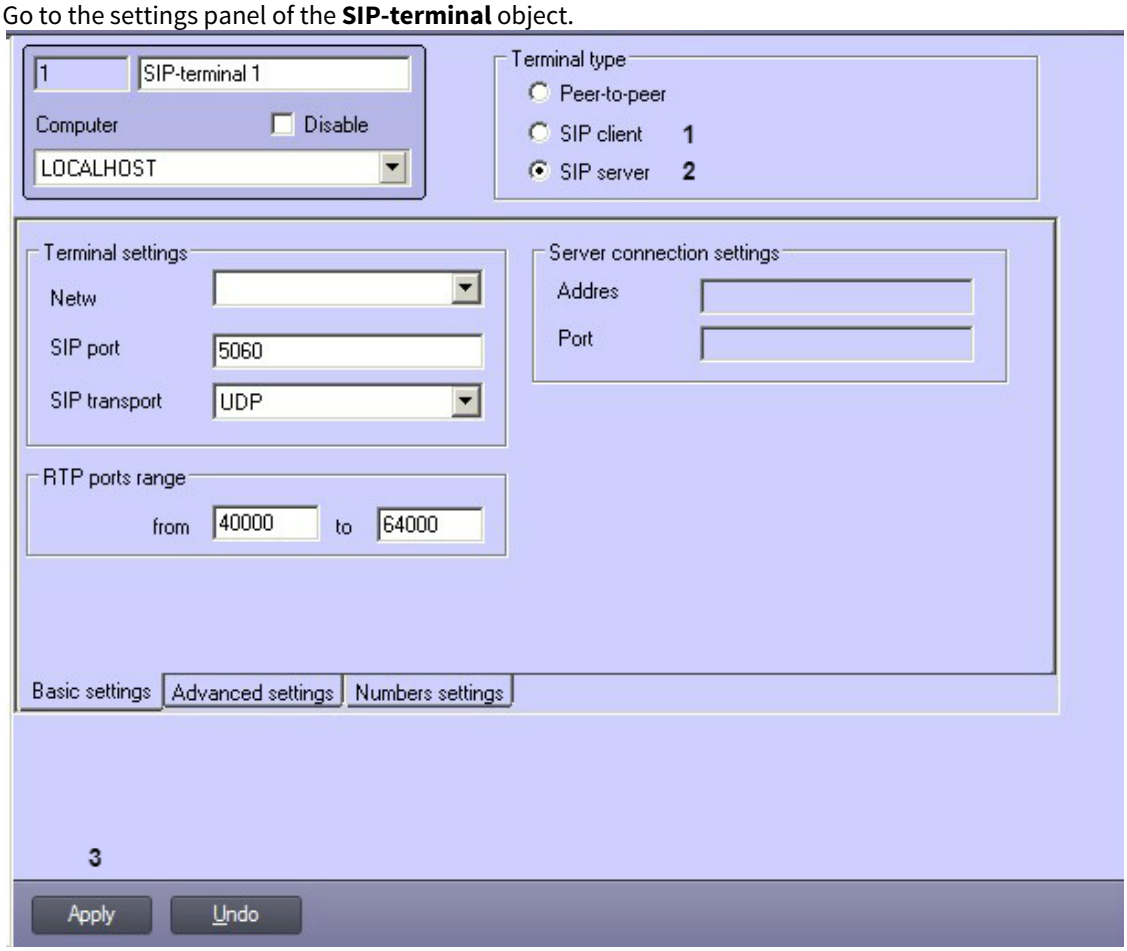
SIP Panel

Configuring the SIP Panel interface object

10.3.21.1 Selecting the SIP-terminal type

The type of SIP-terminal is selected as follows:

1. Go to the settings panel of the **SIP-terminal** object.



2. Set the **Terminal type** switch to the position corresponding to the SIP terminal type:
   a. **SIP client** (**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.

      Note

      To activate the fields in this group, it may be necessary to go to the settings panel of any other object, and then return to the settings panel of the **SIP-terminal** object.

   b. **SIP server** (**2**) — the SIP-terminal acts as a server, any SIP-clients can be connected to it (both *Intellect*-based and the third-party SIP-devices).

> **Note**
>
> The **Peer-to-peer** terminal type is not supported at the present moment.

3. Click **Apply** (**3**).

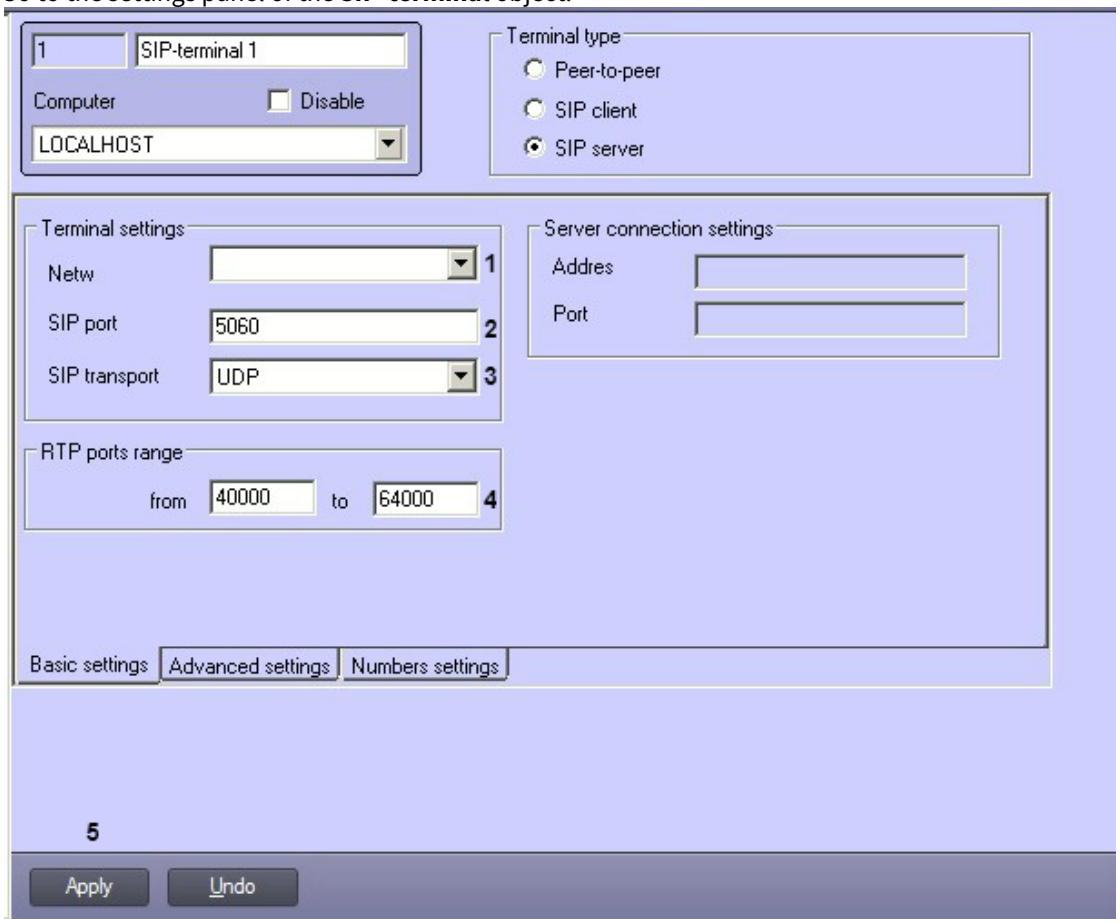
The SIP-terminal type is selected.

10.3.21.2 Configuring the Intellect SIP-server

10.3.21.2.1 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. From the **Netw** drop-down list (**1**), select the IP address of the network adapter that will be used to connect to the network where the SIP-clients are located.
3. In the **SIP port** field (**2**), specify the port number which will receive the data from the SIP-clients.
4. From the **SIP transport** drop-down list (**3**), select the transport level protocol to be used: TCP or UDP.
5. If necessary, specify the RTP ports range in the corresponding text fields (**4**).
6. Click **Apply** (**5**).

The network settings of the *Intellect* **SIP-server** are set.

10.3.21.2.2 Configuring SIP-device connection to Intellect SIP-server

On this page:

- Configuring the SIP-device
- Configuring the SIP-device connection to Intellect
- Configuring the tone DTMF commands

10.3.21.2.2.1 Configuring the SIP-device

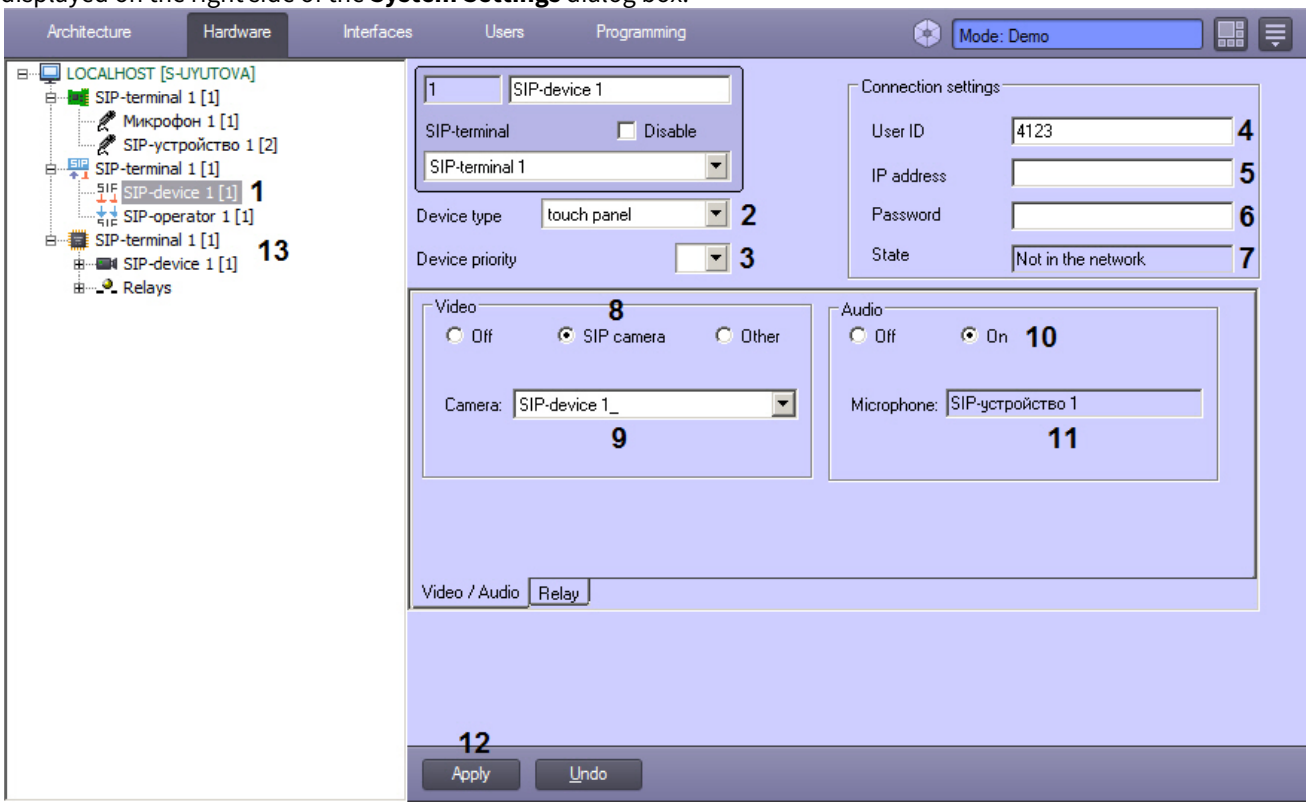
Before you start configuring the SIP-device connection to *Intellect*, it is necessary to configure the device itself. Each SIP-device is configured individually according to the manufacturer's documentation, however, it is always necessary to perform the following basic steps:

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 on Intellect SIP-server).

10.3.21.2.2.2 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**). The object settings panel will be displayed on the right side of the **System Settings** dialog box.



2. From the **Device type** drop-down list (**2**), select the icon type used to display the device on the Map.
3. From the **Device priority** drop-down list, select the priority of calls from this device when displayed on the SIP panel (**3**). If the field is left blank, the priority is considered minimal. The larger the number, the higher the priority, hence, the higher the call is displayed in the list. Calls from devices with the same priority are sorted by time depending on the **New calls to end** setting of the **SIP panel** interface object (see Configuring the SIP Panel interface object)
4. In the **User ID** field (**4**), enter the SIP-device identification number, i.e. the number to call it.

5. In the **IP address** field (**5**), enter the SIP-device IP address. If you are not going to send data to the SIP-device, this field is optional.
6. In the **Password** field (**6**), 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.
7. The **State** field displays the current status of the SIP device (**7**).
8. Set the **Video** switch (**8**) 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** (**9**) 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 (**12**).
   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 (**9**).
9. Set the **Audio** switch (**10**) to the position corresponding to the microphone used for calls:
   a. **Off** — the audio is not used during the call.
   b. **On** — the microphone of the SIP-device is used as shown in the **Microphone** information field (**11**). 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 (**12**).
10. Click **Apply** (**12**).
11. If necessary, the pre-configured missing **Camera** and **Microphone** objects (**13**) will be automatically created in the *Intellect* objects tree.

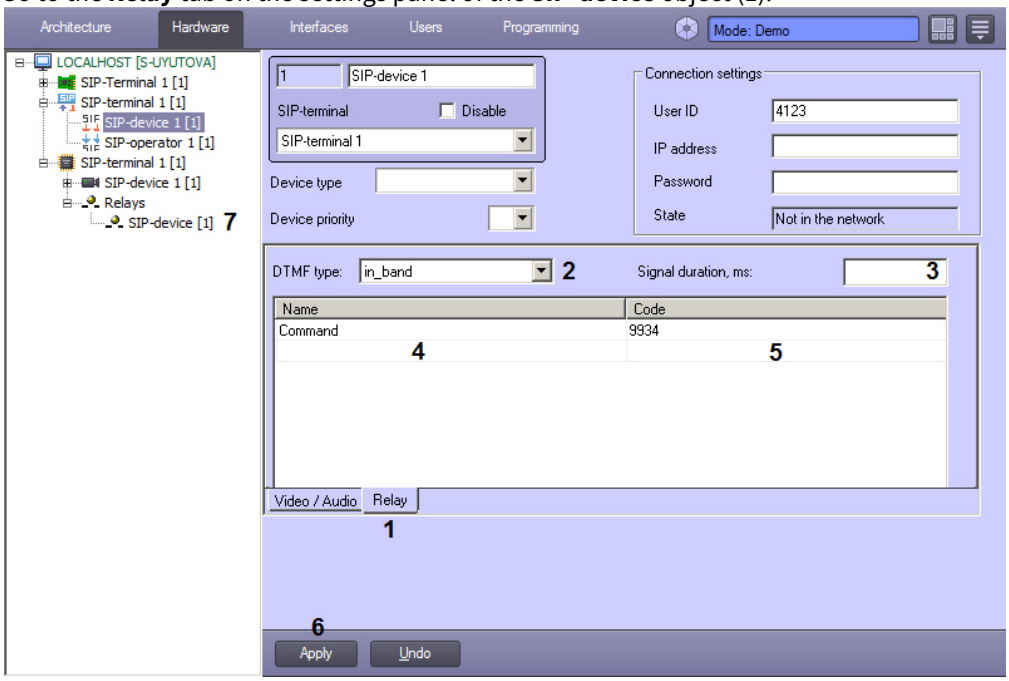
Configuring the SIP-device connection to *Intellect* is complete.

10.3.21.2.2.3 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 on the settings panel of the **SIP-device** object (1).



2. Select the type from the **DTMF type** drop-down list (2):
   a. in_band – the signal is transmitted as normal sound in an audio stream.
   b. rtp_nte – signals are transmitted via RTP separately from the voice stream.
   c. sip_info – signals are transmitted in the SIP INFO message.
   d. sip_notify – signals are transmitted in the SIP NOTIFY message.

3. In the **Signal duration, ms** field set the time period in milliseconds during which the command is to be sent(3). This value is applied if duration is not set for a specific command.
4. In the **Name** field, enter the name of the command displayed on the SIP panel (4).
5. In the **Code** field, enter the unique command code (5).
6. Click **Apply** (6).
7. The corresponding **Relay** object (7) will be created in the *Intellect* hardware tree.

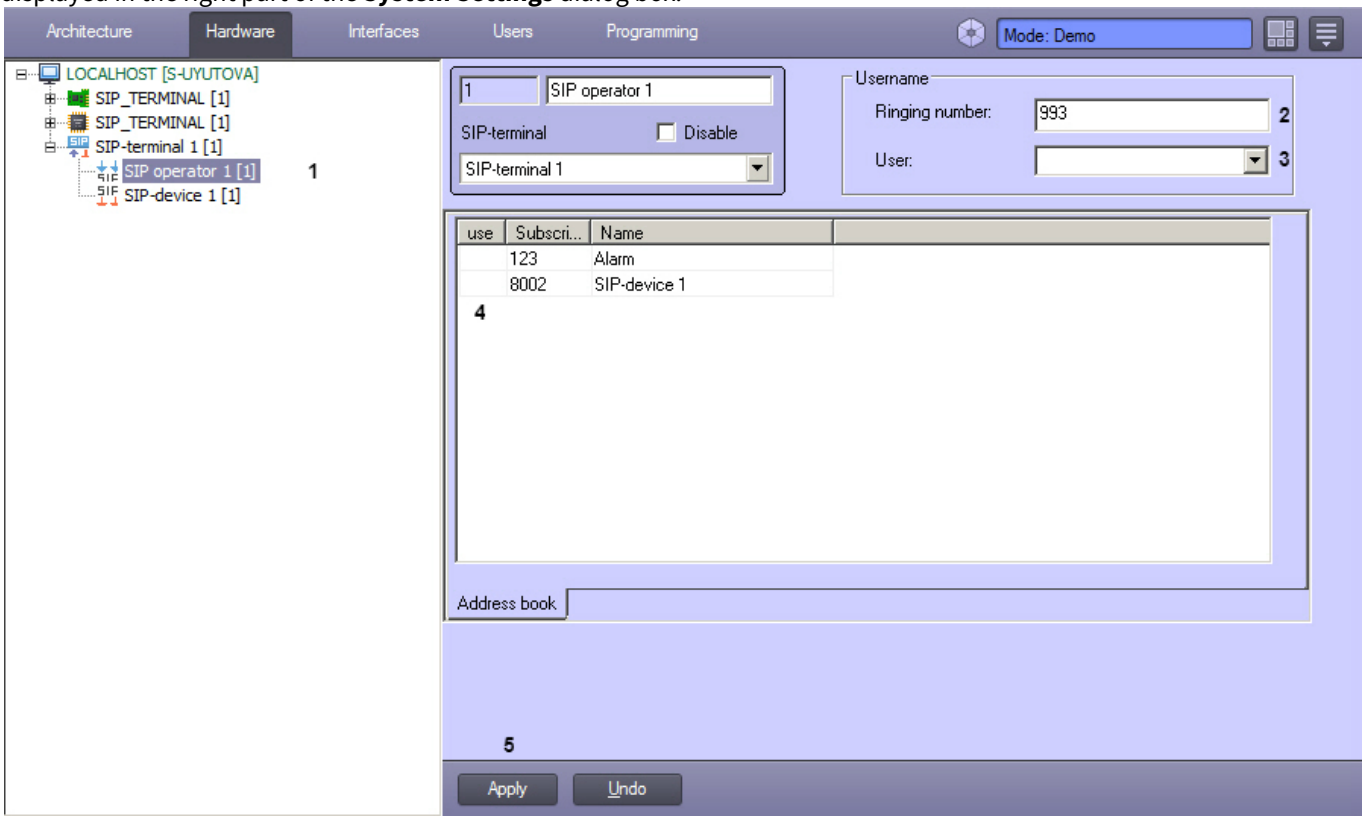
The SIP-device relay is configured.

10.3.21.2.3 Configuring SIP operators on Intellect SIP-server

SIP-operators of the *Intellect* server correspond to the *Intellect* users. Operators are assigned their own identification number for calls, the device and operator numbers, and the special numbers to which they have access.

SIP-operators are configured as follows:

1. Create a **SIP operator** object based on the **SIP-terminal** object (**1**). The settings panel of the created object will be displayed in the right part of the **System Settings** dialog box.



2. In the **Ringing number** field (**2**), enter the operator identification number.
3. From the **User** drop-down list (**3**), select the corresponding *Intellect* user (for the details on creating and configuring the users, see Configuration of users and permissions).
4. In the **Address book** table, in the **use** column (**4**), mark those devices, operators and special numbers that should be available in the SIP panel address book of this operator.
5. Click **Apply** (**5**).

The SIP operators on the Intellect SIP-server are configured.

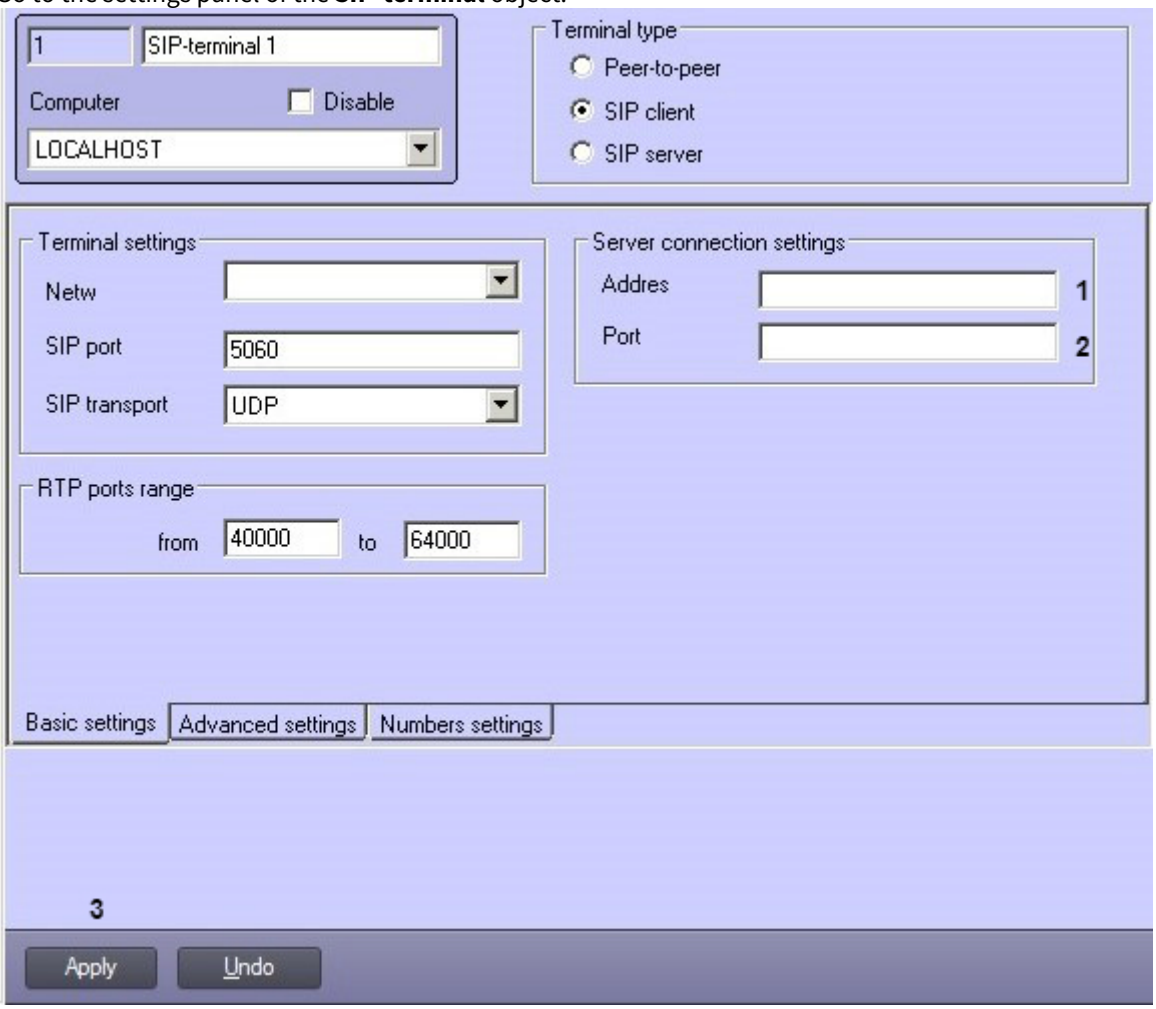
10.3.21.3 Configuring the Intellect SIP-client

10.3.21.3.1 Network settings of the Intellect's SIP-client

The network settings of the *Intellect*'s SIP-client are similar to the network settings of the SIP-server, however, it is necessary to additionally specify the parameters of the SIP server connection (either the *Intellect* installed on another computer, or the Asterisk software).

The network settings of the *Intellect* SIP-client are set in the following order:

1. Go to the settings panel of the **SIP-terminal** object.



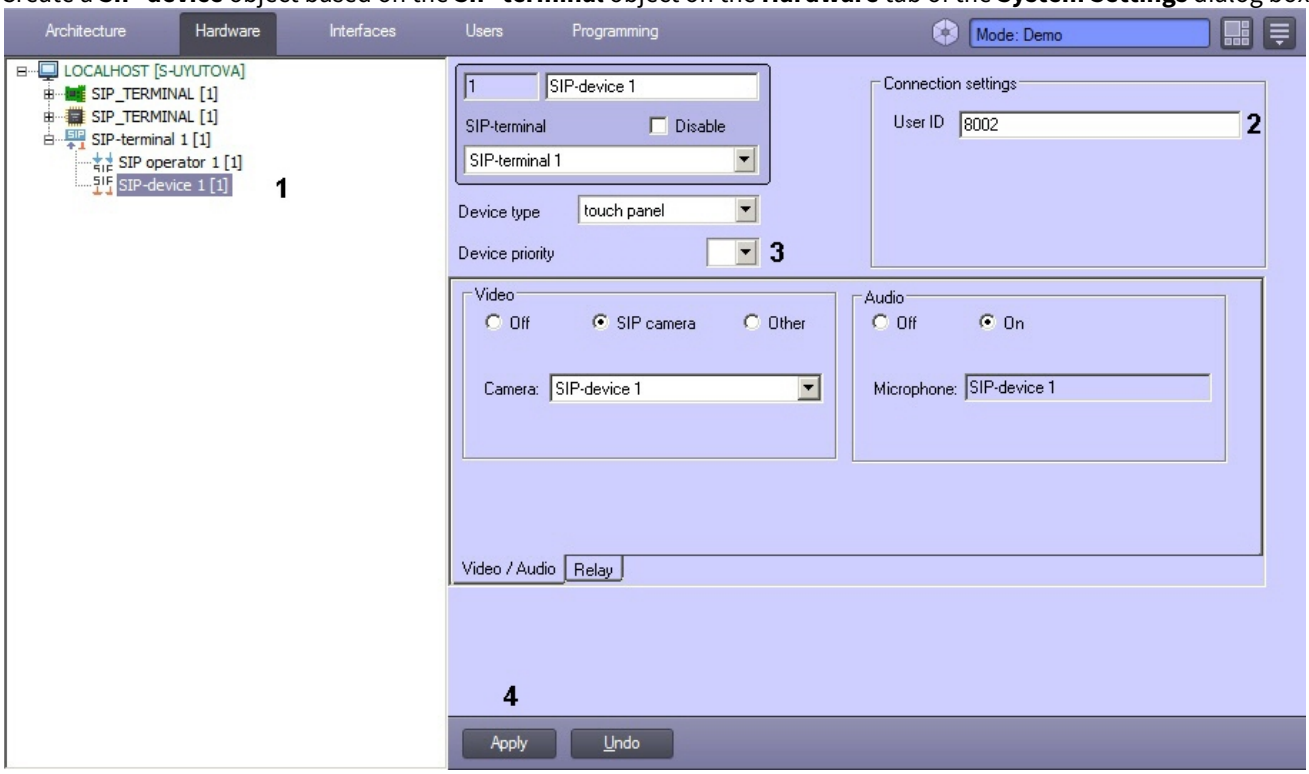
2. In the **Address** field in the **Server connection settings** group (**1**), specify the IP address of the SIP server.
3. In the **Port** field in the **Server connection settings** group (**2**), specify the port for the SIP server connection.
4. In the **Terminal settings** group, specify the SIP client settings in the same way as for the SIP server (see Network settings of the Intellect's SIP-server).
5. Click **Apply** (**3**).

The network settings of the *Intellect* SIP-client are set.

10.3.21.3.2 Configuring SIP-devices on the Intellect's SIP-client

The SIP-device is configured on the *Intellect*'s SIP-client as follows:

1. Create a **SIP-device** object based on the **SIP-terminal** object on the **Hardware** tab of the **System Settings** dialog box (**1**).



2. In the **User ID** field (**2**), specify the SIP-device identification number, i.e. the number to call it.
3. From the **Device priority** drop-down list, select the priority of calls from this device when displayed on the SIP panel (**3**). If the field is left blank, the priority is considered minimal. The larger the number, the higher the priority, hence, the higher the call is displayed in the list. Calls from devices with the same priority are sorted by time depending on the **New calls to end** setting of the **SIP panel** interface object (see Configuring the SIP Panel interface object)
4. Click **Apply** (**4**).

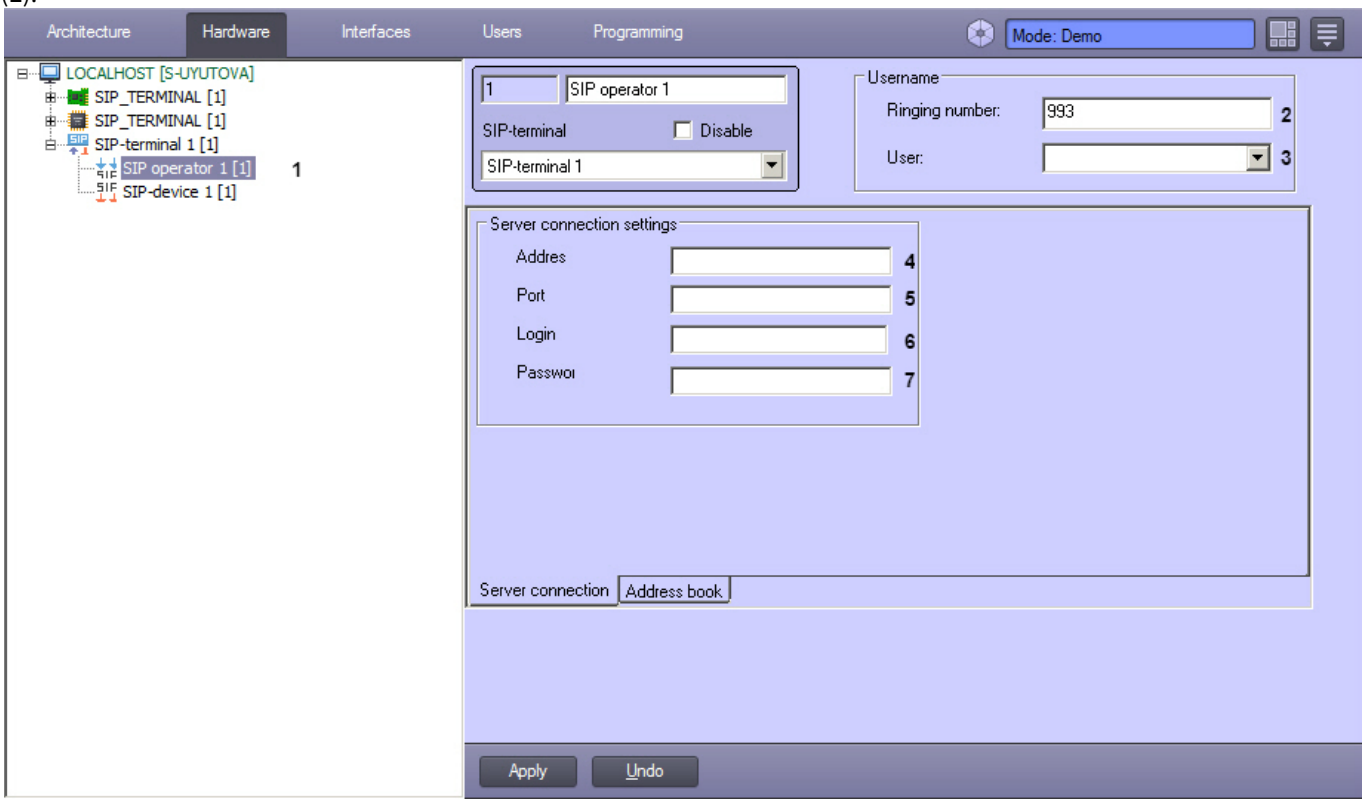
Configuration of the SIP-device on the *Intellect* SIP-client is complete.

10.3.21.3.3 Configuring SIP-operators on the Intellect's SIP-client

SIP operators correspond to the registered *Intellect* users.

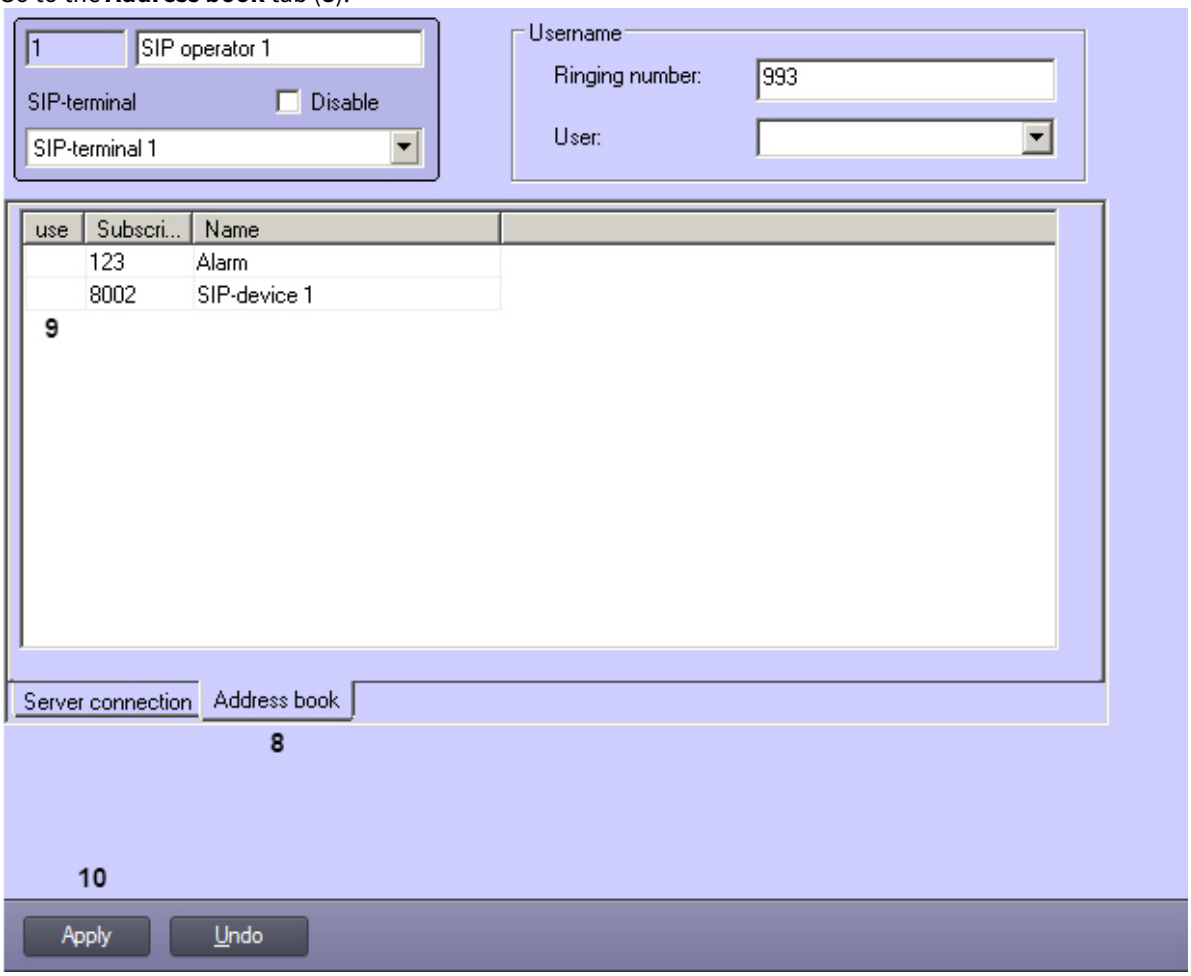
SIP-operators are configured on the *Intellect*'s SIP-client as follows:

1. Create a **SIP-operator** object based on the **SIP-terminal** object on the **Hardware** tab of the **System Settings** dialog box (**1**).



2. In the **Ringing number** field (**2**), enter the operator identification number which one can call.
3. From the **User** drop-down list (**3**), select the corresponding *Intellect* user (for the details on creating and configuring the users, see Configuration of users and permissions).
4. In the **Address** field (**4**), specify the IP address of the SIP-server.
5. In the **Port** field (**5**), specify the port of the SIP-server.
6. In the **Login** field (**6**), enter the username for connecting to the SIP-server.
7. In the **Password** field (**7**), specify the password for connecting to the SIP-server.

8. Go to the **Address book** tab (**8**).



9. In the **use** column (**9**), mark those devices, operators and special numbers that should be available in the SIP panel address book of this operator.
10. Click **Apply** (**10**).

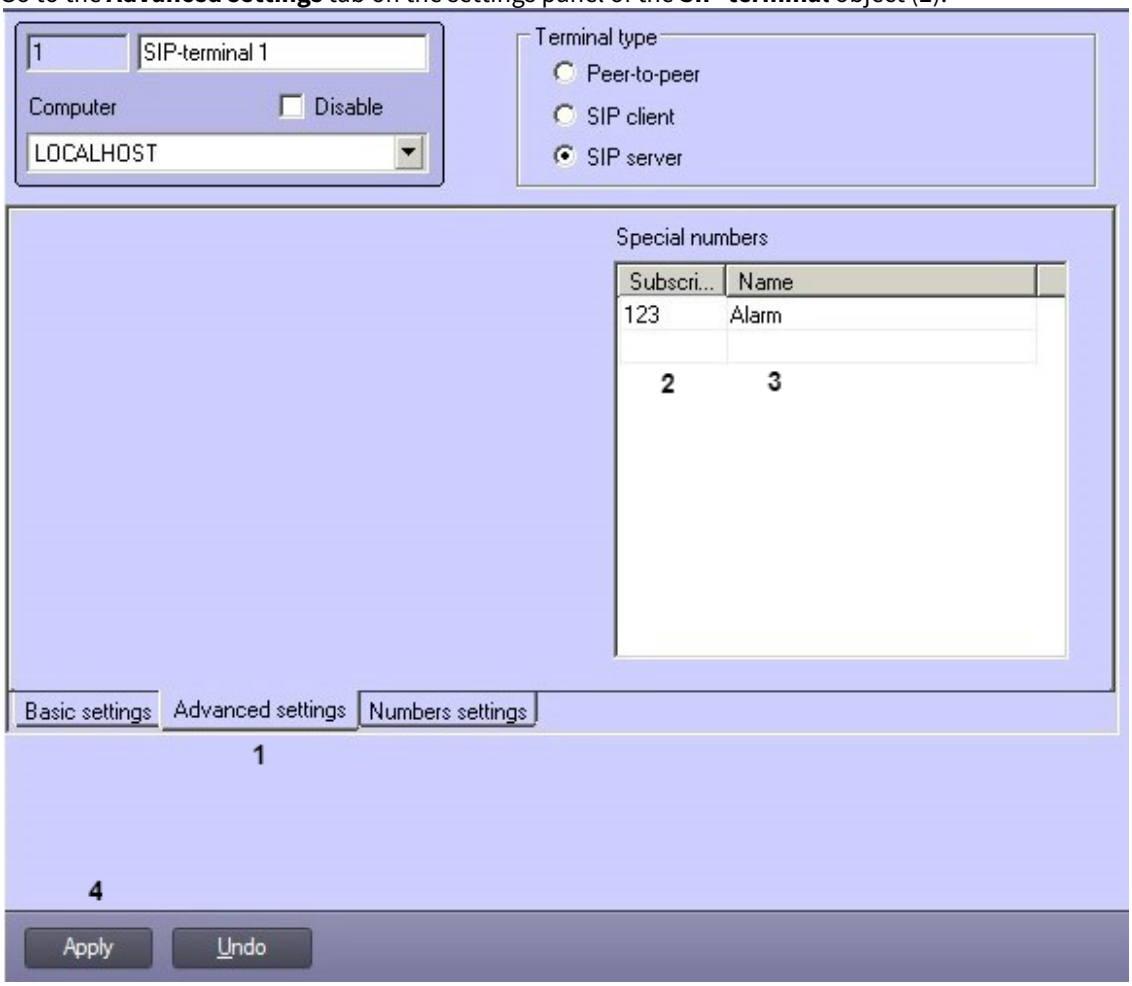
The configuration of SIP-operators on the *Intellect* SIP-client is complete.

10.3.21.4 Configuring special numbers of Intellect's 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 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.

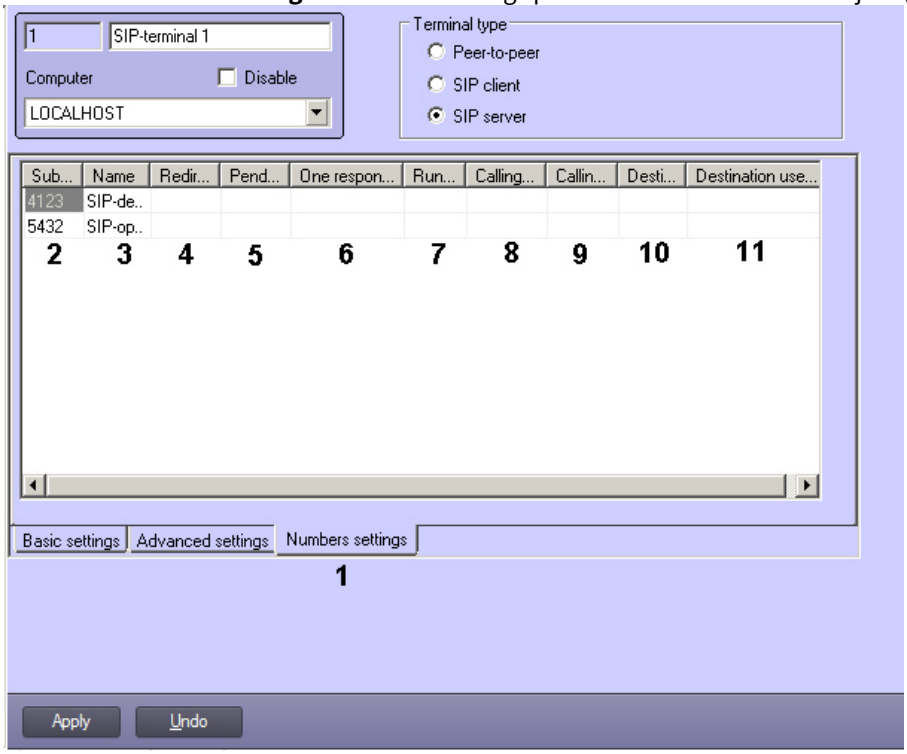
3. Click **Apply** (**4**).

The special numbers of the *Intellect*'s SIP-terminal are configured.

10.3.21.5 Configuring numbers of Intellect's 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 group calls.

   Note.

   "Operator-to-operator" calls are not supported.

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 checked, 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 checked, 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-devices.
8. In the **Calling number multicast (video)** field (**8**), specify the IP address for broadcasting the video stream from the calling device in the multicast mode.
9. In the **Calling number multicast (sound)** field (**9**), specify the IP address for broadcasting the audio stream from the calling device in the multicast mode.
10. In the **Destination number multicast (video)** field (**10**), specify the IP address for broadcasting the video stream from the destination device in the multicast mode.
11. In the **Destination number multicast (sound)** field (**11**), specify the IP address for broadcasting the audio stream from the destination device in the multicast mode.
12. Click **Apply** (**12**).

The numbers of *Intellect*'s SIP-terminal are configured.

10.3.21.6 Macros for working with SIP-devices

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	calling user	The identification number of the subscriber (operator or device) which makes the call.
	call ID	The unique identifier of the call in the system; it is used to end the call.
	playback file	The full path to the .wav file which should play when receiving a call.
	play file on loop	Specifies whether the file should play once (the **no** value) or on a loop until the call ends (the **yes** value).
	group call ID	Not in use.
	address for audio relaying	The IP address of the sound relay.
	port for audio relaying	Port for the sound relay.
	destination user	The identification number of the destination subscriber (operator or device)
End a call	call ID	The unique identifier of the call in the system, specified when initiating the call.
Group call	group call ID	The unique identifier of the group call in the system; it is used to end the call.
	user 1 ... user 10	The identification numbers of the subscribers participating in a group call.
End a group call	group call ID	The unique identifier of the group call in the system, specified when initiating the call.
SIP-device object		
A call (make/receive)	-	-
End a call	-	-

10.3.21.7 Selecting speaker, microphone and camera for SIP operator

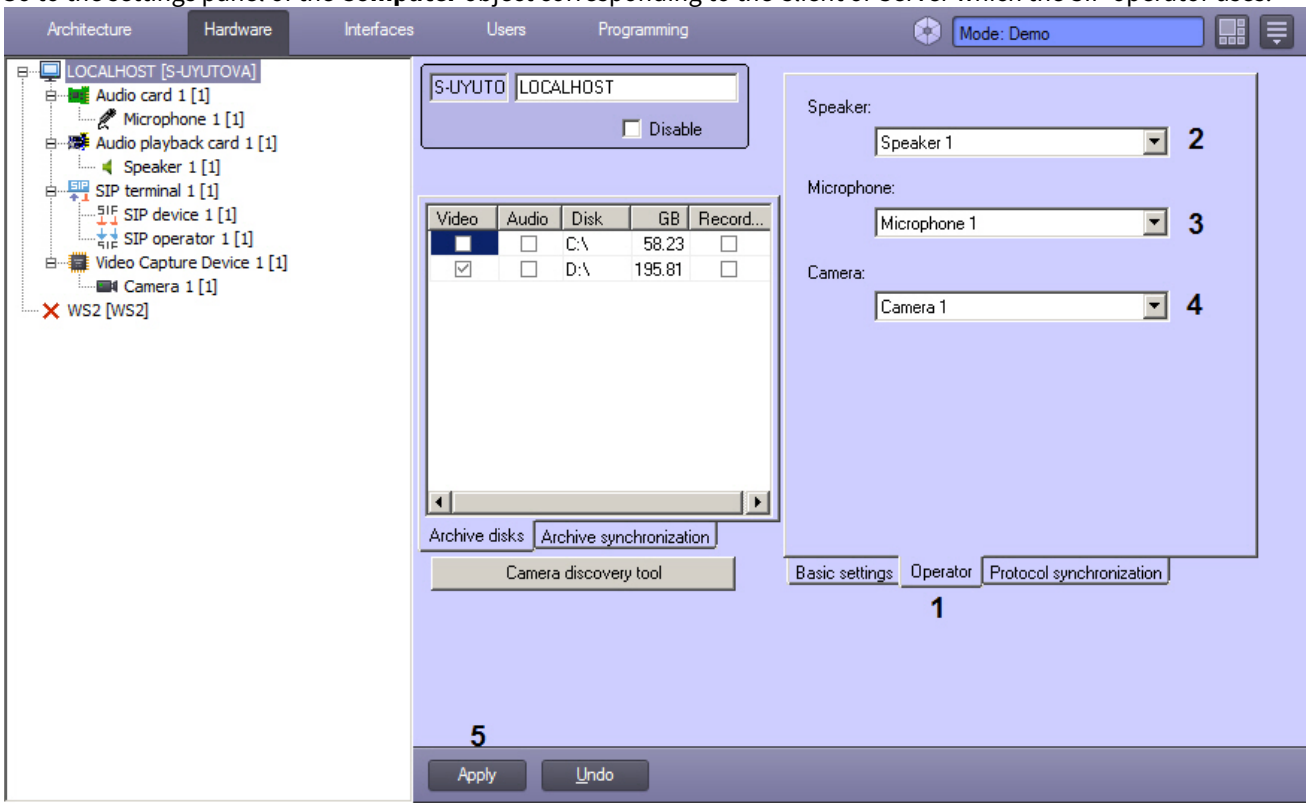
The speaker, microphone and camera are selected for calls via the SIP Panel.

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 dynamic from the **Dynamic** 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 speaker, microphone and camera for SIP operator is now complete.

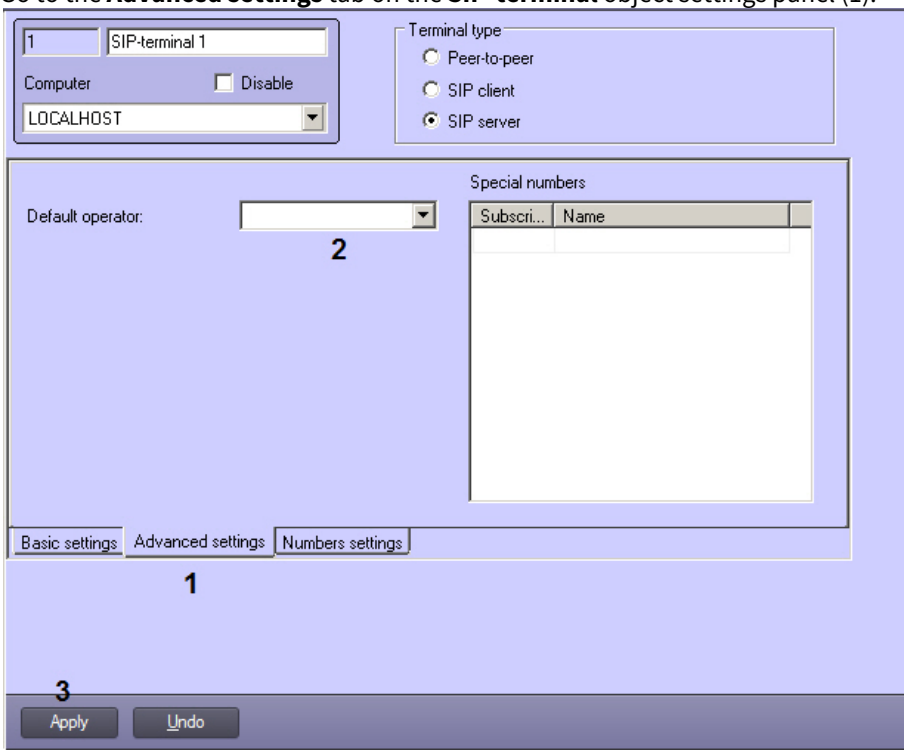
10.3.21.8 Selecting the default SIP-operator

Each SIP-operator is assigned with an own address book available in the SIP Panel linked to the SIP terminal. Some Intellect users may not be assigned with SIP-operator's address book but use the address book of the default SIP-operator while using the SIP Panel. See details in the table below.

Situation	System behavior
Intellect user corresponding to any SIP-operator is logged in, regardless of whether the default SIP-operator is configured	SIP Panel shows address book for the corresponding SIP-operator
Intellect user NOT corresponding to any SIP-operator is logged in, default SIP-operator IS NOT selected	Address book numbers are not displayed on the SIP Panel
Intellect user NOT corresponding to any SIP-operator is logged in, default SIP-operator IS selected	SIP Panel shows address book for the default SIP-operator
Users and/or permissions are not configured in Intellect	Address book numbers are not displayed on the SIP Panel

Select the default SIP-operator as follows:

1. Go to the **Advanced settings** tab on the **SIP-terminal** object settings panel (1).



2. From the **Default operator** drop-down list, select the **SIP-operator** object corresponding to the default SIP-operatoe (2).
3. Click **Apply** (3).

The default SIP-operator is now selected.

> Configuring SIP operators on Intellect SIP-server
>
> Configuring SIP-operators on the Intellect's SIP-client
>
> Rights administration
>
> SIP Panel

10.4 Configuration of interfaces

10.4.1 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 ITV website at http://www.itv.ru/

> **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).

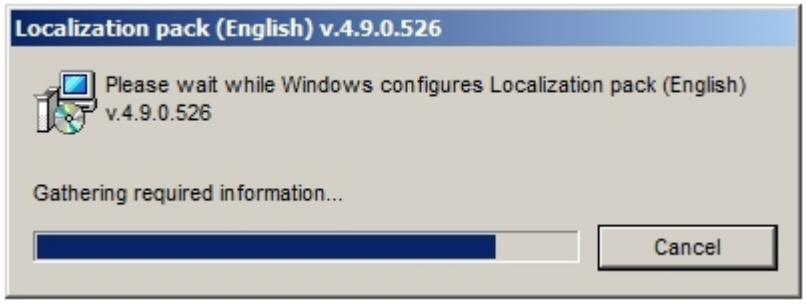
Attention!

Localization files for Intellect-based vertical solution modules are not included into the language package

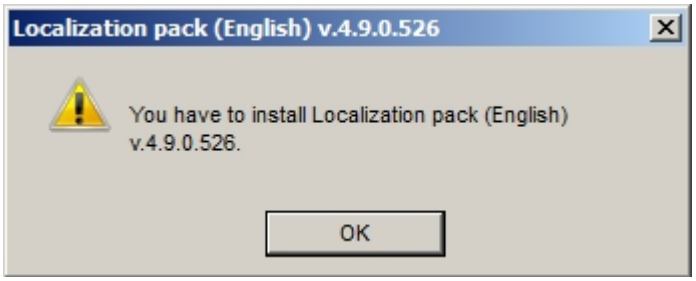
10.4.1.1 Installing the language

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 ITV official website: http://www.itv.ru.
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.



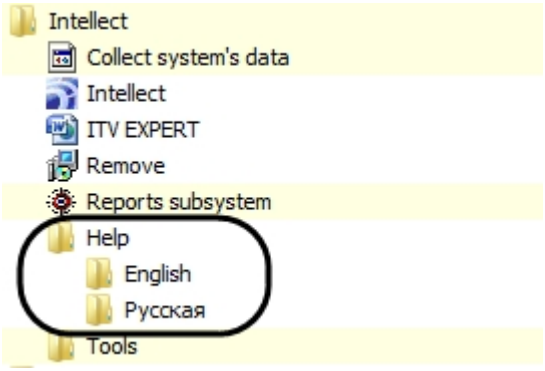
A language cannot be installed if the base product has not been installed. If the *Intellect* Software System has not been installed, a message indicating the need to install it will be shown.



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**.



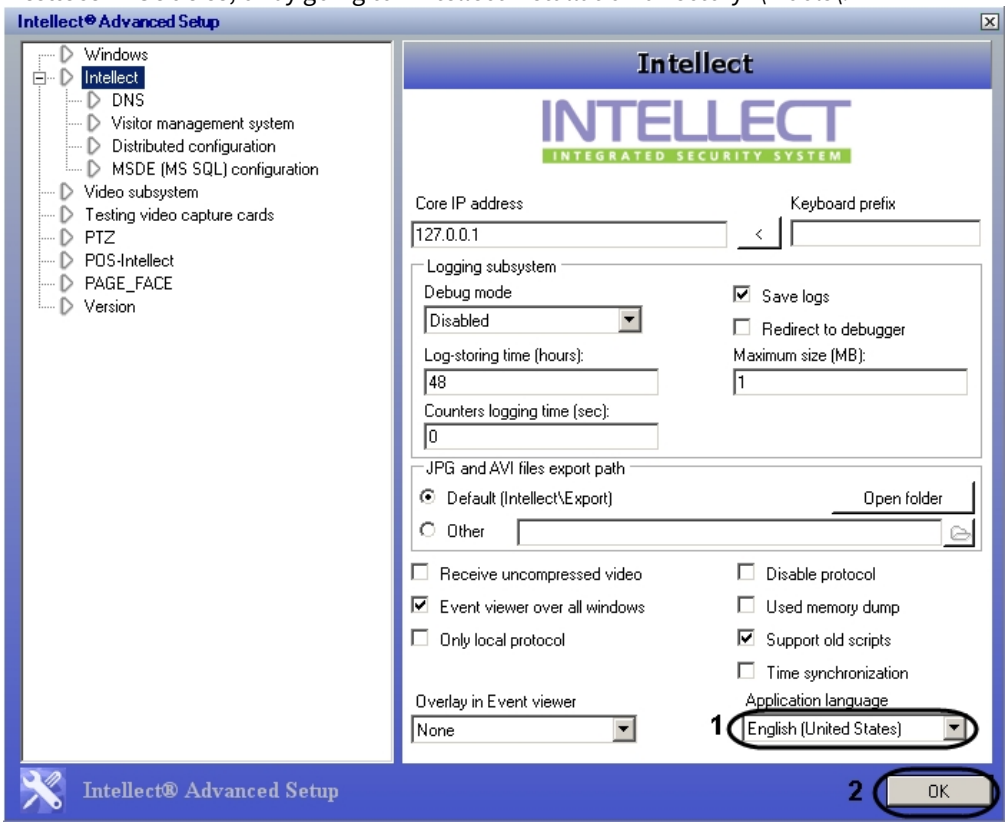
Languages are uninstalled when the *Intellect* Software System is uninstalled.

10.4.1.2 Switching languages in the Intellect Software System

Before switching languages, be sure the desired language has been installed (see see Installing INTELLECT™ software 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** –> **All Programs** –> **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.

10.4.2 Configuring the user interface

10.4.2.1 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.

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. Operator protocol;
14. 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.

10.4.2.2 Setup procedure for the displays

Screen creation is an important stage of the surveillance system design as it is the main working instrument of the Operator.

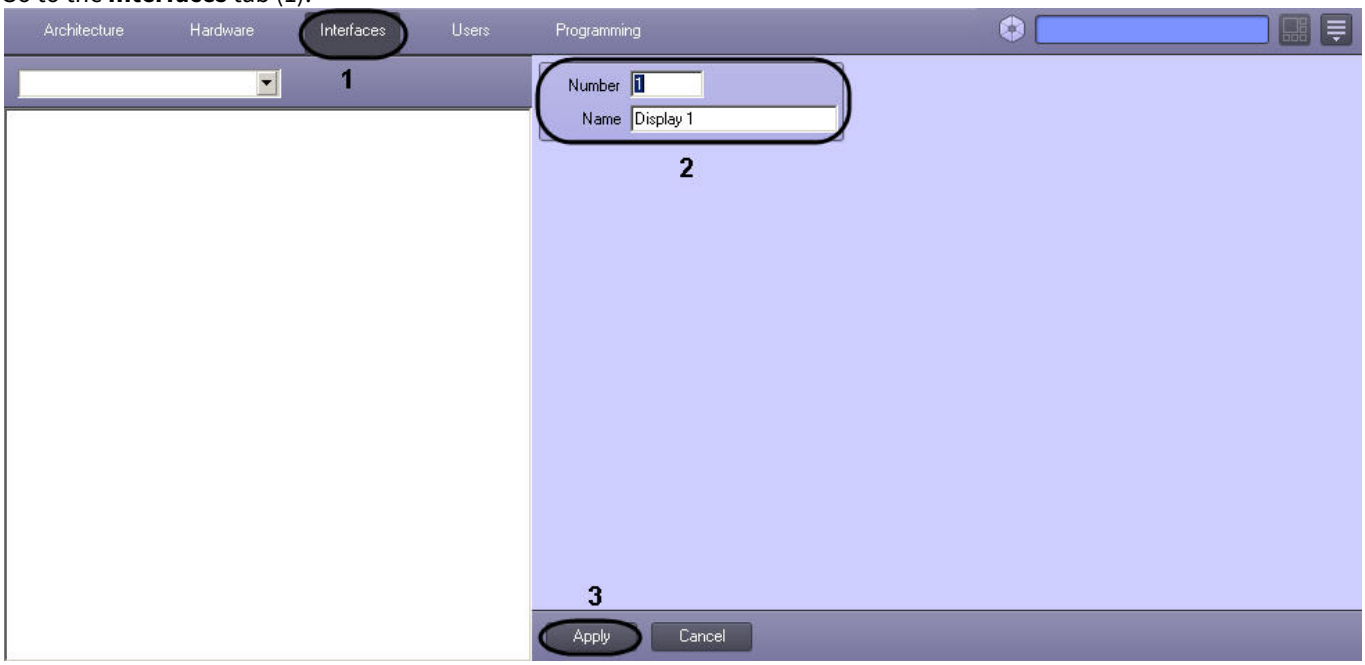
The screen is created in the **Interfaces** tab and includes the following stages:

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.

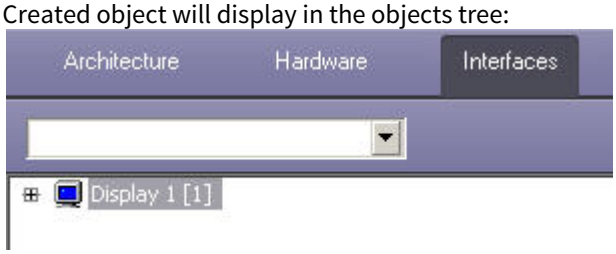
10.4.2.3 Creating a Display object

The **Display** object is created on the **Interfaces** tab of the **System settings** dialog window. After the Intellect software installation no one Display object is created on default. To create the first **Display** object, do the following:

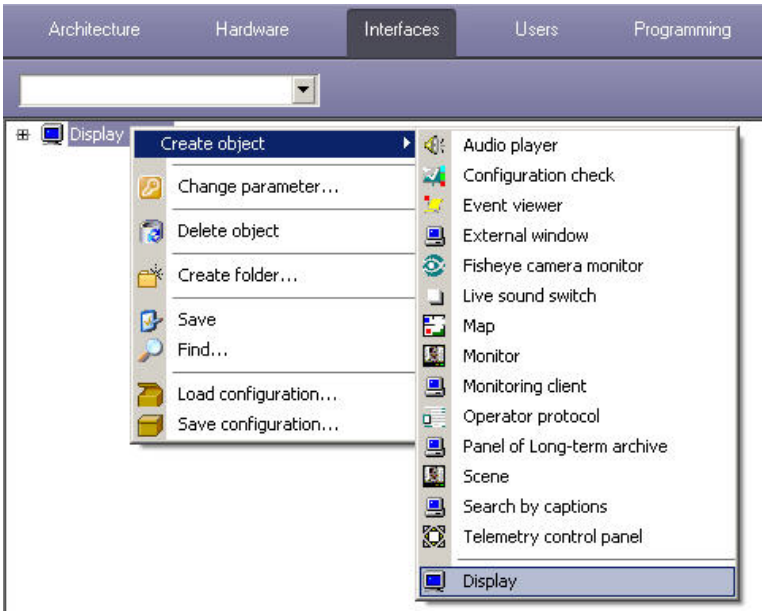
1. Go to the **Interfaces** tab (1).



2. Specify number and name of the creating **Display** object (2).
3. Click the **Apply** button (3).
4. Created object will display 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. Click the right mouse button on the **Display** object and select **Create object – Display** item in the functional menu.



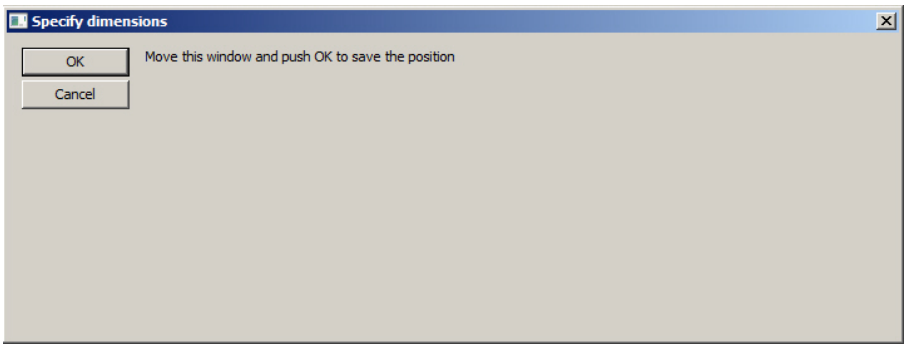
Then follow the instruction presented above from the step 2.

10.4.2.4 Placing the interface components on the screen

To place an interface component on the screen, its position (1) and window size (2) are to be specified.



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.



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). When several monitors are connected to a computer, select from the **Monitor** dropdown list the identifier of monitor in the operating system, for displaying on which the object coordinates are set (6).

> **Note.**
>
> If there is no **Monitor** dropdown list on the object setting panel, it is possible to set object position on non-primary monitor using negative coordinates or coordinates more than 100 depending on physical position of the monitor relative to the primary monitor. In this case it is strongly not recommended to use negative coordinates less than -200 (for example, -250, -300 etc.)

> **Note.**
>
> Intellect does not support NVIDIA® Mosaic™ multi-display technology.

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 shown semi-transparent (see The Settings panel of the Telemetry control panel object section).

Popup windows (**Alarm Message** and Operator's query) have no placing settings. They are displayed on top of other windows and can be moved to any place on the screen using the mouse.

10.4.2.5 Assigning the displays to the operator workstations

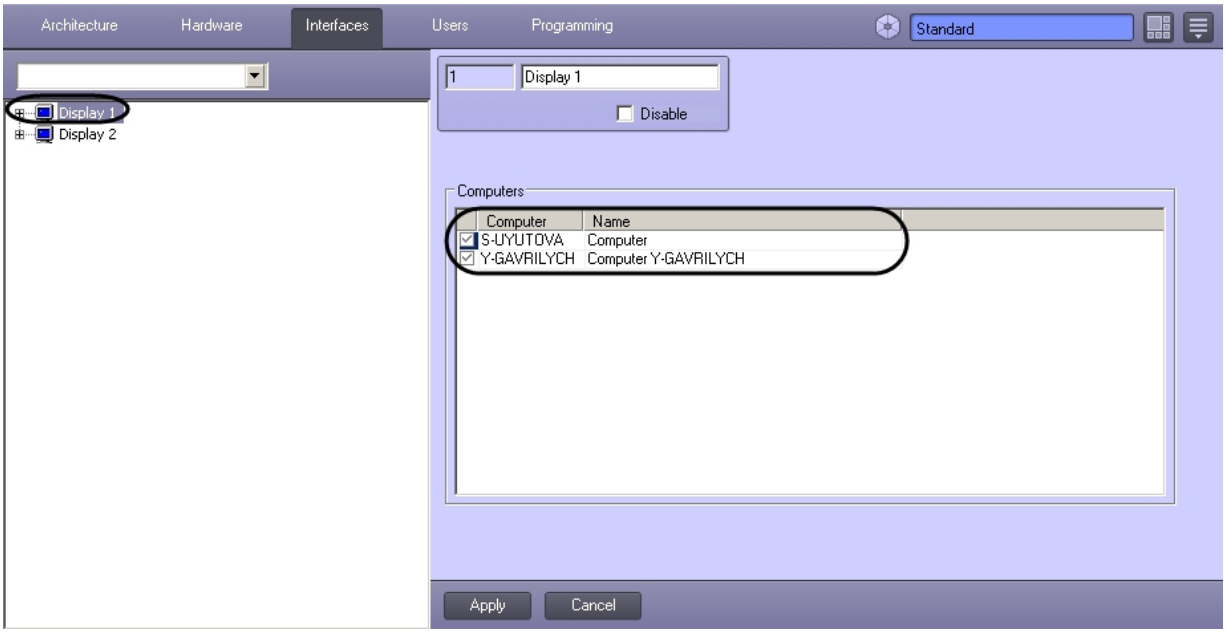
On the page:

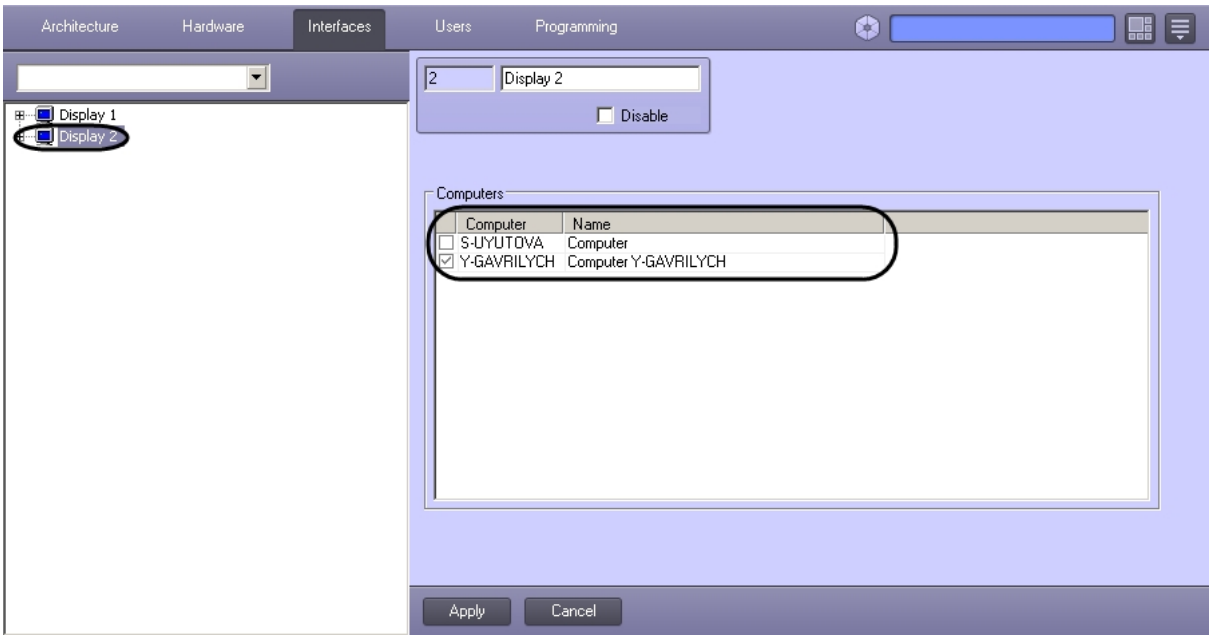
- Assigning displays manually
- Assigning displays via Wizard

To configure the access of several operator workstations to the same interfaces, the corresponding displays are to be assigned to these workstations. This can be done manually for each Display or via display assigning Wizard.

10.4.2.5.1 Assigning displays manually

The displays can be assigned to workstations on the settings panel of the **Display** object . Figures below show the configuration of two objects: **Display 1** and **Display 2**. **Display 1** will be available for both workstations, while **Display 2** will be available only for the Y-GAVRILYCH workstation.





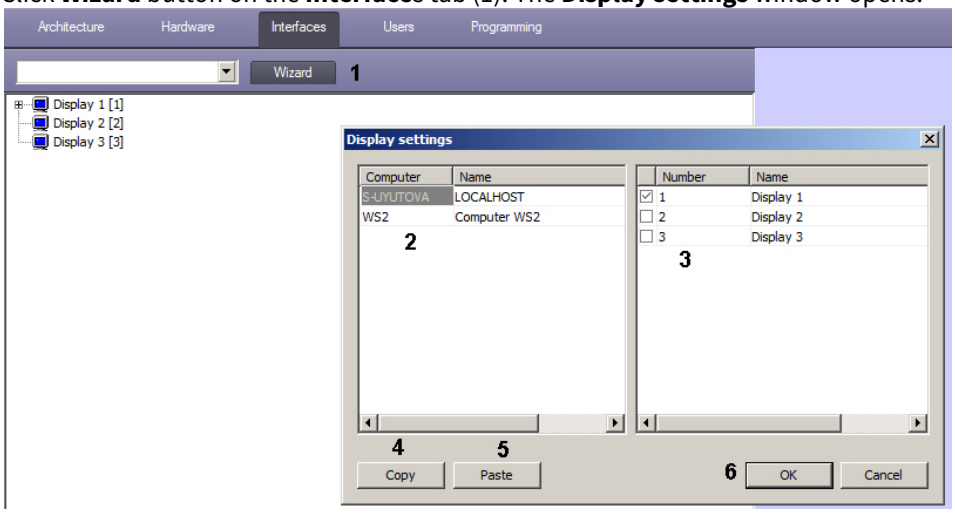
Note.

If the display assigning is performed from the Server which is not connected with some Servers of distributed system (the corresponding checkbox in the Architecture tab is not set – see the Configuring the interaction of distributed system components section), the data from this Server will not be displayed in the list of computers to which the current **Display** can be assigned. Settings of these Servers will not change after completing the display allocation.

10.4.2.5.2 Assigning displays via Wizard

Assign displays to computers via Wizard as follows:

1. Click **Wizard** button on the **Interface**s tab (1). The **Display settings** window opens.



2. Select the computer in the **Computer** column (2).
3. Set check boxes next to Displays to assign them to the selected computer (3).
4. Repeat steps 2-3 for all required **Computer** objects.

Note.

Use **Copy** (4) and **Paste** (5) buttons to copy the display list between computers. For example, to assign the same displays to the WS2 computer as those assigned to the S-UYUTOVA computer, do the following:

1. Select S-UYUTOVA computer in the **Display settings** dialog box.
2. Click **Copy** (4).
3. Select WS2 computer in the **Display settings** dialog box.
4. Click **Paste** (5).

5. Click **OK** (6).

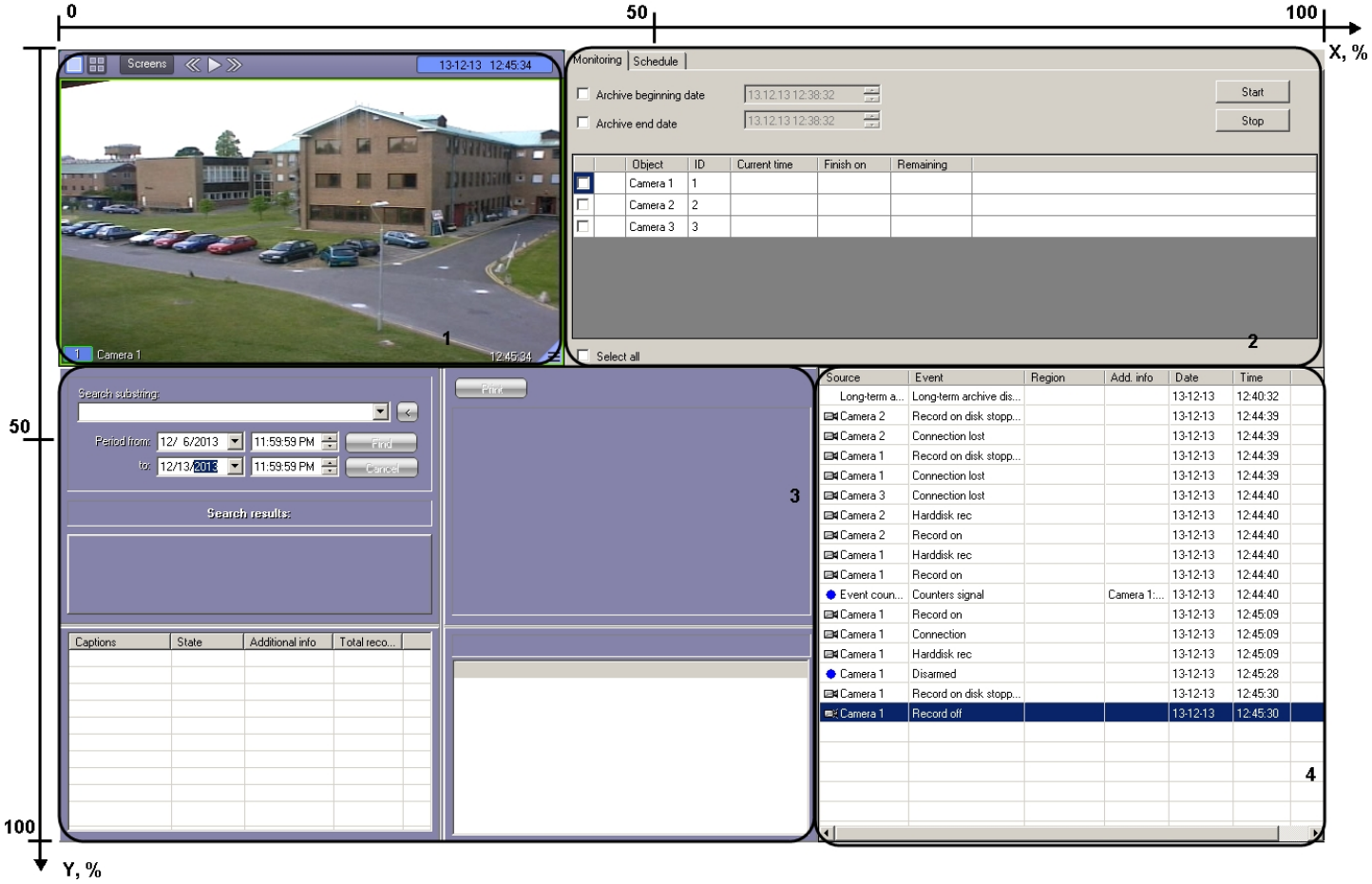
Displays are now assigned to computers.

10.4.2.6 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



10.4.3 Configuration of video display

10.4.3.1 Configuring video display on Video Surveillance Monitor

10.4.3.1.1 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 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.

Video surveillance monitor operation

10.4.3.1.2 Video monitor setup sequence

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.

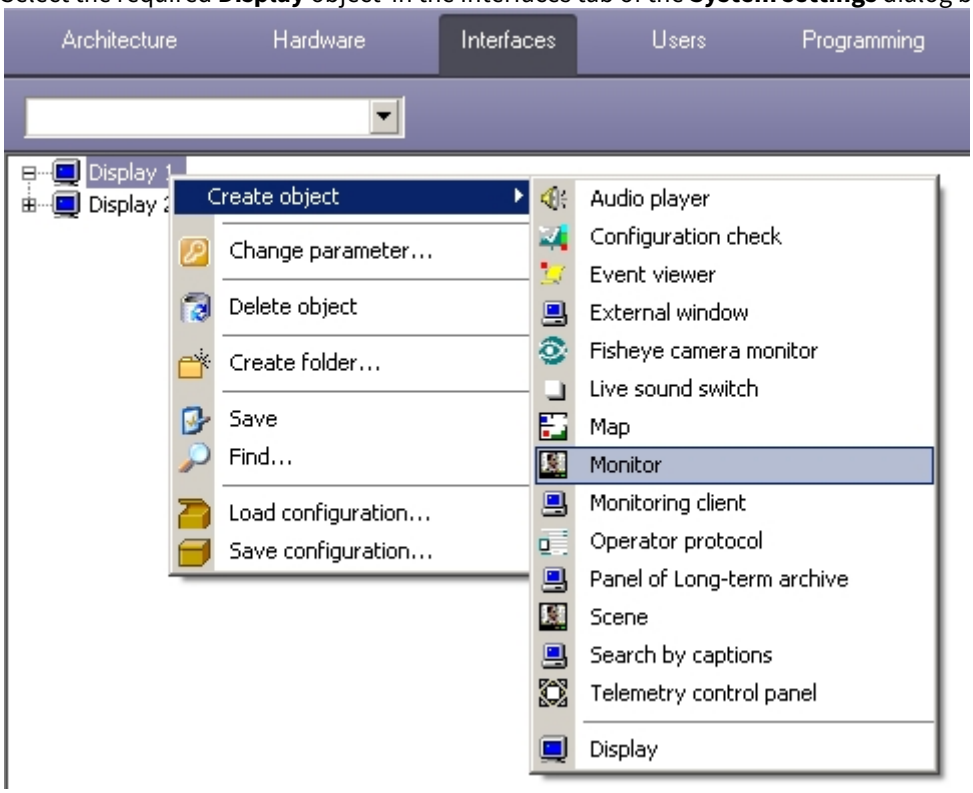
   Display objects are created on the **Interfaces** tab of the **System setting** dialog box (see Creating a Display object).

2. Set the parameters of the **Monitor** interface box (see Selecting 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 as a package).
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 for camera boxes).
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).

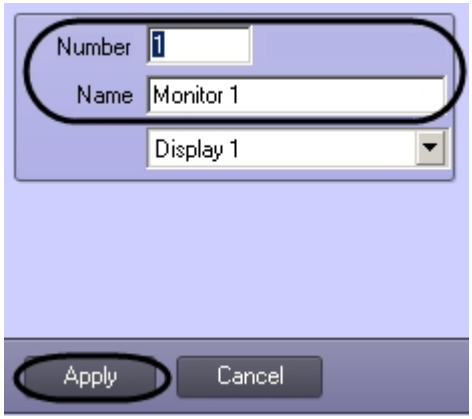
10.4.3.1.3 Creating the Monitor object

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.

10.4.3.1.4 Selecting the parameters of the Monitor interface box

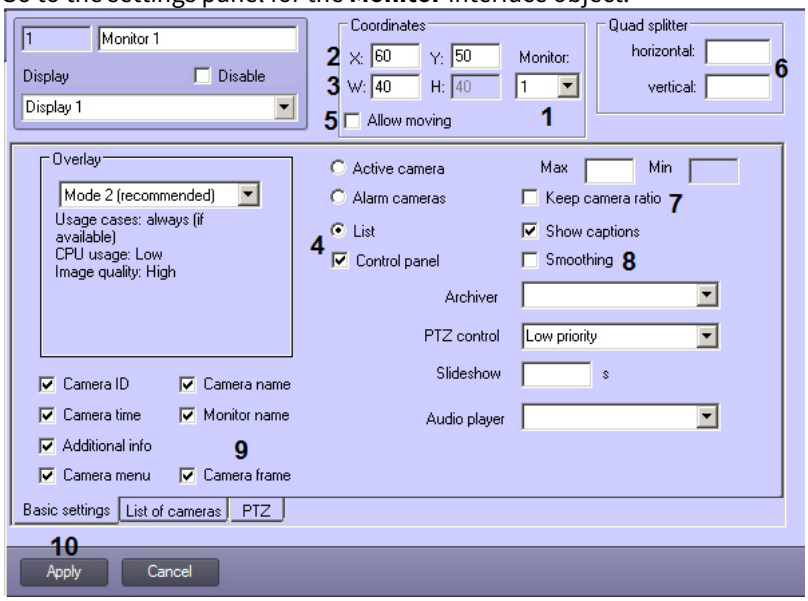
It is possible to set the following parameters of the **Monitor** interface box:

1. Window position.
2. Window size.
3. Toolbar (only in the List mode of camera's windows displaying - see Configuring the display mode for camera boxes 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.

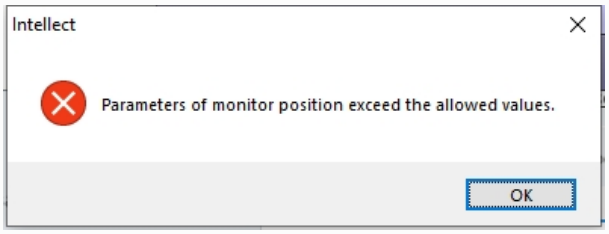
To set the parameters of the **Monitor** interface box, do the following:

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 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.

> **Note.**
>
> If the coordinates are set in such a way that the interface window will not be displayed on any connected computer monitor (for example, coordinates greater than 100 when only one monitor is connected), then corresponding warning is displayed when you click **Apply**. Such change of coordinates will not be applied.



4. 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.
5. 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 (4).

> **Note.**
>
> If the toolsbar 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.

6. If moving the **Monitor** interface box is to be enabled, set the **Allow moving** check box (5).

> **Note.**
>
> This setting is relevant only when the toolbar is in use.

7. 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 (6). 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.

> **Note.**
>
> The maximum number of surveillance windows in horizontal and vertical directions is 64.

> **Note.**
>
> Fields in the **Quad splitter** group are inactive if the **Alarm cameras** mode is selected (see the Configuring the display mode for camera boxes section).

8. If one wants 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 checked box on the **Basic settings** tab (7). If the checkbox is set checked, there may be some empty space in the Surveillance window. If the checkbox is set unchecked, 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.

9. Set the **Smoothing** checkbox to display video with greater resolution on which the ladder effect appears while displaying in the small window (8).

> **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

10. 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 unchecked (9).

> **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.

11. To save all the changes click the **Apply** button (10).

The parameters of the **Monitor** interface box are now set.

10.4.3.1.5 Selecting and configuring video cameras

One can select and configure cameras for displaying in two ways:

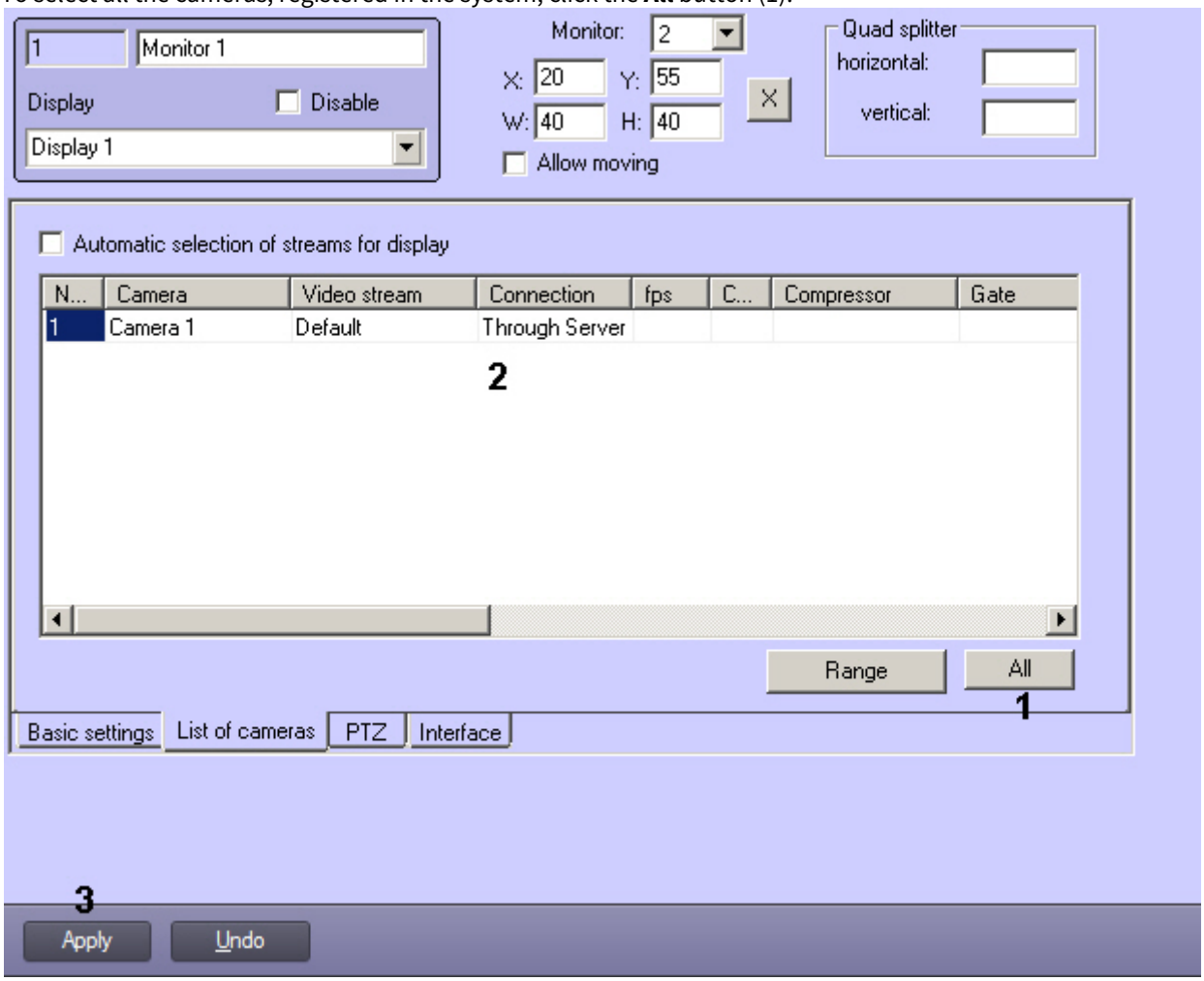
1. Separately. The settings panel for the **Monitor** object is in use.
2. As a package. The **Add/Edit Camera Objects** dialog box is in use.

Note.

Order of selecting video cameras as a package todisplay in the **Monitor** interface box is described in Selecting and configuring video cameras as a package section.

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 the cameras, registered in the system, click the **All** button (1).



3. To add a separate camera perform the following settings in table (2):
   a. Select the number of the required camera in the drop-down list of the **Number** column.
   b. As a result the name of the selected camera is automatically displayed in the **Camera** column.
   c. If multistream mode has been selected for a camera, in the **Video stream** drop-down list, select the number of the video stream that you want to display in the Monitor (4). If no stream is indicated, the default stream is used.

      Note.

      Configuration of Server video streams is described in the section 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 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 a camera directly, in the **Connection** drop-down list select **Direct**.
   e. If a video signal is to be thinned for its transmitting to the Monitor of the Client, then select the required frame rate of video signal in the drop-down list of the **fps** column.

Attention!

It is strongly not recommended to use additional thinning and / or compression of video signal which is displayed on the Monitor of a Server as it will lead to additional spending of Server resources and deterioration of video quality.

Note.

The selected fps value is to be less than the frame rate for video digitising by a video capture card. Otherwise the frame rate of video signal will be the same as the fps of digitising.

Note.

For correct thinning 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).

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 total fps is 10 (4 x 2,5fps) for one chip.

f. 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. 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.

g. To change the procedure of video signal compression during displaying on the Monitor, select the required procedure of compression from the **Compressor** drop-down list.The value in the **Compression** list is to be selected if the compressor is specified.

Note.

Compression is performed at the Gate.

h. If the Monitor is to receive live and archive video from the selected camera via the **Gate** object, then select the name of this object in the drop-down list of the **Gate** column.

i. 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 drop-down list of the **Backup archive** column.

Note.

In case of access to the Backup archive is performed through the Video gate, specified value is to be coincide with selected value for this video camera while configuring the **Video gate** object – see the Selecting and configuring the cameras for the Backup archive section.

j. If the selected video camera is used for video archive viewing from the external storage, then select the required **External storage** object in the **External storage** drop-down list.

k. If the tansmission from the **Backup archive** object is performed via the **Gate** object, then select the name of this object in the drop-down list of the **Gateway 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 trajectories database intended to use for smart search from the **VMDA metadata storage** drop-down list.
m. If there is a fisheye or anamorphic lens on the camera (see Configuring fisheye cameras), then in the **Display type** dropdown list select the way of displaying video from camera on the viewing tile: virtual telemetry or panorama.

> **Note.**
>
> Conversion is enabled in the Video surveillance monitor when zooming-in (see Mouse PTZ control) or in the feature menu of the Surveillance window (see Enabling fisheye).

> **Note.**
>
> **This feature will be invalid if:**
>
> - only alarm cameras are displayed on the monitor (see Configuring the display mode for camera boxes);
>
> - PTZ control on the Video surveillance monitor is forbidden (see Setting the Telemetry control priority using the Monitor object).

n. If macros are to be run from the camera functional menu in the Video Surveillance Window, select the **Macro** objects in the **Macro 1** and **Macro 2** lists. See also Creating and using macros.
o. Repeat steps a-n for all required video cameras.

4. To save all the changes click the **Apply** button (3).

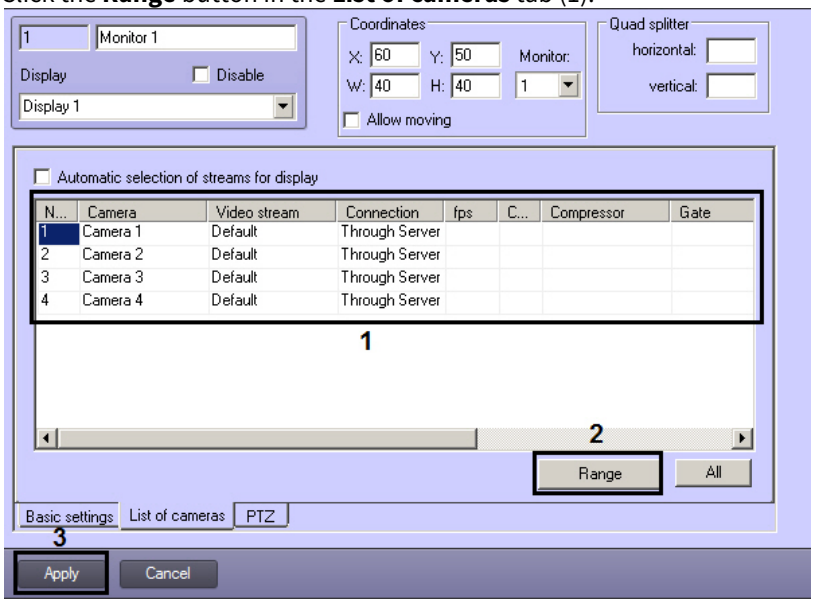
Video cameras on the settings panel of the **Monitor** object are now selected.

10.4.3.1.6 Selecting and configuring video cameras as a package

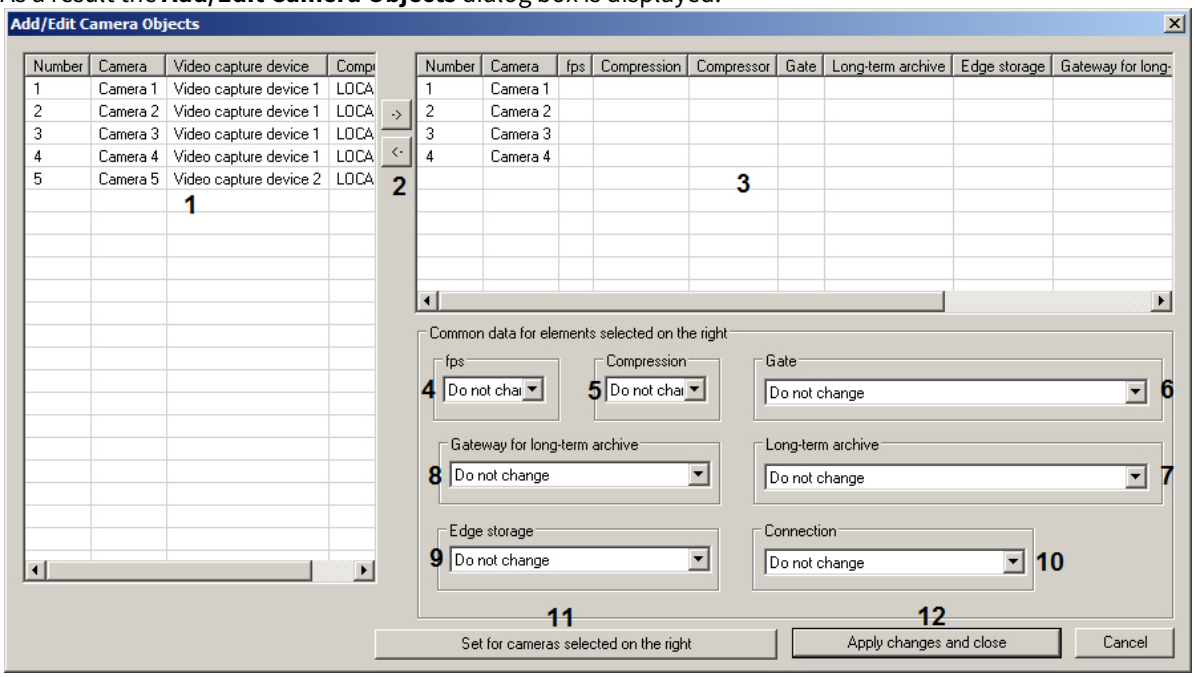
One can select and configure video camera parameters as a package to display them in the **Monitor** interface box.

To select video cameras as a package, 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).

6. As a result the selected cameras will be displayed in the list on the right of the 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. If a video signal is to be thinned for transmitting to the Monitor of the Client, then select the required frame rate of a video signal in the fps drop-down list (4).

> **Note.**
>
> The selected fps value is to be less than the frame rate for video digitising by a video capture card. Otherwise the frame rate of video signal will be the same as the fps of digitising.
> The **fps**, **Compression**, **Gate**, **Backup archive** and **Gateway for Backup Archive** settings are in the **Common data for the elements selected in the list on the right** group.
> For correct thinning 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. 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 (7).
12. If the tansmission 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 (8).
13. Select the required object from the **External storage** drop-down list if cameras are in use to view the video archive from the external storage (9).
14. 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** (10).
15. To save the set parameters, click the **Save for the cameras selected in the list on the right** button (11).
16. As a result set parameters will be displayed in the list on the right of the **Add/Edit Camera Objects** box (3).
17. Repeat steps 6-12 for complex editing of all required cameras.
18. To save all the canges and close the **Add/Edit Camera Objects** box, click the **Apply** changes and close button (12).
19. Set camera settings will be displayed in the **List** table on the settings panel of the **Monitor** object (2).
20. To save all the changes click the **Apply** button (3).

Video cameras are now selected as a package.

10.4.3.1.7 Configuring an auto select of video stream for displaying

In the Intellect software 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 video image. For example, if a large number of 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 function of video stream auto select is enabled, the *Intellec*t software 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.

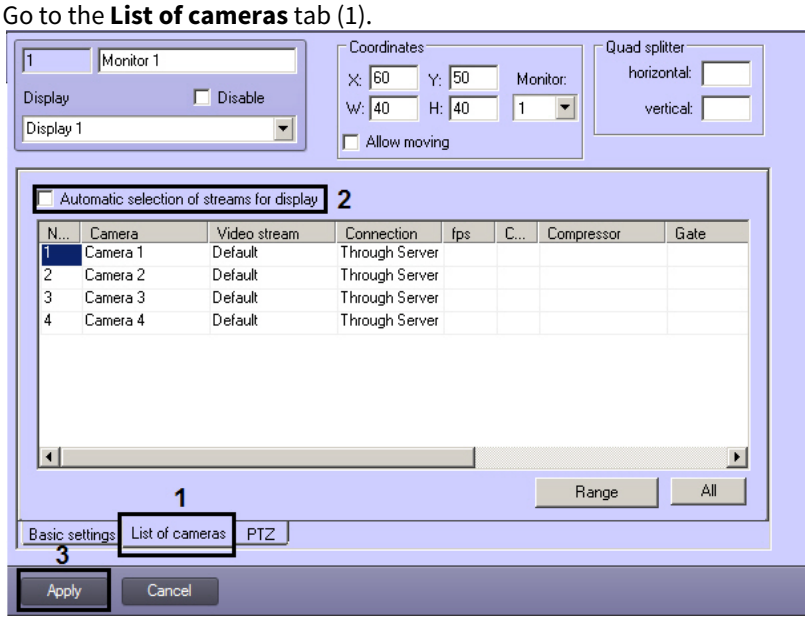
If automatic stream selection is enabled, selection will be performed for the cameras for which the **Default** video stream has been selected.

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 **Auto selection of streams for display** checkbox (2).
4. Click the **Apply** button (3).

Configuring an auto select of video stream for displaying is completed.

10.4.3.1.8 Configuring the display mode for camera boxes

To display camera boxes (windows with video images) one of the following modes is in use:

1. The **Active camera** mode. Only active camera box is displayed in the Monitor interface box.

> **Note.**
>
> To make camera box active click upon it with the left mouse button. A camera box is switched to the active mode using another Video surveillance monitor. So, when the **Active camera** display mode is in use, more than one **Monitor** object is to 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 camera selected on Map or Operator Protocol created based on the same **Display** object as the **Monitor** object is also displayed on the Video surveillance monitor in the **Active camera** mode.

2. The **Alarms cameras** mode. The boxes of alarm cameras are displayed in the **Monitor** interface box.
3. The **List** mode. Camera boxes are displayed in the **Monitor** box according to the selected layout.

Functions available in the **List** mode:

1. Control panel;
2. Slideshow.

The control panel is displayed in the the **Monitor** interface box and enables the following operations:

1. Select the number of dislayed cameras;
2. Set and use the layouts of cameras;
3. Control the slideshow.

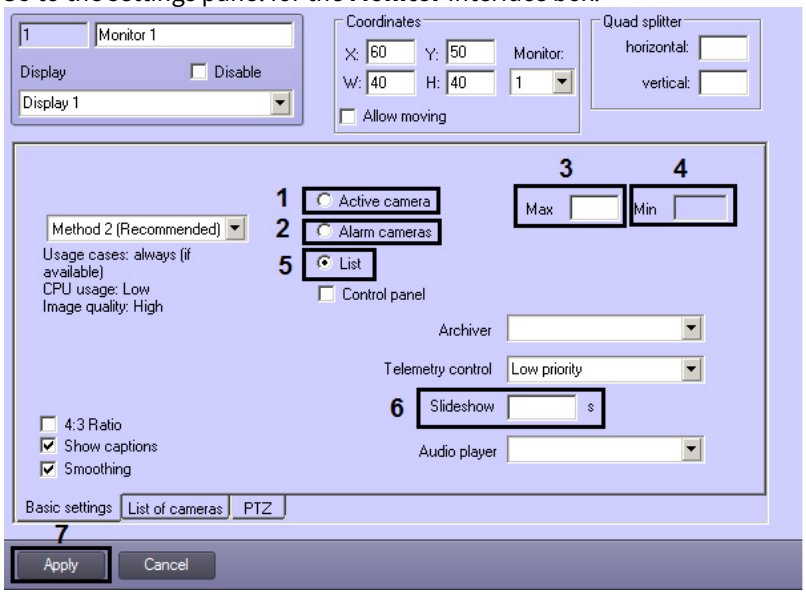
Current date and time are also displayed on the control panel.

Slideshow is used for successive close-up displaying of camera boxes on the Monitor. Slideshow is performed with the help of the buttons on the toolbar of the Monitor in two ways:

1. Manually. Buttons of switching to the previous or next camera box are in use.
2. Automatically.Switching to the next camera box is performed automatically in a set period of time.

To set the display mode for camera boxes, do the following:

1. Go to the settings panel for the **Monitor** interface box.



2. To activate the **Active camera** mode, set the **Active camera** switch in the **Basic settings** tab (1).
3. To activate the **Alarm cameras** mode, set the **Alarm cameras** switch in the **Basic settings** tab (2). As a result the **Min.** field is available.
4. In the **Max** field specify the required maximum number of cameras boxes which are to be displayed on the Monitor (3). If the number of alarm cameras exceeds the maximum one, then displaying of camera boxes, alarms on which have been registered earlier, is stopped.

   Example.

   The **Monitor** object is set for operation with maximum number of alarm cameras, equal to 5. Boxes of 4 alarm cameras are displayed in the Monitor box. Alarms on these cameras have been registered in the following sequence: Camera 1, Camera 2, Camera 3 and Camera4. When alarm has been registered on three more cameras, seven cameras are alarmed at the same time.This exceeds a maximum acceptable number, so the displaying of Camera 1 and Camera 2 boxes is stopped.

5. In the **Min** field specify the required minimum layout to be displayed on the Monitor (4). If the number of alarm cameras is less than a minimum one, then less than minimum boxes of cameras are displayed on the Monitor while size of boxes stays according to the **Min.** field. The following layouts (number of camera boxes) are available: 1, 4, 9, etc.

   Example.

   The **Monitor** object is set for operation with minimum number of alarm cameras, equal to 3. Boxes of 5 alarm cameras are displayed in the Monitor box. When alarm on 4 cameras is stopped in the consequence: Camera 1, Camera 2, Camera 3 and Camera 4, one camera is in the alarm mode. This is less than a minimum number, so Camera 5 is displayed on the Monitor in a size corresponding to layout with 4 camera boxes.

6. On no- alarm if the default value (0) of the **Min** parameter is set, camera boxes are not displayed in the Monitor box.
7. To activate the **List** mode, set the **List** switch in the **Basic settings** tab (5).

8. If necessary specify the required value (in seconds) of automatic slideshow for camera boxes in the **Slideshow** field (6).

   Note.

   This setting is relevant only if the toolbar is in use in the **List** mode.

9. To save all the changes click the **Apply** button (7).

The display mode for camera boxes is now configured.

10.4.3.1.9 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 improvs the image due to optimization of the pixel color settings. At the same time, the CPU's load is reduced, as the video image is processed with the resources of the video card.

There are three display modes in INTELLECT™ software:

1. **Direct3D**. In this mode, more modern, but less stable Windows graphics libraries are used. The mode is used when it is necessary to display the video from Fisheye cameras or the signal decoded using Intel QuickSync technology. This mode is also used if the DirectDraw mode is not supported by a video card.

   Note

   The Direct3D mode will be enabled automatically when its usage is specifically necessary to display the video, for example, if there is a Fisheye camera on the layout. The manual modes selection is available for the cases when there are display problems, and it is necessary to swith modes manually.

2. **DirectDraw (recommended)**. In this mode, more stable Windows graphics libraries are used. Currently, the DirectDraw and Direct3D features are about the same. This mode is used by default if Direct3D is not specifically required to display the video (see the note above).
3. **Programmed**. Video signals from cameras are not processed by a video capture card.

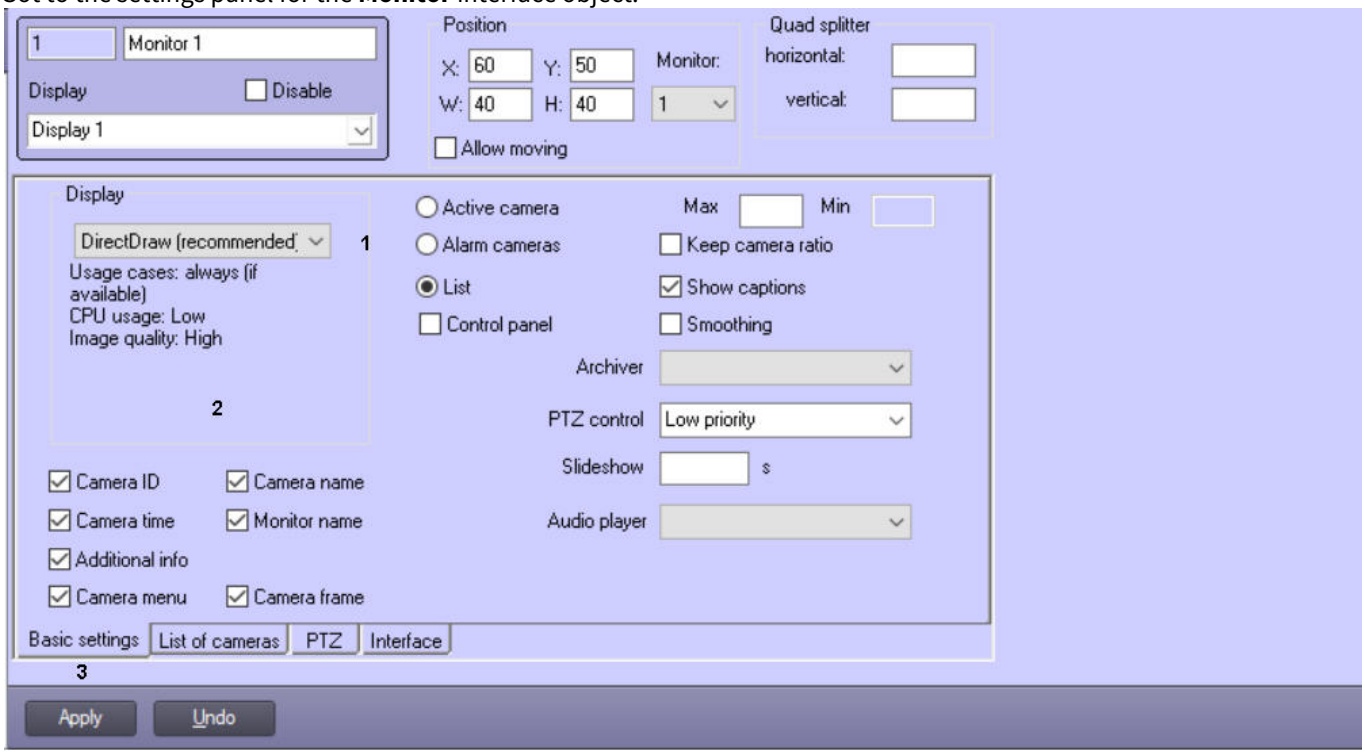
As a rule, the **DirectDraw** is the optimal display mode. This mode is supported by the most of video capture cards. If a video capture card doesn't support the chosen display mode, then a video signal is displayed with a big slowing-down.

Note.

For correct display mode operation in INTELLECT™ software, installed as a Server, 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 for displaying icons on the user desktop.

To select a display mode, do the following:

1. Got to the settings panel for the **Monitor** interface object.



2. Select the required display mode in the **Display** drop-down list in the **Basic settings** tab (1).

> **Note.**
>
> There is a description of the selected display mode in the field below the **Display** drop-down list (2).

3. To save all the changes, click the **Apply** button (3).

The display mode is now selected.

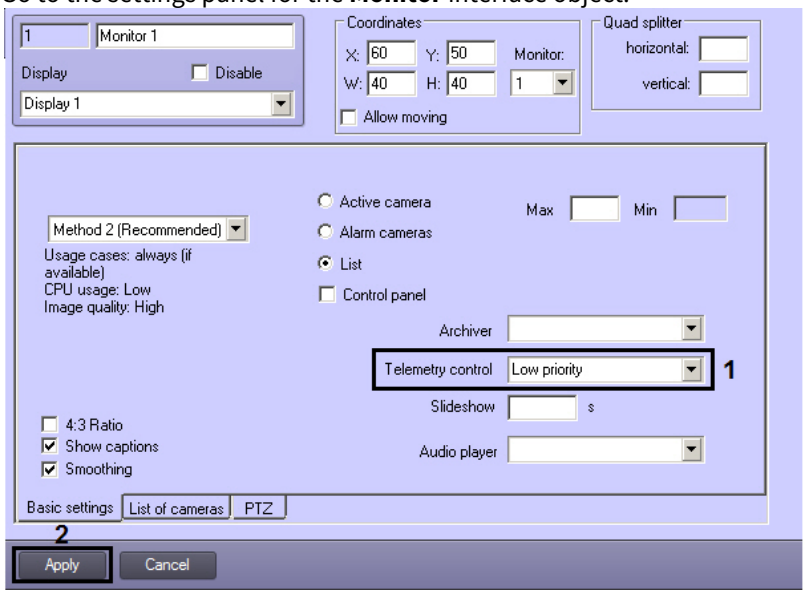
10.4.3.1.10 Setting the Telemetry control priority using the Monitor object

INTELLECT™ software 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 **Telemetry control** drop-down list in the **Basic settings** tab (1).

> **Note.**
>
> To disable **Telemetry 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.

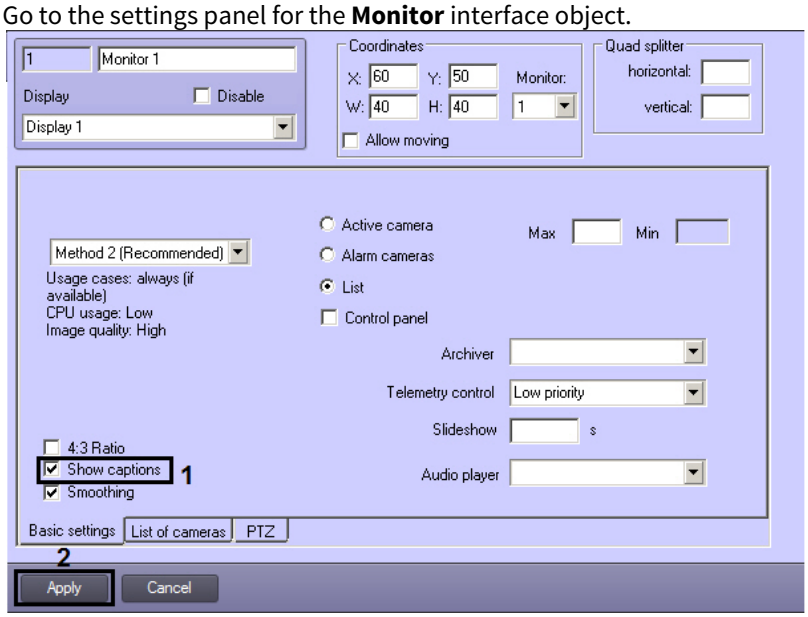
10.4.3.1.11 Configuring the captions showing

10.4.3.1.11.1 Enabling the captions showing

INTELLECT™ software 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, uncheck 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.

10.4.3.1.11.2 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.

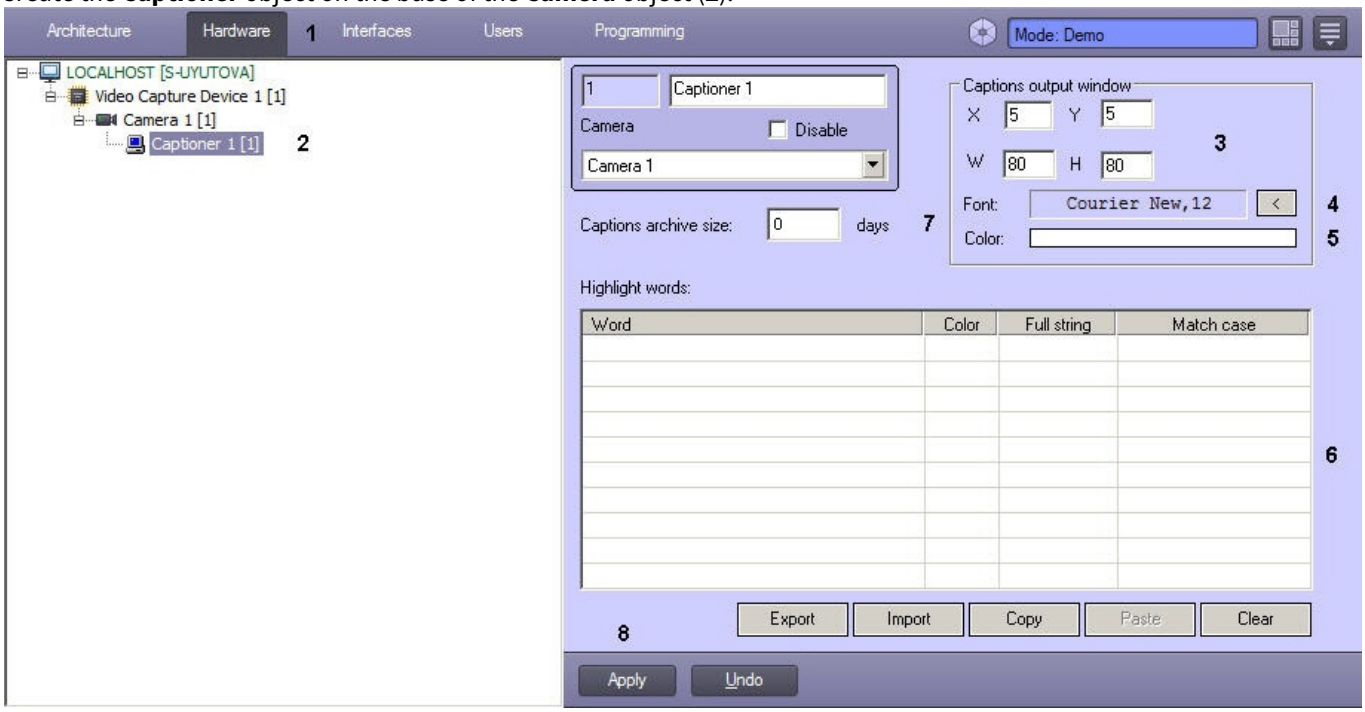
This object allows setting the limits of titles output, font parameters and color of words. Titles are output into the field on a video recording from a camera.

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 Programming Guide (JScript)).

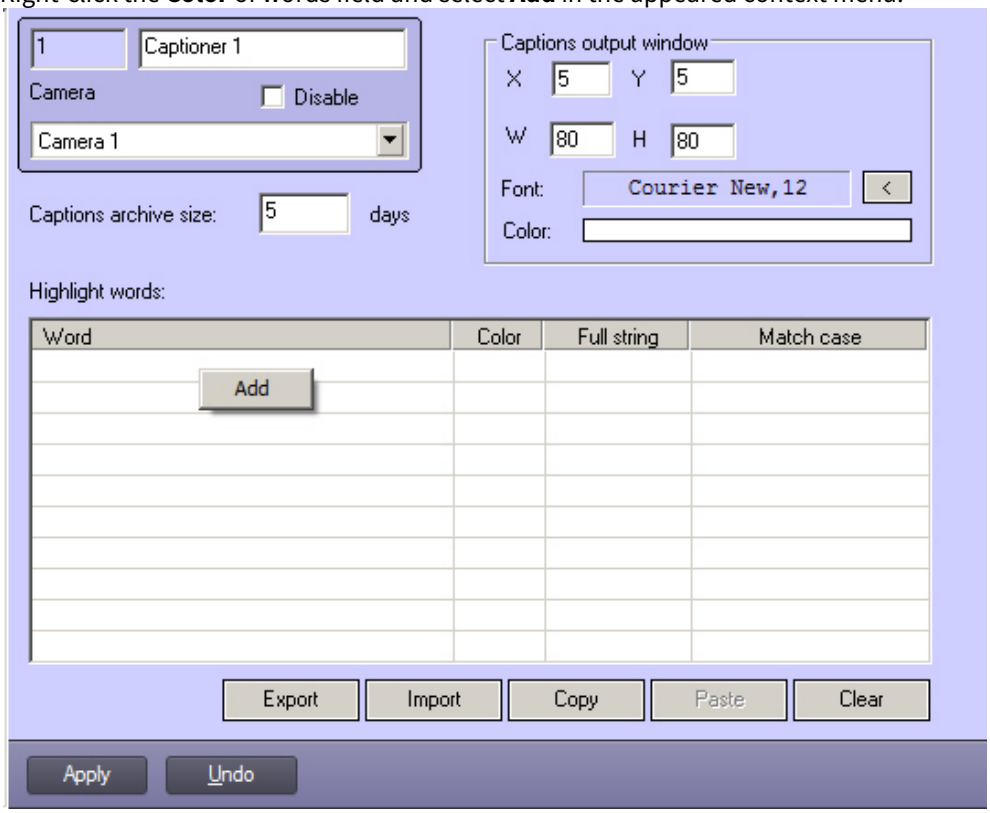
To configure the **Captioner** object, do the following:

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.

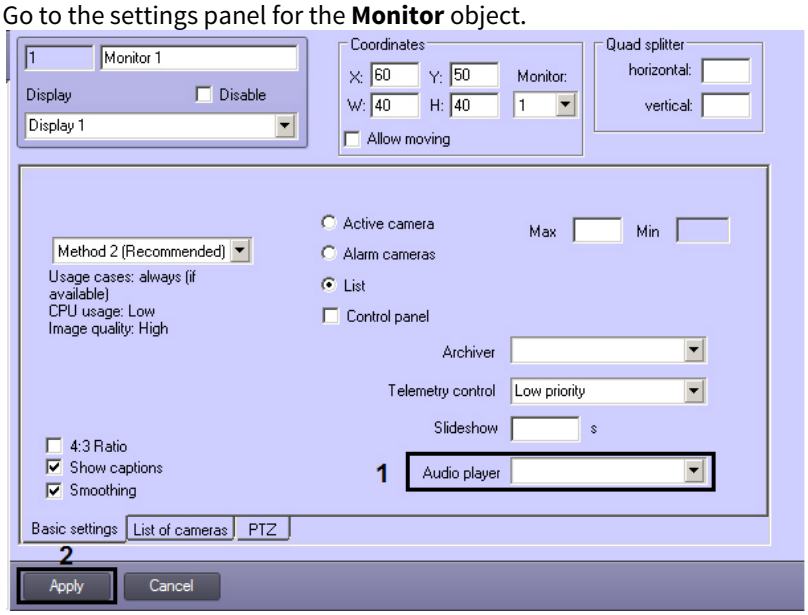
10.4.3.1.12 Binding Audio player to the Monitor

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 ho create and configure the **Audio player** object is given in the Configuring audio signals playback using the Audio player object section.

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** dropdown 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).

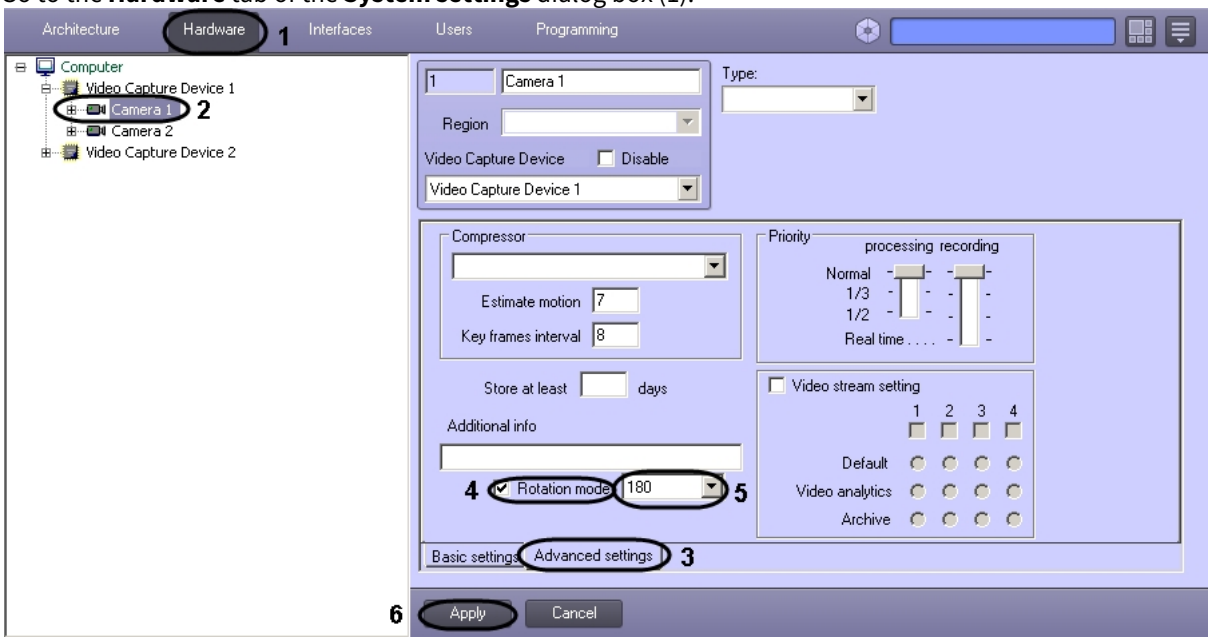
The Audio player is now bound to the Monitor.

10.4.3.1.13 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.

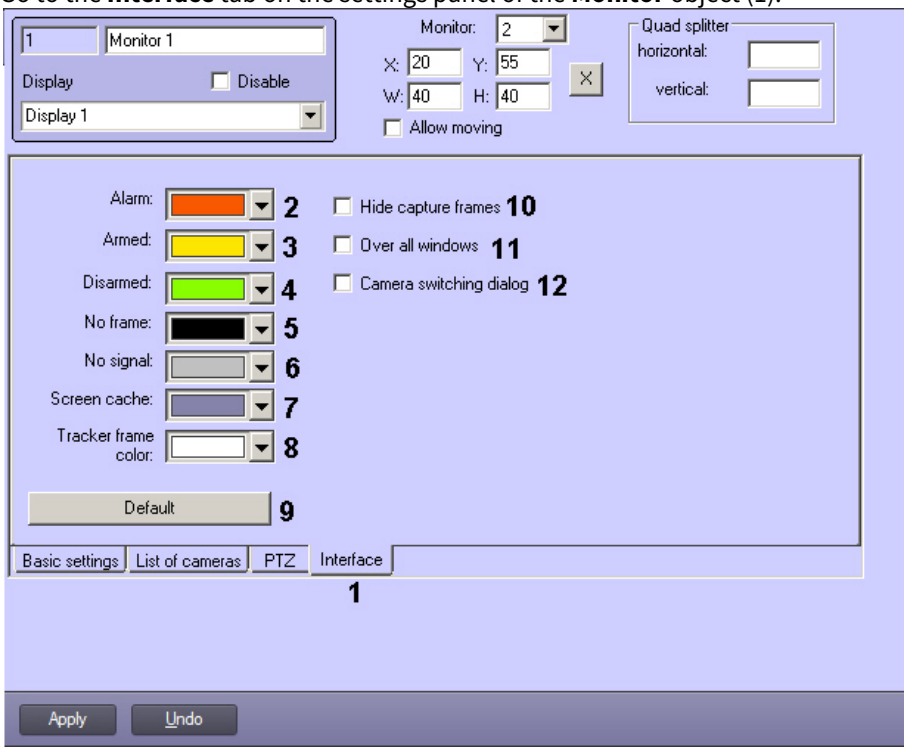
Configuring a rotation angle of the video image is completed.

10.4.3.1.14 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.

10.4.3.2 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.

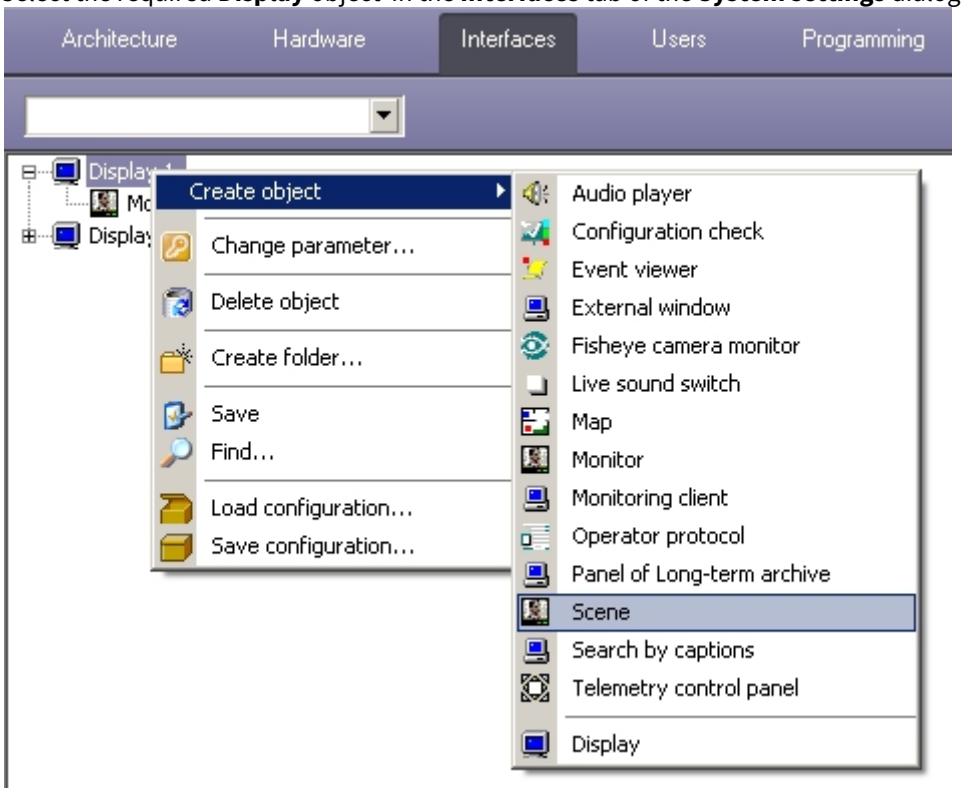
Working with Panoramic view window is described in detail in Operator's Guide.

Working with panoramic video surveilance window

10.4.3.2.1 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.

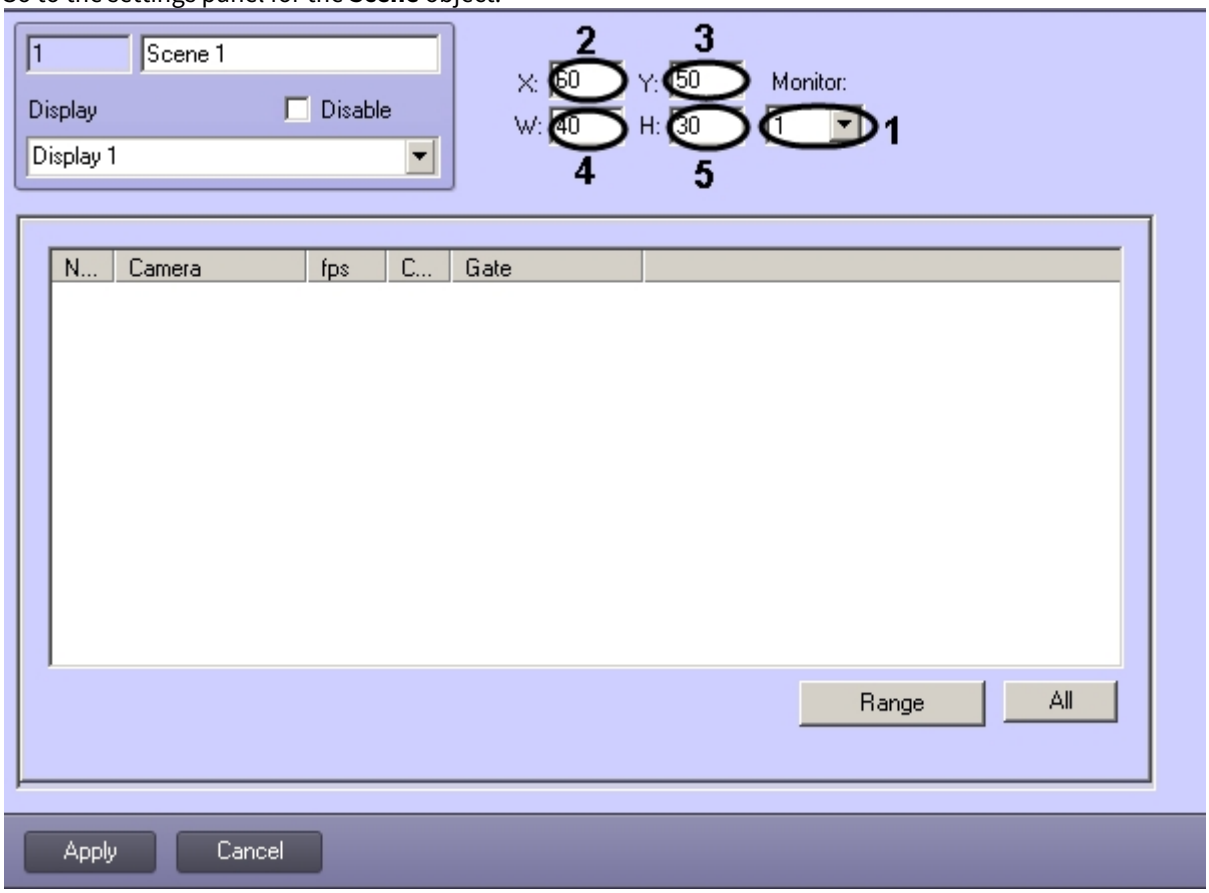
4. Repeat steps 1-3 for all required **Display** and **Scene** objects.

The **Scene** object is now created.

10.4.3.2.2 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.

10.4.3.2.3 Selecting and configuring cameras for the Scene object

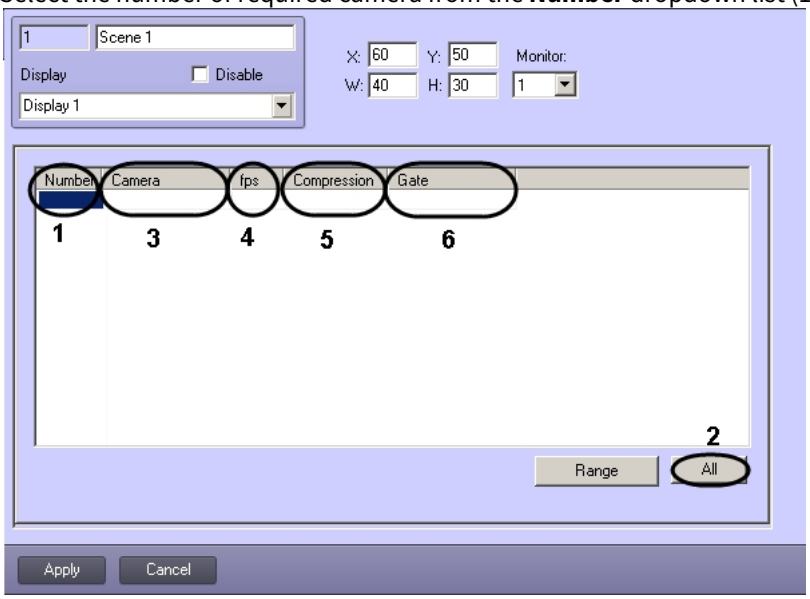
One can select and configure cameras for displaying in the interface box in two ways:

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 thinned, 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.

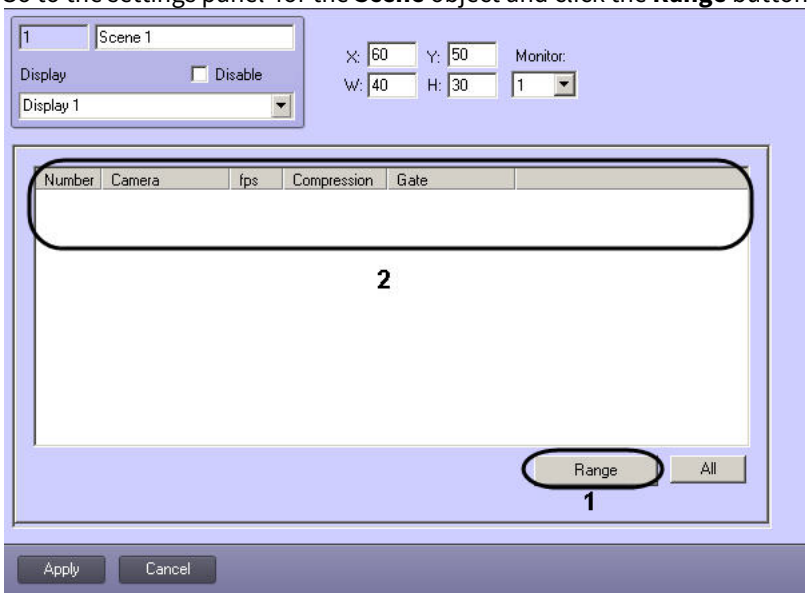
8. Click the **Apply** button to save the changes.

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 as a package 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.

10.4.3.3 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 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 scaling 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 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.

10.4.4 Configuration of audio

10.4.4.1 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

10.4.4.2 Configuring audio signals playback using the Audio player object

10.4.4.2.1 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 **Audio player** object do the following:

1. Select the screen and create for it **Audio player** object.
2. Set the parameters of **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 transmition of audio signals to IP-device is described in the Setting up the transmission of video signals to IP-devices and the Setting up the transmission of audio signals to IP-device Bosch.

Note.

The Audio player uses PCM (preferrable) or GSM (legacy) codecs. The codec is selected automatically.

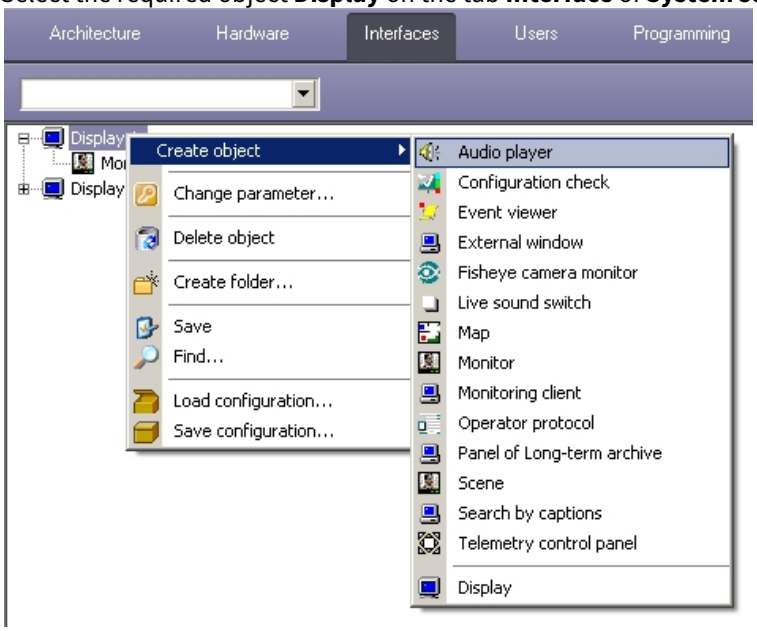
Audio bitrate does not change when played back via the Audio player.

Audio player operation

10.4.4.2.2 Creating the Audio player object

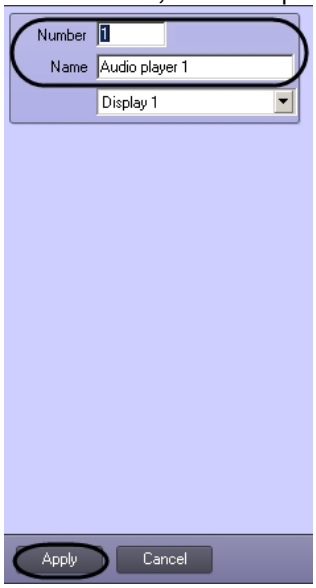
To create the **Audio player** object do the following:

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 contectual 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.

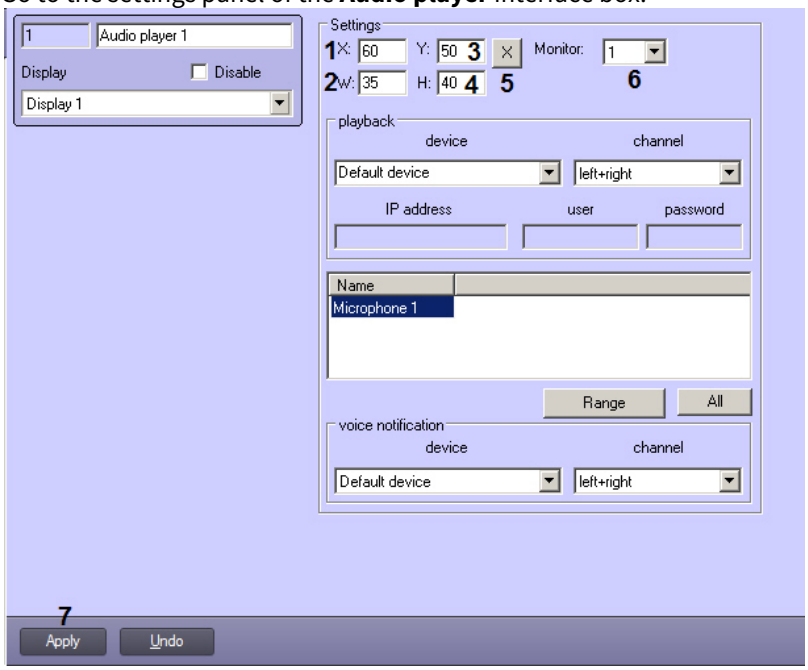
4. Repeat steps 1-3 for all the required objects **Display** and **Audio player.**

Creation of **Audio player** object is over.

10.4.4.2.3 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.

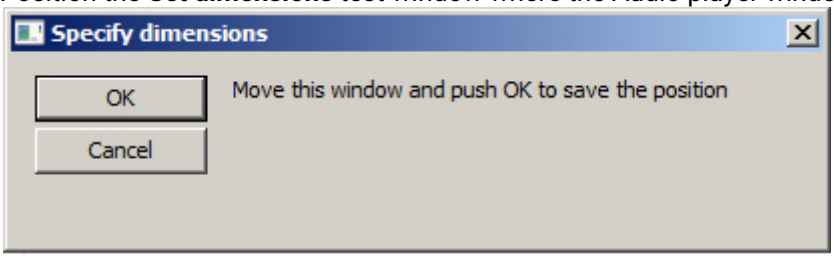


2. Set the **Audio player** interface box position in one of the following ways:
    a. Manually:
        i. Set the coordinates of **Audio player** window's left upper corner: fields **X** (horizontal indent from the left image border) and **Y** (vertical indent from the upper image border - 1 and 2. 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.

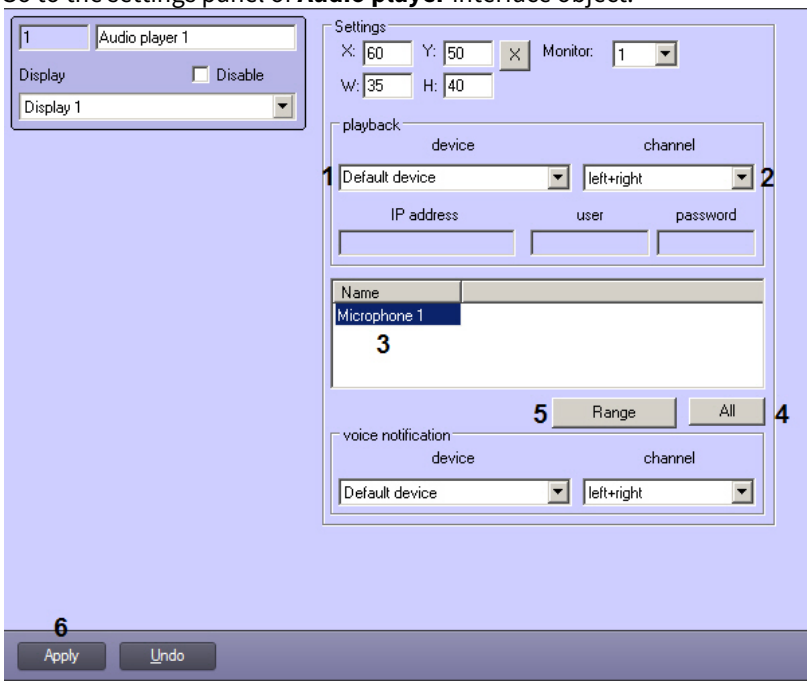
10.4.4.2.4 Setting up the recording and audio signals' playback

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).

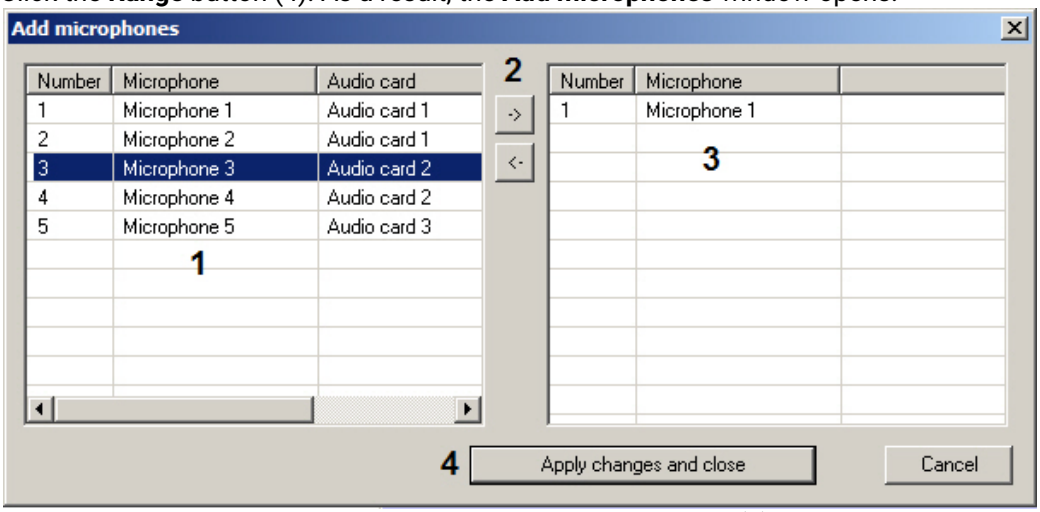
> **Note.**
>
> Standard sound map corresponds to to the value **Default device**.

3. From the dropdown list **Channel** of **Playback** group select the required channel of audio signals backup (2).
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.

10.4.4.3 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 supported with sound section of Operator's Guide.

10.4.4.4 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.

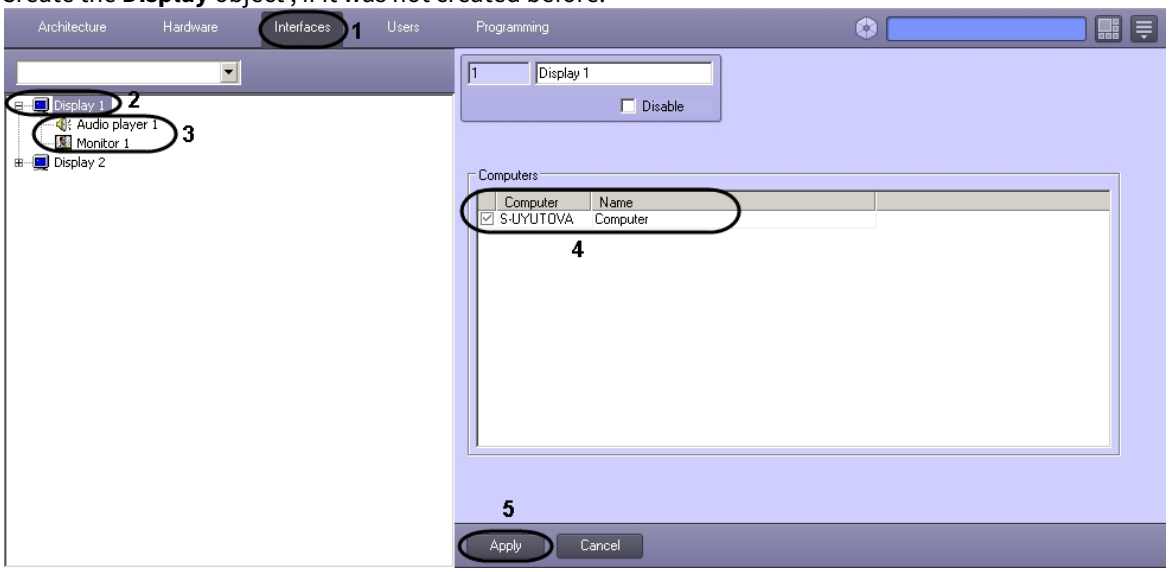
Audio signal transmission to Remote Workplaces and servers, connected by the TCP/IP net, is performed only via **Video surveillance monitor** or **Audio player** interface objects.

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.

10.4.5 Configuring the interactive map for object state indication and controlling the objects

10.4.5.1 General information on the structure of the interactive map of the guarded location

The interactive map of the *Intellect* system uses graphical diagrams of the guarded 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

10.4.5.2 Configuring the interactive map

10.4.5.2.1 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 location 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).

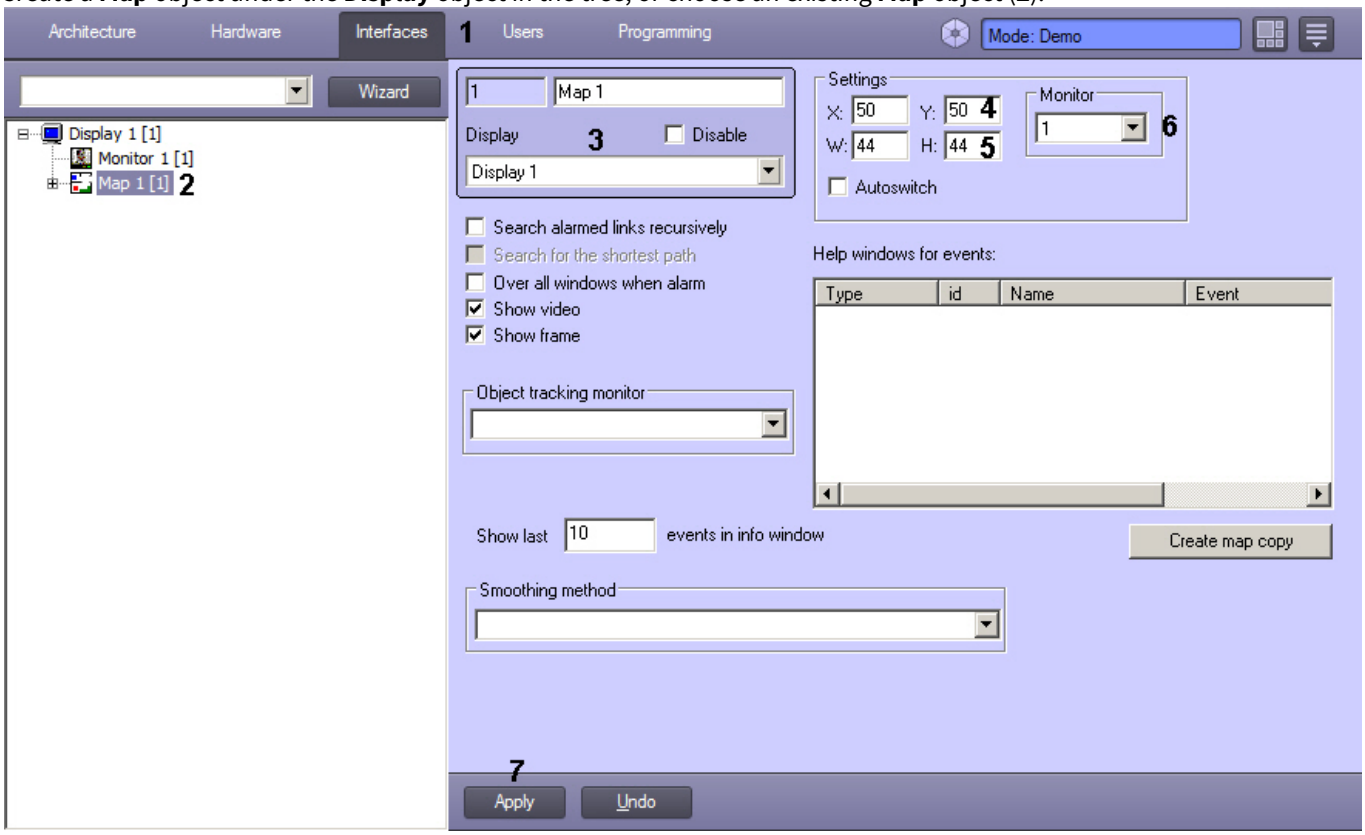
10.4.5.2.2 Setting up the location of the map on the screen

To register the interactive map in the *Intellect* system, create the **Map** interface object.

When setting up the **Map** object, specify the position of the map on the screen.

To register the map and specify its position on the screen, do the following:

1. Open the **Interfaces** tab of the **System Settings** window (**1**).
2. Create a **Map** object under the **Display** object in the tree, or choose an existing **Map** object (**2**).



3. Specify an id and name for the **Map** object, and choose the **Display** object to become the parent of the map (**3**).
4. Set the coordinates **X** and **Y** of the upper left corner of the **Map** window, as a percentage of the corresponding screen dimensions (**4**).
5. Specify the width (**W**) and height (**H**) of the **Map** window, as a percentage of the corresponding dimensions of the screen (**5**).
6. From the **Monitor** drop-down list select the number of monitor for which coordinates are specifying (**6**).
7. Press the **Apply** button to save all changes made to the settings (**7**).

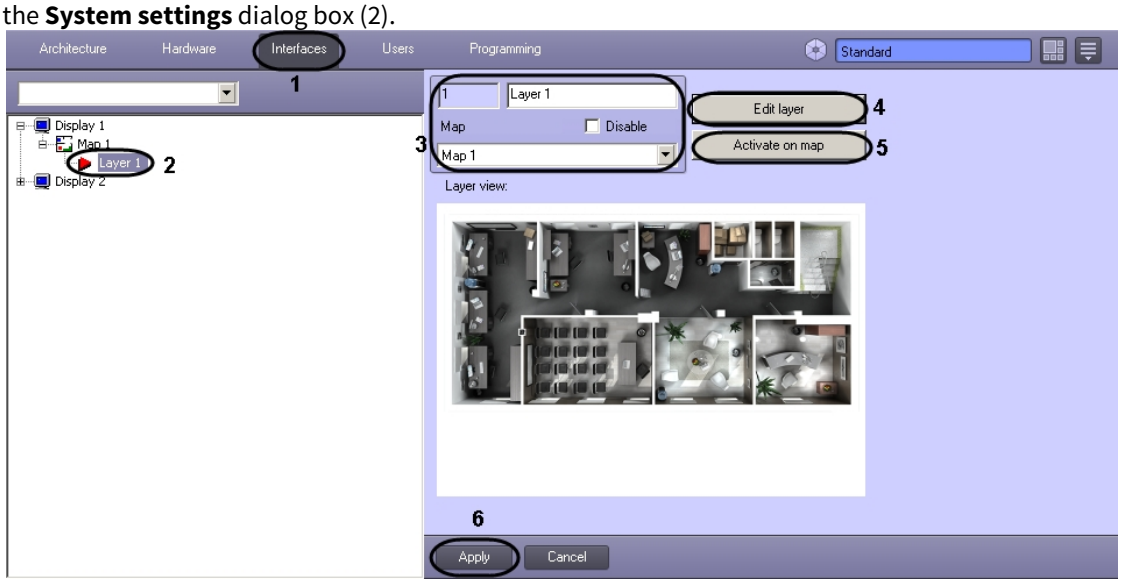
This completes the setup of the map position on the screen.

10.4.5.2.3 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:

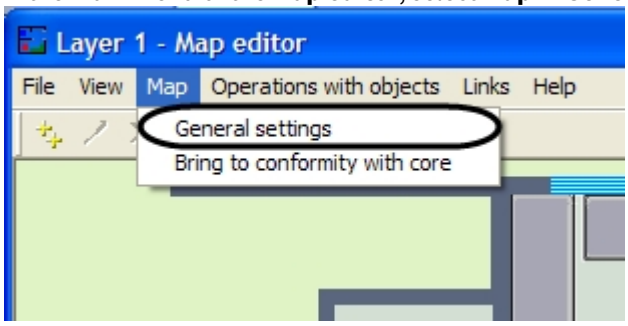
1. Go to the settings panel of the **Layer** object.
2. Open the *Map editor* application.

> **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.

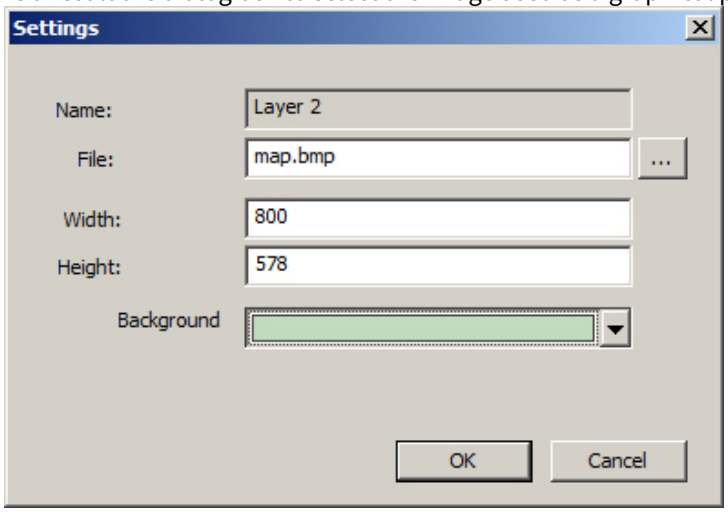
To open the *Map editor*, click the **Edit layer** button on the settings panel of the **Layer** object.



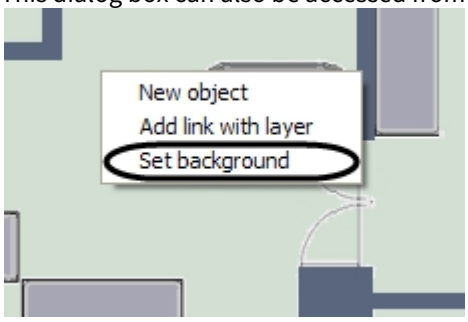
3. In the main menu of the **Map editor**, select **Map** -> **General settings**.



As a result the dialog box to select the image used as a graphical plan of the guarded area will open.

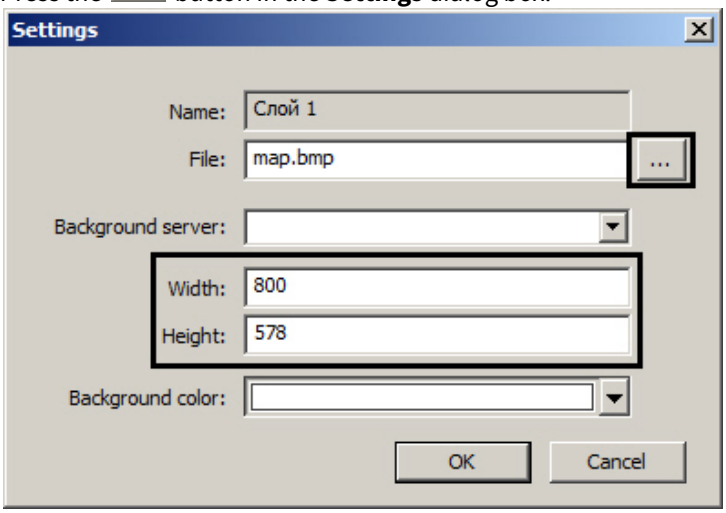


This dialog box can also be accessed from the **Set background** item of the context menu of the map area.



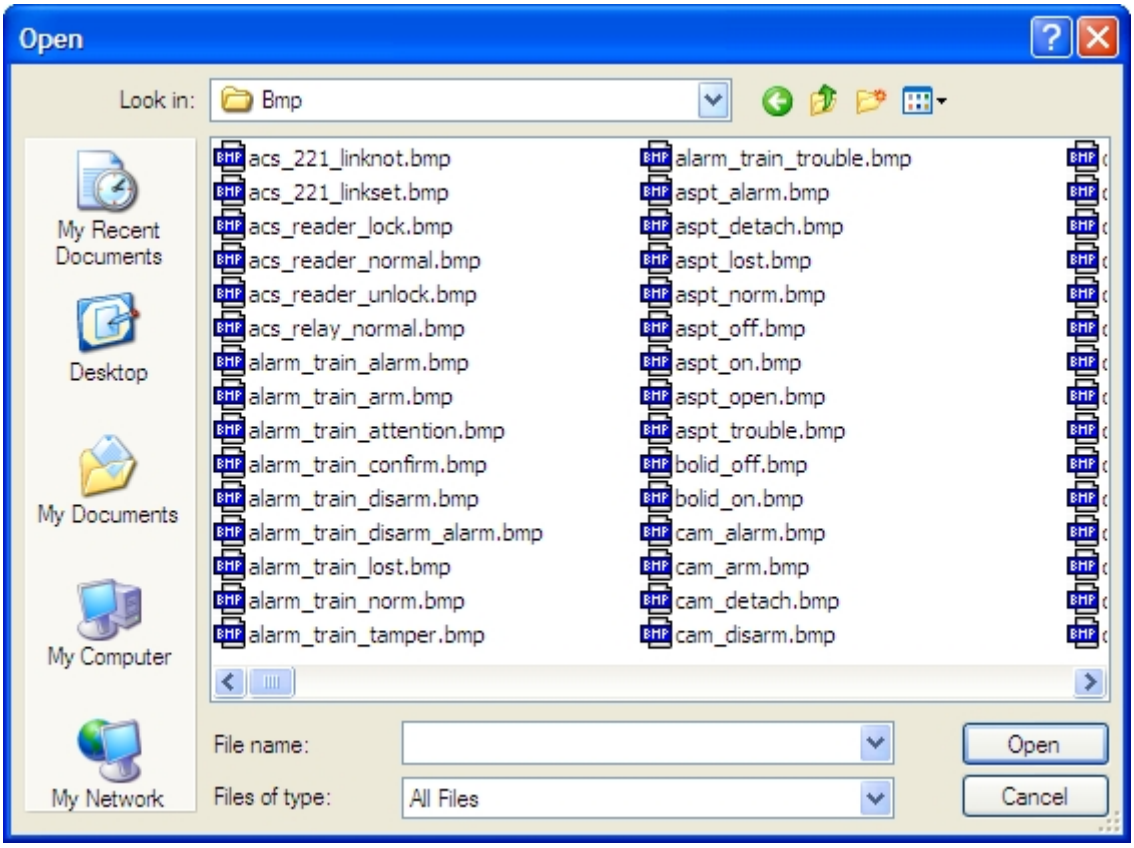
4. Select the background file as follows:

   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, phg, tiff, emf or svg image file.



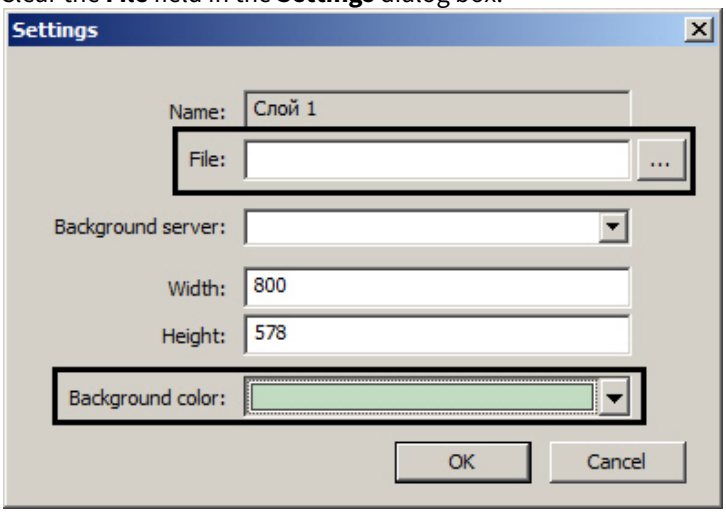
Open the .bmp file and click the **Open** button.
When the layer file is selected, it is copied to the **Bmp** folder in INTELLECT™ installation folder.

> **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:

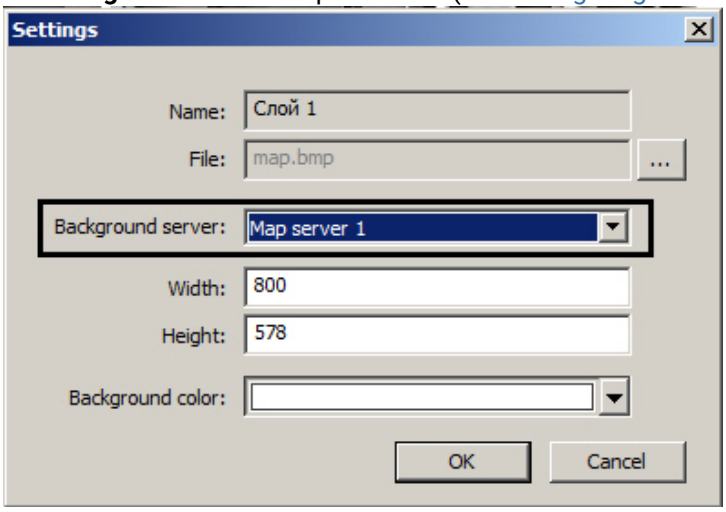
a. Clear the **File** field in the **Settings** dialog box.



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.

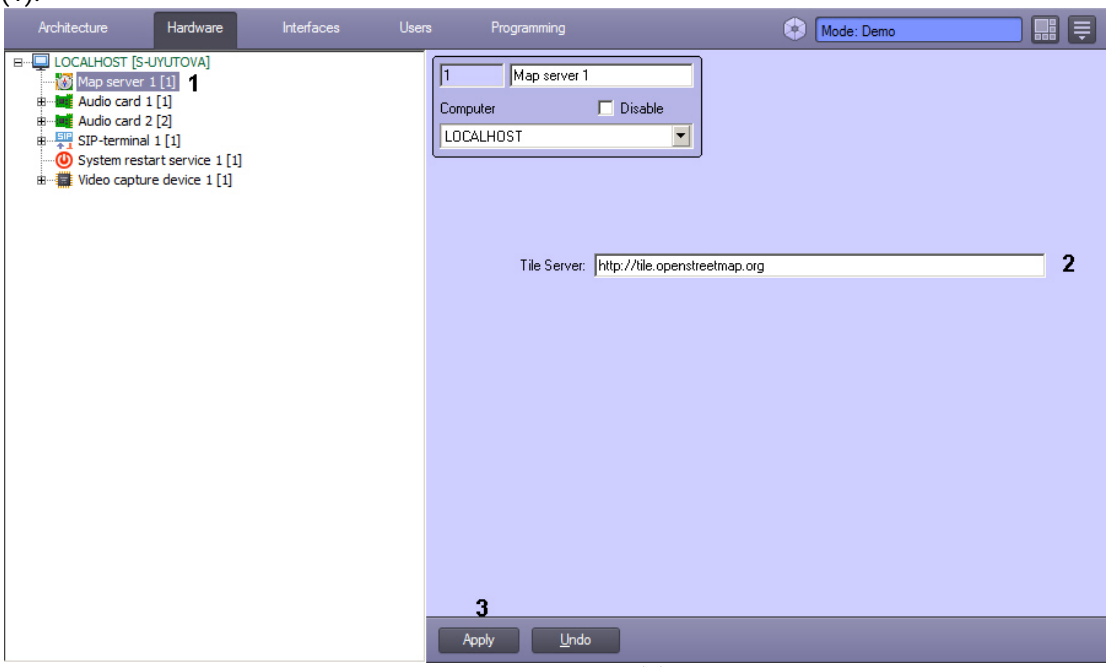
7. To apply all the changes click the **OK** button in the **Settings** dialog box.
The *Map editor* will display the new graphical plan of the guarded area.

10.4.5.2.3.1 Configuring the external map server

The external map server corresponds to the source from which the *Intellect* Map layer receives images for the layer substrate.

Configure the external map server as follows:

1. Create the **Map server** object under the **Computer** object on the **Hardware** tab of the **System settings** dialog box (1).



2. In the **Tile Server** field, enter a link to an external map (2). By default, a link to the free OpenStreetMap map is set: http://tile.openstreetmap.org
3. Click **Apply** (3).

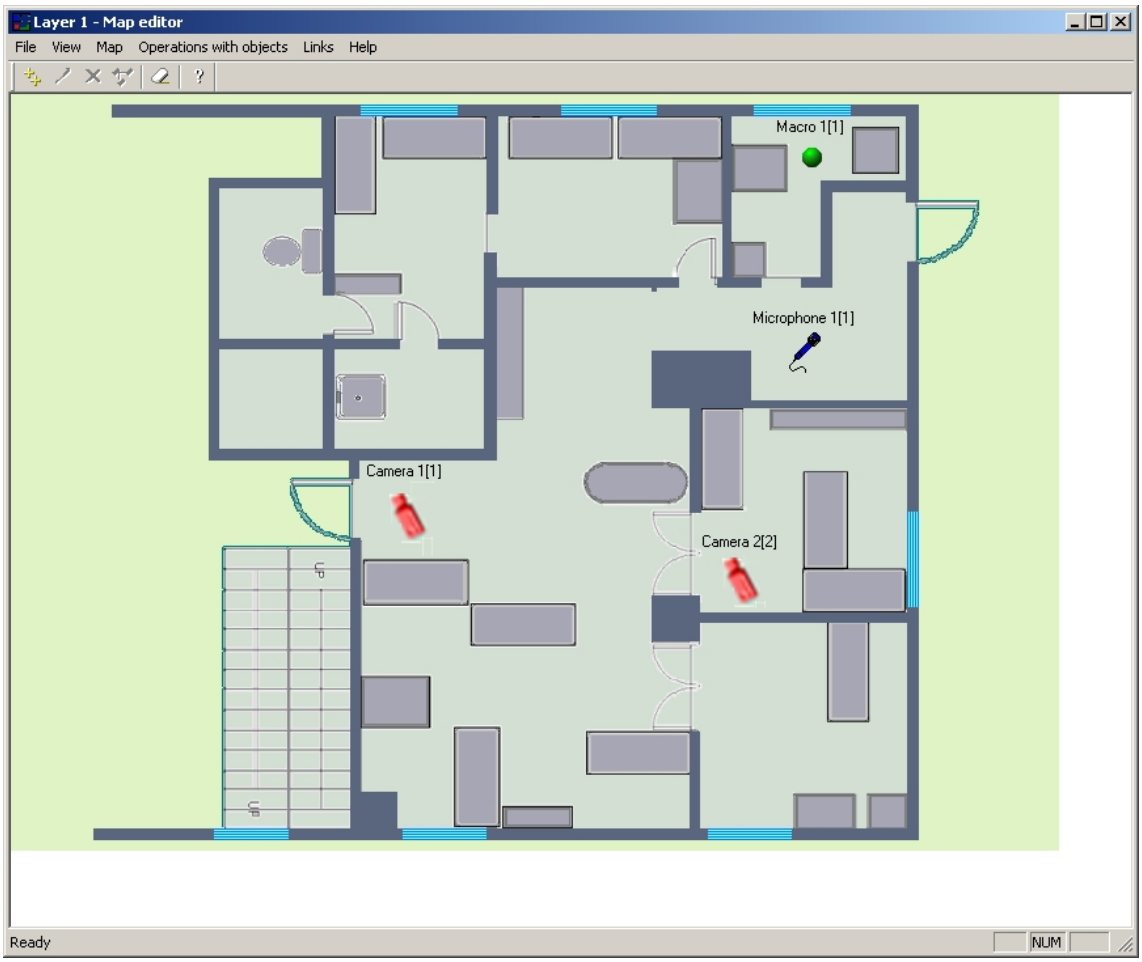
Later select this map server as the background when creating a Map Layer – see Creating the layers of the interactive map.

The external map server configuration is completed.

10.4.5.2.4 Attaching objects to the layers of interactive map

The objects are attached to the layers on the interactive map with the use of 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).



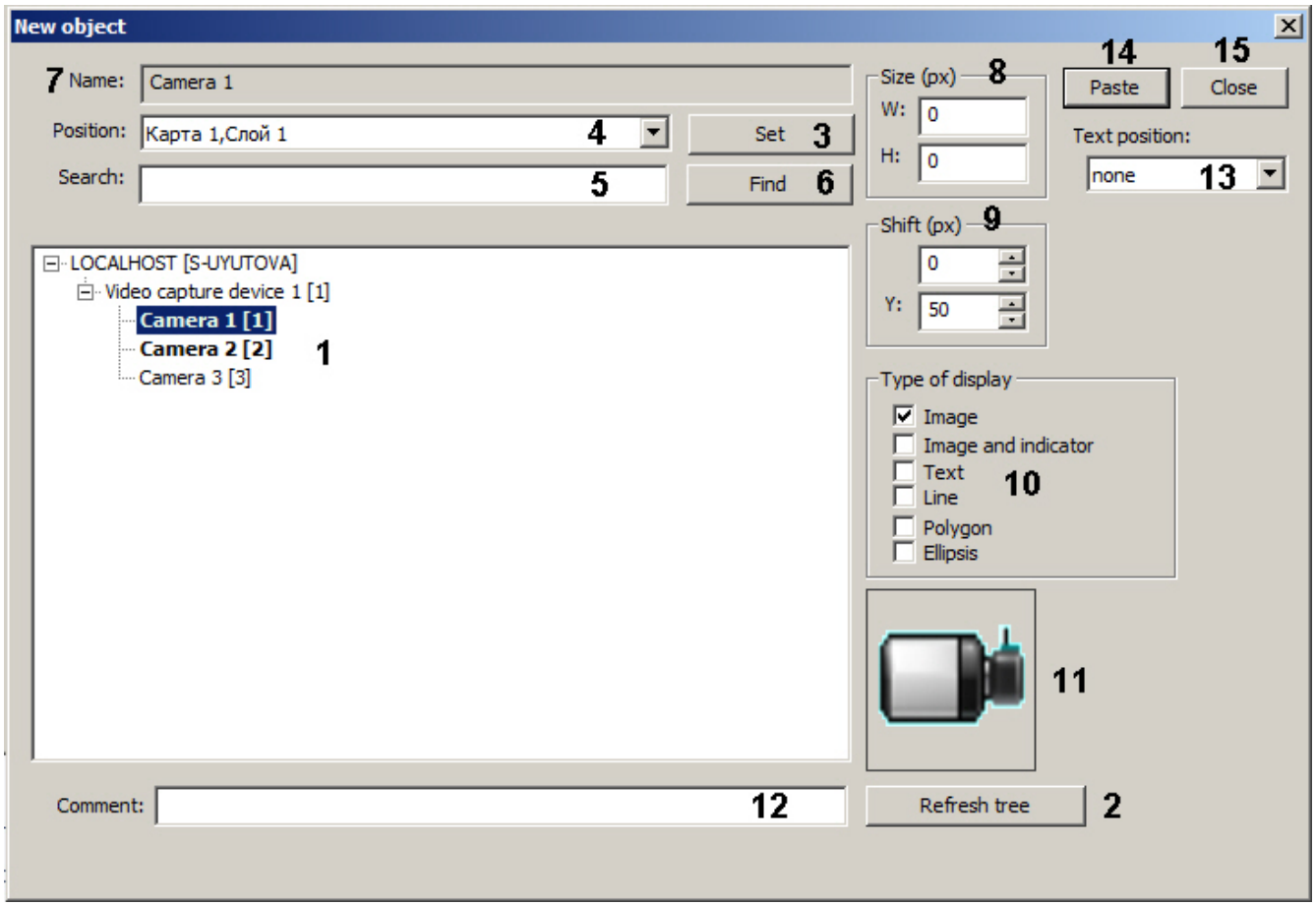
Attach the objects to the layers of the interactive map as follows:

1. Activate the **New object** dialog window of the *Map editor* utility in one of three possible ways:
   a. Execute the main menu operation **Objects operations** -> **New object**.
   b. Click the  button on the tools panel.
   c. Execute the context menu operation **New object** (to activate it, right-click anywhere on the map).
2. Select the required object in the objects tree of the **New object** dialog box (**1**).

> **Note**
>
> To refresh the objects tree, click the **Refresh tree** button (**2**).

> **Note**
>
> Click the **Set** button (**3**) to highlight with bold font the objects in the object tree which were already added to any layers of any maps. If you click the highlighted object in the object tree, the layers and the maps to which this object belongs, 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**).



3. As a result the name of the selected object is automatically displayed in the **Name** field (**7**).
4. Enter the icon size in the **W** (Width) and **H** (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 the 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 required checkboxes. 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's schematic view	Objects of main configuration
Image and indicator	Object's schematic view and indicator of object's state	SCADA objects

Type of display item	Object icon display type	Usage
Text	Object name and text defined by script (see the Examples of scripts in JScript language section of the Programming Guide (JScript)) The icons with the **Text** type of display can be used to place a comment on the map (containing descriptions, notes, any 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) *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)*	SCADA objects
Line	Objects' images in the form of straight line or polyline	SCADA objects
Polygon	Object representation as the polygon with specified color and transparency with arbitrary number of apexes.	SCADA objects
Ellipsis	Object representation as the ellipse with specified color and transparency.	SCADA objects

Note

If the **Image and indicator** or **Text** type of display is selected, the object's values/states will be saved after the *Intellect* restarts only if the object receives new values/states during the Map operation. If no new values/states were received before the *Intellect* closing, they are not be saved.

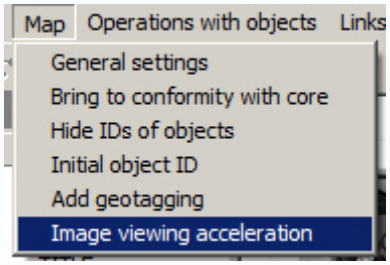
Note

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 if necessary.
8. From the **Text position** drop-down list (**13**) select the object name display position with respect to the icon: none (i.e. only icon without a name is displayed), above, to the right, below, to the left.
9. Click **Paste** button (**14**) or press **Insert** on the keyboard to attach the object to the layer of interactive map.
10. Repeat steps 2-8 for all required objects.
11. Click **Close** button to close the **New object** dialog window (**15**).

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.

Attachment of objects to the layers of interactive map is complete.

10.4.5.2.5 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 object's displaying
- Editing the font, color, background or frame size of object's name
- Editing the object's size
- Editing the position of object
  - Using the Position of object dialog window
  - Using the mouse
  - Using the Properties panel
- Editing color and transparency (polygon and ellipsis)
- Adding or removing apexes to polygon or polyline
- Setting order of displaying objects on map
- Configuring object states displaying

10.4.5.2.5.1 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	Call for operation			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	-
Edits additional data and type of displaying the icon for the selected object	Edit object	Edit	The 3 button	Is 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's name	Set the font	-	-	Is 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' sizes	-	-	Is performed in the **Object size** dialog box
Edits the position of the selected object	Object's position	Object's position	-	Is performed in the **Object position** dialog box or with the help of the mouse
Selects objects of one group	-	Selects all the similar	-	For example: all the **Camera** objects are selected
Selects all the identical objects within a group	-	Selects all the identical	-	For example: all the **Sensor** objects of the **Gerkon** type are selected

The **Map editor** utility enables to perform the operations with a group of objects. For selecting the several objects it is necessary to hold the Ctrl key on the keyboard.

> **Note**
>
> The **Object position** operation is not performed with a group of objects.

10.4.5.2.5.2 Editing the additional data and type of object's displaying

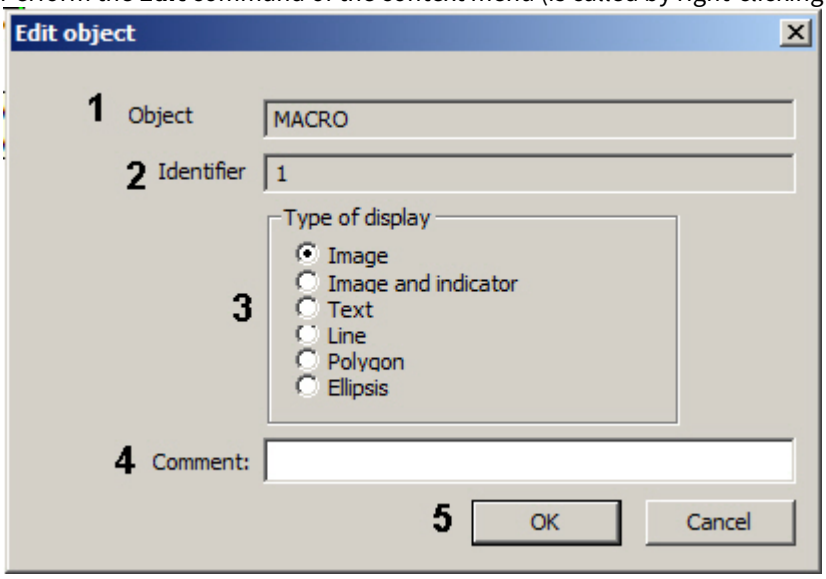
Edit the additional data and type of object's displaying as follows:

1. Select an object that is to 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 (is called by right-clicking the object's 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's displaying with the help of the **Type of display** switch (3).

The switch position	Type of object's displaying	Note
Image	Schematic object's image	Basic configuration objects, SCADA objects
Image and indicator	Schematic image and identifier of object's 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 JScript language in the Programming Guide (JScript)).	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 ellipis	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).

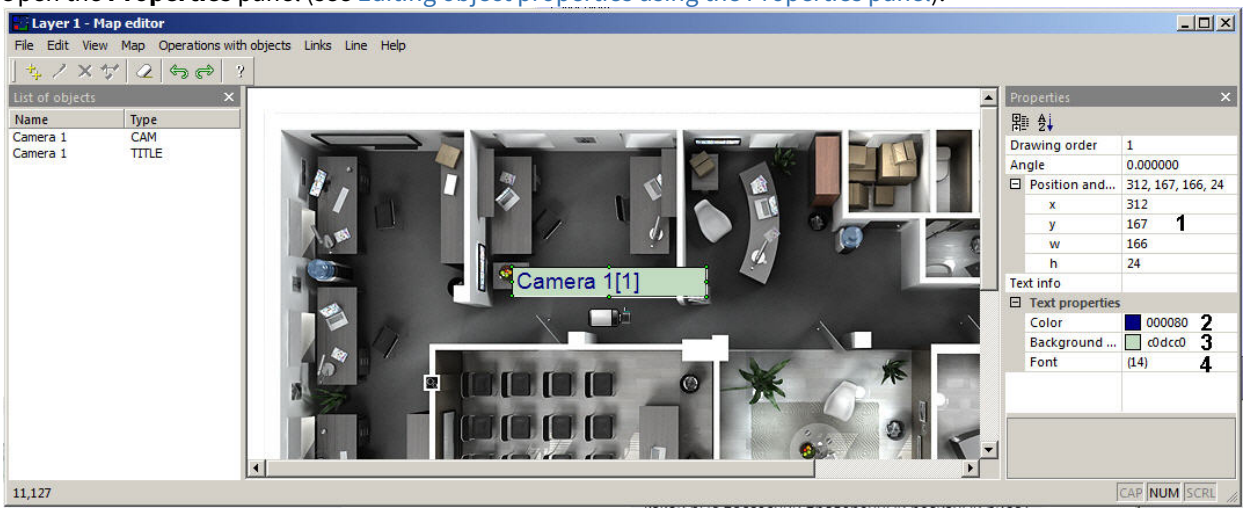
6. If required change object's additional data in the **Comment** field (4).
7. To save the changes click **OK** (5).

Editing the additional data and type of object's displaying is completed.

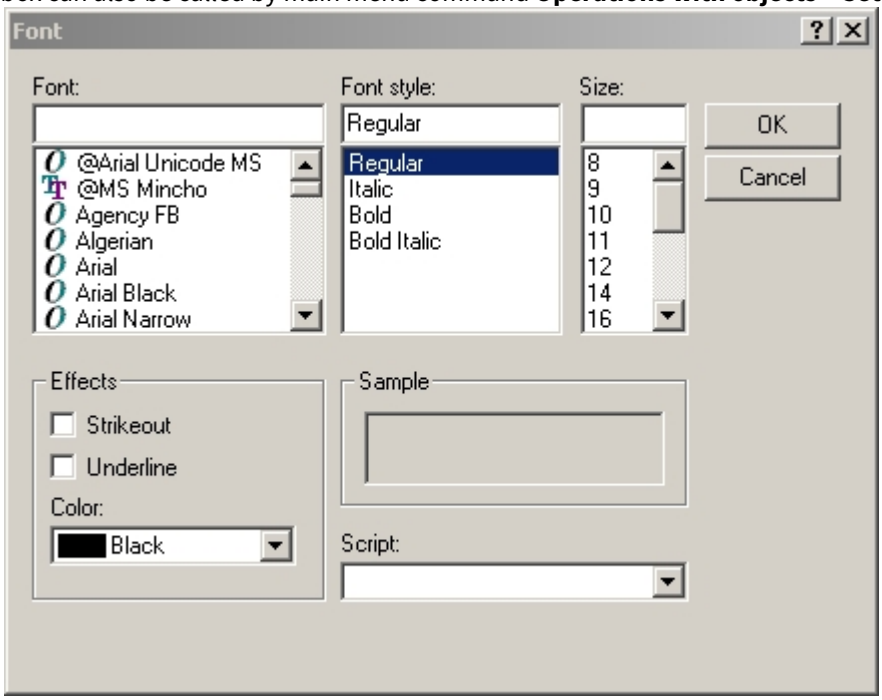
10.4.5.2.5.3 Editing the font, color, background or frame size of object's name

Edit the font, color, background or frame size of object's name as follows:

1. Select object's name the font, color or background of which is to 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's height and width (**w** and **h**) and clockwise rotation **Angle** (1).
4. In the **Color** field select the object's name font color (2).
5. In the **Background color** field select the object's 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 **Ok** to save the changes.

Editing the font, color or background is completed.

10.4.5.2.5.4 Editing the object's size

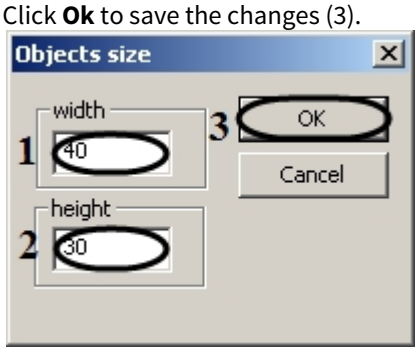
Edit the object's size as follows:

1. Select the object the size of which is to be edited. Green-pointed frame will appear around the image as a result.

2. Call for the **Object's size** dialog window of the **Edit map** utility by the main menu command **Operations with objects** > **Object's size**.
3. Specify the size of the image: **Width** (icon's width) and **Height** (icon's height) fields – 1, 2. Icon's size is expressed in pixels.

> **Note**
>
> If 0 value is entered in the fields **Width** and **Height** , object's icon will be displayed in the original size.

4. Click **Ok** to save the changes (3).

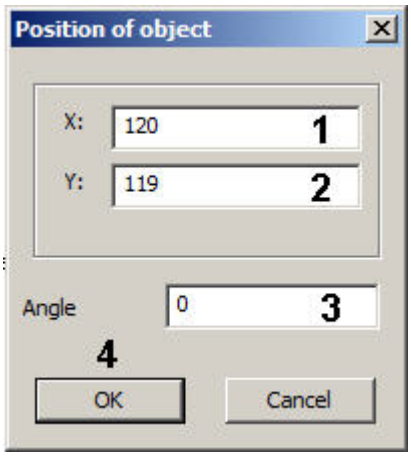


Editing the object's size is completed.

10.4.5.2.5.5 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 is to be edited.
2. Call for the **Position of object** dialog window of the **Map Edit** utility in one of two ways:
   a. Perform the command of the main menu **Operations with objects > Object's position**;
   b. Perform the command of the context menu **Object's position** (is called by right-clicking the object's image).



3. Set the coordinates of the object's 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 guarded object are set, to which this layer corresponds (see. Creating the layers of the interactive map).

4. Enter the angle in degrees of object's image turn in the **Angle** field. The angle is set counterclockwise from the contour line (3).
5. To save the changes click **OK** (4).

Note

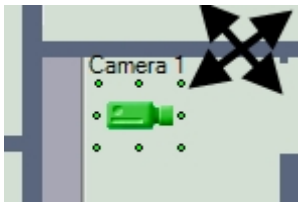
In case when at least one coordinate oversteps the bounds of the map, the message window will be displayed. Click **OK** and then repeat step 3.



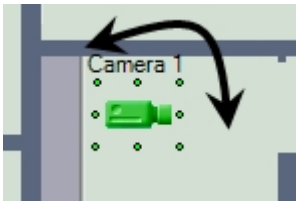
Editing the object's position with the help of **Object's position** dialog window is completed.

Using the mouse
The **Map edit** utility also enables to edit the object's position with the help of the mouse.

To set the position of the icon, point and left-click it. Then drag the icon to the desired location and release the mouse.

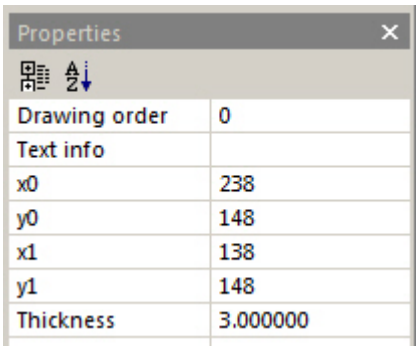


To rotate the icon, point and left-click it. Green-pointed frame will appear around the icon as a result. Point at one of the corner dots. A bended arrow will appear. Move the mouse in the desired direction to rotate the symbol and release the mouse.

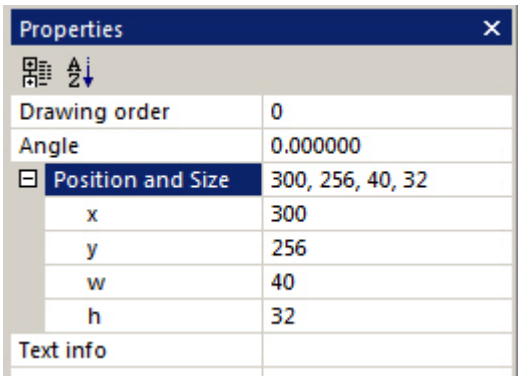


Using the Properties panel
You can also change the coordinates, rotation angle and the icon size of the **Line**, **Image**, **Image and indicator** and **Text** object types using the **Properties** panel:

Open the **Properties** panel for the required object (see Editing object properties using the Properties panel).
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.



For other icons, specify the coordinates of the upper left corner (**x, y**), width (**w**) and height (**h**).

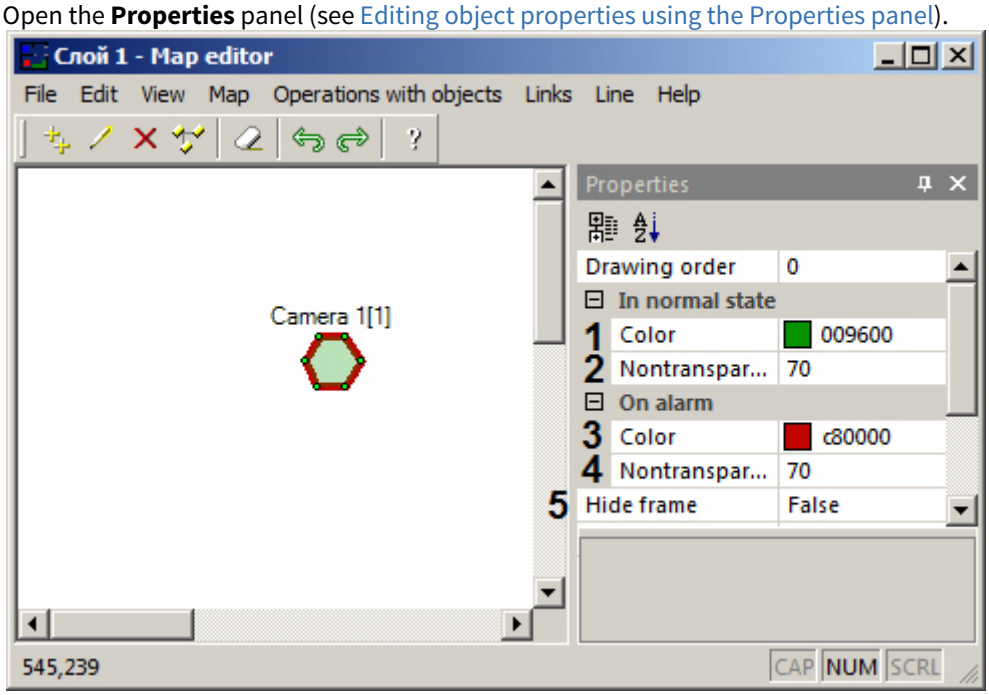


Editing the object position using the **Properties** panel is complete.

10.4.5.2.5.6 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. In the dropdown 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. In the dropdown 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 is to be hidden, then set the value to **True** in the **Hide frame** field (5).

10.4.5.2.5.7 Adding or removing apexes to polygon or polyline

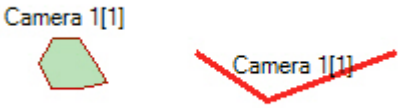
Add apexes of object icon as follows:

> **Note**
>
> Maximum number of apexes in the polygon is 51.

1. Call the context menu of the object icon by right-clicking and holding the Ctrl key in the polygon area or on the polyline.

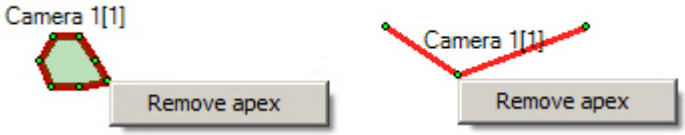


2. Select **Add apex**.
3. Select the required position of a new apex and left-click.
4. The apex will be added to the polygon or the polyline.



Apexes of object icon are now added.

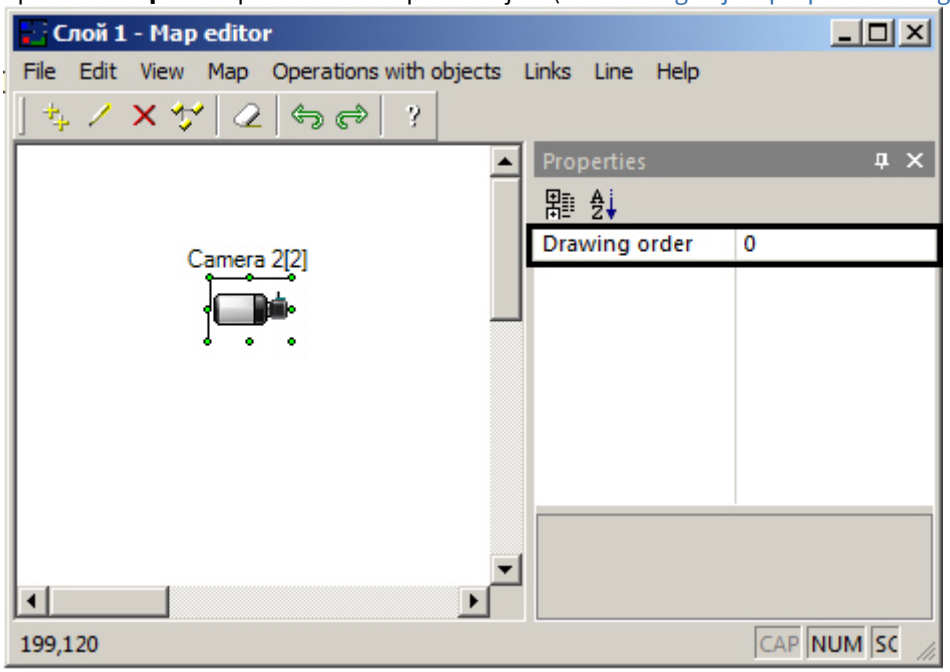
To remove the apex, right-click it holding the Ctrl key and select **Remove apex**.



10.4.5.2.5.8 Setting order of displaying objects on map

The order of displaying object icons when they are laid over can be set. For this:

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. Icons with bigger value of this parameter will be displayed over icons with smaller value.

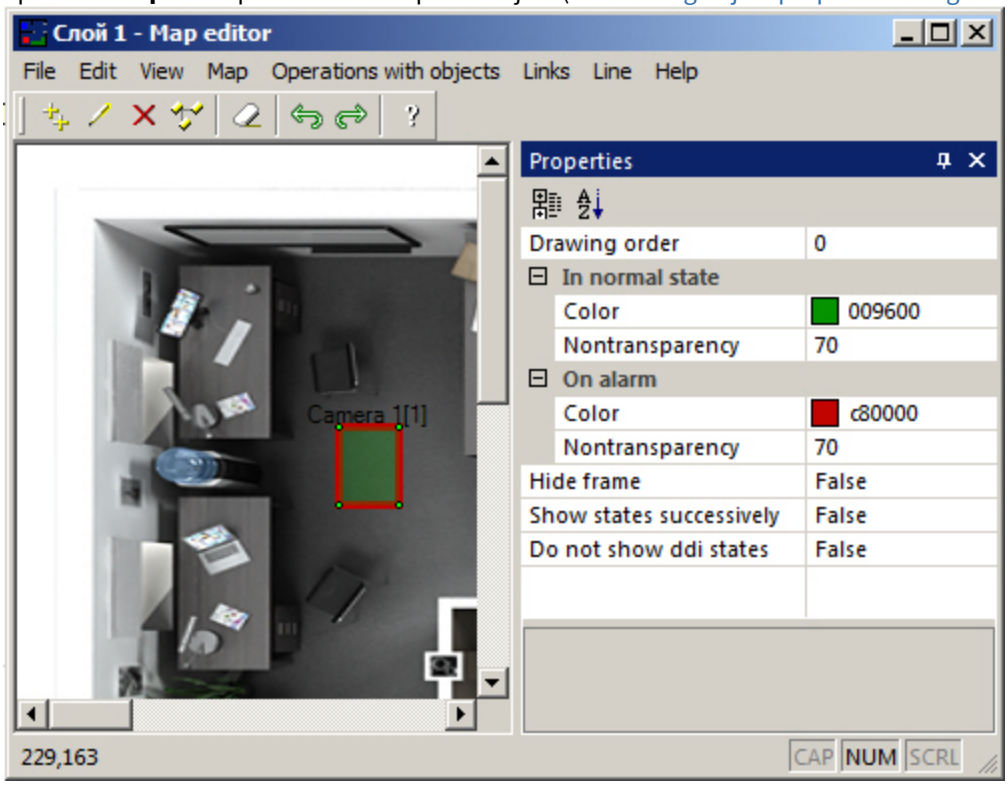
The order of displaying objects on map is now set.

10.4.5.2.5.9 Configuring object states displaying

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 section in Operator's Guide).

It is possible to disable displaying states thumbnails. For this:

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 **True** value in the **Show states successively** dropdown list. To enable their display, select the **False** value in this dropdown list.

The display of the state of objects is configured.

10.4.5.2.6 Linking the layers of the interactive map

Intellect system allows creating multilevel maps comprised of several layers.

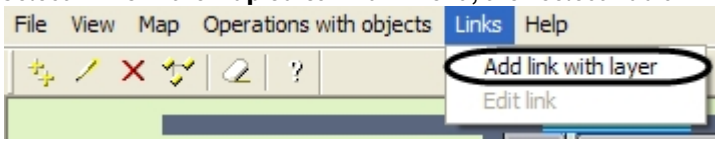
In case of multiple layers, the links should be established between the layers. These links help move to other layers for operative control and viewing of the device objects located on them.

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.

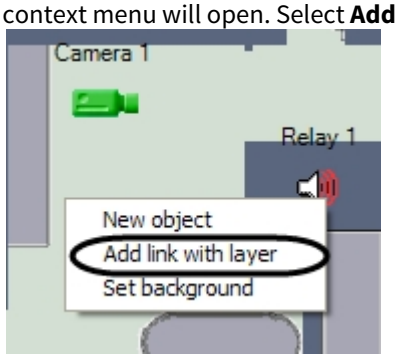
To create a new link from the current layer to another, do the following:

1. Select **Links** in the **Map editor** main menu, then select **Add link with layer**.



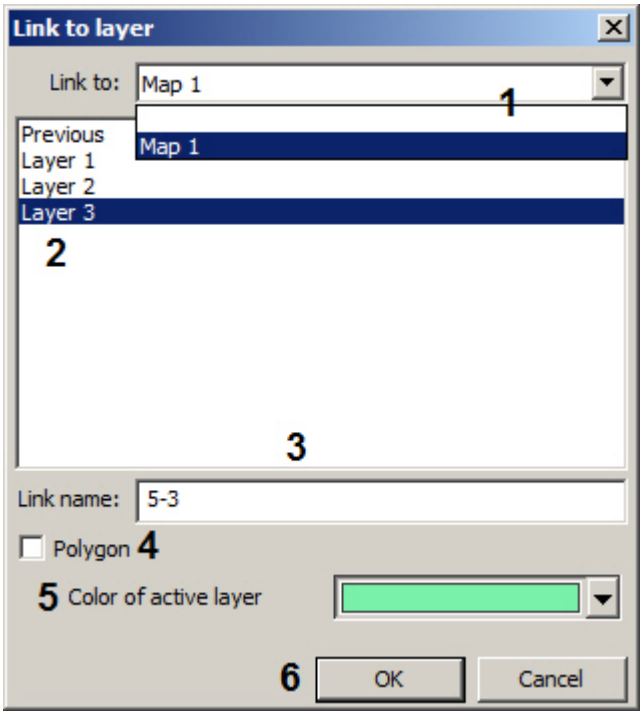
The **Link to layer** window opens, allowing to choose the layer to link to.

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.

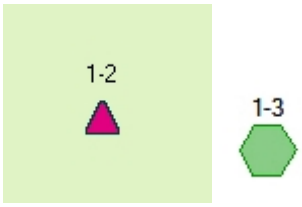


   b. Select a layer the switch is to be performed to (2).
   c. Enter the name for this link in the **Link name** field (3).
   d. If the link on the map is to be displayed as a polygon, set the **Polygon** checkbox checked (4).

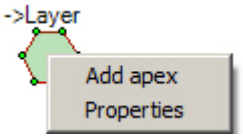
> **Note.**
>
> The color and shape of the polygon are set after adding it to the layer. By default, the link is represented by a green hexagon.

   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).

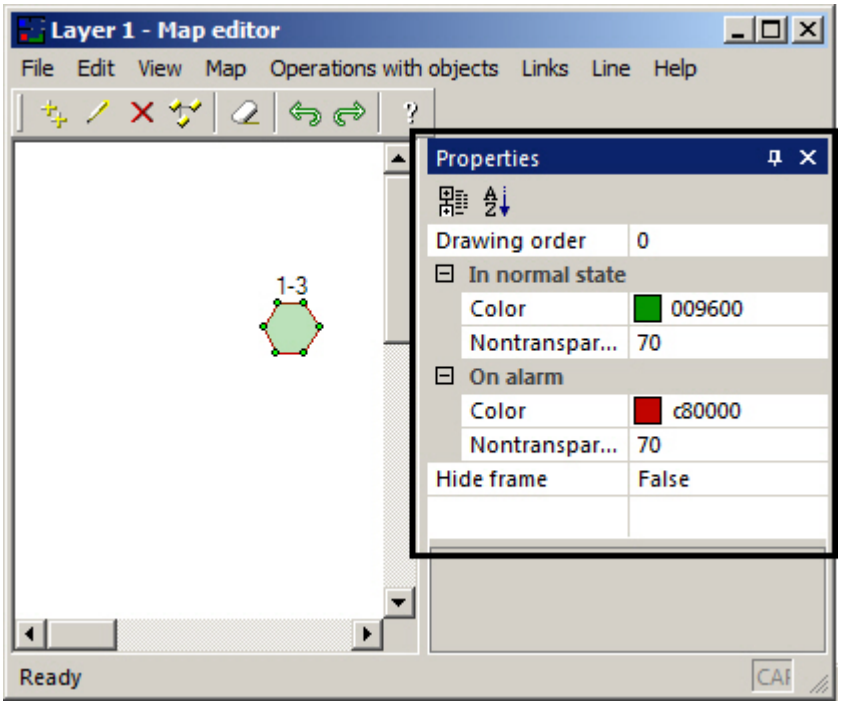
A symbol will appear on the map representing the link. The icon of the link is represented by a red triangle or a polygon if the **Polygon** checkbox was checked (see step 2.d):



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.

Switch-over between Map layers

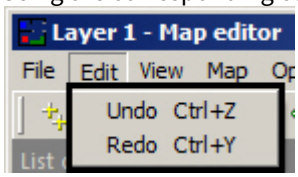
10.4.5.2.7 Cancelling the last action in Map editor

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.



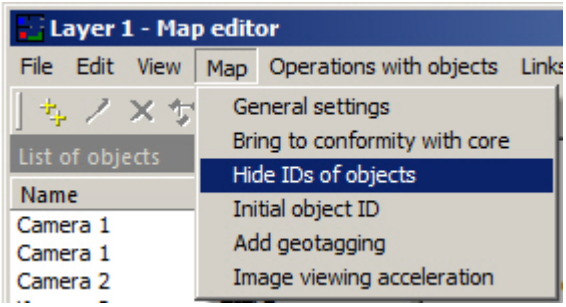
It is possible to cancel not more than 30 actions.

10.4.5.2.8 Configuring object ID is displaying

By default the object ID is displayed in square brackets next to the object name on the interactive map.



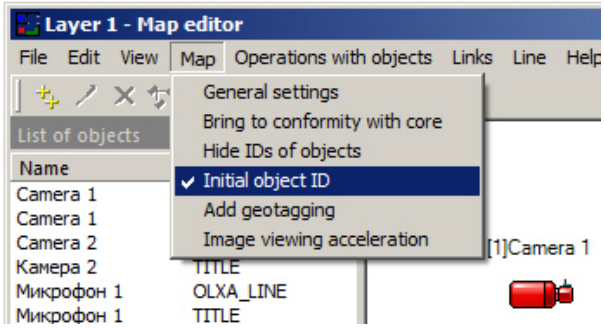
One can hide object IDs on each layer of the interactive map. For this set the **Hide object ID** checkbox checked in the **Map** menu of *Map editor*.



As a result object IDs are hidden on the layer that being edited on the interactive map.

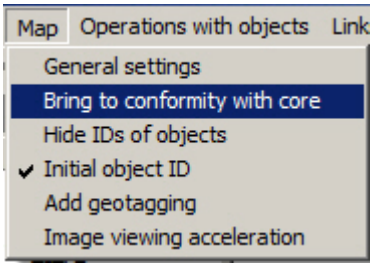


Object ID can also be configured to display before object's name. For this set the **Initial object ID** checkbox checked in the **Map** menu of *Map editor*.



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.

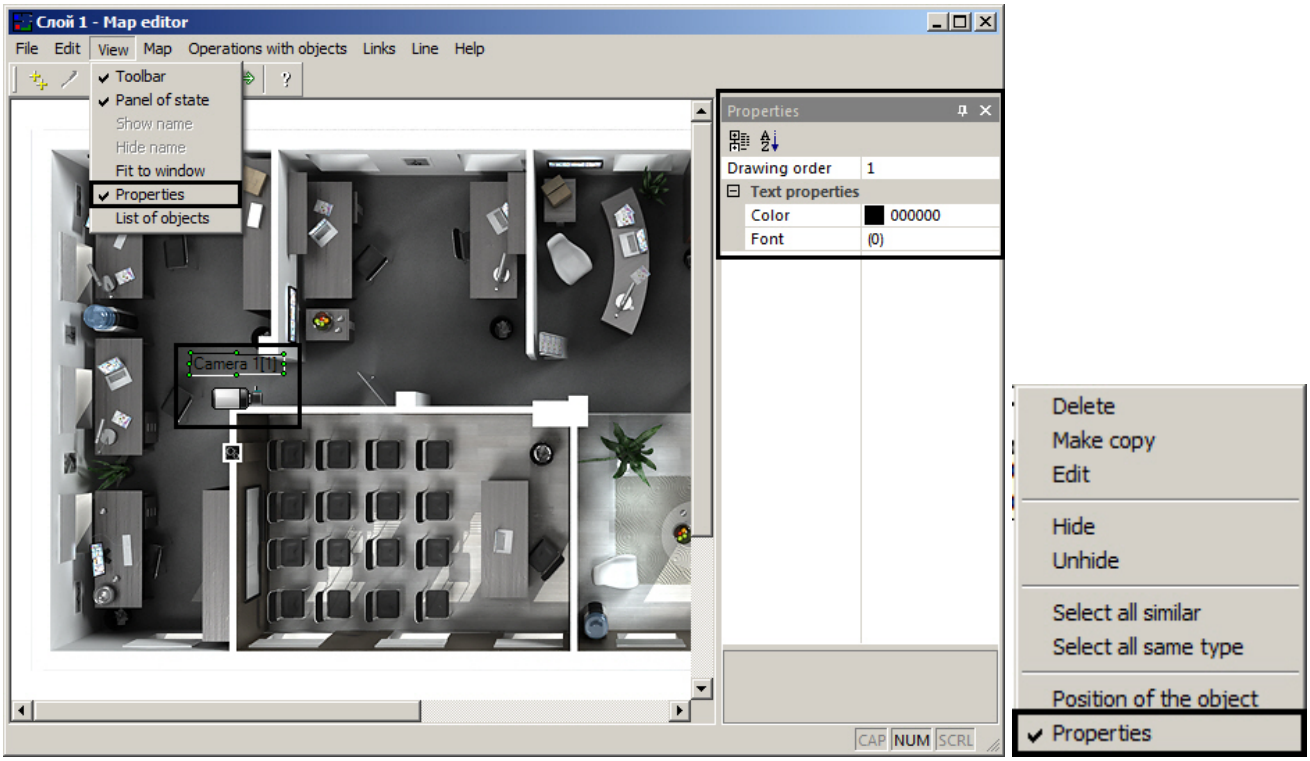
> **Note.**
>
> This will also delete icons of non-existing objects from the layer.



10.4.5.2.9 Editing object properties using the Properties panel

The **Properties** panel is displayed on the right of the **Map editor** utility box when the **View -> Properties** is selected.

This panel can also be opened by selecting the **Properties** item in the context menu of any object.



When selecting the object on the layer of the interactive map, the list of object parameters is displayed on the **Properties** panel. These parameters can be also edited with the help of this panel.

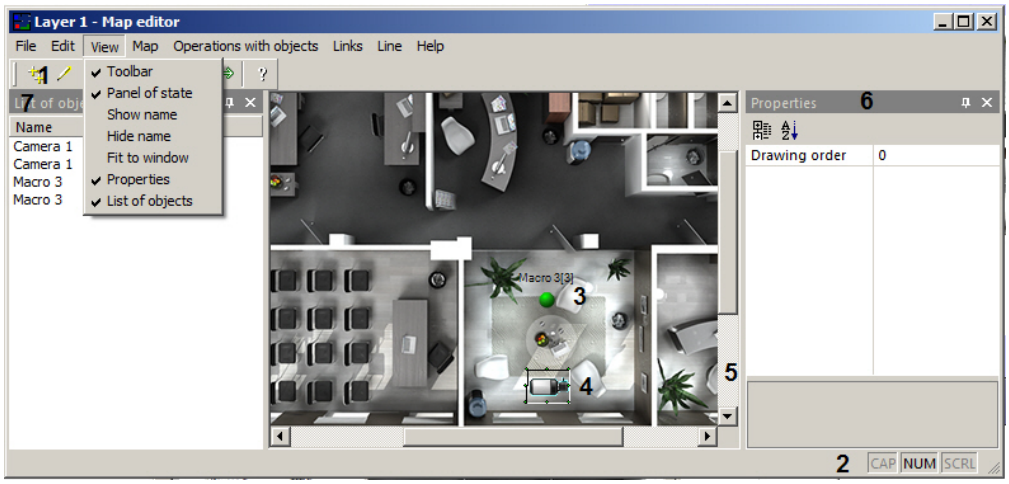
For instance, the color and font of the object caption as well as the color and other parameters of the object icon (in the form of polygon) can be set using this panel.

To edit parameters of displaying several objects' icons select required icons by holding CTRL and left-clicking them. Then change parameters as usual.

If several different objects' icons are selected (for instance, image and line or polygon and text), then group changing of their properties is not available.

10.4.5.2.10 Configuring viewing Map editor utility

Configuration of viewing the *Map editor* window is performed using the **View** menu.

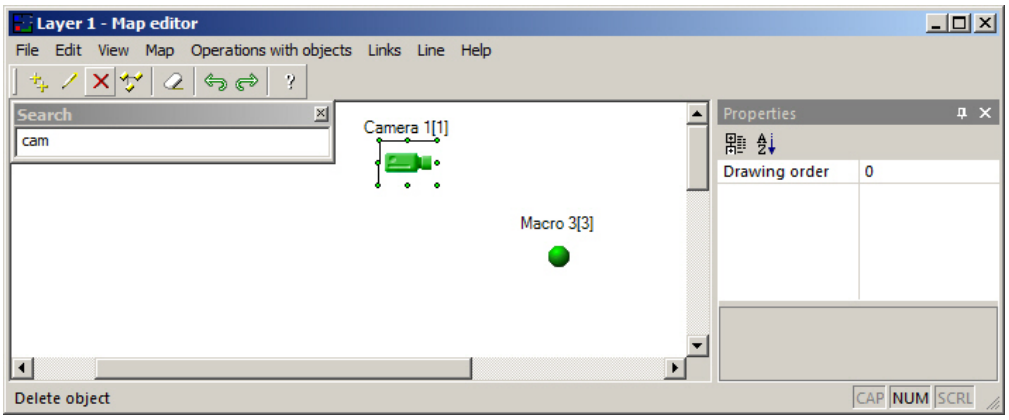


Find the description of menu items in the table.

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).

10.4.5.2.11 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.

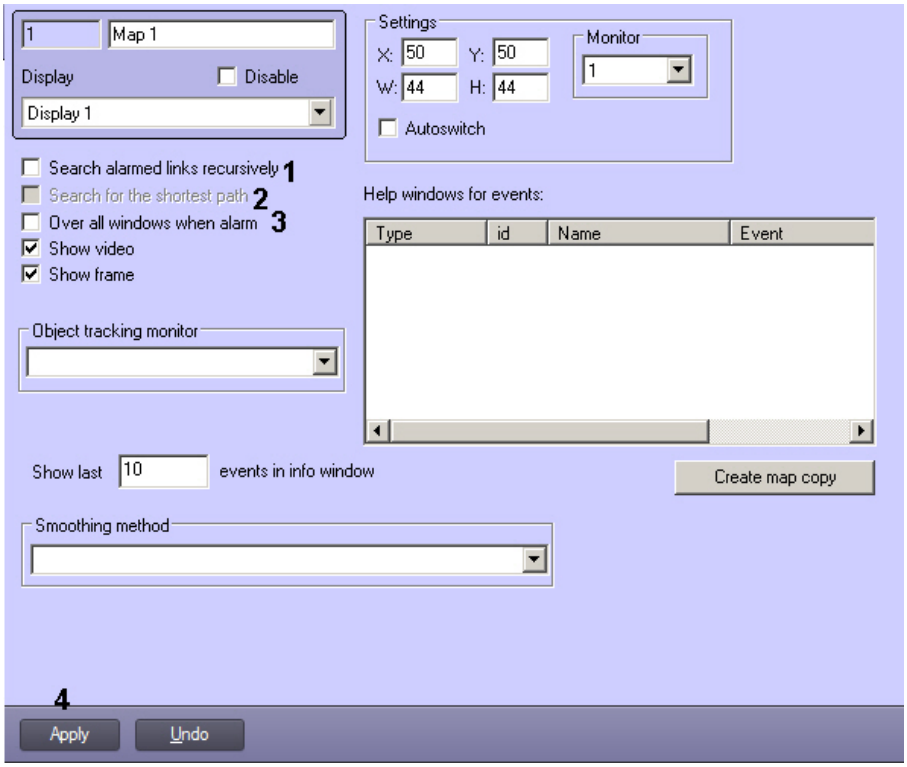
10.4.5.3 Setting up the display of the alarm signals on multilevel maps

The rules for transition to the layers with alarmed devices can be set up for multilevel maps.

The following ways of displaying the layer with an alarmed device exist in the system:

1. When an alarm occurs, the **Map** window opens above all other active windows showing the layer containing the alarmed device.
2. The link symbols recursively lead to the layer containing the alarmed device.

To open the **Map** window above all other windows, set the **Over all windows when alarm** checkbox (**3**) in the settings panel of the **Map** object. The **Map** window will now open on top of other windows in case of alarm registration.



To make it possible to move from the current layer to any other layer, the links should be established in the multilevel maps. If the links recursively connect all layers of the map, they can be used for recursive transition to the alarmed layer. To enable this option, check the **Search alarmed links recursively** checkbox (**1**) in the settings panel of the **Map** object.

When the recursive search is on, the blinking links on each layer eventually lead the operator to the alarmed layer. If the **Search for the shortest path** checkbox is checked (**2**), the shortest path to the alarmed layer will be chosen.

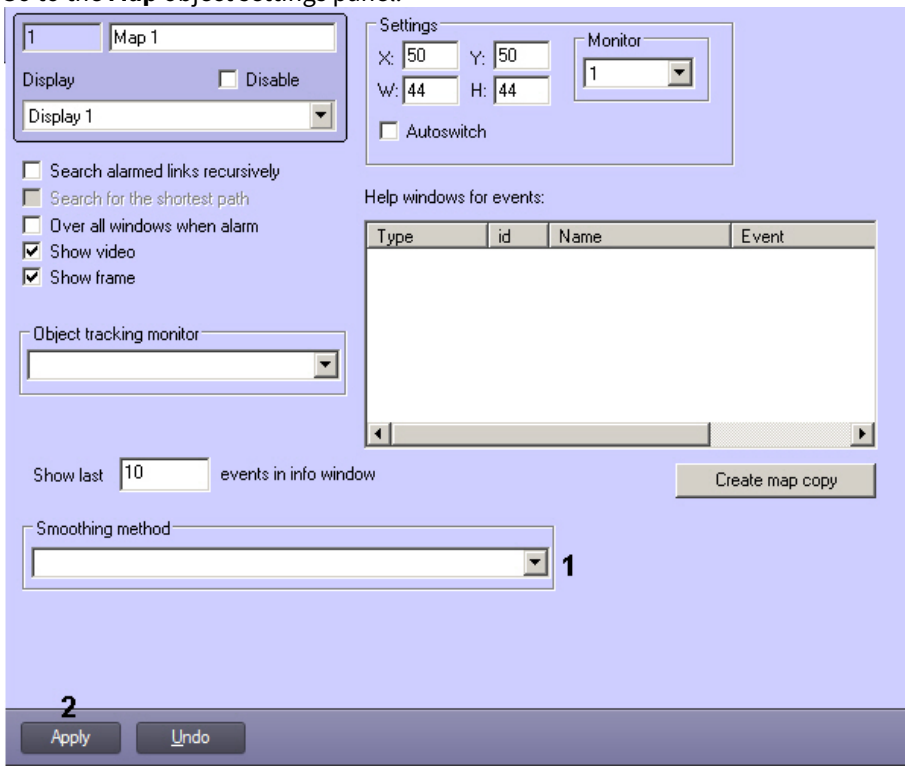
> **Example**
>
> The 1st layer contains the link to the 2nd layer, and the 2nd layer contains the link to the 3rd layer. The 1st layer is currently active. An alarm is triggered on the 3rd layer. If the recursive search is on, the link from the 1st to the 2nd layer will blink, and the link from the 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 3d layer, and the 2nd layer contains the link to the 3d layer (i.e. there are to ways to reach the 3d layer from the 1st layer: directly or via the 2nd layer). Let's the 1st layer is currently active. An alarm comes from the 3d layer. If both checkboxes are checked, only the link to the 3d layer will blink on the 1st layer. If the **Search for the shortest path** checkbox is unchecked (**2**), both links (to the 2nd and 3d layers) will blink.

10.4.5.4 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 (**1**), 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 (**2**).

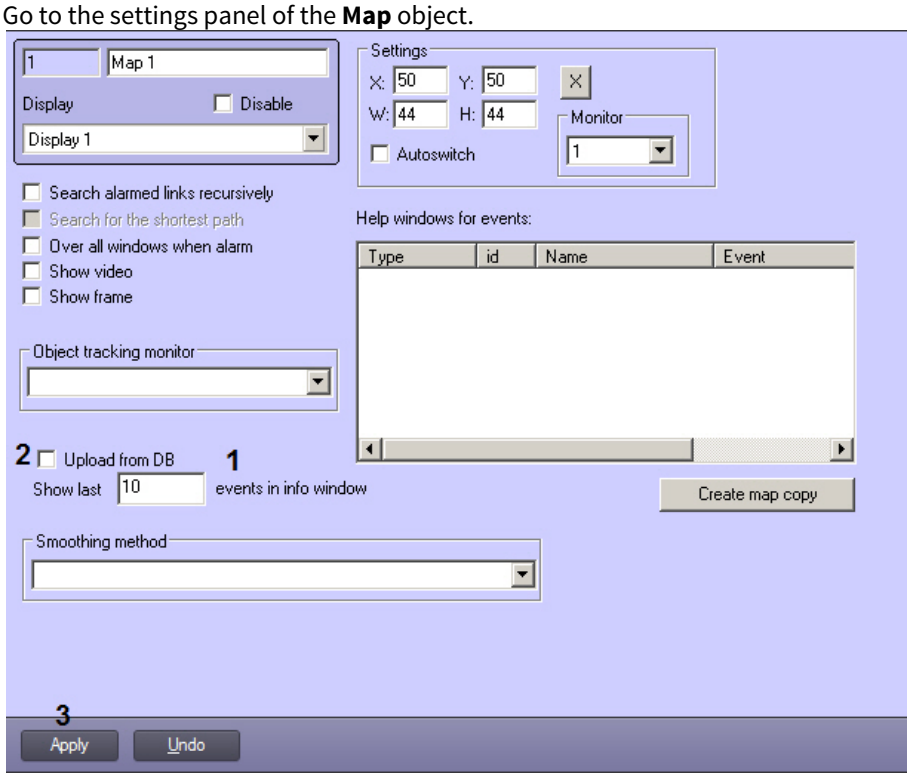
The smoothing method of the Map when scaling is configured.

10.4.5.5 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 (**1**) 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 (**2**). If the checkbox is cleared, only events registered after the *Intellect* start are displayed.
4. Click the **Apply** button (**3**).

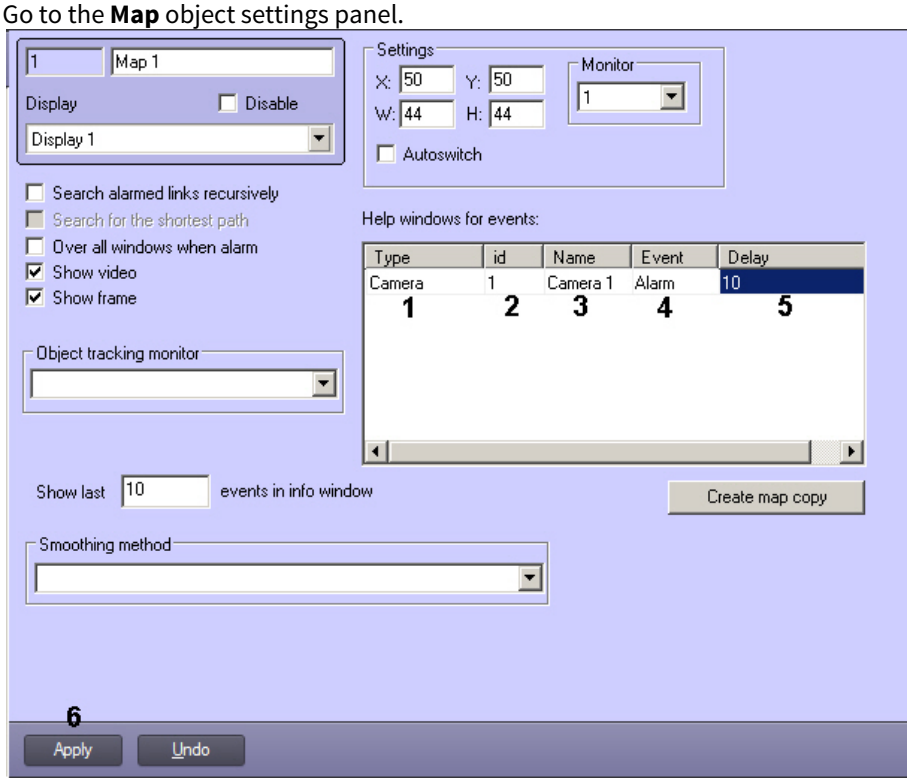
The number of events to be displayed in the Map window is now configured.

10.4.5.6 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 comes (**1**).
3. From the **id** drop-down list, select the object identifier (**2**). 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 (**3**) will be filled automatically.
5. From the **Event** drop-down list, select the event name (**4**). 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 (**5**). 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 (**6**).

The event tooltips are configured.

10.4.5.7 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*.

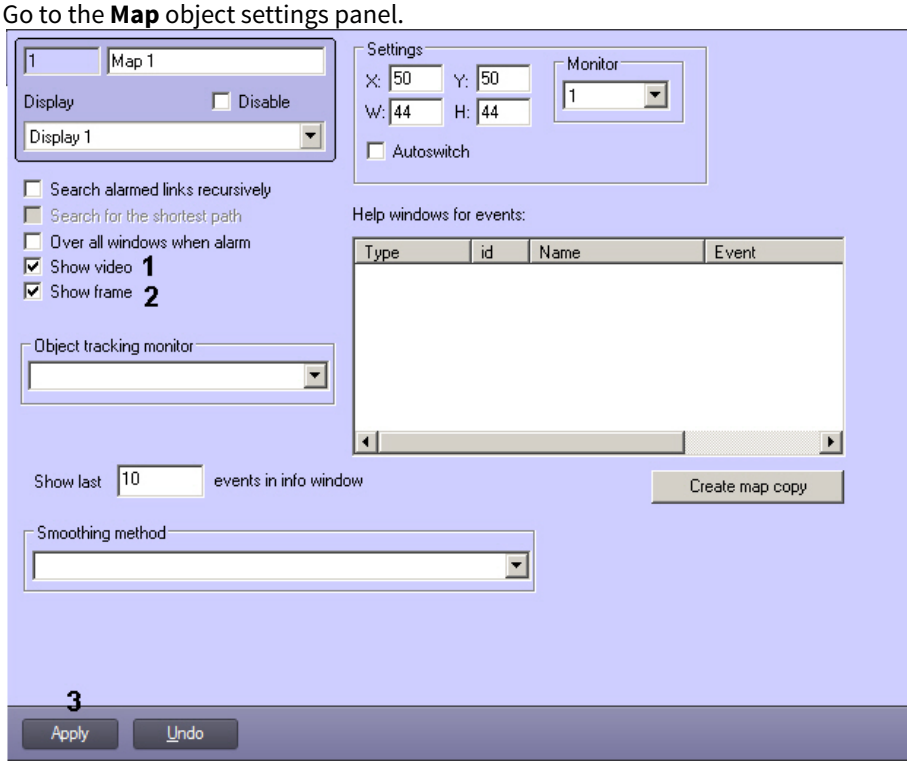
After starting the Map, this file will be rewritten: the reactions will be numbered according to sorting, starting with 0, the same numbers will be eliminated.

10.4.5.8 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 (1).
3. Set the **Show frame** checkbox in order to enable frame request (2).
4. Click **Apply** (3).

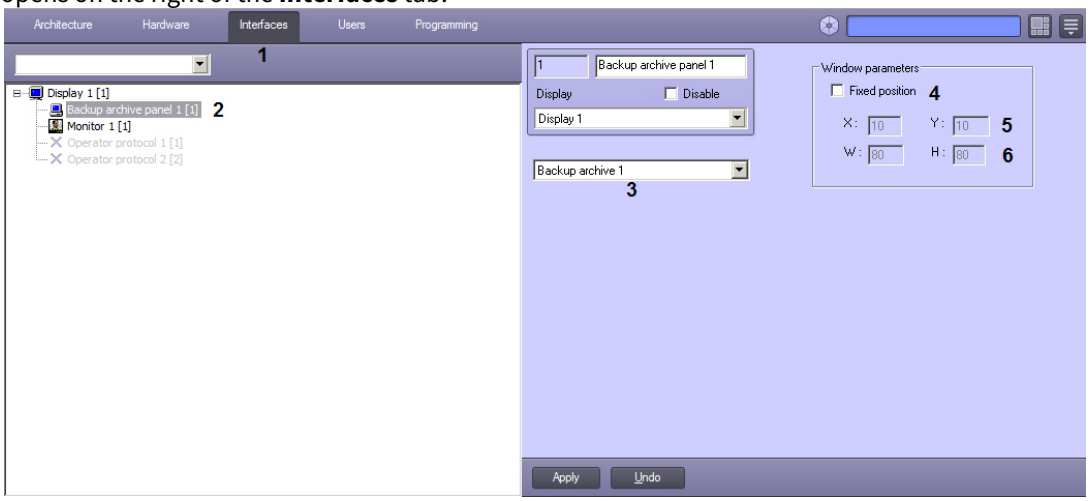
Enabling frame and video request functions is completed.

10.4.6 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

10.4.7 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.

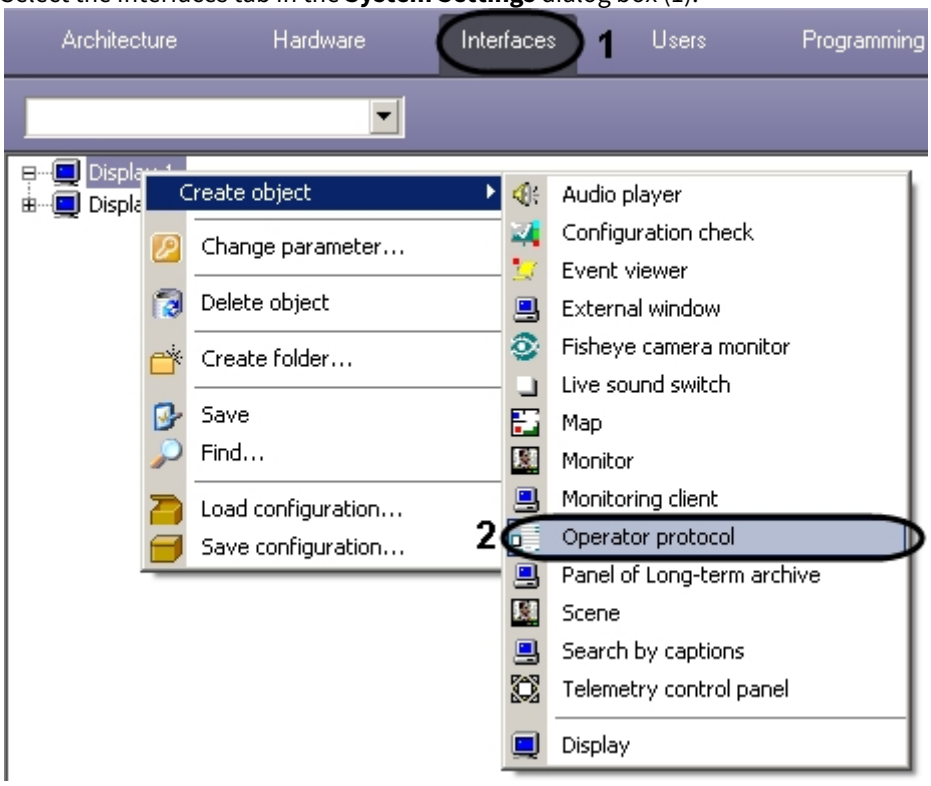
7. Optional: Connecting external DBs.

Event processing using the Operator protocol

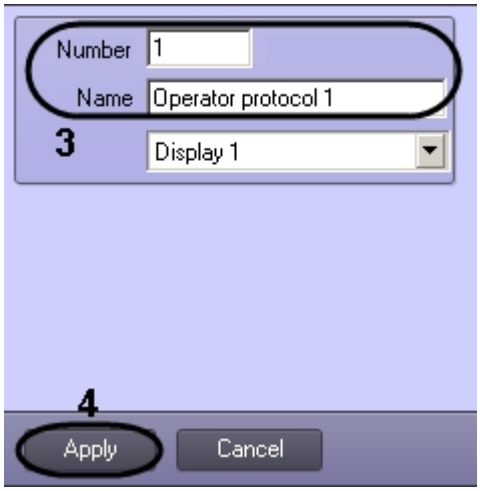
10.4.7.1 Creating the Operator protocol object

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).



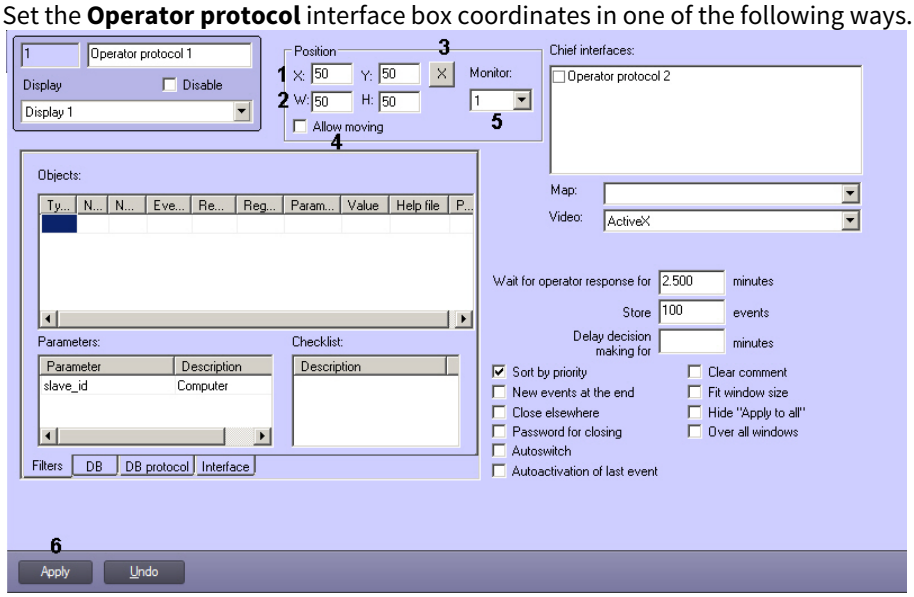
4. To create an object, click the **Apply** button (4).

As a result the settings panel for the Operator protocol is displayed.

10.4.7.2 Configuring the position of the Operator protocol object

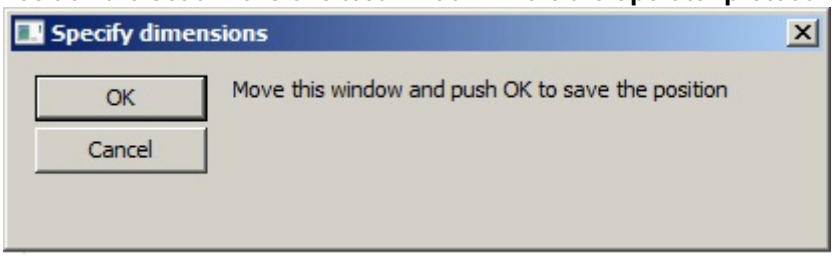
To configure the **Operator protocol** object position, do the following on the settings panel of the object:

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.

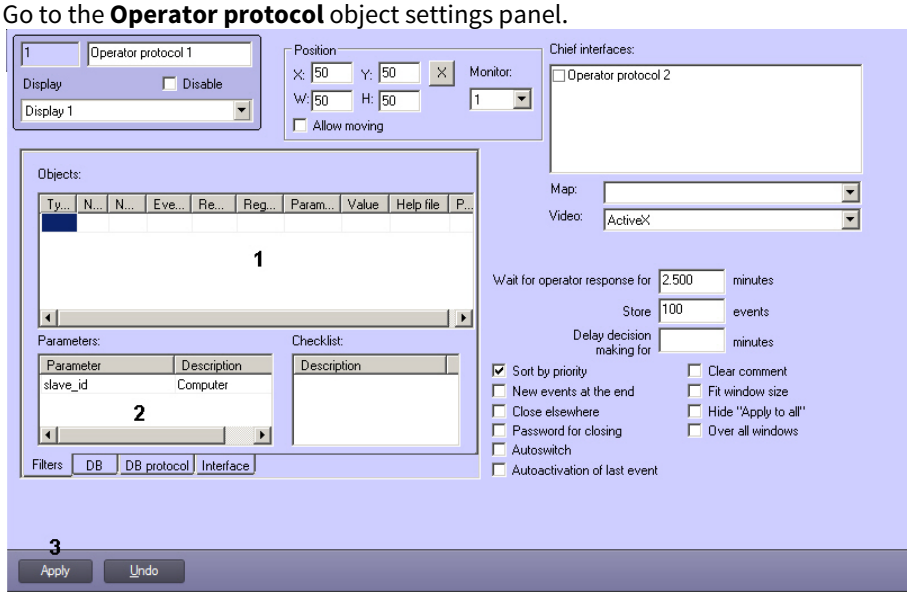
2. Set the **Allow moving** checkbox if the position and size of the **Operator protocol** interface box are to be changed manually (4).
3. In the **Monitor** dropdown list select the the system ID of a monitor for which the coordinates are set and on which the **Operator protocol** interface box is to be displayed (5).
4. Click **Apply** (6).

The **Operator protocol** object position is now configured.

10.4.7.3 Setting up the event filter for the Operator protocol

None of the events are displayed in the Operator protocol by default. Specify the objects the events from which are to be received and processed as follows:

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):

> **Important!**
>
> 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).

3. Repeat actions described in step 9 for all required objects. To add a line go to the last line of the table and click the ↓ key.

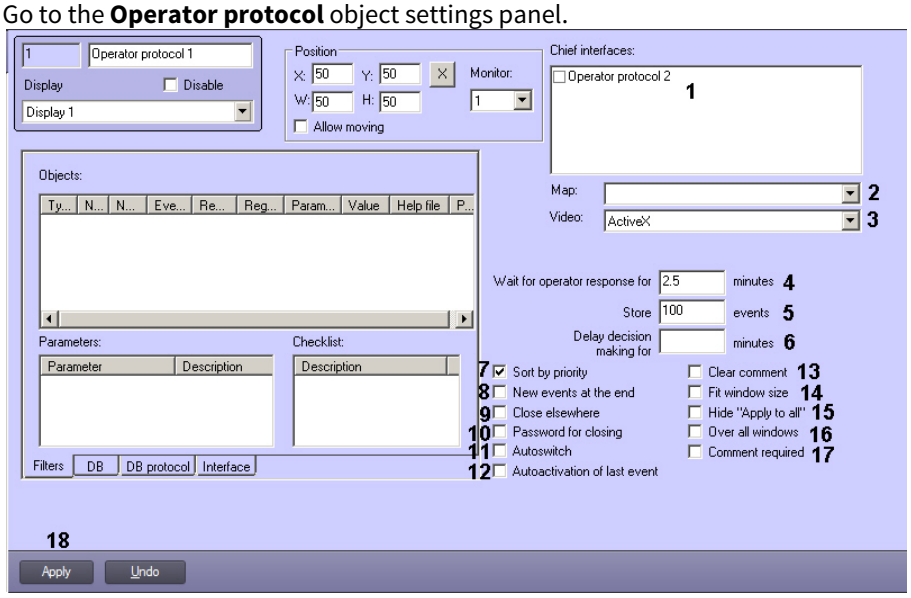
> **Note.**
>
> To remove the lines from the table use the Ctrl + Del key combination.

4. In the **Parameters** table, specify additional settings for an object event. These settings are to be displayed in the **Operator protocol** interface box (2).
   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** (3).

10.4.7.4 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 set the checkboxes checked next to **Operator protocol** objects to which events are to be sent when the specified time period expires (1).
3. In the **Map** dropdown list select the precreated **Map** object for event monitoring (2).
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 for camera boxes.
5. In the **Wait for the operator response** field specify the time period at the end of which an event will have the **Non-processed** event type or it will be escalated (4). 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.
6. In the **Store ___ events** field, set the maximum of events displayed in the Operator protocol interface box (5).

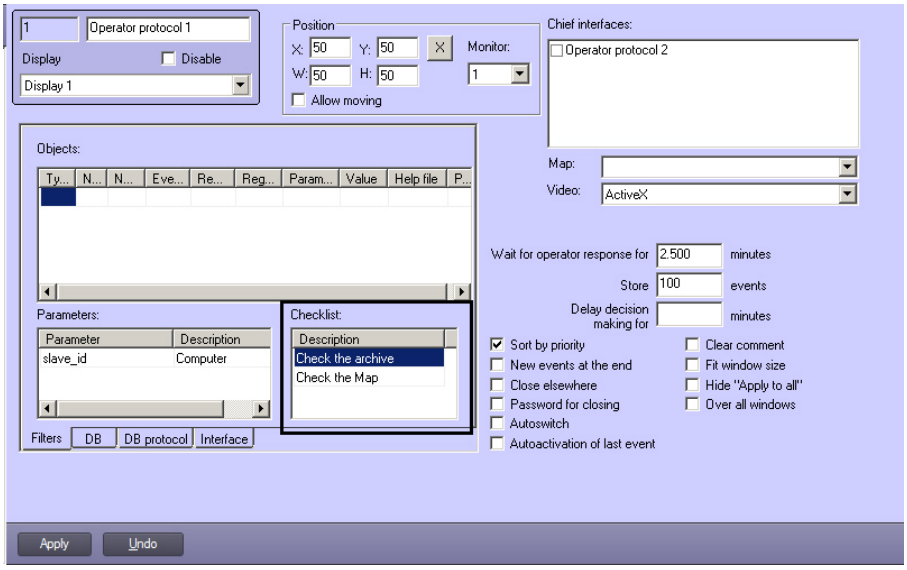
> **Important!**
>
> The number of events displayed in the Operator protocol interface box affects the main memory capacity. If 100 non-processed events are displayed in the interface box, then the **Operator protocol** module can use up to 200 Mb of main memory. When the value of the **Store ___ events** 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 specify the time period (in minutes) for which the event procession will be delayed (10). The time period is specified in minutes, though noninteger values can be set - in this case the dot is used to separate integer and noninteger 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 checked (11). 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 checked if new events are to be added to the end of the list of current events (12).
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 checked (13).
11. If the processing of all events is to be confirmed with a password, set the **Password for closing** checkbox checked (14).
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 checked (15).
13. If it is necesary to automatically activate the last received event, set the **Autoactivation of last event** checkbox (16).
14. 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 (17).
15. 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 (18).
16. If it is necessary to prohibit the Operator from processing all alarms at once, set the **Hide "Apply to all"** checkbox (19).
17. If the Operator protocol interface window is to be displayed on top of all other windows, set the **Over all windows** checkbox (20).
18. To prevent the Operator from processing the event without entering a comment, set the **Comment required** checkbox (17). 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.
19. Click **Apply** to save changes (18).

The options for handling events in the Operator protocol are now configured.

10.4.7.5 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.

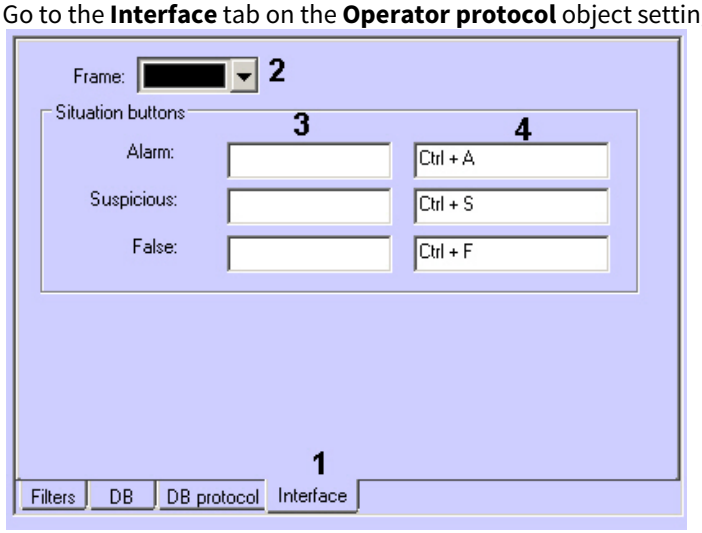


10.4.7.6 Configuring the Operator protocol interface

Button names and hotkeys for event classification as well as the active event cell frame color are configurable.

Configure the Operator protocol interface as follows:

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 (1).
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 (2).
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 (3) 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. To save the settings click the **Apply** button.

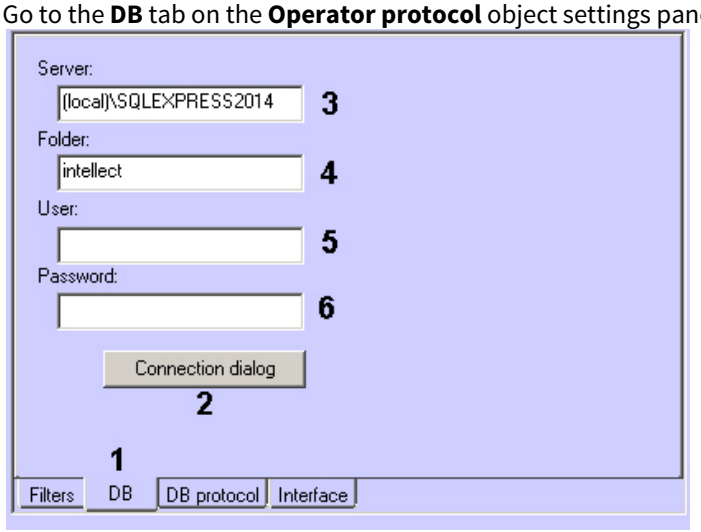
The Operator protocol interface is now configured.

10.4.7.7 Connecting external DBs

10.4.7.7.1 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.

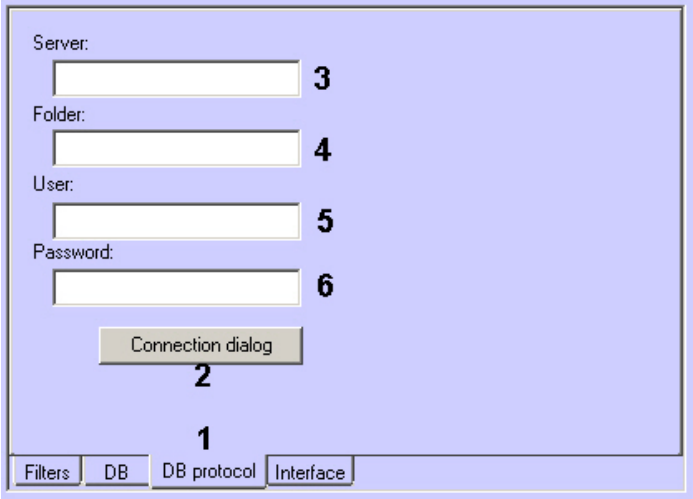
Working in the distributed configuration it is needed to enter the name of computer without the (local) value where the database is stored. For example, "WS1\SQLEXPRESS", where WS1 is the name of computer on which the database is stored.

      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**.

10.4.7.7.2 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).

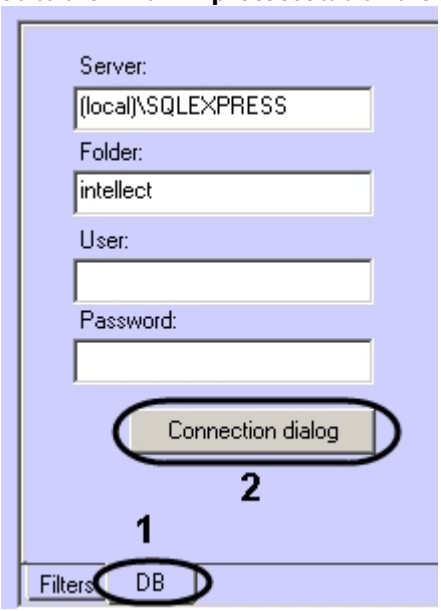
iv. In the **Password** field set the password for the authorization on the database server (6).

3. Click **Apply**.

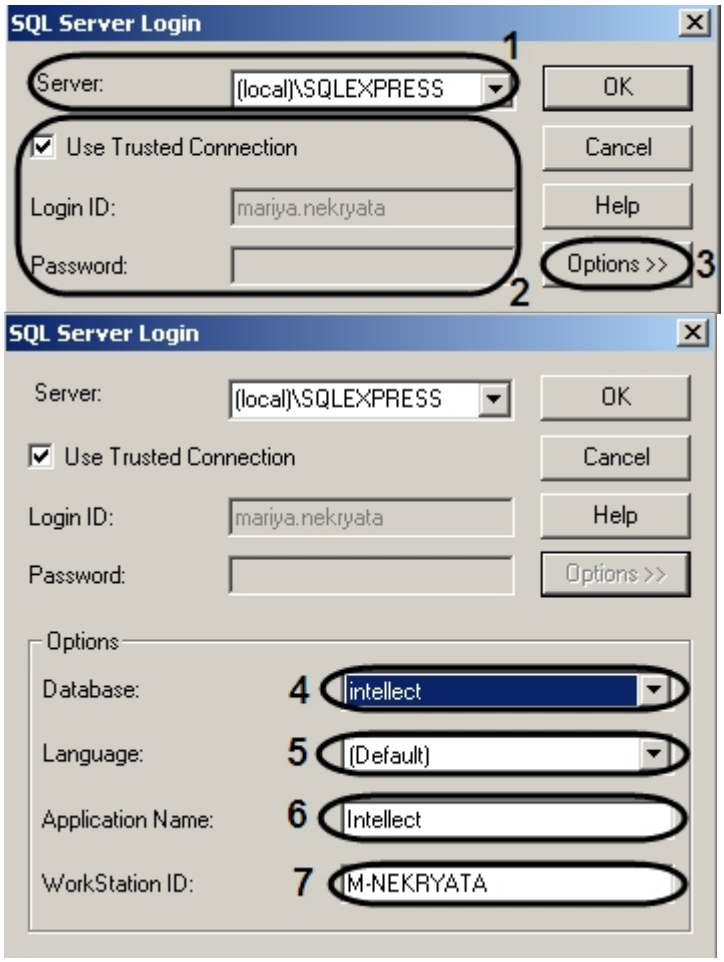
10.4.7.7.3 Configuring the database server connection in a dialog mode

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.

10.4.8 Configuring the Event Viewer interface object

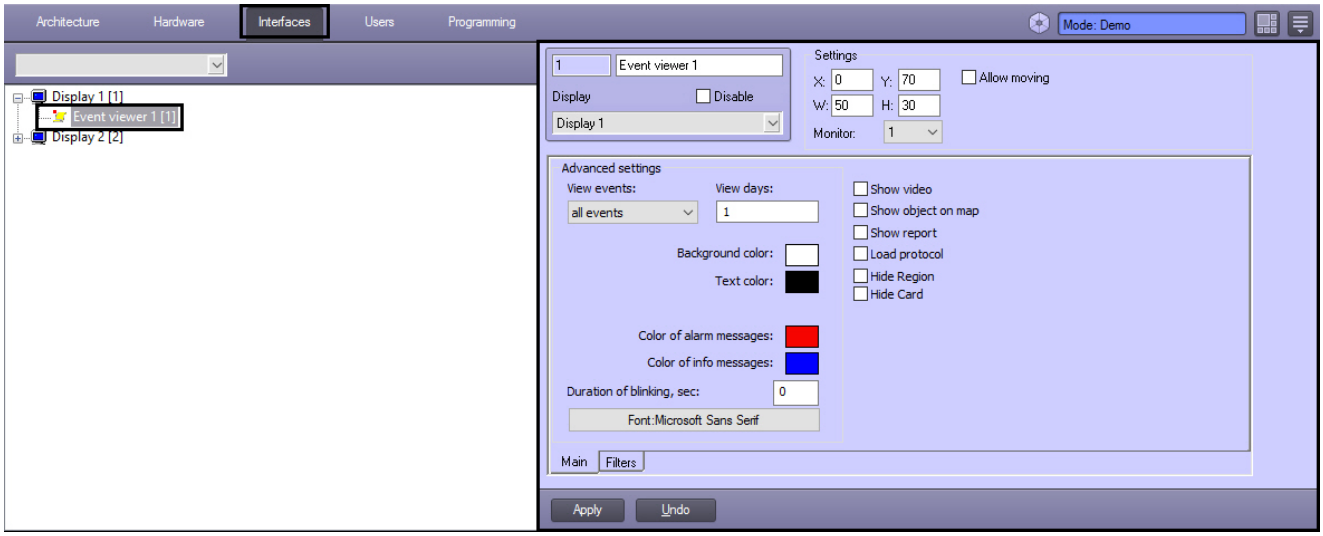
10.4.8.1 Order of configuring the Event Viewer interface object

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:

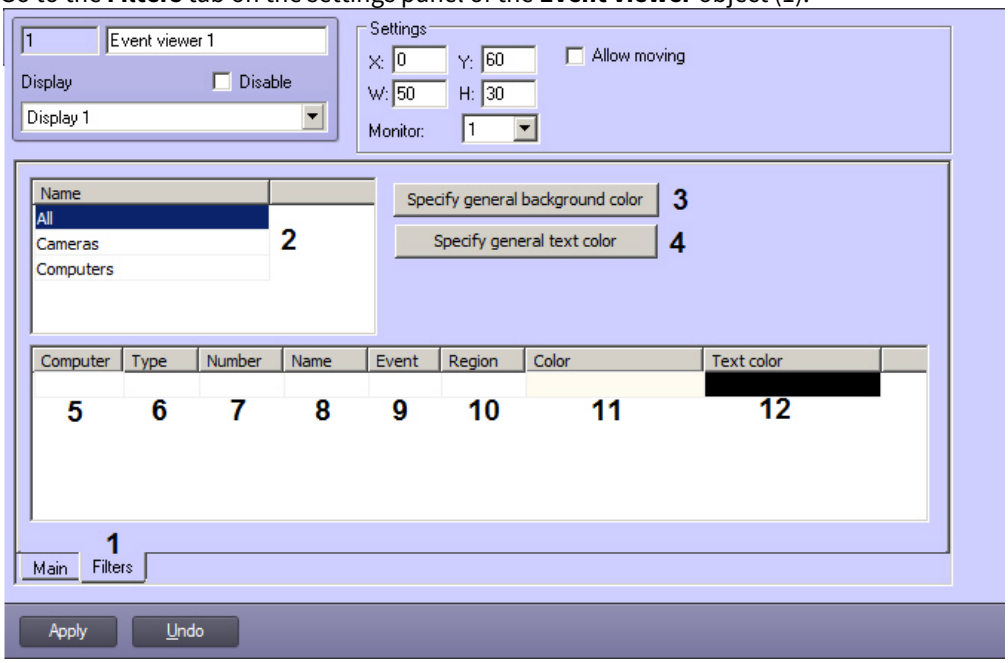
1. Choose the events, information on which should be logged to the **Events viewer** interface object in case of its registration in the system (see Configuring event filters for displaying in the Event viewer).
2. Set the parameters of the event viewer (see Event viewer parameters).
3. Configure the displaying of the **Event viewer** interface box (see Parameters of displaying the Event Viewer interface box).

Event control via event log

10.4.8.2 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).

> **Note.**
>
> 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

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** dropdown 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 dropdown 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.**
>
> Activation of the drop-down list in the **Objects** tab and in the **Areas** list is made by LMC upon the corresponding cell. Detailed description of actions with tabs and lists is in the Object settings panel.

> **Important!**
>
> A blank filter (i.e. filter with blank columns) is to 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.

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. In the **Areas** table select the region which object's events are to be logged (10). If the objects are identified (see step 3) or no region is set, then the events are logged without object's belonging to any region.
11. In the **Color** dropdown list select the background color for the message about event in the Event viewer (11).
12. In the **Text color** dropdown list select the text color of the event message in the Event Viewer (12).
13. Repeat steps 3-9 for all required objects and sections in the filter.
14. Repeat steps 2-10 for all required objects and regions.
15. Click the **Apply** button to save all the changes.

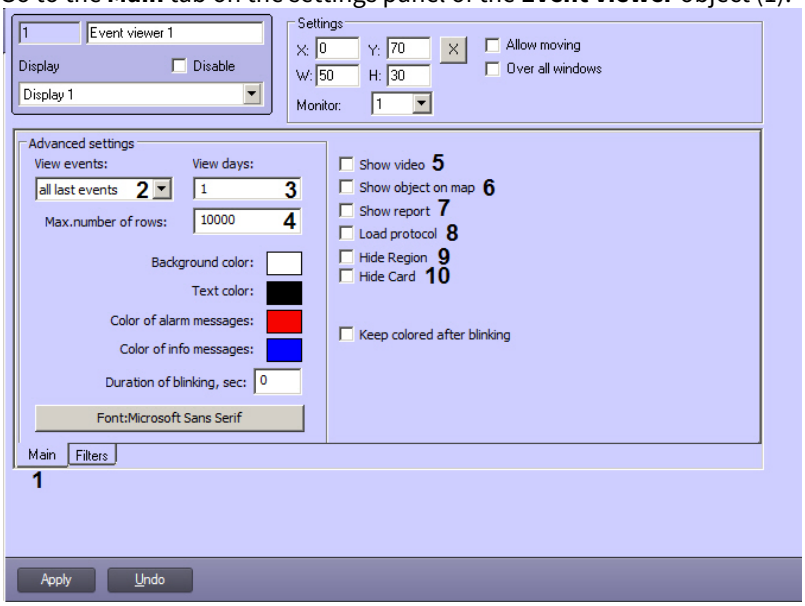
Events for logging to the **Events viewer** interface object are now selected.

> Event control via event log

10.4.8.3 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.

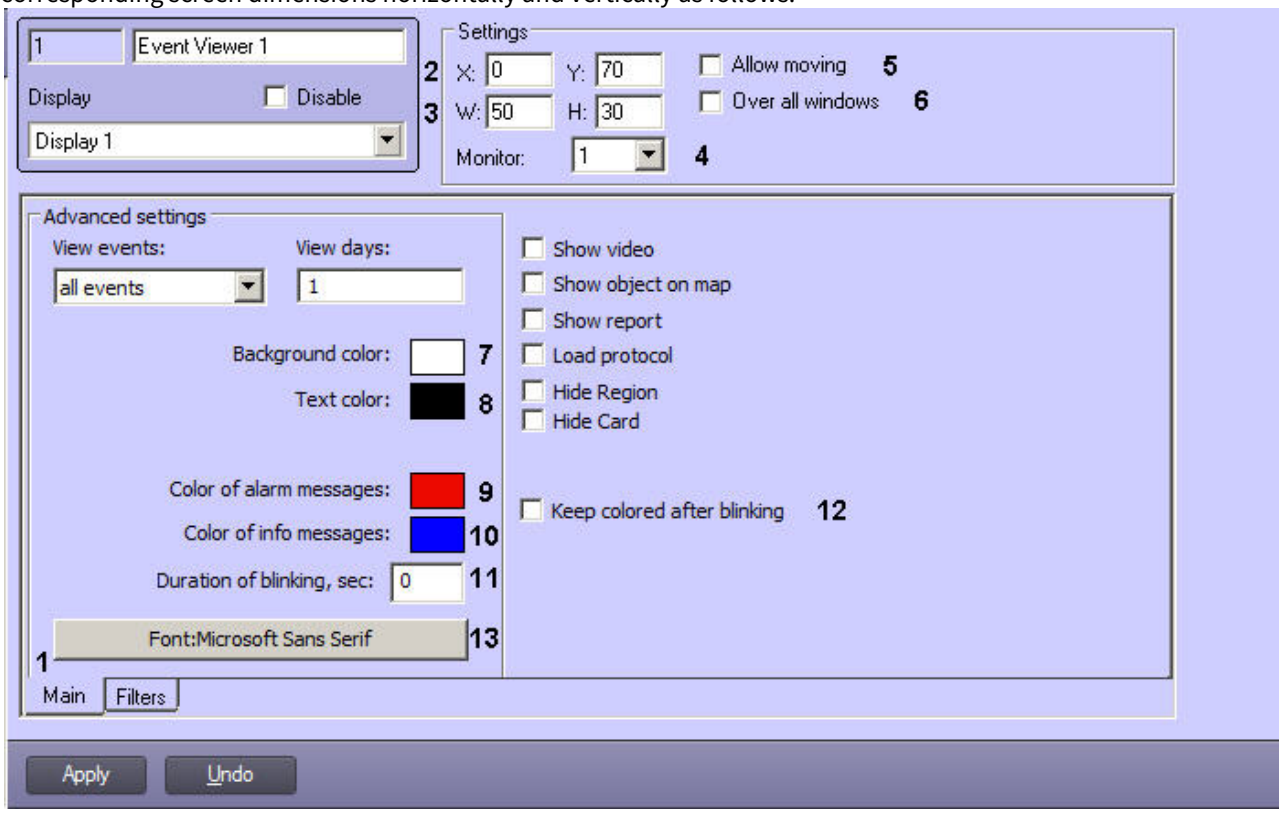
Event viewer parameters are now set.

10.4.8.4 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. If the **Operator** is to be allowed moving the **Event Viewer** by left-clicking on it, then set the **Allow moving** checkbox (**5**) checked.
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 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.**
>
> The **Duration of blinking**, **sec** must not be 0 in order for the setting to apply.

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.**
>
> The **Duration of blinking**, **sec** must not be 0 in order for the setting to apply.

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.

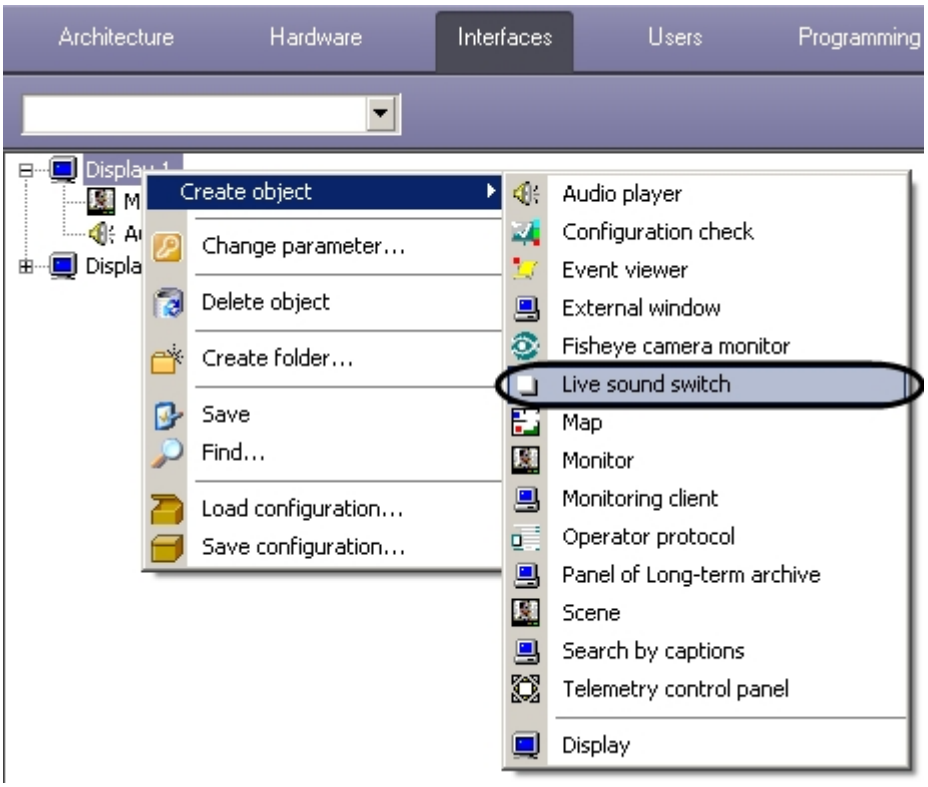
Parameters of displaying the **Event viewer** interface box are now set.

10.4.9 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.

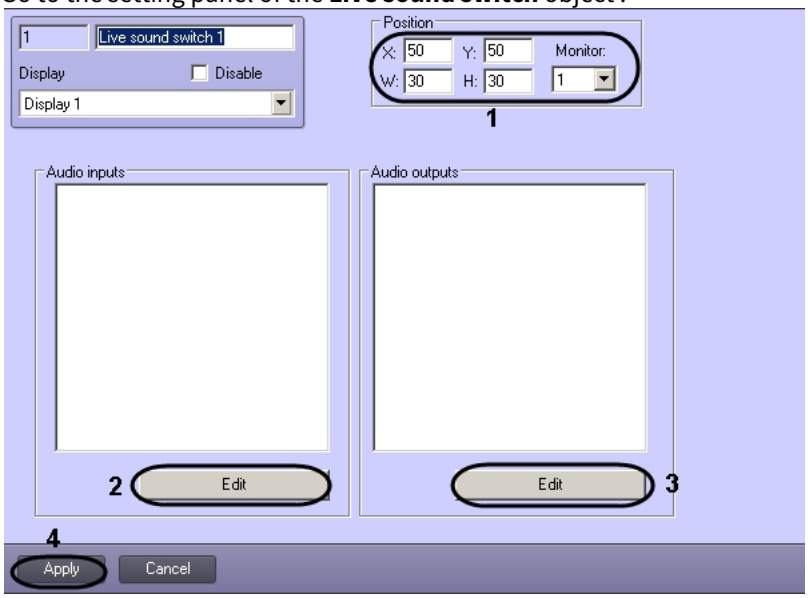
10.4.9.1 Creating and configuring the Live sound switch object

The **Live sound switch** object is created on the basis of **Display** object in Interfaces tab of **System setting** dialog box.

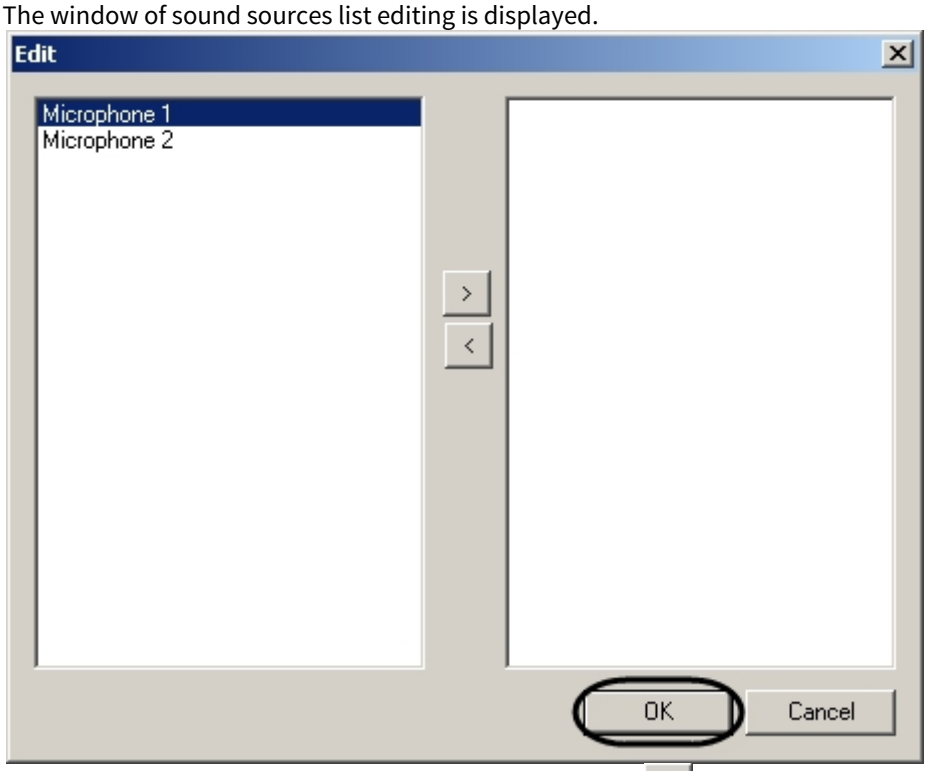


To set up the Live sound switch object do the following:

1. Go to the setting panel of the **Live sound switch** object .



2. To set the position of the **Live sound switch** object dialog box, set a value of the position data of the left upper corner in **X:**, **Y:** fields and value of width and height of the box in **W:, H:** fields (1).
3. To add sound sources click **Edit** in **Audio inputs** (2).
   The window of sound sources list editing is displayed.



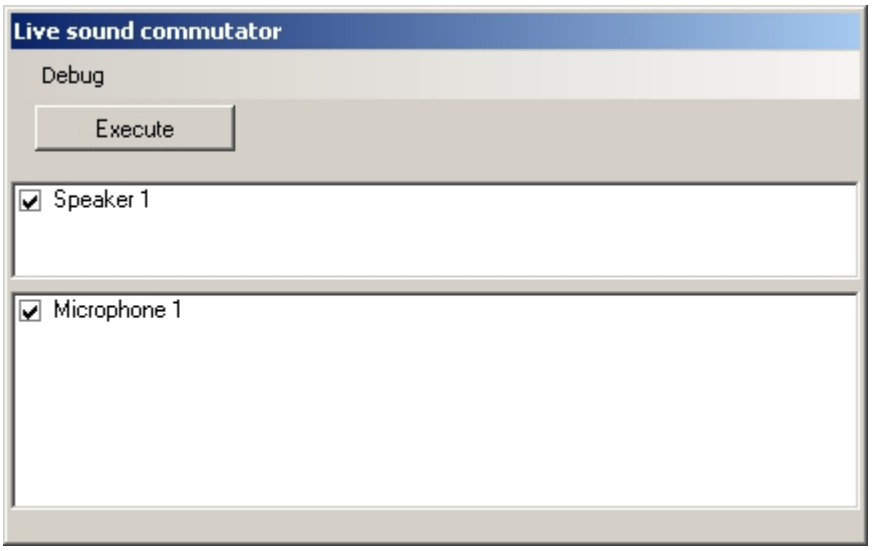
4. Select the required sound sources in the left list and click  .
   As a result the selected sound sources are moved to the right list

> **Note.**
>
> To remove the sound sources from the right list select them and click  .

5. Click **OK** to save the changes.
6. To add the sound detectors click **Edit** in **Audio outputs** (3). The sound detectors adding is made by analogy with sound sources adding (item 4-5).

7. Click **Apply** to save all the changes (4).

The dialog box of the **Live sound commutator** object is displayed.

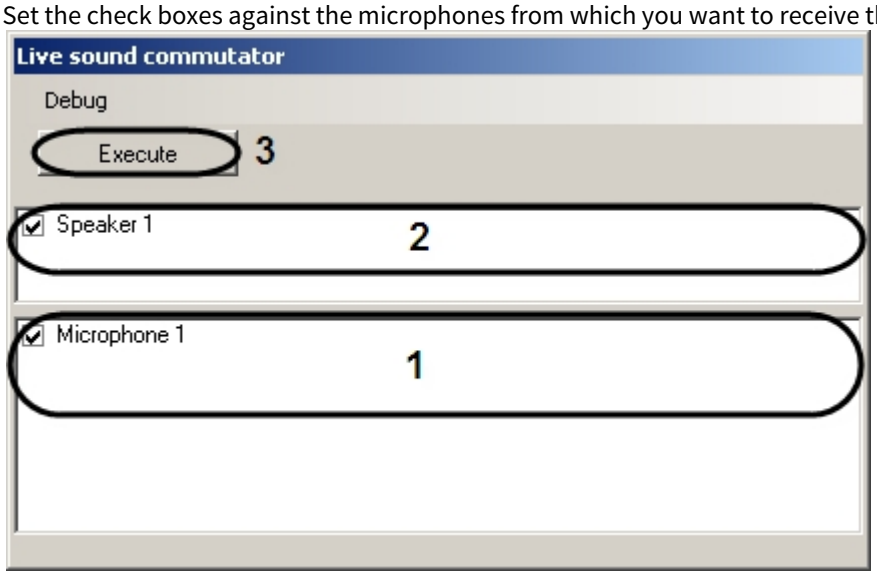


Setting up the **Live sound commutator** object is completed.

10.4.9.2 Using the Live sound switch object

Working with the **Live sound switch** object is carried out in the dialog the following way:

1. Set the check boxes against the microphones from which you want to receive the sound (1).



2. Set the check boxes against the speakers on wich the sound should be played (2).
3. Click **Execute** (3).

As a result the sound from selected microphones will go to the selected speakers.

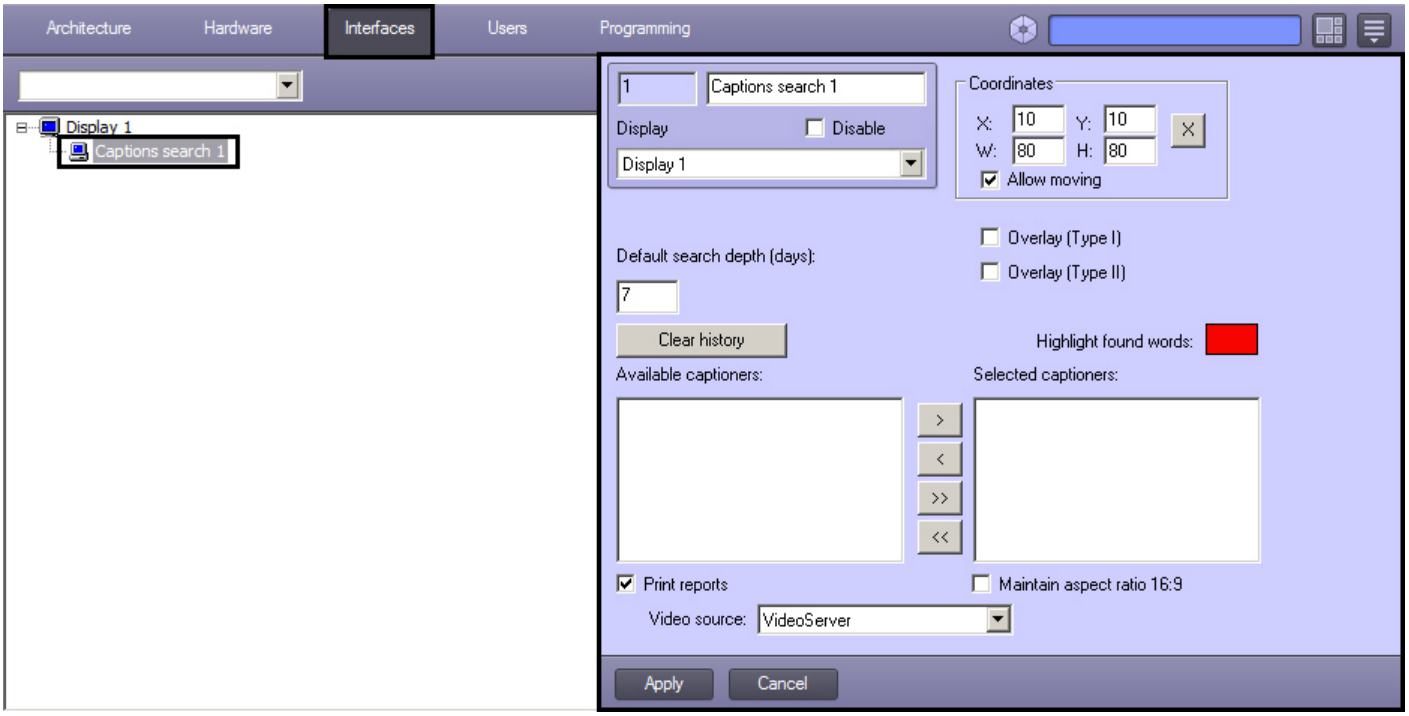
> **Note.**
>
> Sound in the speaker is mixed (overlayed) if several microphones are selected.

10.4.10 Setting up the Captions search window

10.4.10.1 The Captions search window setup procedure

The **Captions search** object is a child of the **Screen** object; it is used for creating user queries on the titles database.

To create and set up the **Captions search** object, use the **Interfaces** tab in the **System Settings** window.



The **Captions search** object setup includes the following steps:

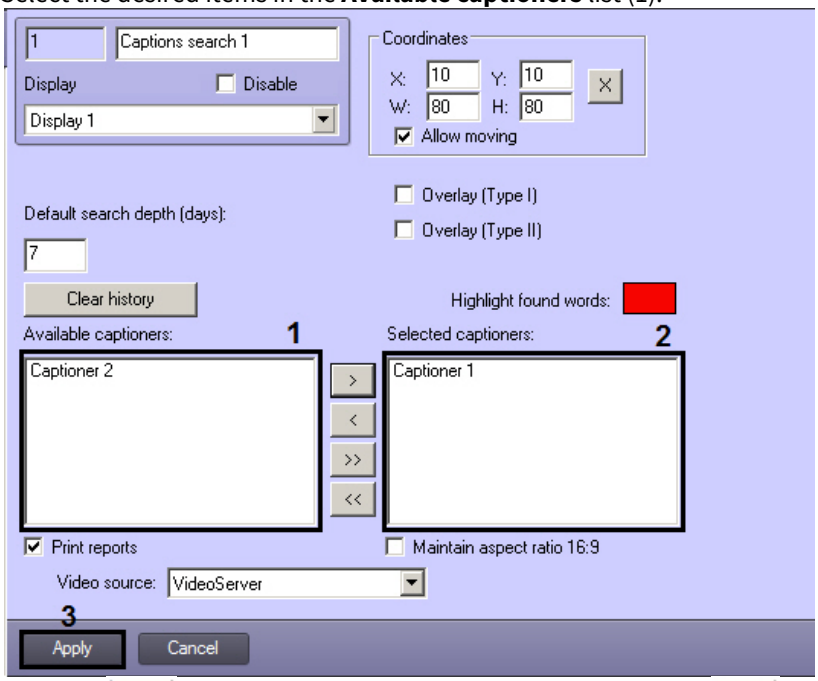
1. Select the captioners
2. Specify the search criteria
3. Set up the **Captions search** window

> Working with Captions search interface object

10.4.10.2 Selecting the captioners

Select the captioners to be used for searching the data. To select the captioners, do the following:

1. Select the desired items 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 available captioners to the **Selected captioners** list (2).

> **Note.**
>
> Alternatively, the < and << buttons are used to remove the selected or all captioners from the Selected captioners list.

3. Click **Apply** (3).

The captioners are now selected.

10.4.10.3 Specifying the captions search parameters

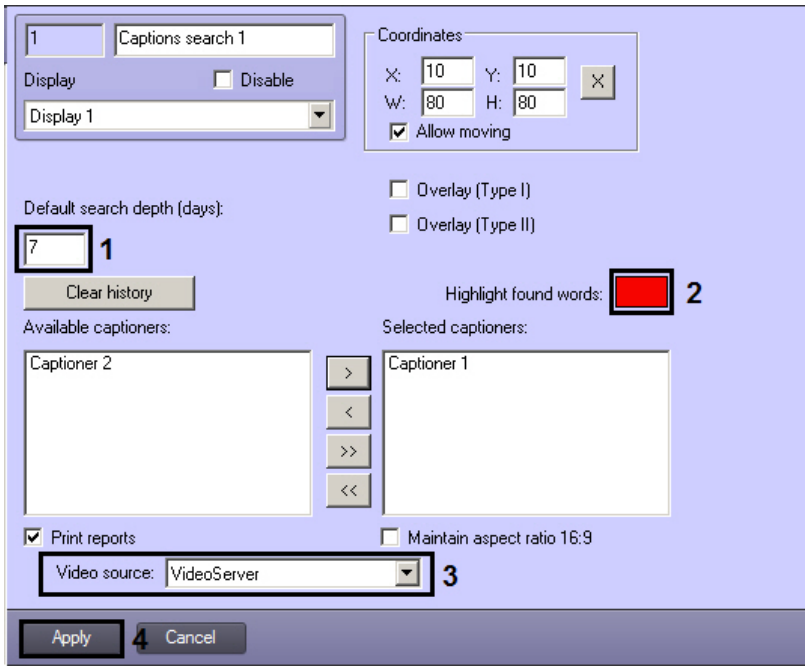
To set up the captioner search, the following parameters should be specified:

1. **search depth** – the captioner search depth;
2. **highlighting a found word** – 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.

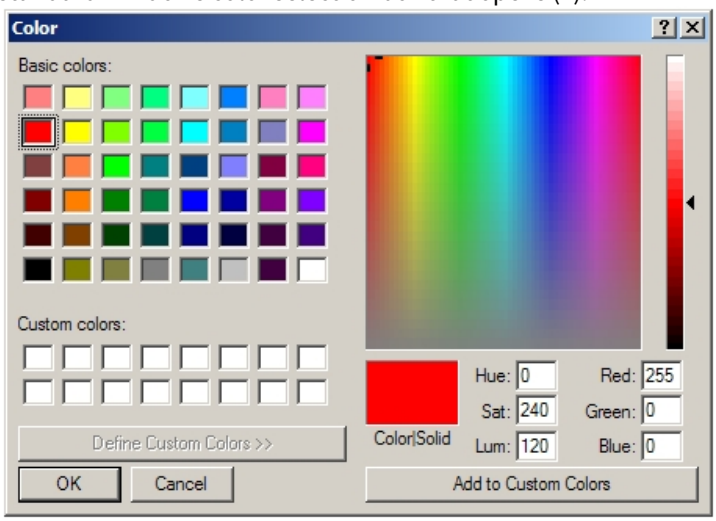
> **Note.**
>
> Storing captions can be disabled by **NoSaveTitles** registry key – see Registry keys reference guide.

To specify the captioner search criteria, do the following:

1. Enter the archive search depth (in days) in the **Default search depth** 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. In the **Video source:** dropdown list select an archive from which video data is displayed as search results: video server main or backup archive (3).
4. Click **Apply** (4).

The captioner search criteria are now set.

10.4.10.4 Setting up the Captions search window displaying

To set up the **Captions search** window, the following parameters should be specified:

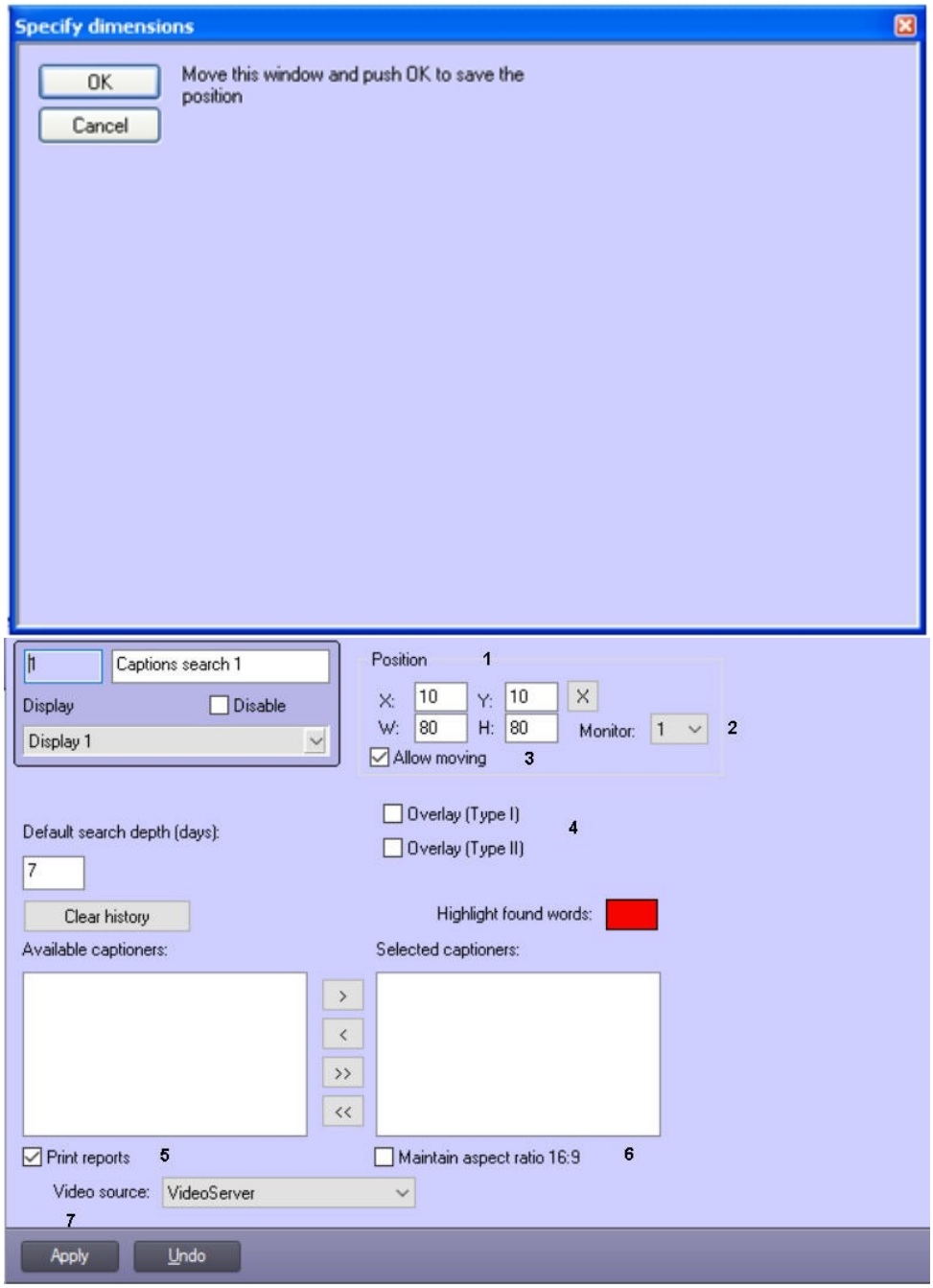
1. coordinates – the position and size of the window;
2. overlay type – the type of the overlay of the synchronous display of video image and search results;
3. print reports – the user can print the search results.

To set up the **Captions search** window, do the following:

1. Specify the position and size of the **Captions search** window (1): **X** is the indent relative to the left border of the video image, **Y** is the indent relative to the top border of the video image, **W** is the window width, **H** is the window height.

   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 sample window, then click OK. The coordinates of the sample window will be filled in the X, Y, W and H fields

automatically.



2. In the **Monitor** drop-down list, select the number of the computer monitor to display the **Captions search** window (2).
3. By default, the option of moving the **Caption search** window by dragging with left mouse button is enabled. To disable it, uncheck the **Allow moving** checkbox (3).
4. Set the overlay type by checking the **Overlay (Type I)** or **Overlay (Type II)** checkbox (4).

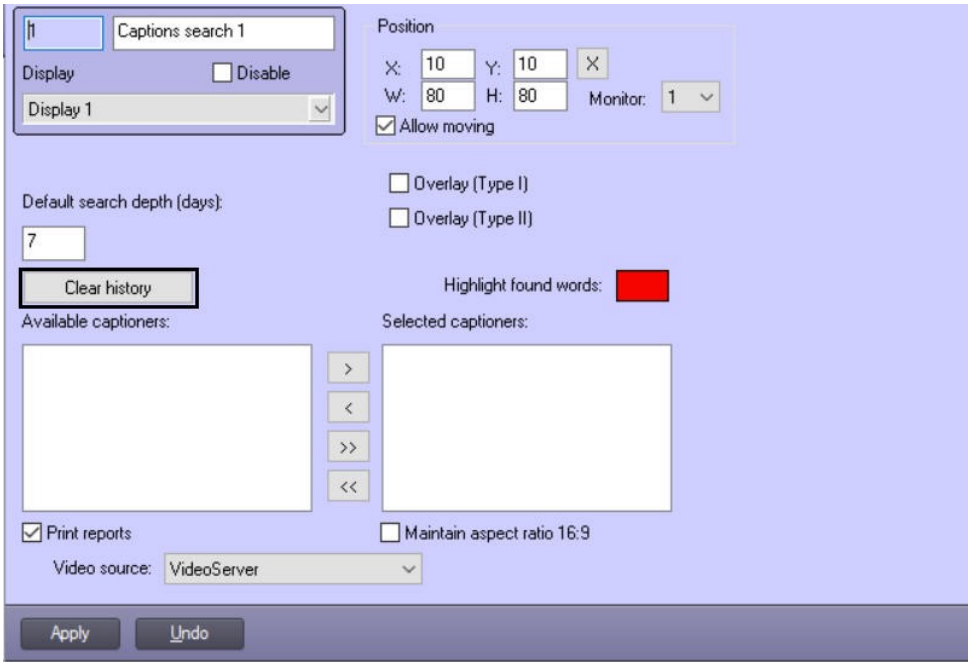
> **Note.**
>
> In most cases, the optimal mode of processing the video is DirectDraw — **Overlay (Type II)**. If it is necessary to display the video from Fisheye cameras or the signal decoded using Intel QuickSync technology, select the **Overlay (Type I)** — Direct3D. Also, the Overlay can be disabled completely.

5. To allow the operator to print the search results, check the **Print reports** checkbox (5).
6. If archive video is to be displayed in the **Captions search** window in the 16:9 format, then set the **Maintain aspect ratio 16:9** (6) checkbox checked. If the checkbox is set unchecked, then 4:3 aspect ratio is set even for HD video.

7. Click **Apply** (7).

The **Captions search** window is now set.

> **Note.**
>
> To clear the history of user queries in the **Captions search** window, click the **Clear history** button.



10.4.11 Configuring HTML interface

10.4.11.1 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

10.4.11.2 Procedure of HTML interface configuring

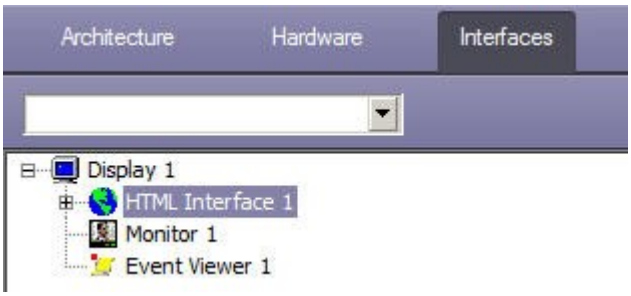
To configure HTML interface in the *Intellect* software, do the following:

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.

10.4.11.3 Creating HTML interface object and setting its position

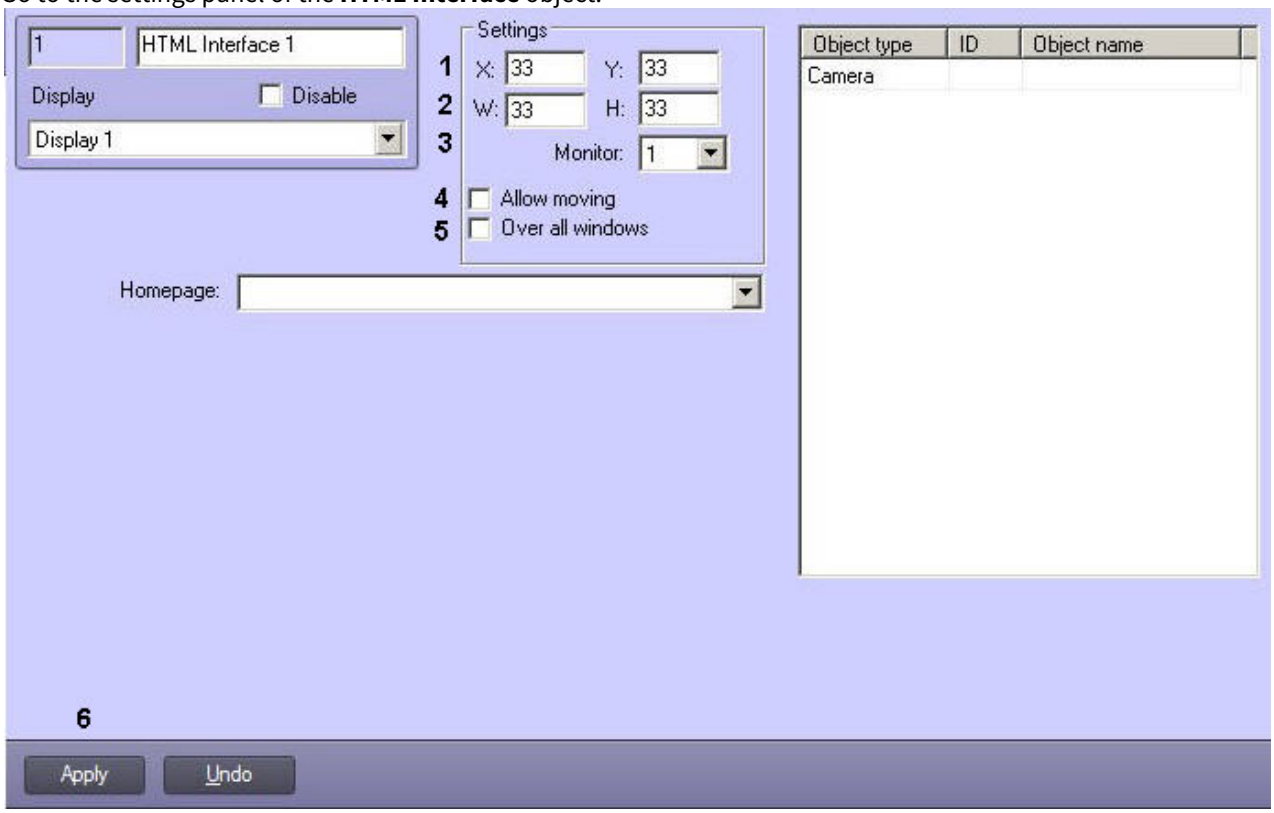
The **HTML interface** object is created on the basis of the **Display** object on the **Interfaces** tab of the **System settings** dialog window.



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.



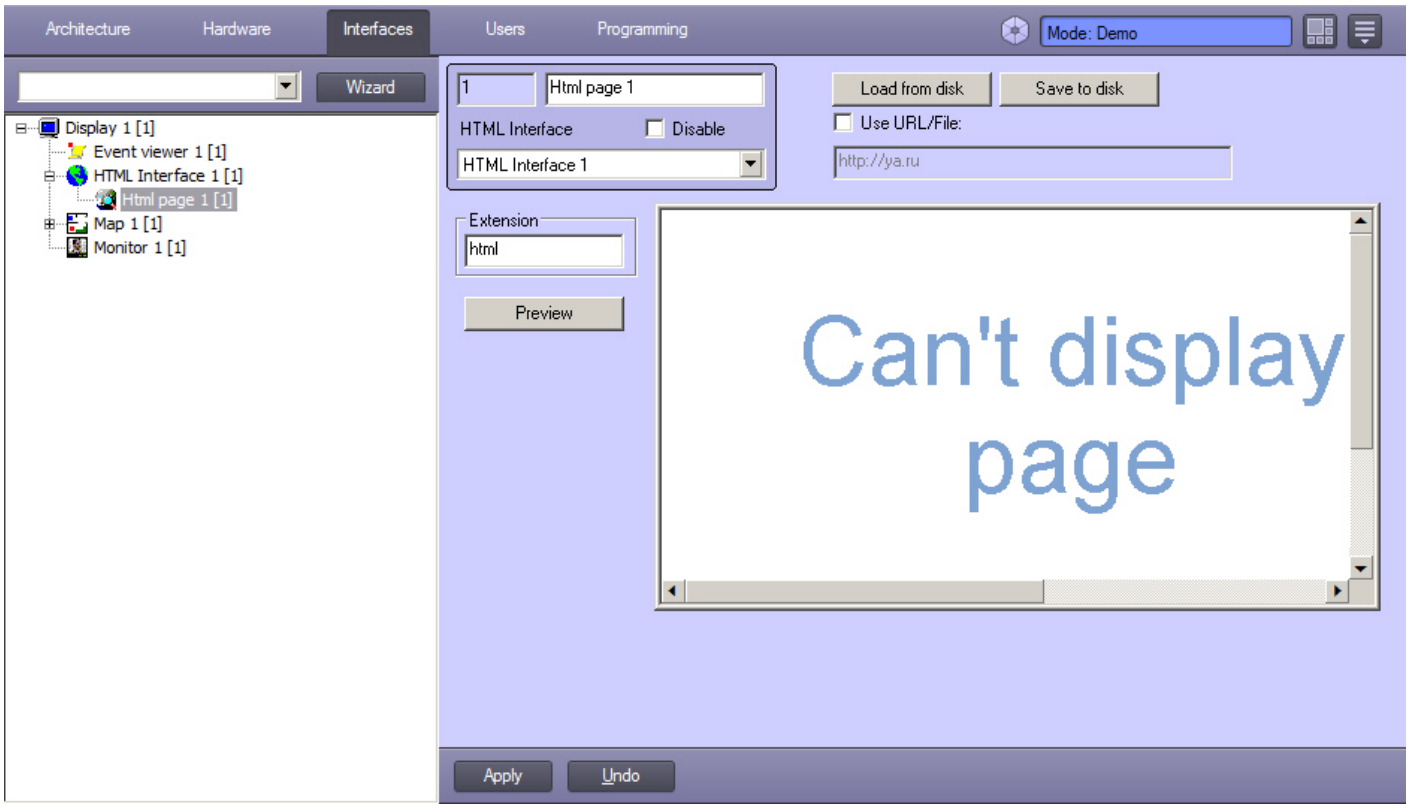
2. In the **X:** and **Y:** fields specify coordinates of the interface window's upper left corner (**1**). Coordinates are counting from the display's upper left corner and expressing as a percentage of the screen width and height respectively.
3. In the **W:** and **H:** fields specify width and height 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.

10.4.11.4 Creating and configuring the HTML page object

10.4.11.4.1 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.



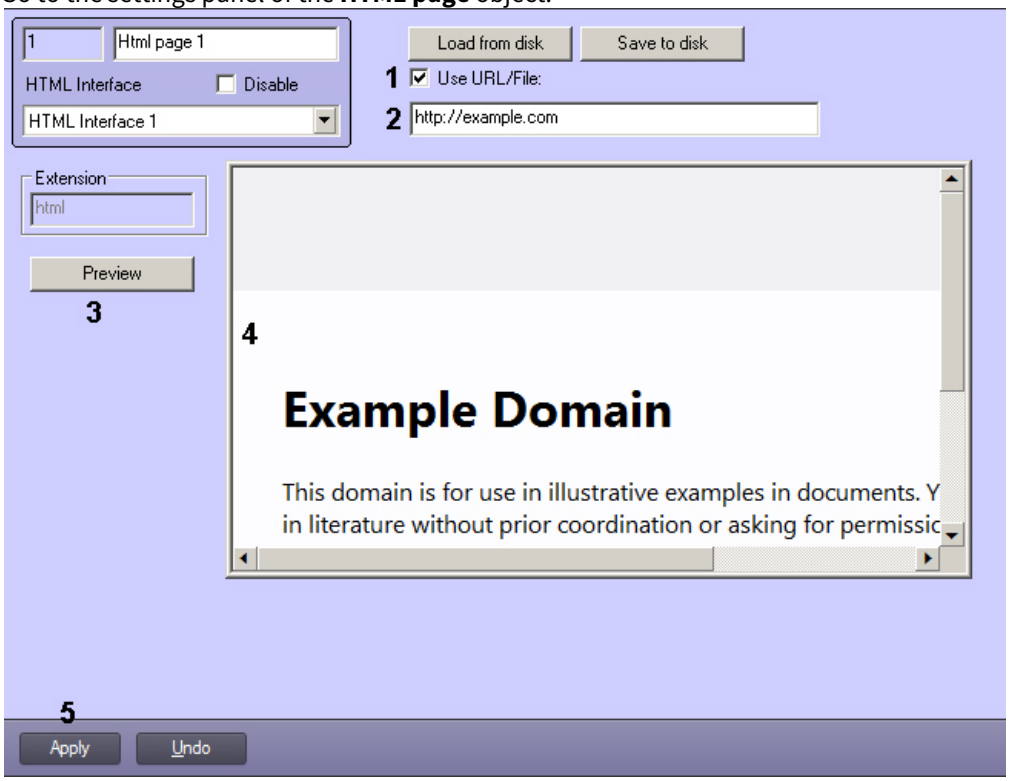
Object's settings panel will display on the right part of the **System settings** dialog window after the object creation.

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.

10.4.11.4.2 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.



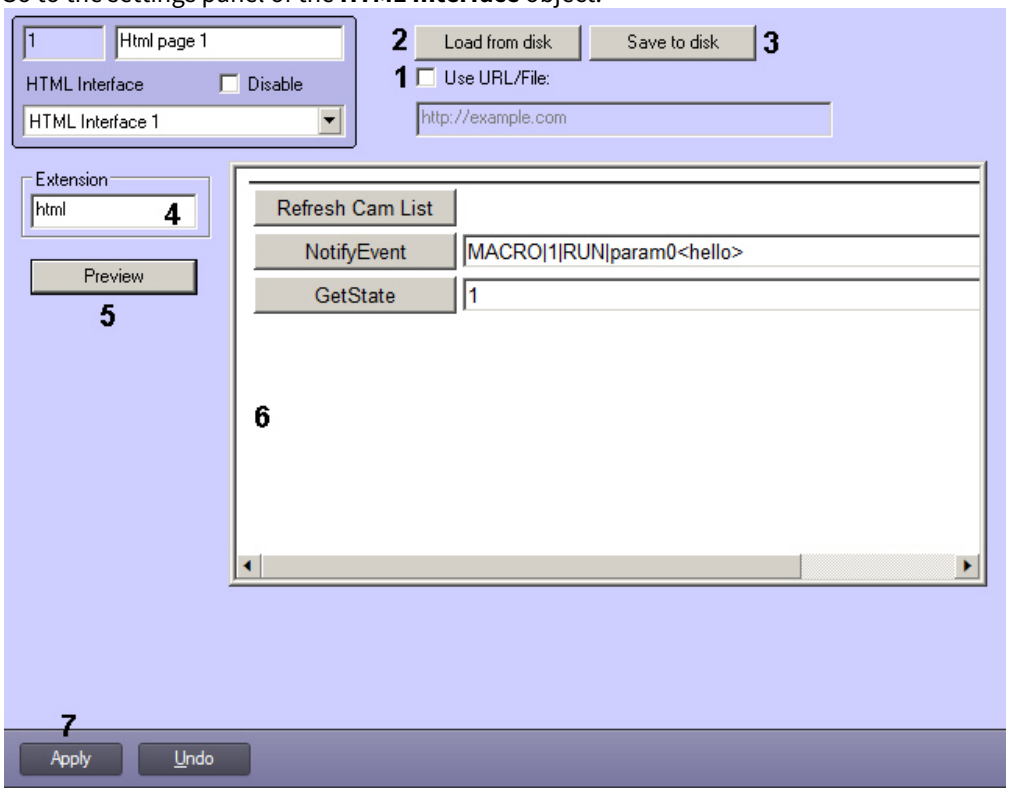
2. Set the **Use URL/File** checkbox (1).
3. In the text field enter the URL-address of required page (2).
4. Click the **Preview** button to display the selected HTML page (3). As a result the page content will display in the preview box (4).
5. Click **Apply** (5).

Configuring of opening web-page by specified URL is completed.

10.4.11.4.3 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.

10.4.11.4.4 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:

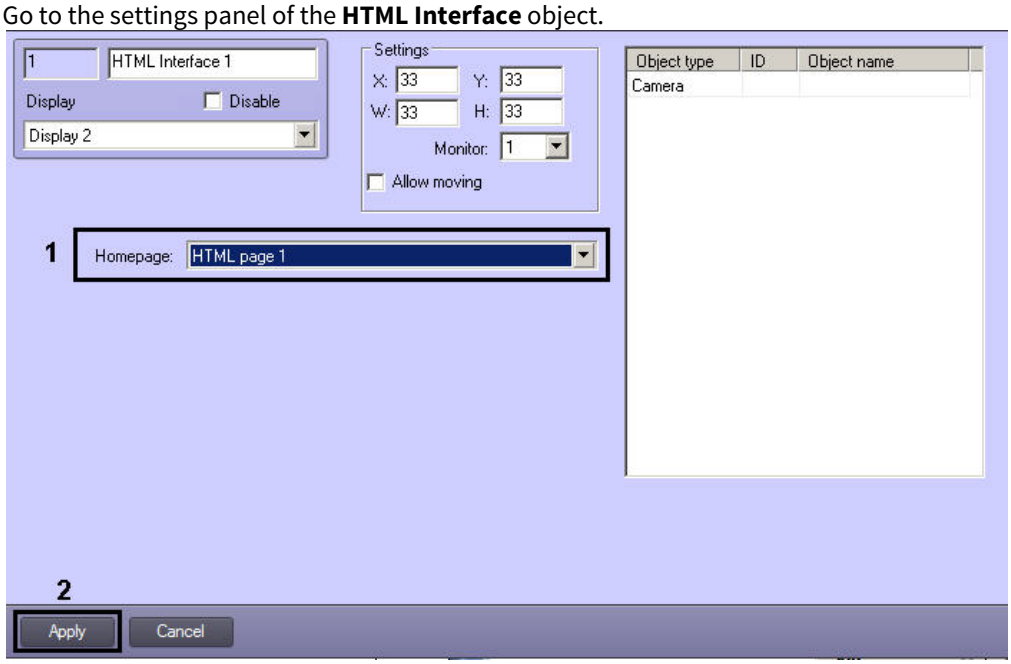
HTML page 2

> **Note.**
>
> If web-page is not opened by URL, the empty file will be saved.

10.4.11.5 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).

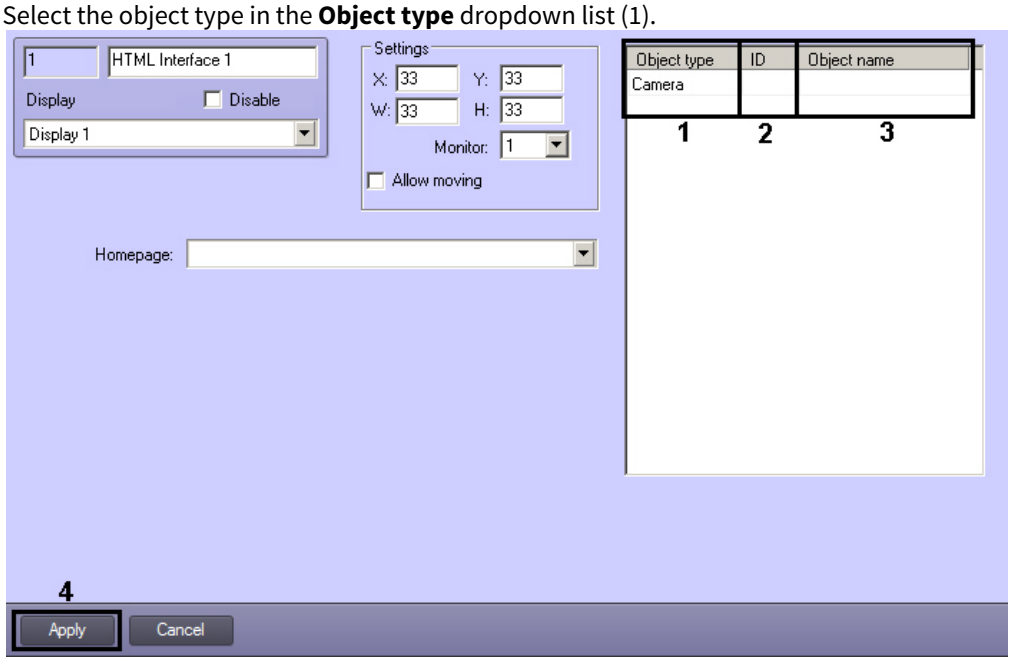
Configuring the start page is completed.

10.4.11.6 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).

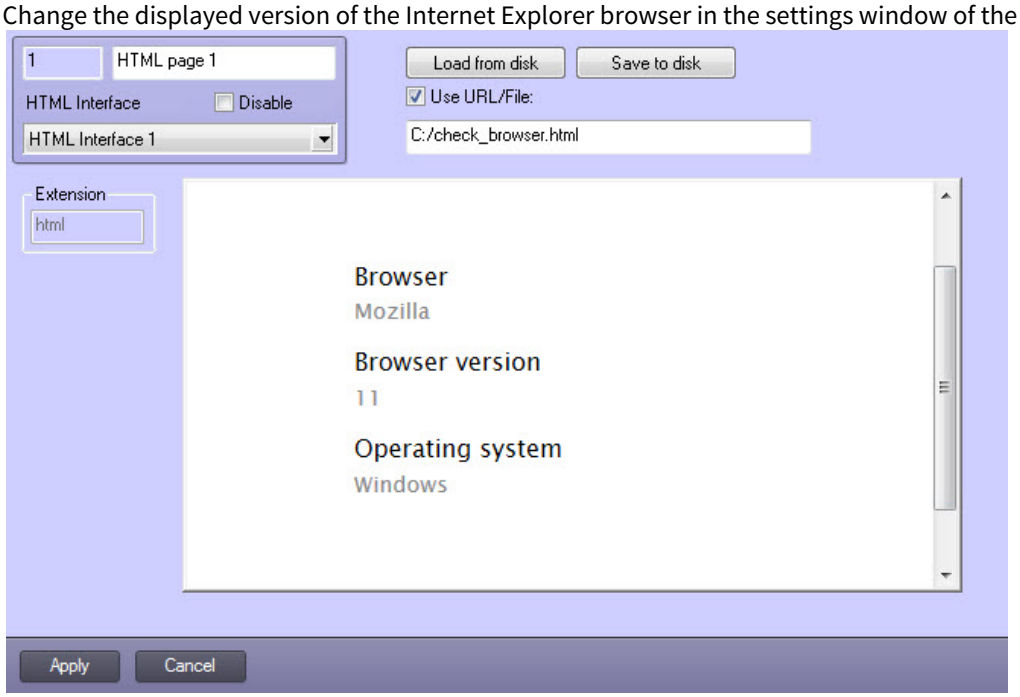
4. When left clicking in the **Object name** field it is automatically filled with the name of the object with this ID (3).
5. Repeat steps 2-4 for all required objects.
6. To save the settings click the **Apply** button (4).

Objects states of which are to be tracked are now selected.

10.4.11.7 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.



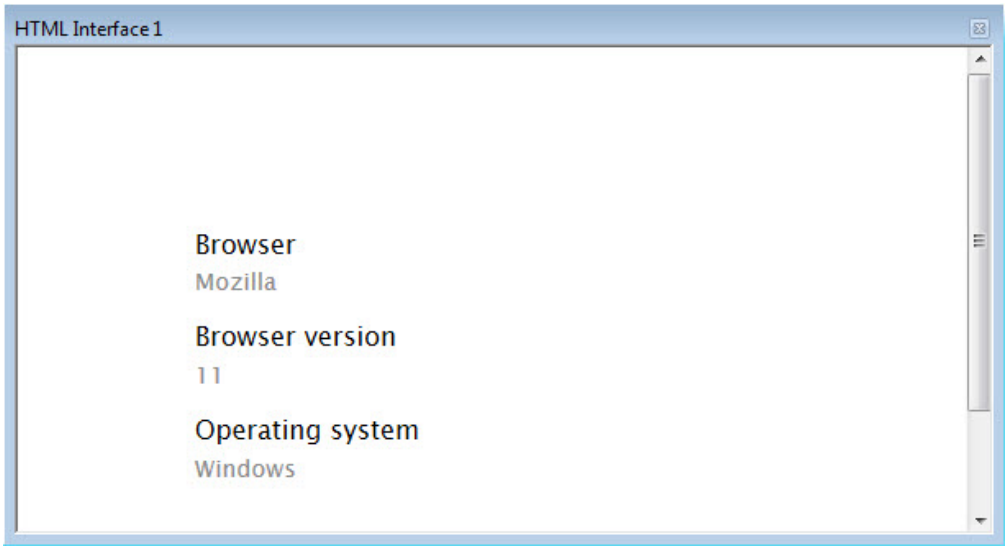
To do this, change the values of the **OpcIe.run** and **Intellect.exe** parameters to the required ones from the table below:

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.

10.4.12 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_alarm_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_alarm_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:

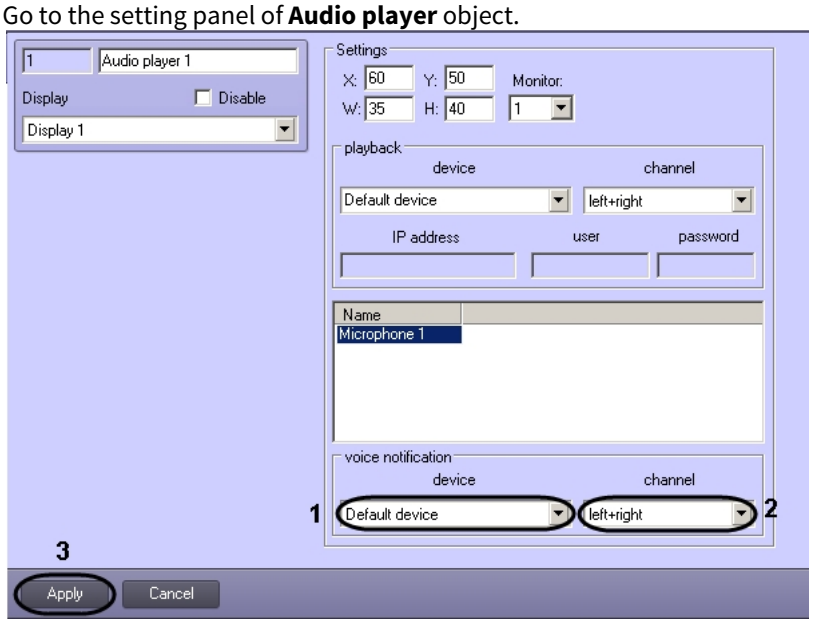
1. Using **Audio player** object;
2. Using **Sound notification** object;
3. Using **Voice Notification Service** object – this way allows selecting any audio file for voice notification, including a custom one.

It's recommended to use only one variant.

10.4.12.1 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**.

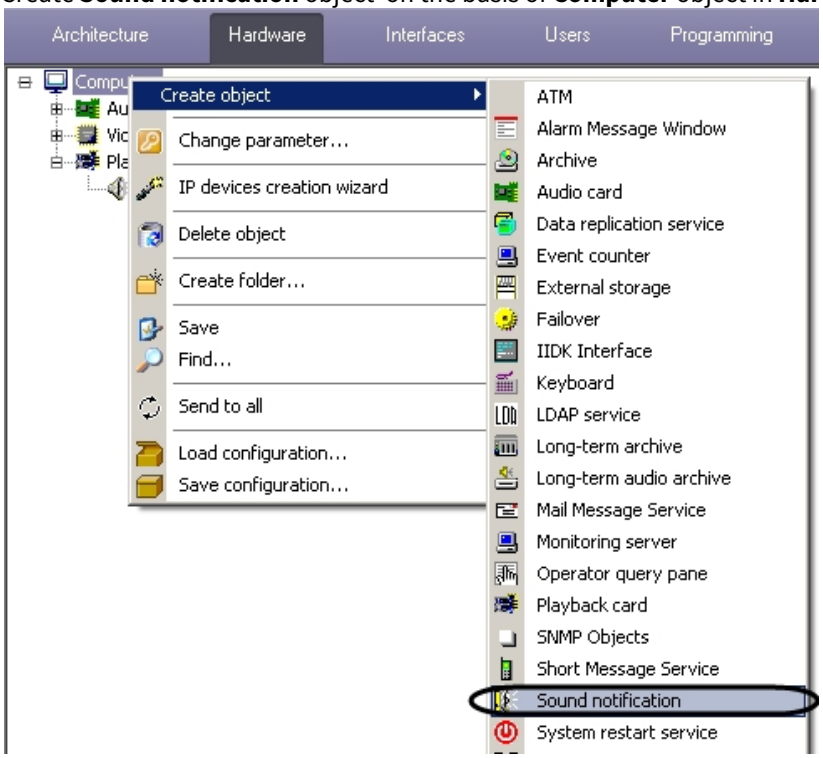
3. Select required voice notification channel in **Channel** dropdown list of **Voice notification** group (2).
4. Click **Apply** button to save all the changes (3).

Setting up the voice notification using **Audio player** object is completed.

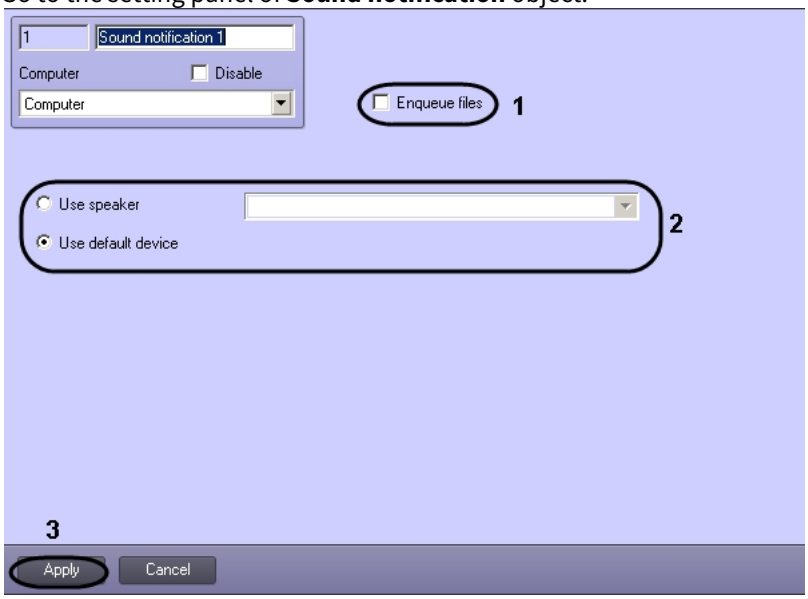
10.4.12.2 Setting up the voice notification using Sound notification object

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).

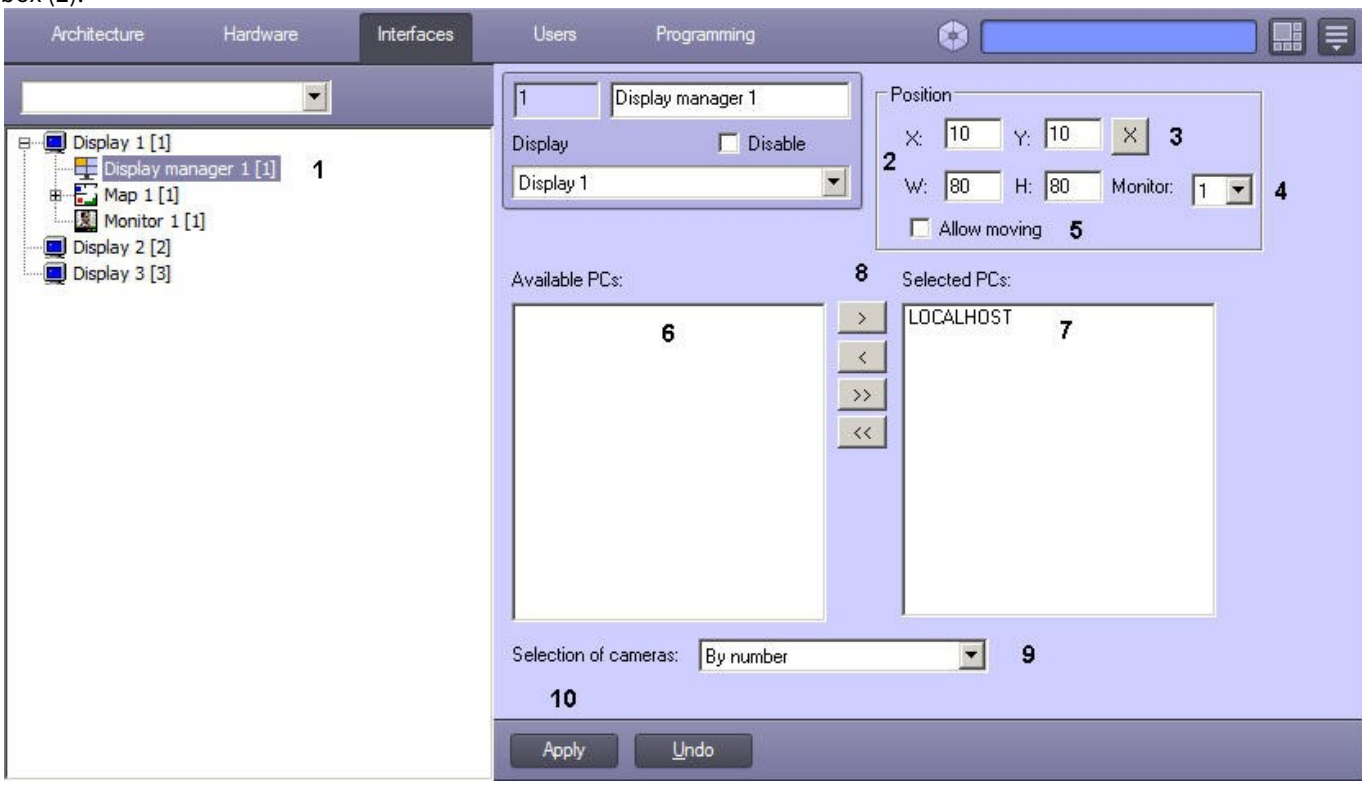
Setting up the voice notification using **Sound notification** object is completed.

10.4.13 Configuring the Display manager

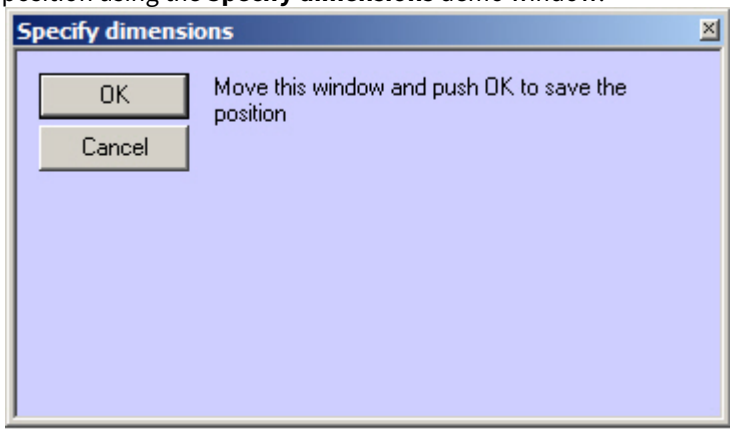
The **Display manager** interface object is designed to manage the video walls. It allows the Operator to conveniently configure the Video surveillance monitor layouts on the specified computers.

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**).

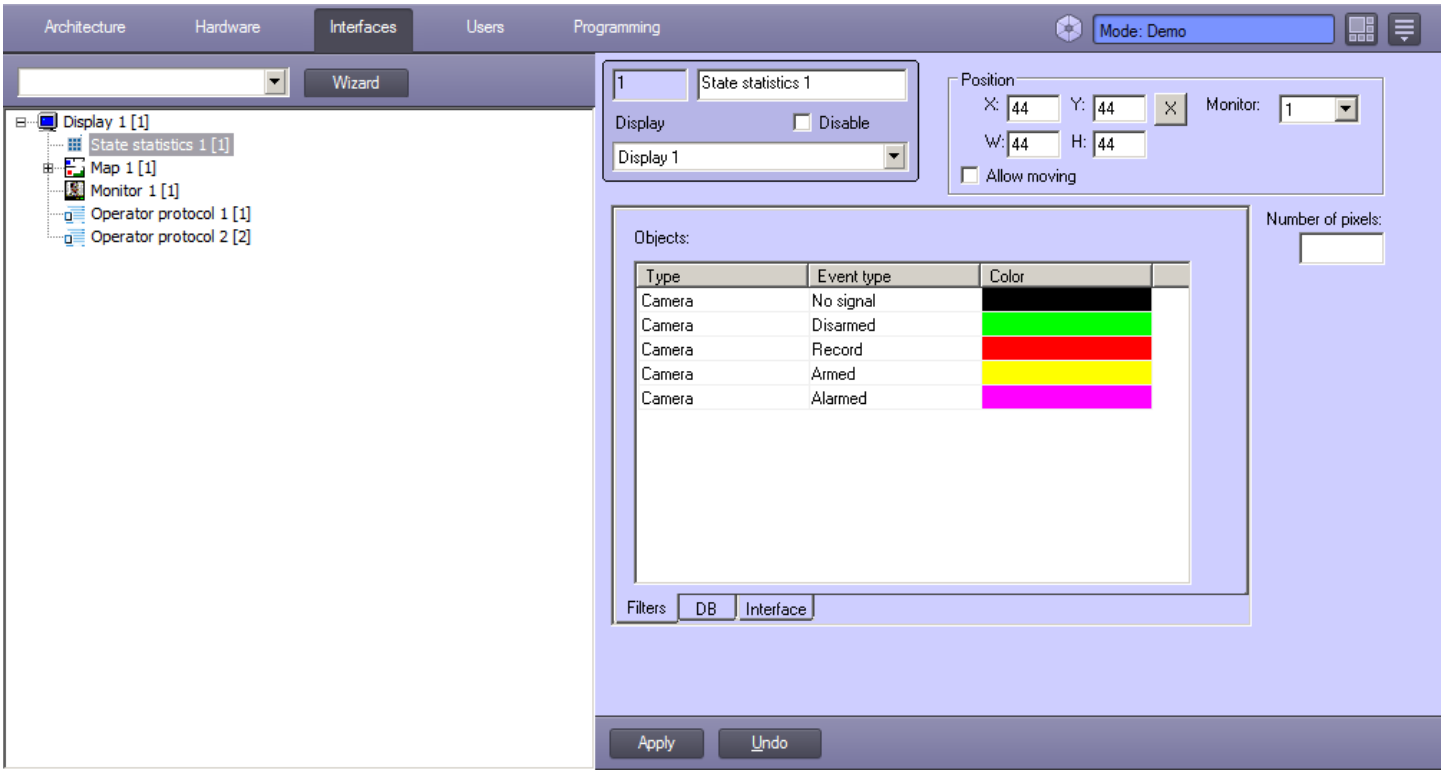
Configuring the **Display manager** interface object is complete.

> Managing the displays using the Display manager

10.4.14 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.



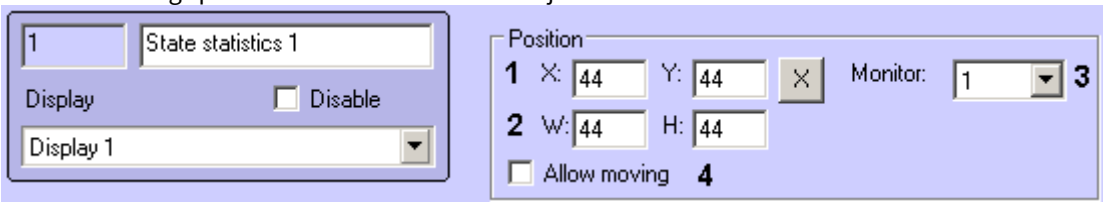
The **State statistics** display is configured in the following order:

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

10.4.14.1 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.



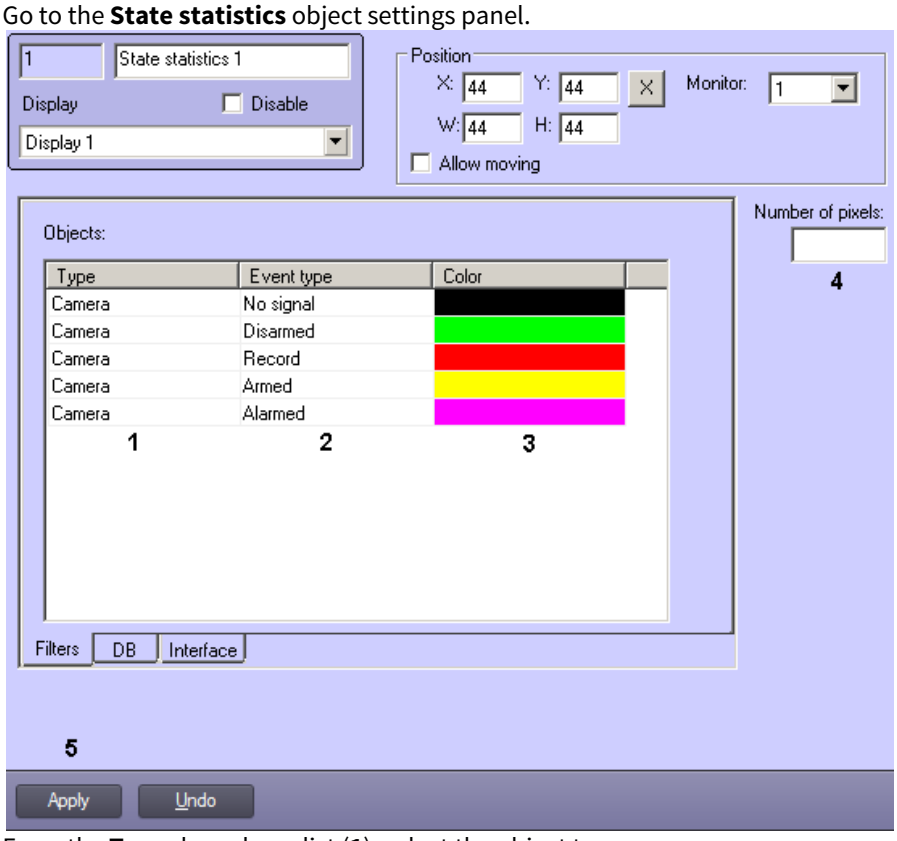
2. In the **X** and **Y** fields (**1**), specify the coordinates of the upper left corner of the interface window.
3. In the **W** and **H** fields (**2**), specify the width and height of the interface window.
4. From the **Monitor** drop-down list (**3**), select the physical monitor where the interface 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.

10.4.14.2 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.



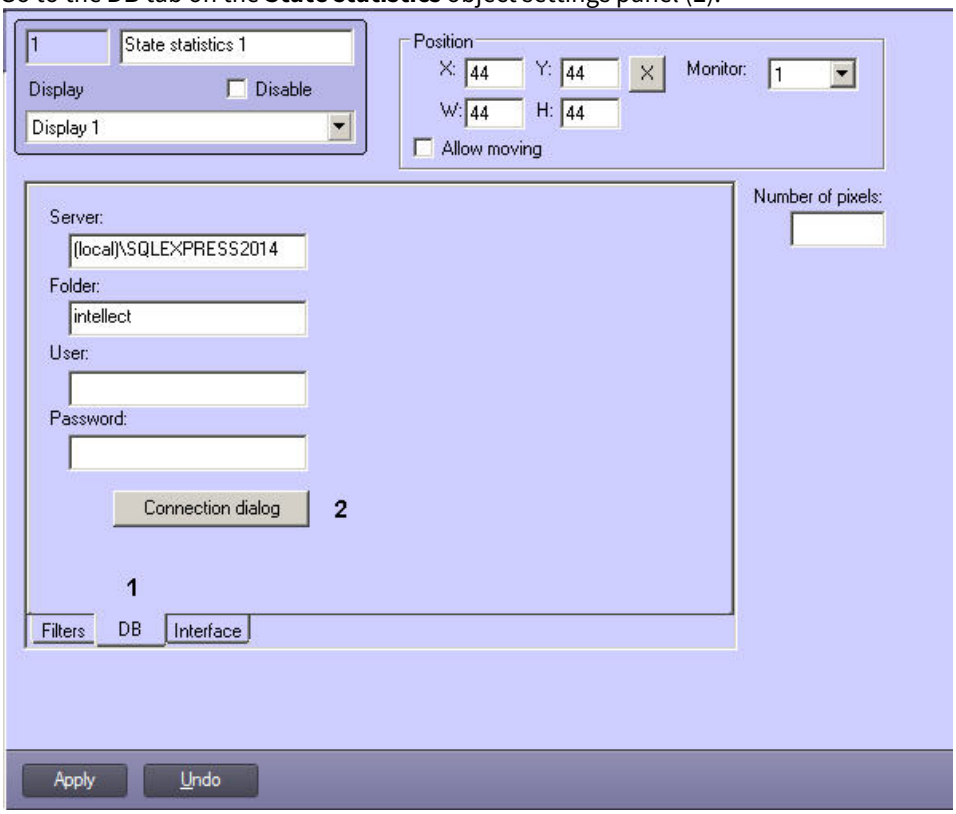
2. From the **Type** drop-down list (**1**), select the object type.
3. From the **Event type** drop-down list (**2**), select the state of objects of the selected type which should be included in the statistics. If the state is not selected, then the statistics on all states will be displayed.
4. From 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.

10.4.14.3 Configuring the database connection

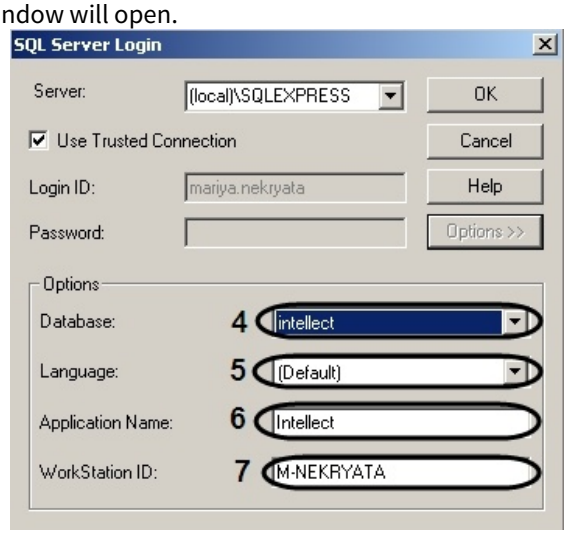
By default, the *Intellect* local database is used as a data source for the State statistics displaying. In order to use a remote database, configure the connection to it as follows:

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.

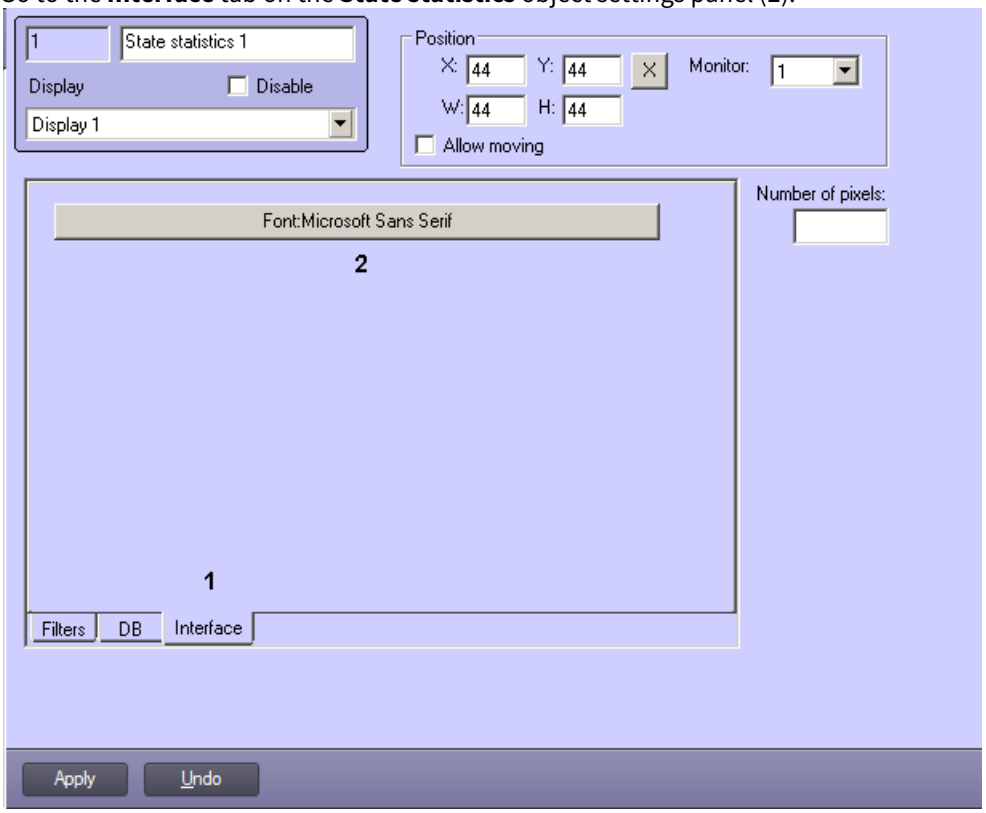
   > **Note**
   >
   > For the help information about the **Login to SQL Server** dialog box, click the **Help** button.

Setting up database connection is complete.

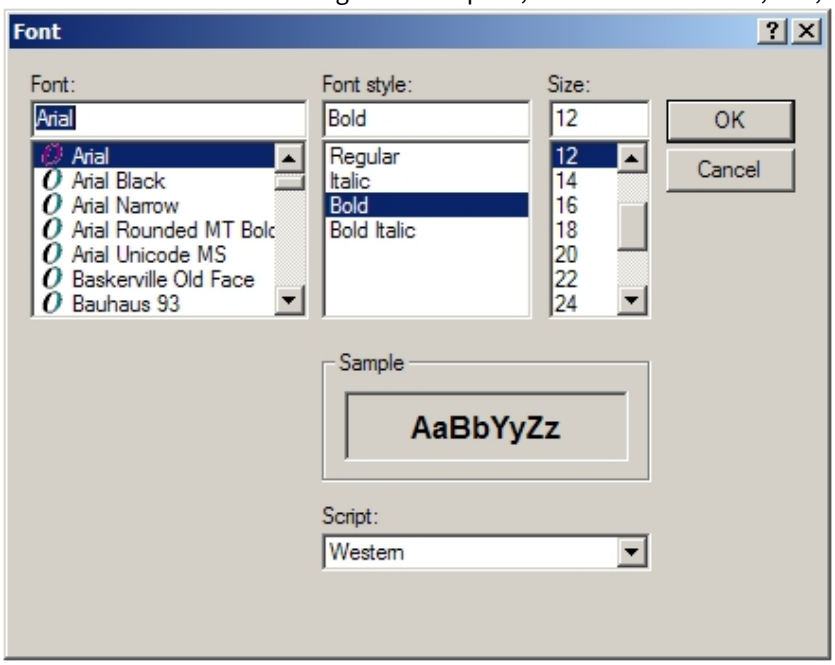
10.4.14.4 Configuring the interface parameters of the State statistics window

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**).

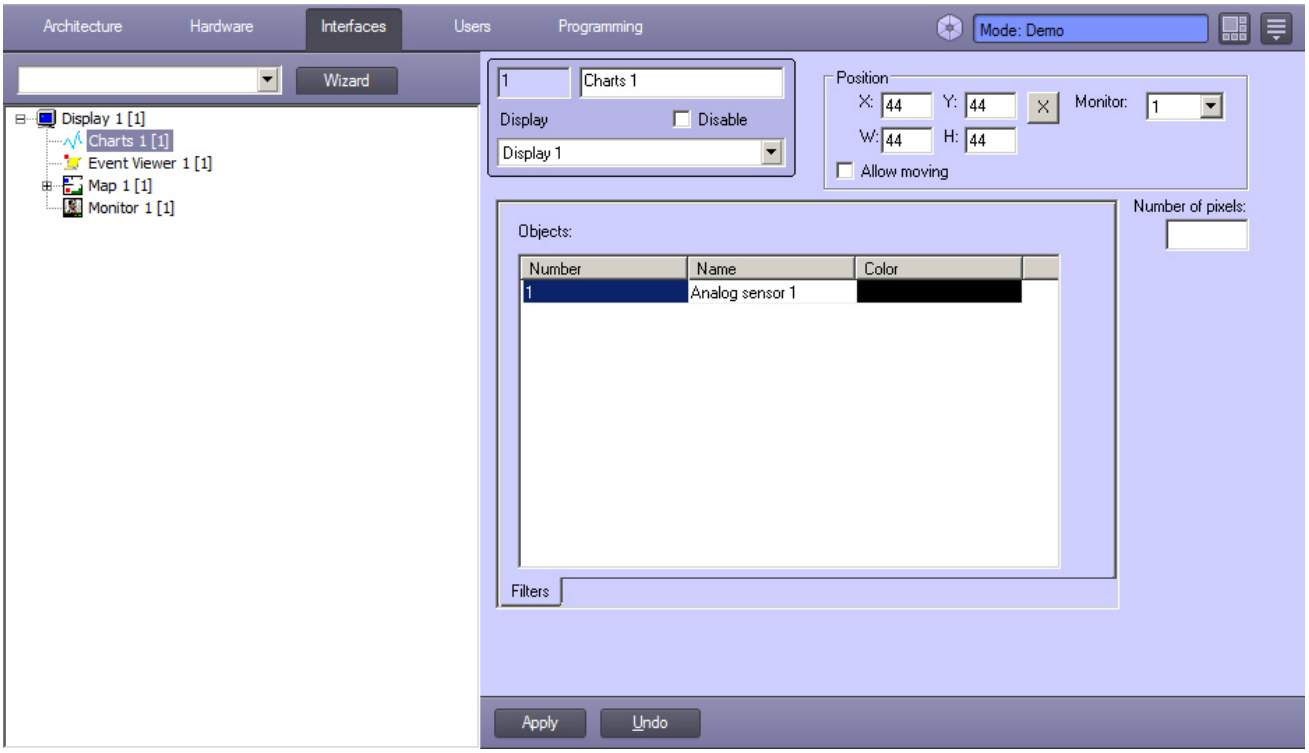
Configuring the interface parameters of the **State statistics** window is complete.

10.4.15 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.



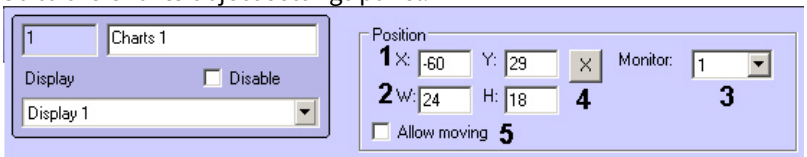
The analog sensor readings chart is configured in the following order:

1. Setting the Charts window position on the screen.
2. Selecting objects to display on chart and setting the number of points.

10.4.15.1 Setting the Charts window position on the screen

Set the **Charts** window position on the screen as follows:

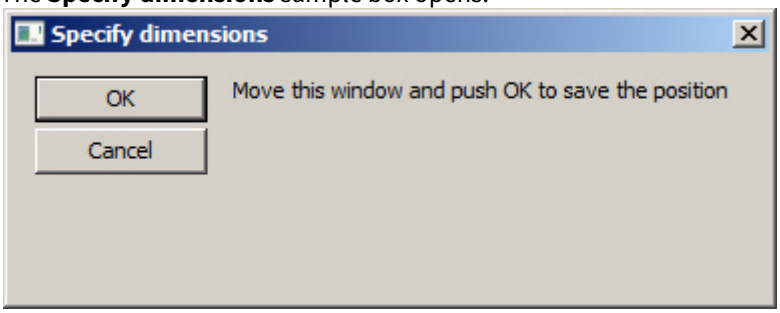
1. Go to the **Charts** object settings panel.



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.

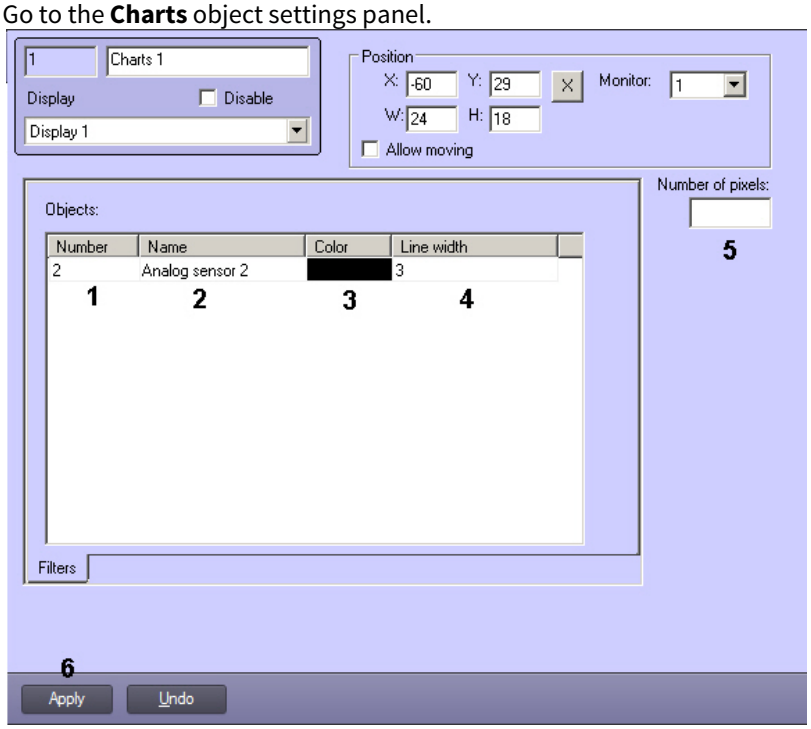
3. If an Operator should be able to move the **Charts** window on the screen, set the **Allow moving** checkbox (5).
4. Click **Apply** to save settings.

Setting the **Charts** window position on the screen is now complete.

10.4.15.2 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).

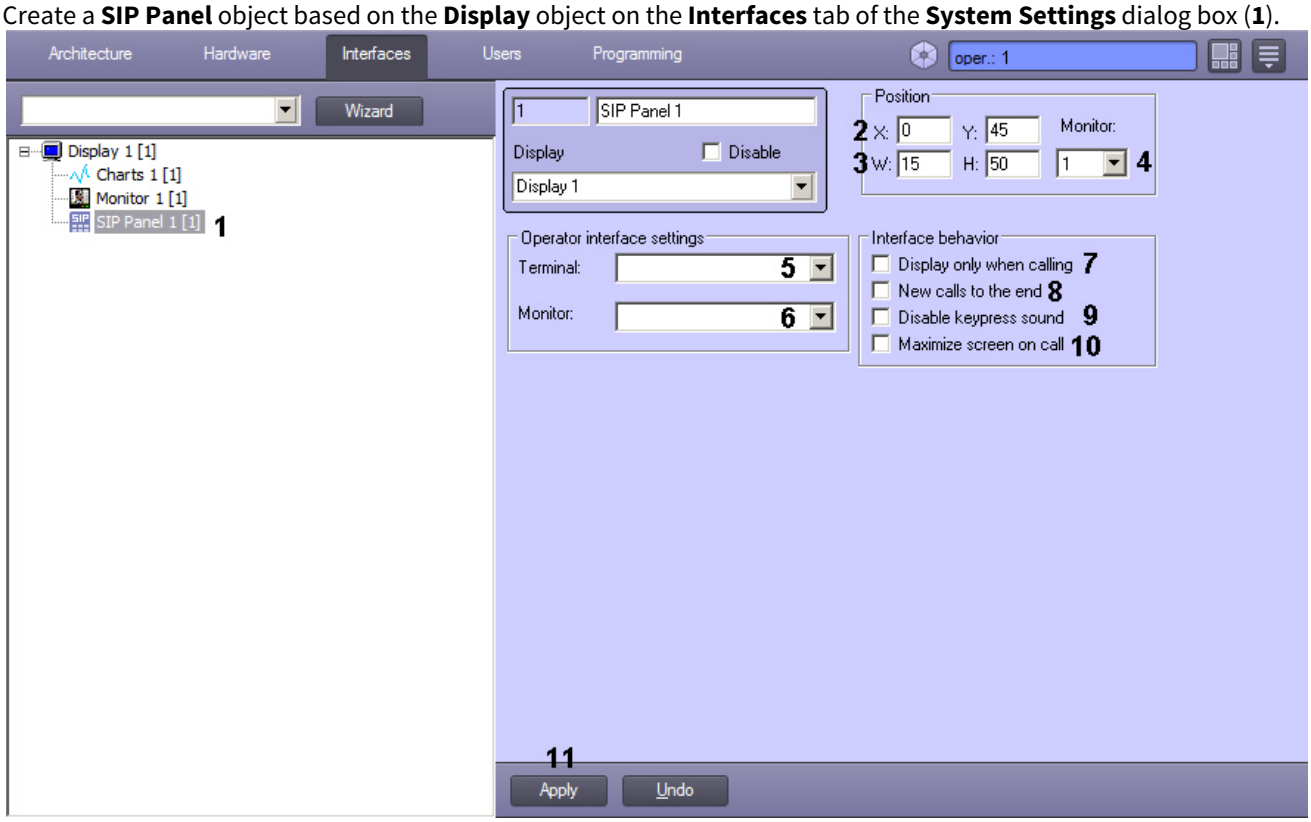
Selecting objects to display on the chart and setting the number of points is now complete.

10.4.16 Configuring the SIP Panel interface object

The **SIP Panel** interface object is used to work with SIP-devices in *Intellect*. For details about configuring these devices, see Configuring SIP-devices.

The **SIP Panel** is configured as follows:

1. Create a **SIP Panel** object based on the **Display** object on the **Interfaces** tab of the **System Settings** dialog box (**1**).



2. Set the coordinates of the upper left corner of the interface window in the **X** and **Y** fields (**2**).
3. Set the width and height of the interface window in the **W** and **H** fields (**3**).
4. From the **Monitor** drop-down list (**4**), select the computer monitor on which the interface window will be displayed.
5. From the **Terminal** drop-down list (**5**), select the SIP-terminal object which SIP-devices use the **SIP Panel**.
6. 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.
7. If it is necessary to display the **SIP Panel** only during a call, set the **Display only when calling** checkbox (**7**).
8. If new calls should be added to the end of the list on the SIP panel, select the **New calls to end** check box (**8**). By default, new calls are added to the top of the list.
9. To turn off sound when pressing keys on the SIP panel, select the **Mute keypress sound** check box (**9**).
10. To show the Display with the SIP panel when making a call, set the **Maximize screen on call** check box (**10**). If this check box is not set, there is a chance to miss a call to the SIP panel when the corresponding Display is hidden.
11. Click **Apply** (**11**).

> **Note.**
>
> 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

The **SIP Panel** is configured.

SIP panel

10.5 Configuration of users and permissions

10.5.1 Rights administration

10.5.1.1 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.

10.5.1.2 User registration and removal

10.5.1.2.1 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.

10.5.1.2.2 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.

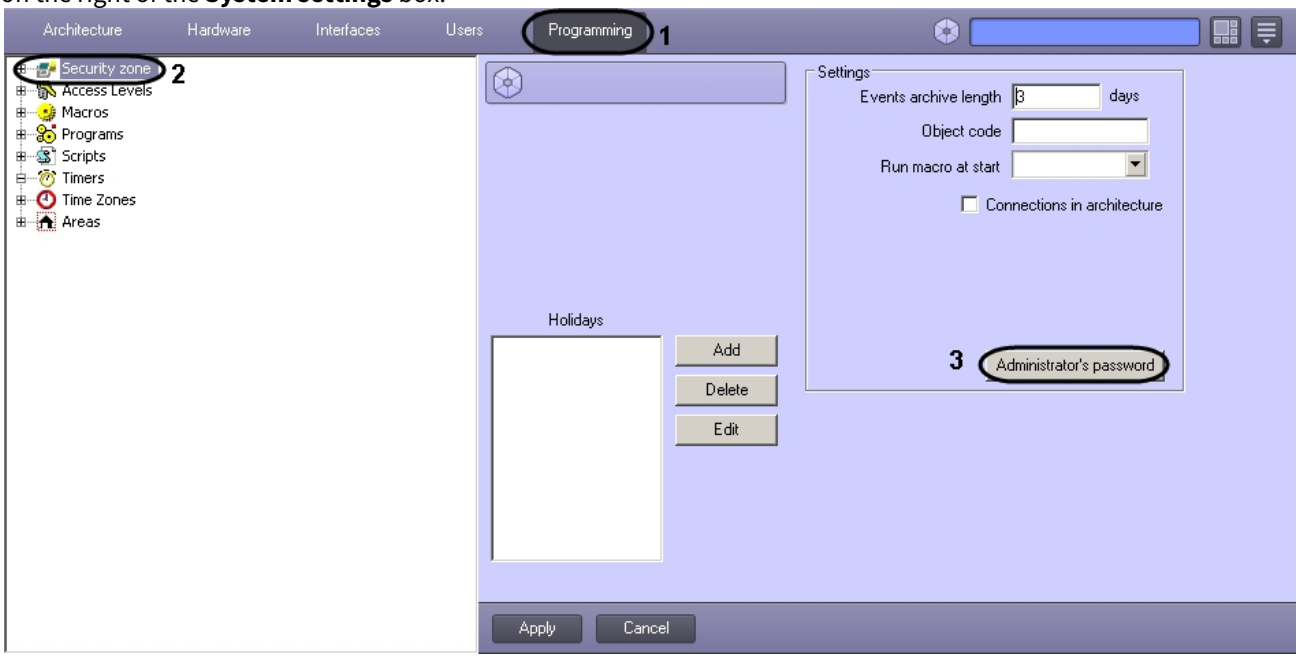
3. Registering operators by creating the **User** objects.

10.5.1.2.3 Administrator password registration

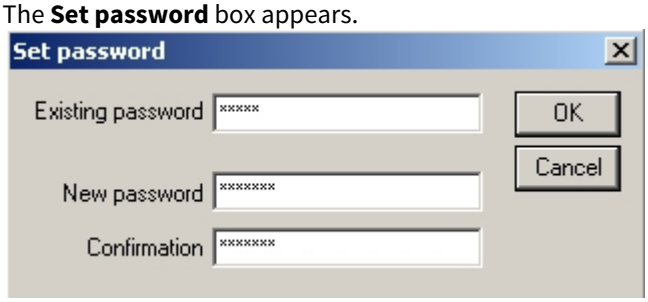
The administrator password gives access to administrative functions of all system components. Only one administrator password can be registered in the system. The administrator password is to be registered on the administration server when the system is configured.

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.



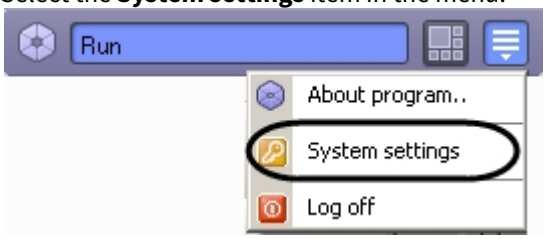
5. Specify the existing administrator's password in the **Existing password** field. If there is no administrator's password, this field is left empty
6. Type-in the sequence of letters and figures, that will be used as administrator's password in the **New password** field.
7. Retype-in the new administrator's 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 (8).

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.



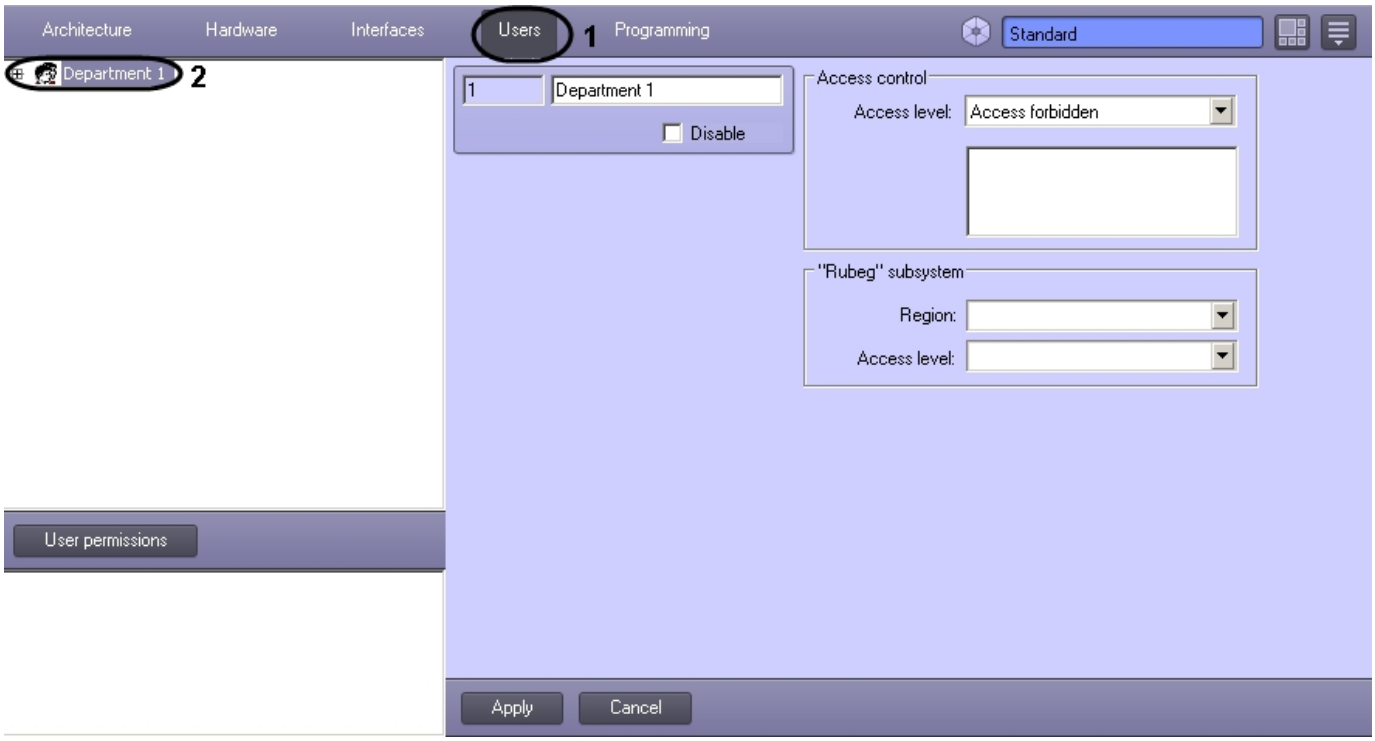
10.5.1.2.4 Department registration

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.

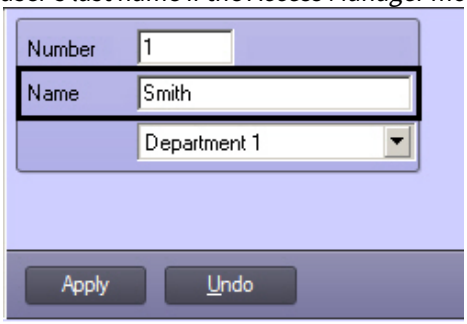
> **Note.**
>
> Settings on the settings panel of the **Department** object are used to configure the access control system (see Visitor Management System Module Settings and Operation Guide).

10.5.1.2.5 Registration of Operator accounts

To register Operator accounts, the **User** objects are to be created.

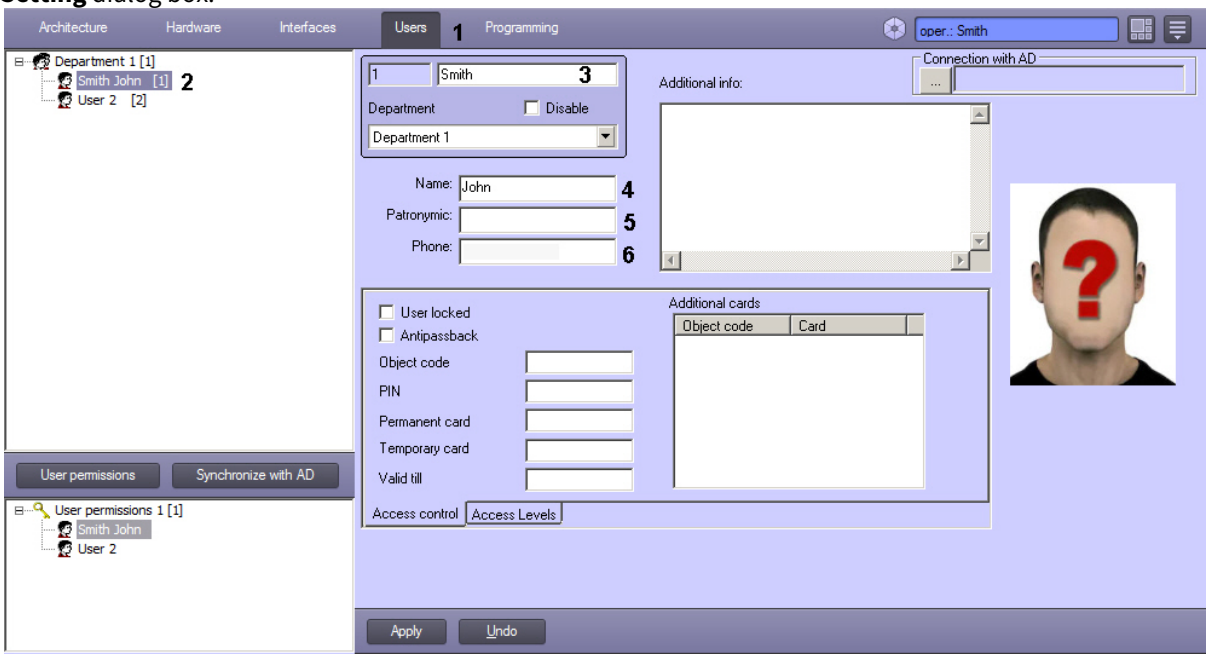
An individual account is to be created for each Operator. To register an Operator account, do the following:

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.

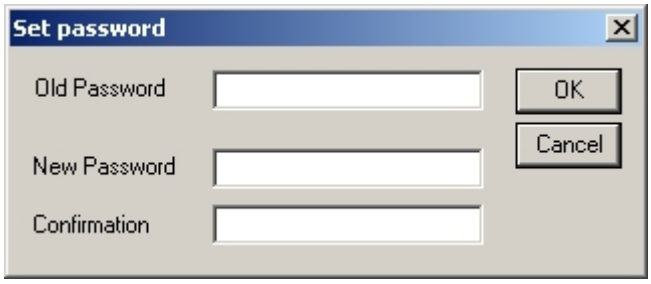
Face recognition and search interface being part of *Face-Intellect* software also allows adding and editing user's photo (see *Face-Intellect* documentation in AxxonSoft documentation repository for details on its setting up and configuration).

10.5.1.2.6 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. To remove the administrator password, specify the current Administrator password in the **Old Password** field and then clear the **New Password** and **Confirmation** fields in the **Set Password** box.

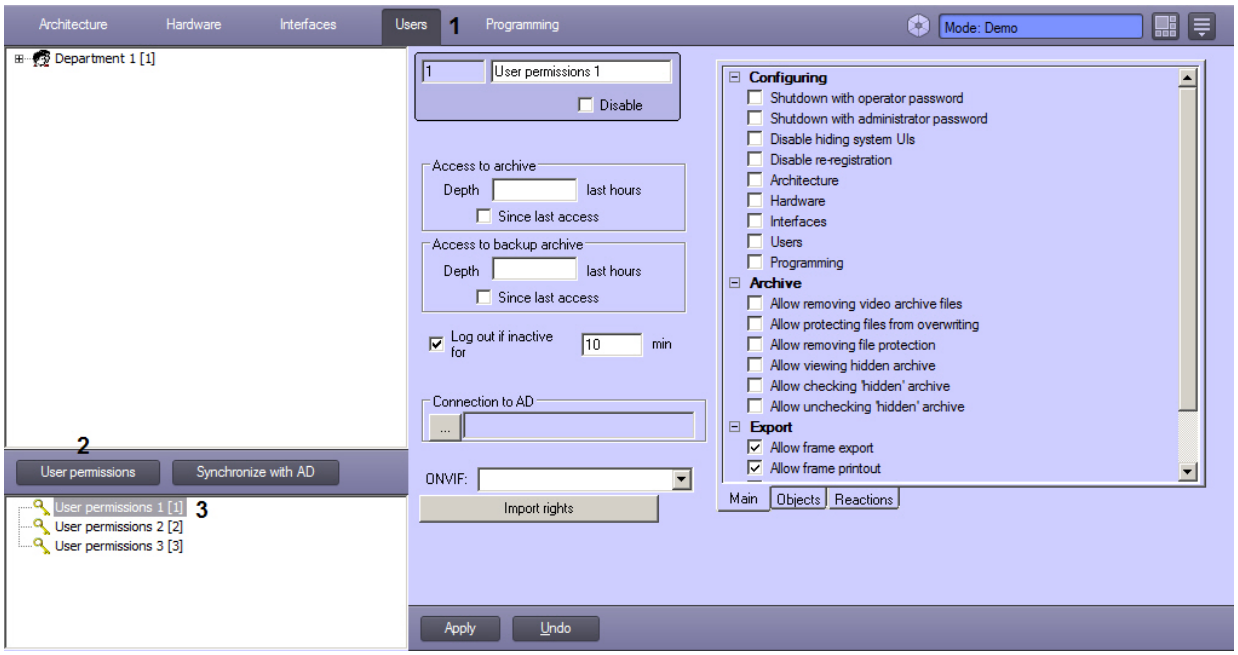


10.5.1.3 Registration of users' rights

10.5.1.3.1 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.
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.

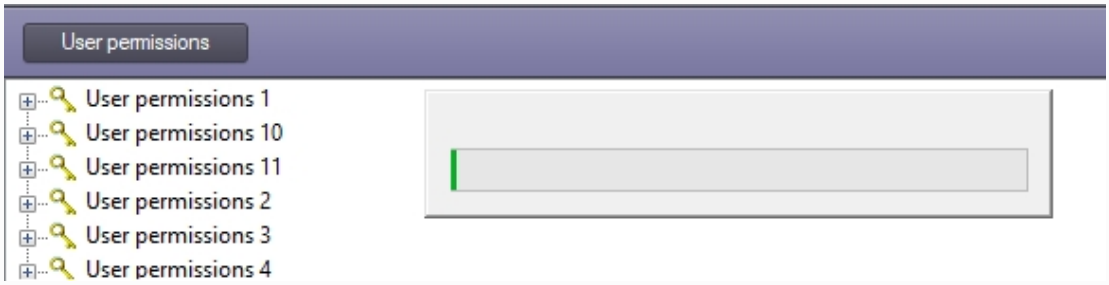


If at least one registered rights object exists, which is shown in the objects tree below the **User permissions** button, the new rights object can be created from the context menu of the existing object.

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.

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.

10.5.1.3.2 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.

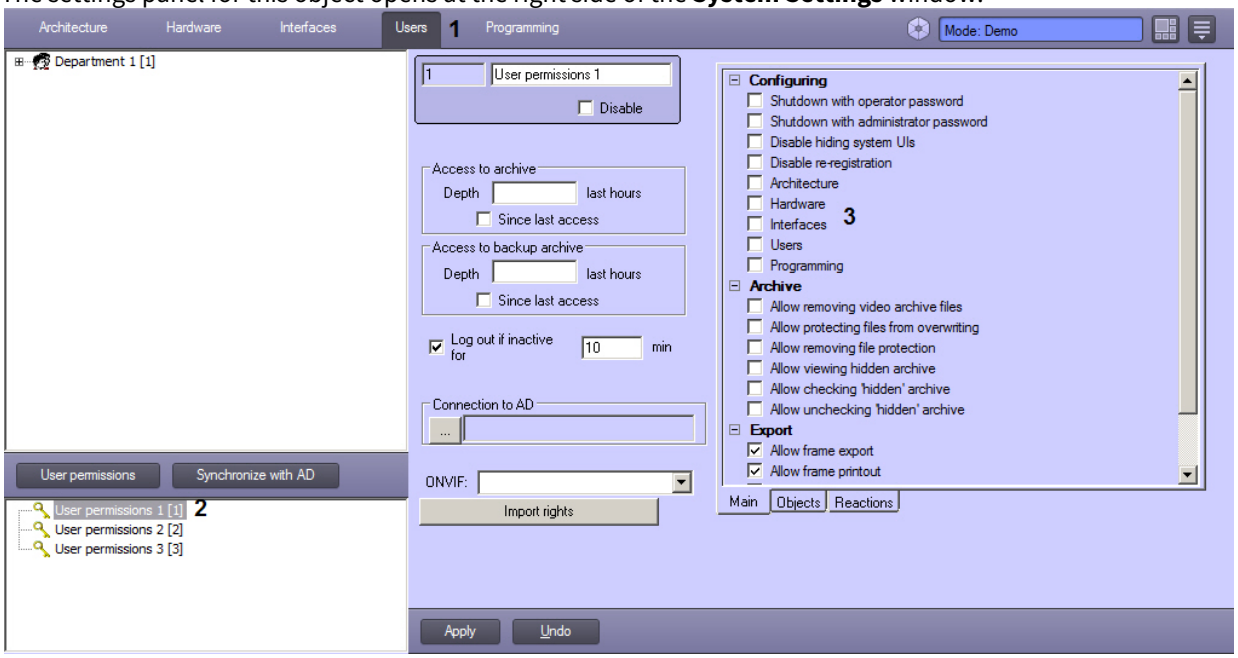
10.5.1.3.3 Limiting access to the tabs of the System Settings window

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.
2. Open the required **User permissions** object in the objects tree under the **User permissions** button.
3. The settings panel for this object opens at the right side of the **System Settings** window.



   The first 5 checkboxes of the **Configuring** group correspond to the tabs of the **System Settings** window. Check the checkboxes for the tabs that the operator will be allowed to access.
4. Press the **Apply** button.

This completes the setup of the operator access to the **System Settings** tabs.

10.5.1.3.4 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, he (she) automatically receives the rights to administer, control and view all system objects on these tabs.

When the operator has the rights for control functions, he (she) 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)).

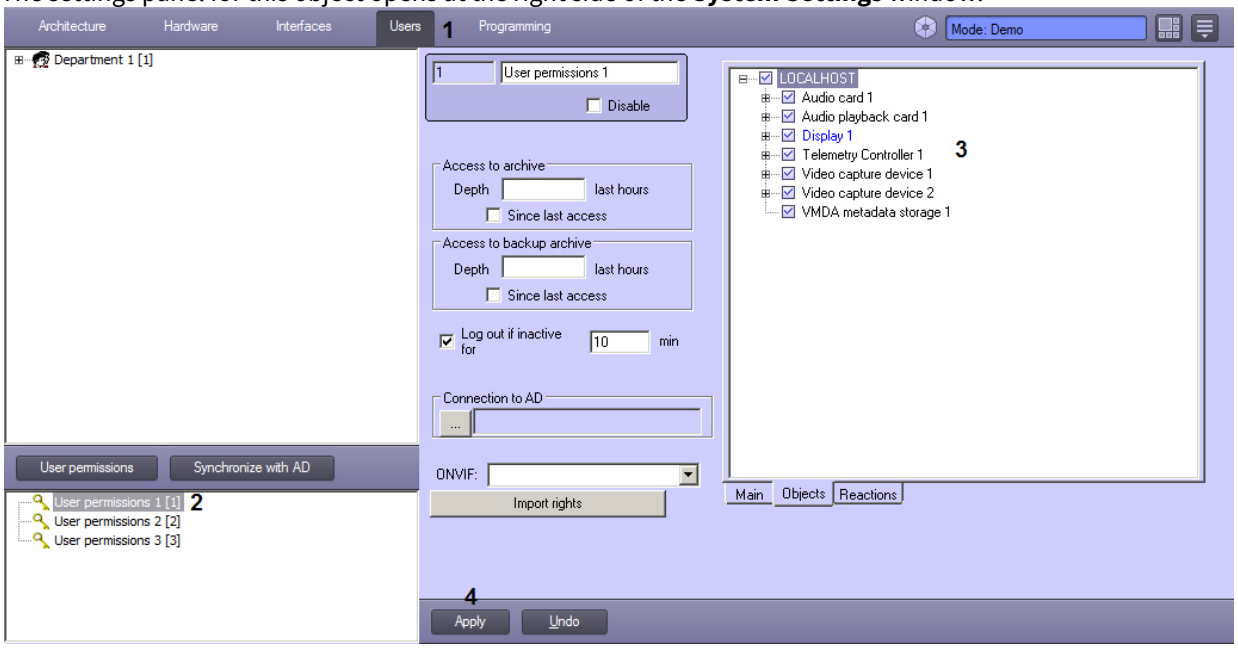
Viewing functions allow the operator to view the interface components (user screens, surveillance monitors, Backup archive window, microphone indicators, etc.).

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 ban 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 configuraion rights will not be available.

To limit operator access to the administration of certain objects of Intellect program software 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 at the right side of the **System Settings** window.



The tree in the lower part of the settings panel represent the rights of the current operator. Checkboxes to the left of the objects indicate and allow changing the administrative, control or viewing rights for these objects. The components of the tree represent the system objects which the current user can administer according to his (her) rights' settings. Name of marks corresponds to object names, which administration, control and monitoring may be accessible to Operator with proper rights (**3**).

Correspondence of mark type to Operator rights is given in the table.

Type of mark	Right to administer	Right to control the object	Right to monitor 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

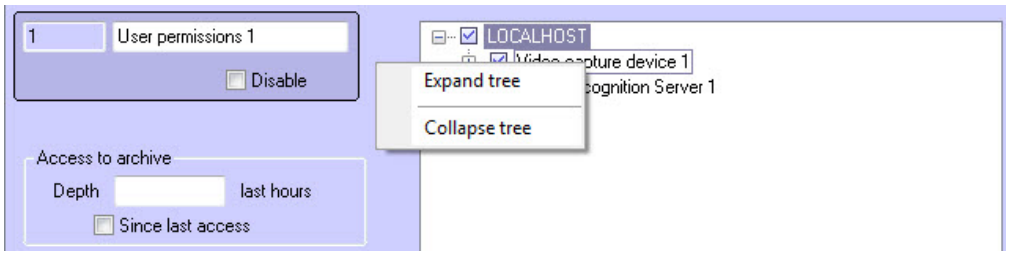
The following hotkeys can be used for objects tree control:

Key	Function
"+" on the numeric keypad	Grants all rights to the selected objects (sets the gray mark)

"-" on the numeric keypad	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.
"/" on the numeric keypad	Fully collapse the selected branch of the objects tree
"*" on the numeric keypad	Fully expand the selected branch of the objects tree
"Shift"+"/" on the numeric keypad	Fully collapse all branches of the objects tree. This view will be saved for the current user even after the *Intellect* restart.
"Shift"+"*" on the numeric keypad	Fully expand all branches of the objects tree. This view will be saved for the current user even after the *Intellect* restart.

Note

Expanding and collapsing the tree functions are also available when you right-click on an object in the object tree (see Expanding the tree and Collapsing the tree).



3. After finishing the setting, click **Apply** (**4**).

Setting up the administration of the system objects, control and viewing functions is completed.

10.5.1.3.5 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. An operator cannot shut the system down.

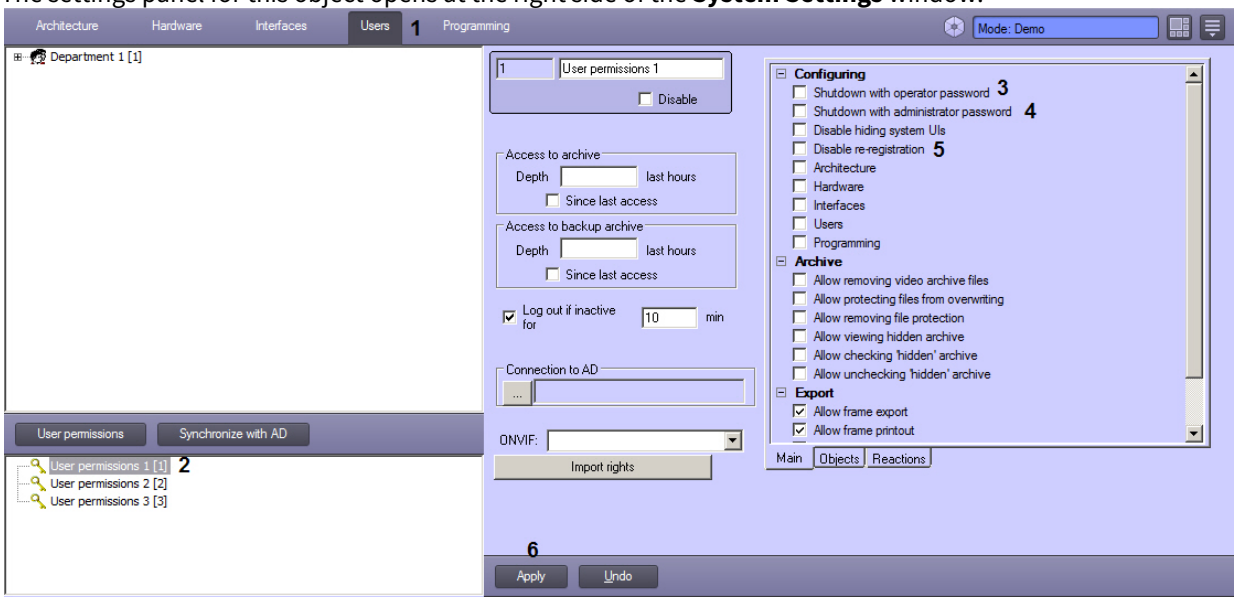
If the operator is forbidden from shutting the system down, the **Run** menu of the **Main Control Panel** does not contain the **Shut Down** option. This menu item appears only after opening the administrator password window and entering the valid administrator password. To shut the system down, the 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.

2. Open the required **User permissions** object in the objects tree under the **User permissions** button.
   The settings panel for this object opens at the right side of the **System Settings** window.



3. To enable system shutdown by the current operator's password only, check the **Shutdown with operator password** checkbox.
4. To enable system shutdown by the administrator password only, check the **Shutdown with administrator password** checkbox.
5. To forbid the current operator from shutting the system down, check the **Shutdown with administrator password** and the **Disable re-registration** checkboxes.
6. To revert to the default shutdown option, deselect all the related checkboxes: **Shutdown with operator password**, **Shutdown with administrator password**, **Disable re-registration**.
7. Press the **Apply** button.

This completes the setup of the system shutdown options.

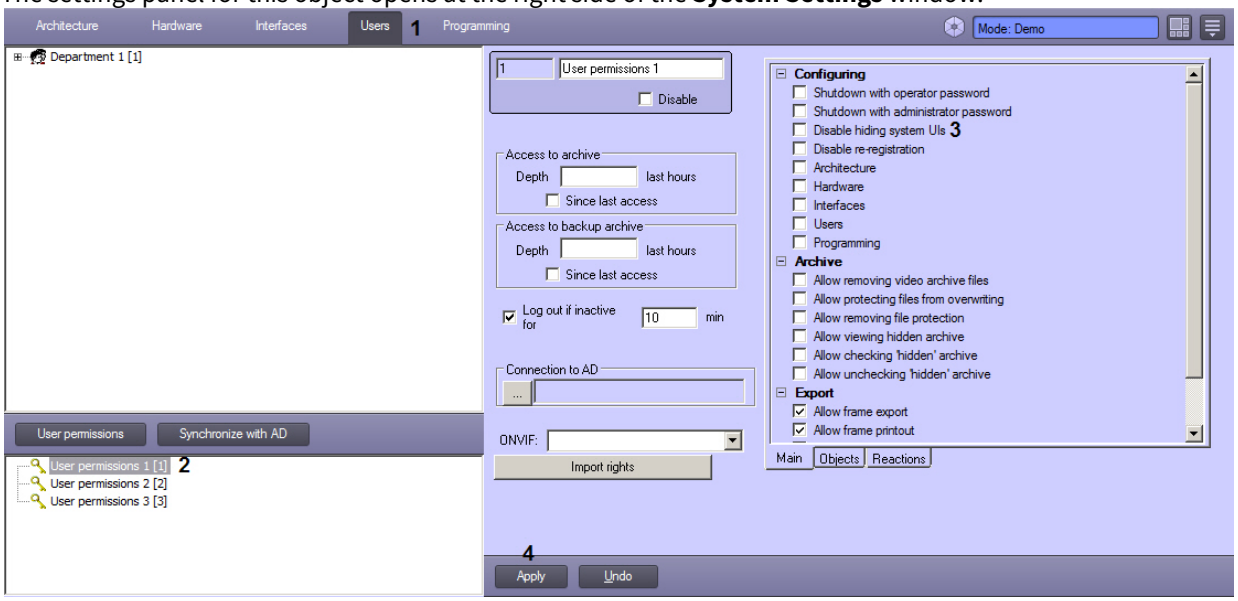
10.5.1.3.6 Limiting the rights to hide the interface components

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.

2. Open the required **User permissions** object in the objects tree under the **User permissions** button.
   The settings panel for this object opens at the right side of the **System Settings** window.



3. Check the **Disable hiding system UIs** checkbox.
4. Press the **Apply** button.

This completes the process of forbidding the hiding of all interface components.

10.5.1.3.7 Permissions for working with archives

The operator can be forbidden to play the video recordings (from the videoserver, Backup archive or Archiver) in the surveillance monitor.

In this case, the button for entering the archive on the surveillance monitor will not be displayed, and the functions for viewing, exporting and frame printing will be unavailable.

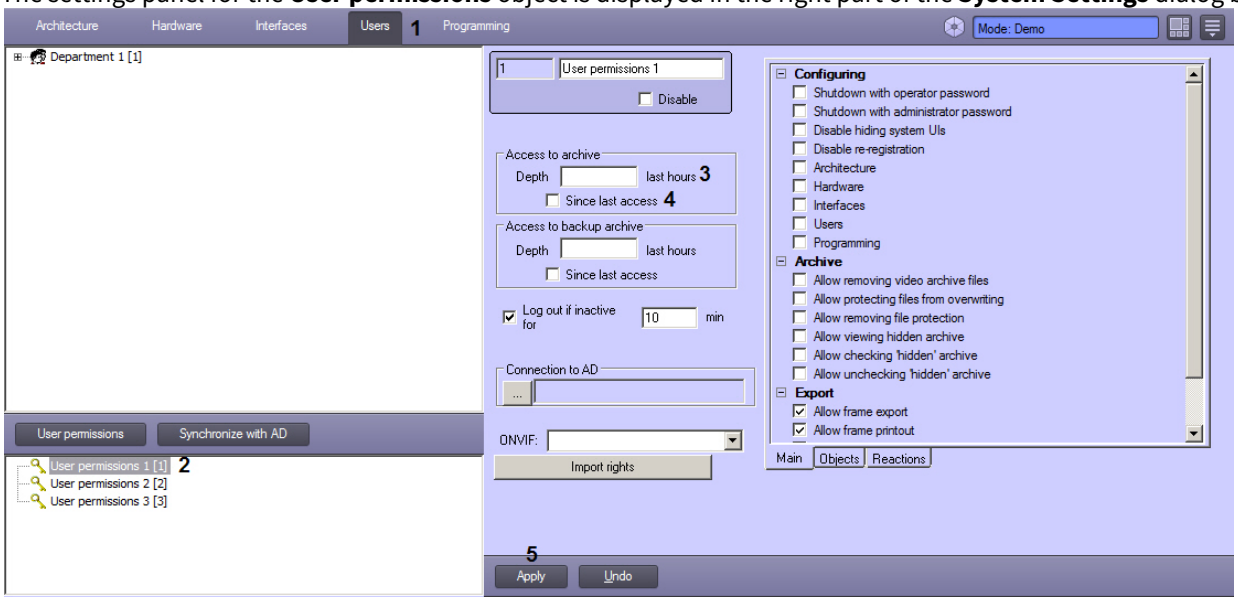
By default, the operators are allowed to play the archives.

10.5.1.3.7.1 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 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 is to be whole.

> **Note.**
>
> Input the 0 value in the **Depth ___ last hours** field todisable 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 the **Since last access** box unchecked.

> **Note.**
>
> If the **Since last access** box is checked and the number of hours for viewing is specified, then last hours are counted till the registration moment.

> **Note.**
>
> If the **Since last access** box is checked, 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).

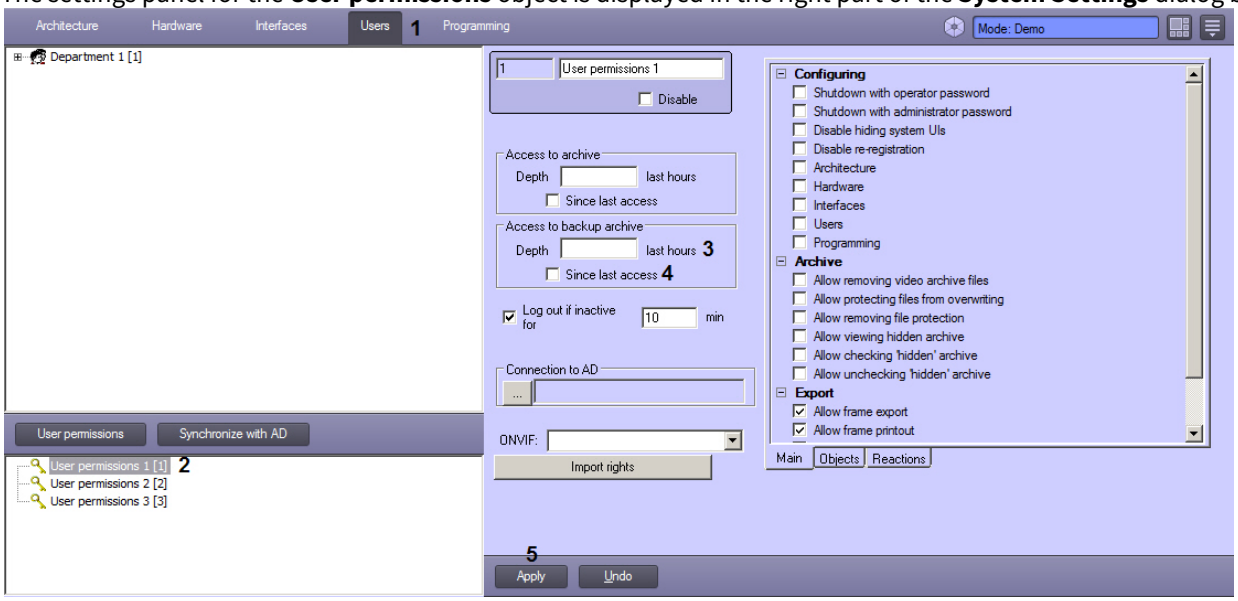
The access to archive playback is now limited.

10.5.1.3.7.2 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 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 is to 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 the **Since last access** box unchecked.

> **Note.**
>
> If the **Since last access** box is checked and the number of hours for viewing is specified, then last hours are counted till the registration moment.

> **Note.**
>
> If the **Since last access** box is checked, 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.

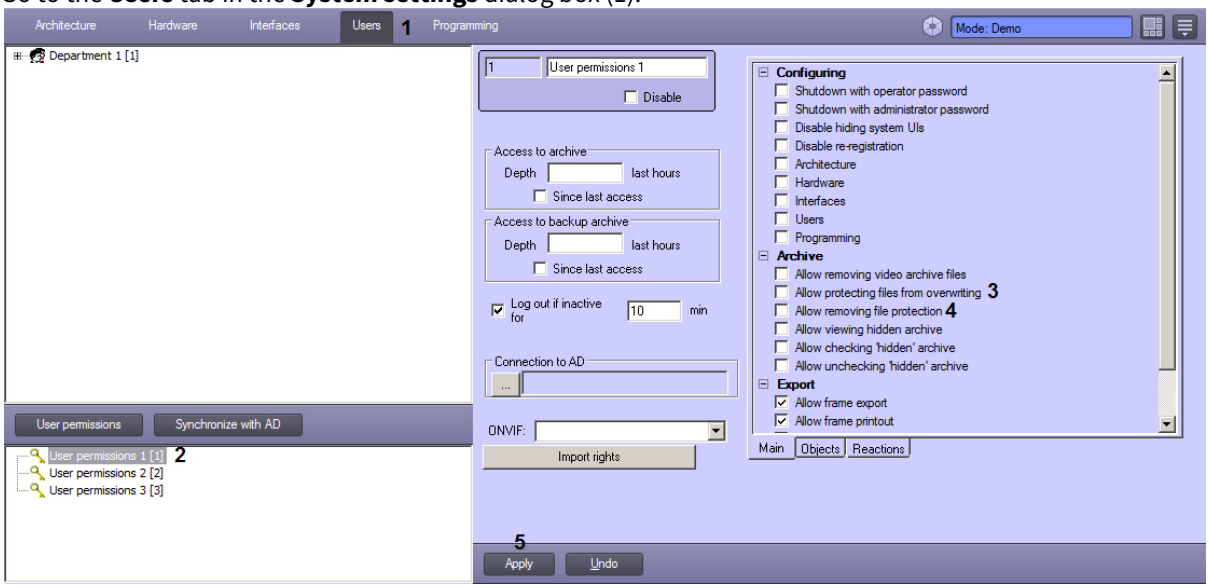
10.5.1.3.7.3 Permission protecting archive files from rewriting

Recording to archive is performed on a loop in the *Intellect* software package (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 are to 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 Operator to protect archive files from rewriting, set the **Allow rewrite protection** checkbox checked (3). Don't set this checkbox checked if the operator should not have this permission.
5. To allow Operator to disable protection of files protected from rewriting set the **Allow to disable file protection** checkbox checked (4). Don't set this checkbox checked if the operator should not have this permission.
6. To allow Operator to export protected files, set the **Allow export** checkbox checked (5). Don't set this checkbox if the operator should not have this permission.
7. Click the **Apply** button.

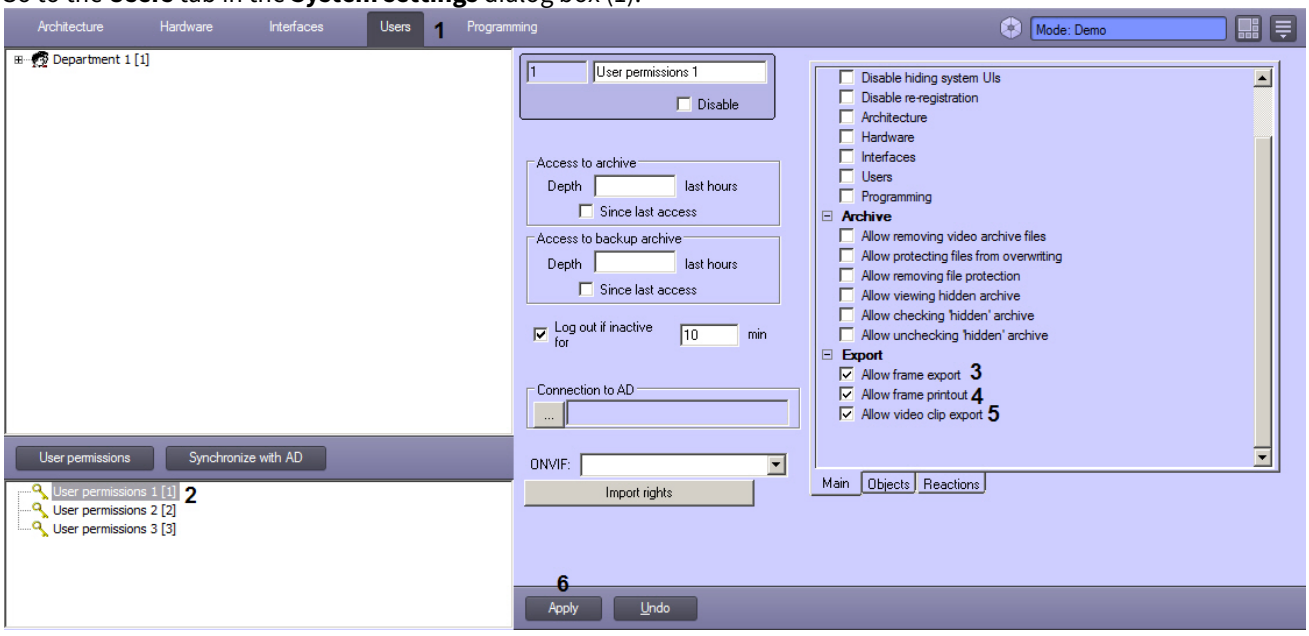
Permissions for the Operator to protect archive files from rewriting are now set.

10.5.1.3.7.4 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 are to 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 unchecked (3).
5. In order to forbid the Operator to print archive frames, set the **Allow frame printout** checkbox unchecked (4).
6. In order to forbid the Operator to export archive clips, set the **Allow video clip export** checkbox unchecked (5).
7. Click the **Apply** button (6).

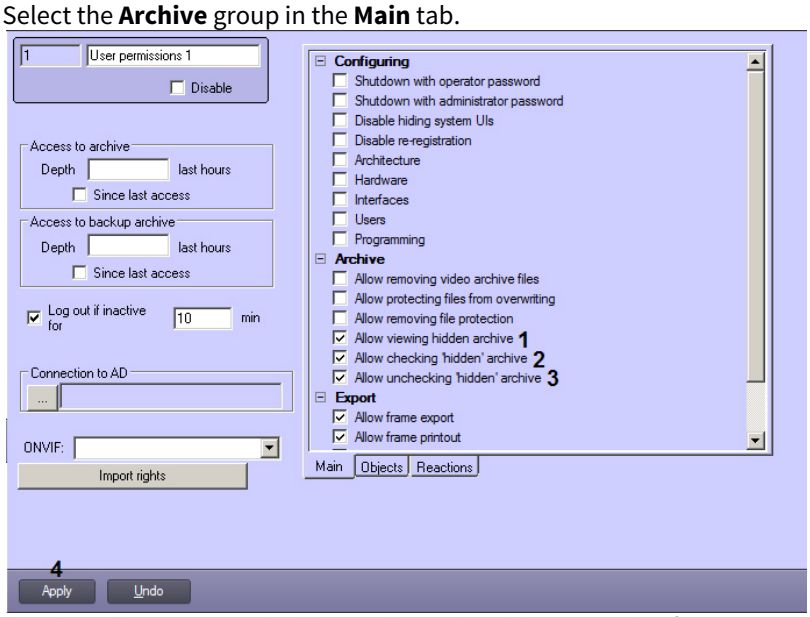
Export and printout permissions are now set.

10.5.1.3.7.5 Permissions to the hidden archive

The hidden archive is not shown 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 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** check box in order for an Operator with these rights to be able to view a hidden archive (1).
4. Set the **Allow checking "hidden" archive** check box in order for the Operator to be able to hide archive entries (2).
5. Set the **Allow unchecking "hidden" archive** check box in order for the Operator to be able to unhide archive entries (3).
6. Click **Apply** (4).

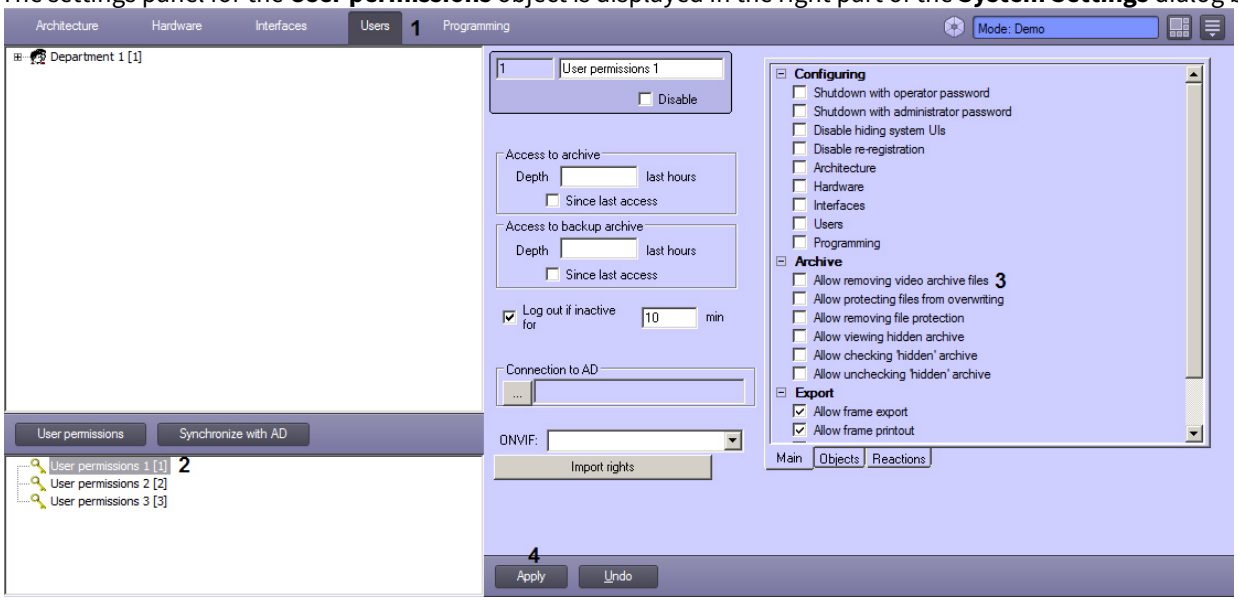
Restriction of rights to hide the archive is completed.

10.5.1.3.7.6 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 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 an Operator remove video archive files, set the **Allow to remove video archive files** checkbox (3). If the Operator is not allowed to remove video archive files, leave this box unchecked.
4. To save the changes in INTELLECT ™ software, click the **Apply** button (4).

An Operator now can remove video archive files.

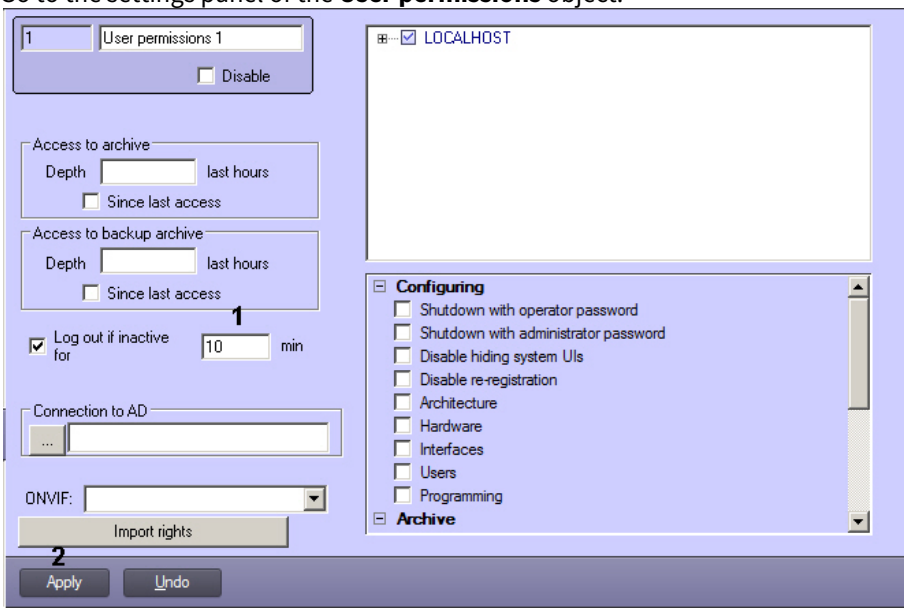
> **Note.**
>
> Video recordings are deleted as follows:
>
> 1. From the Video surveillance monitor interface – see Deleting video recordings from the archive section of Operator's Guide.
> 2. Using ARCH_DEL_RECORD reaction of the CAM object that is executed using the script or program – see *CAM* section of *Programming Guide* (not available in English).

10.5.1.3.8 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 __ minutes** (1) checkbox checked 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.

10.5.1.3.9 Configuring rights to use ONVIF Server

If ONVIF Server module is in use, the user rights can be configured to connect to it.

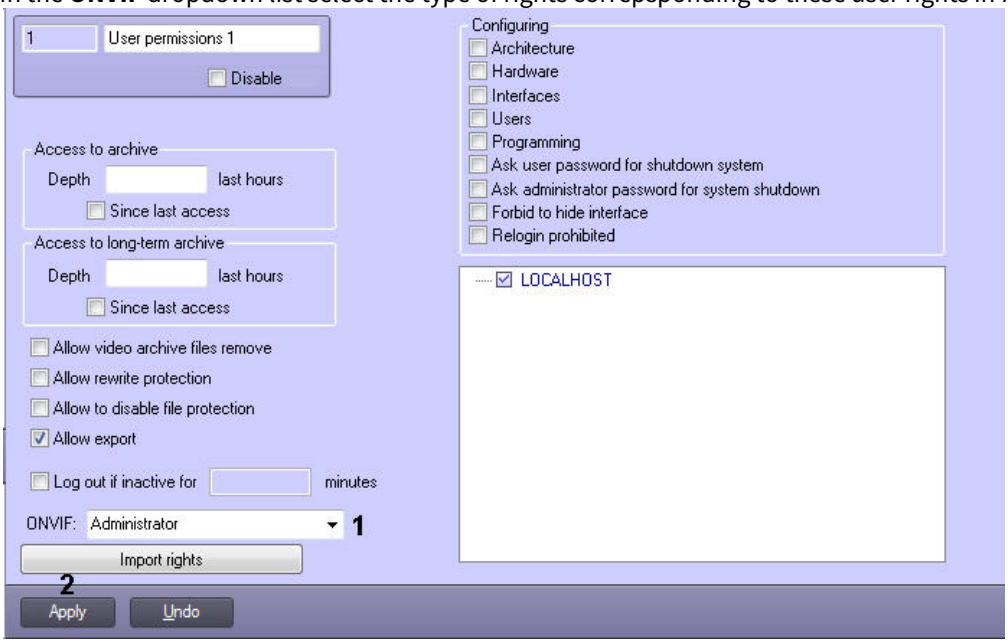
There are 4 types of rights in ONVIF specififcation: Administrator, Operator, User and Anonymous. Users with Anonymous rights can get data via ONVIF Server without authentication. Fo the rest three types the correspondence between user rights in *Intellect* and user rights in ONVIF Core specififcation is to be configured.

> **Note**
>
> Find details about types of rights in ONVIF Core specififcation 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 correpsponding to these user rights in *Intellect* (1).



3. Click the **Apply** button (2).
Intellect rights to use ONVIF Server are now configured.

10.5.1.3.10 Combining (importing) permissions

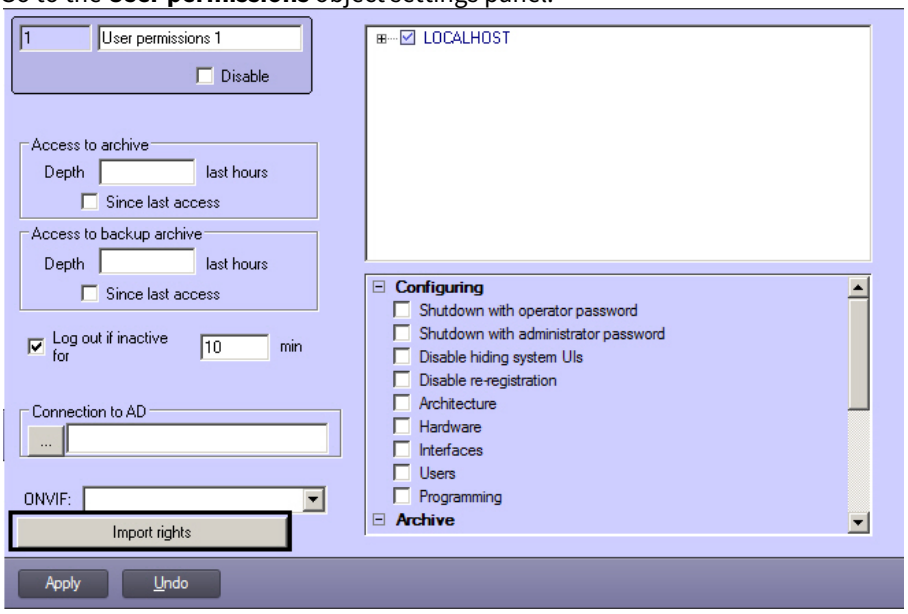
Intellect software allows several users' rights to be combined into a newly created **User permissions** object. While the copy-paste function (Ctrl+C - Ctrl+V) just copies all users' rights parameters, the function of permissions combining unites several users' permissions into the configured object.

The following rules are applied for combining process:

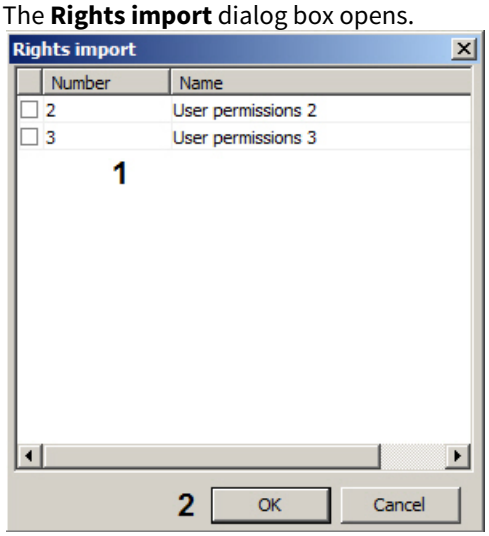
1. The permissions set by template rights are added, i.e. if an action is prohibited in one of the rights, but is permitted in the other, then the action is allowed in the new rights as a result of their combination.
2. The rights for the administration, control and viewing functions are set to the maximum 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 **Import rights.**
3. The **Rights import** dialog box opens.



4. Set checkboxes next to **User permissions** objects to combine (1).
5. Click **OK** (2). The results of combination are displayed on the object settings panel.
6. Click **Apply** to save changes.

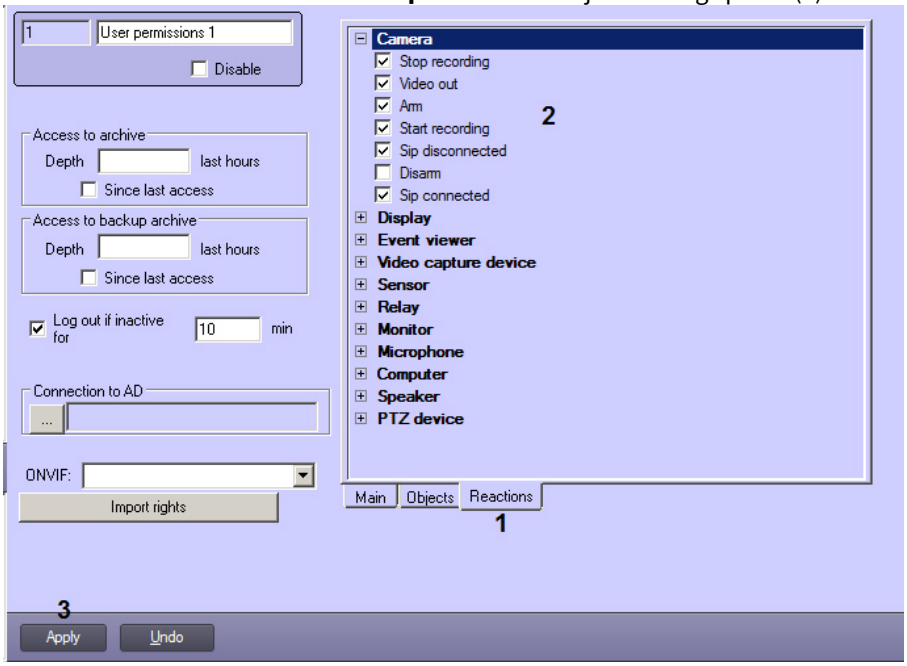
Combine several user rights is completed.

10.5.1.3.11 Limiting access to sending commands (reactions)

By default, *Intellect* software 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 checkboxes next to the reactions that are to be forbidden for the Operator (2).
3. Click **Apply** (3).

Setting limits to execution of selected commands is completed.

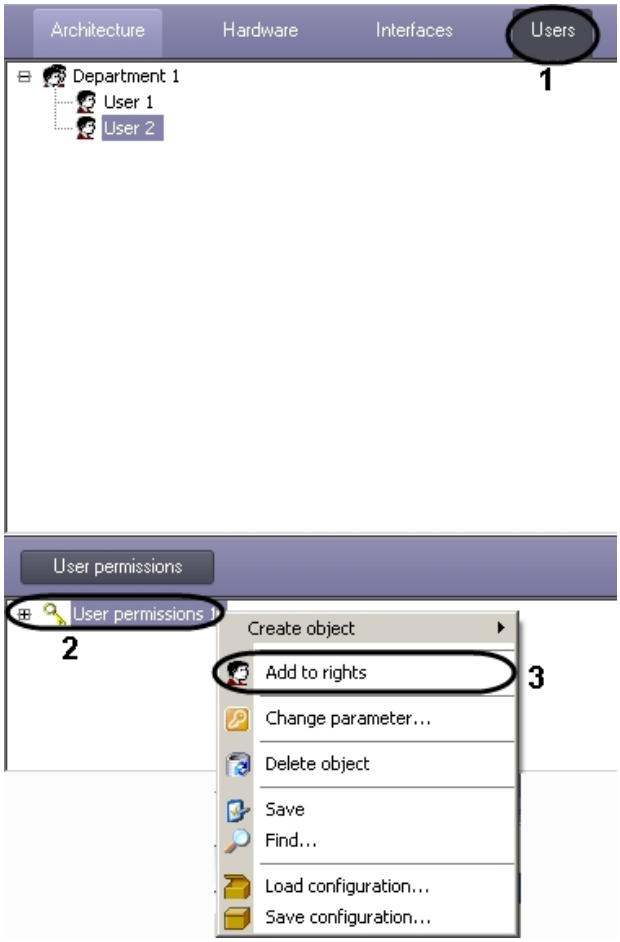
10.5.1.4 Assigning the rights and password to operators for authorization in the Intellect

User accounts are stored separately from operator accounts in INTELLECT™ software. The same rights may be assigned to several operators. But the operator may be assigned only single rights.

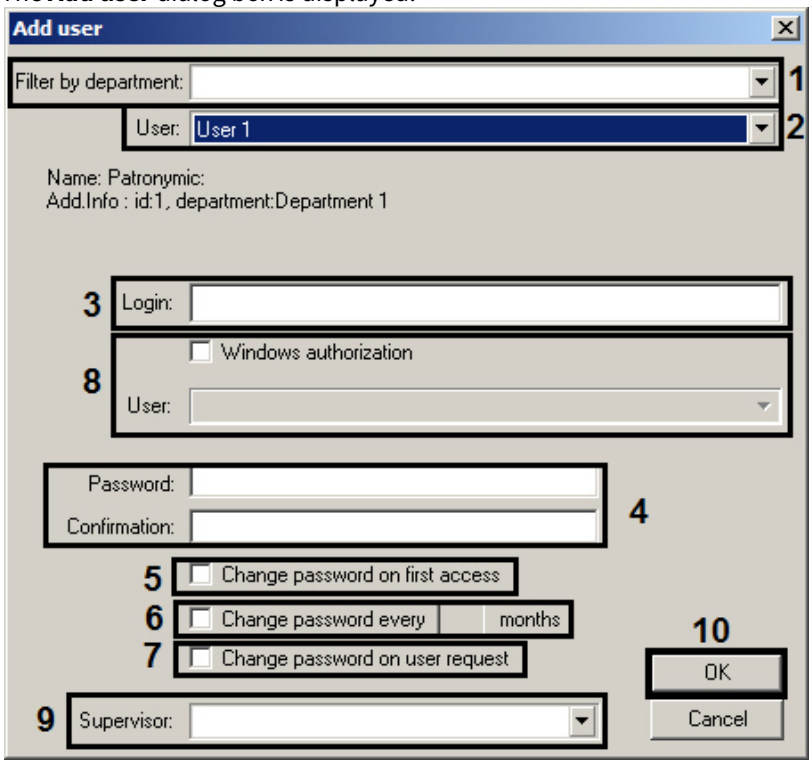
To assign the rights and password to the operator for authorization in INTELLECT™, do the following:

1. Go to the **Users** tab in the **System settings** dialog box (1).
2. Select an object, corresponding to the rights account that have 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** dropdown 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** dropdown list. If the department is not selected, then accounts of all users registered in the system will be displayed in the **User** dropdown 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 checked 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 log-in 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™.

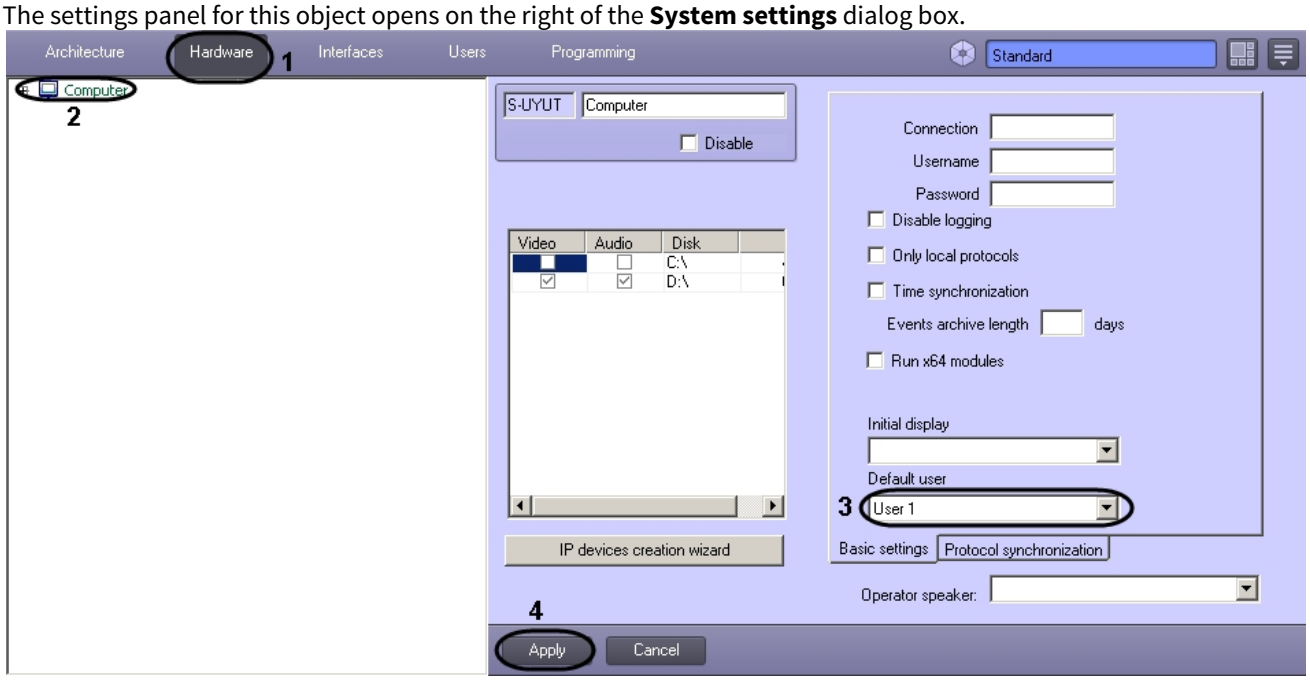
10.5.1.5 Setting up the default user

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 (4).

The administrative, controlling and viewing functions will then be limited according to the rights of the default user.

10.5.2 Configuration of the LDAP Service

10.5.2.1 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.

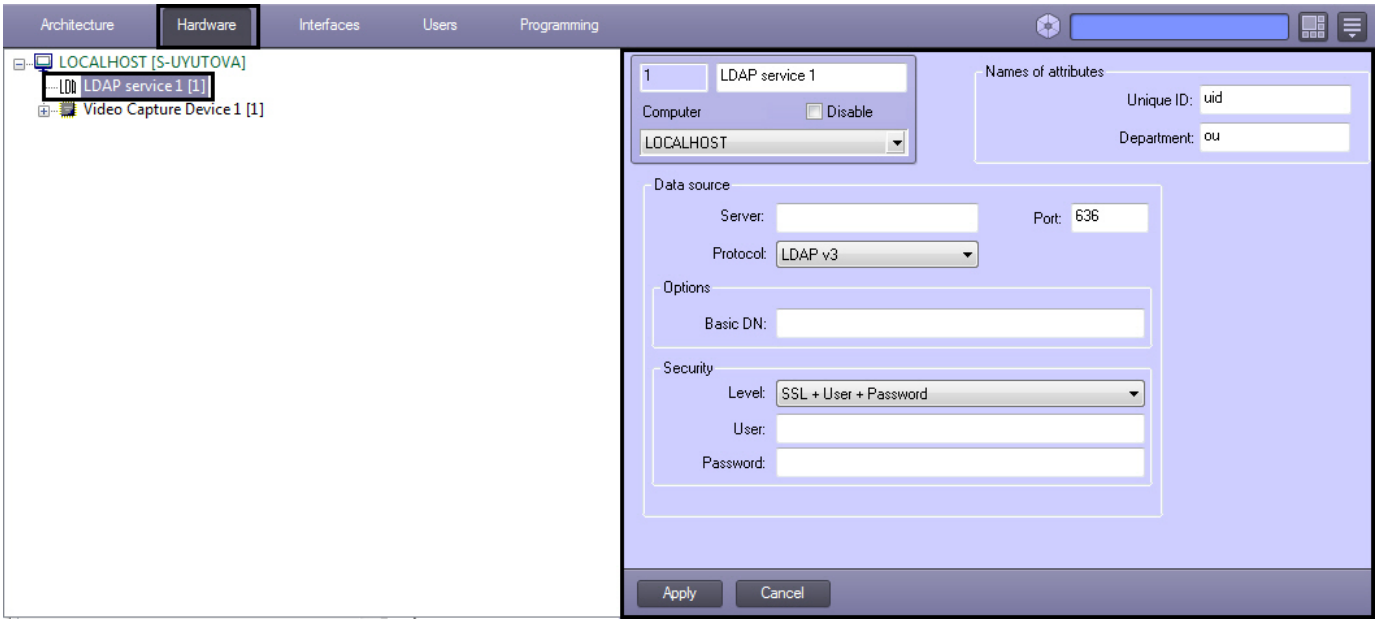
Importing data and synchronizing the *Intellect* database with an LDAP address book are accomplished using macros (the **LDAP Service** object's **Get all employees** action – see Example macro for user import from LDAP address book; see Creating and using macros for detailed information about macros). 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.

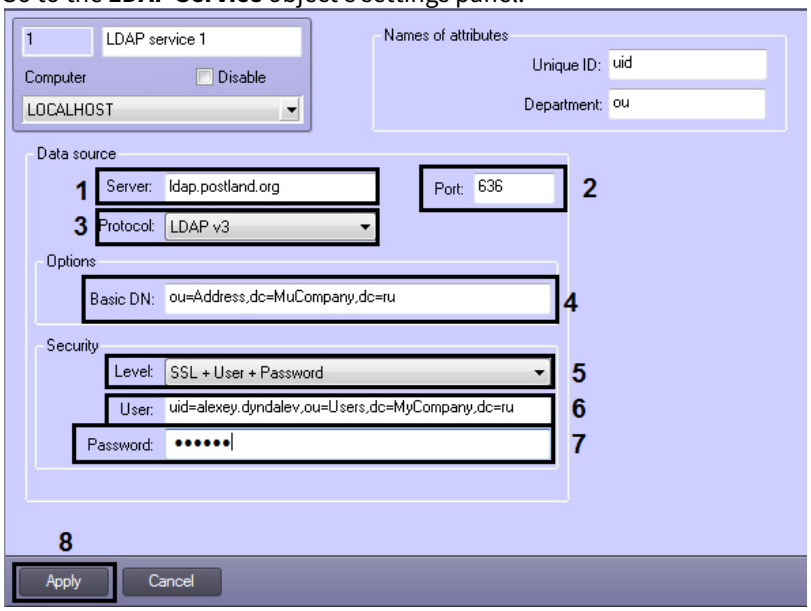
10.5.2.2 Configuring the connection to the LDAP address book

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. Select the connection security method being used by the LDAP server from the **Level** dropdown list (5).
7. In the **User** field specify the unique name of the user with rights to access the LDAP address book (6). *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

8. Enter the user's LDAP address book password in the **Password** field (7).

   Note.

   The username and password should not be entered if the selected connection security method does not require them.

9. To save the settings, click the **Apply** button (8).

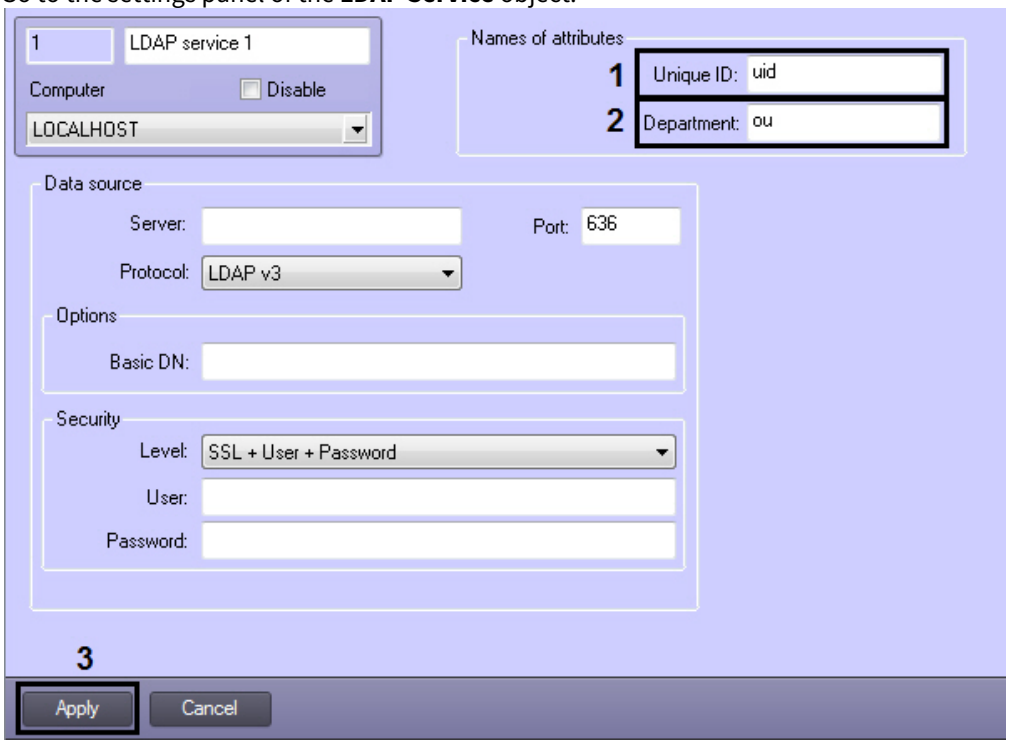
This completes the process of configuring the connection to an LDAP address book.

10.5.2.3 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.

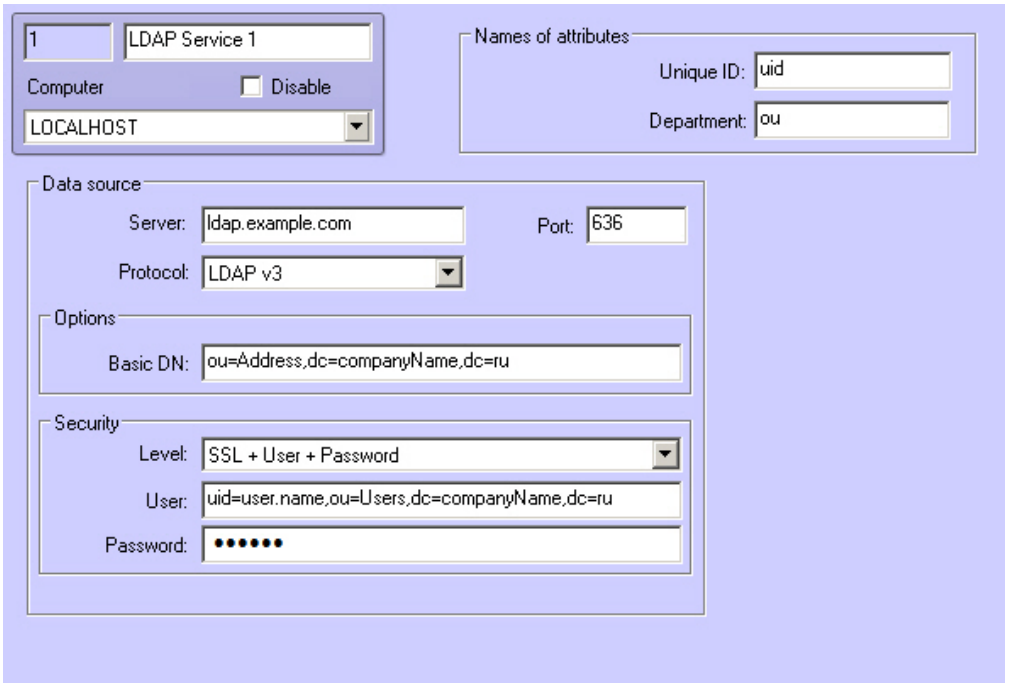


2. In the **Unique ID** field specify the attribute name that is a unique ID corresponding to external_id parameter of the **User** object in *Intellect* (1).
3. In the **Department** field specify the attribute name that is the name of the department and corresponding to the name field of the **Department** object in *Intellect* (2).
4. To save the changes click the **Apply** button (3).

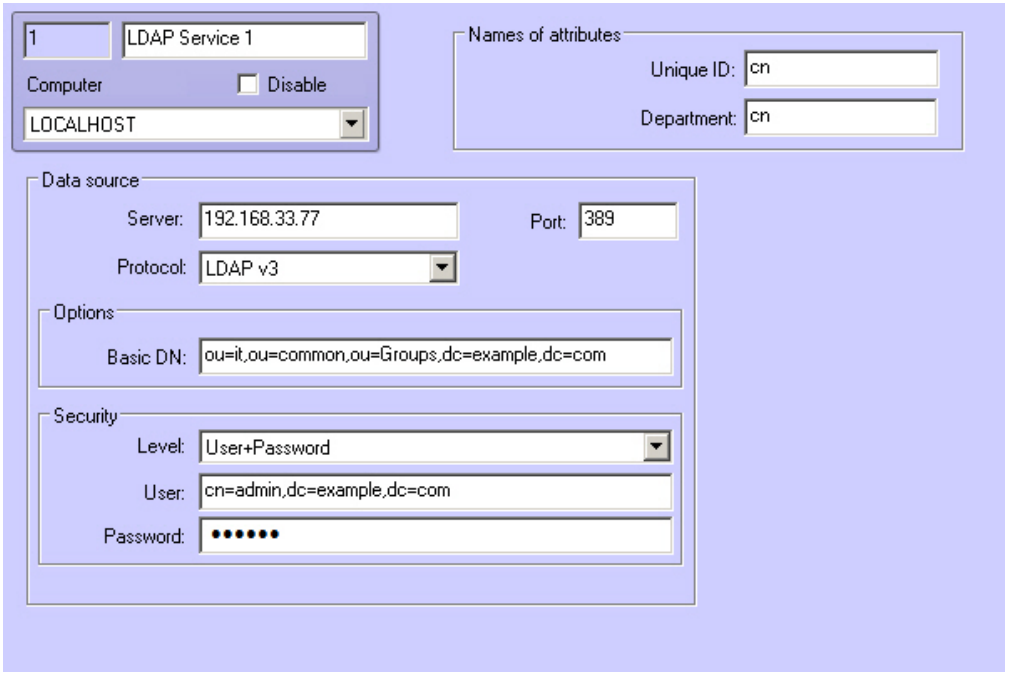
Configuration of correspondence between address attributes and *Intellect* DB fields is now complete.

10.5.2.4 Examples of LDAP Service configuration

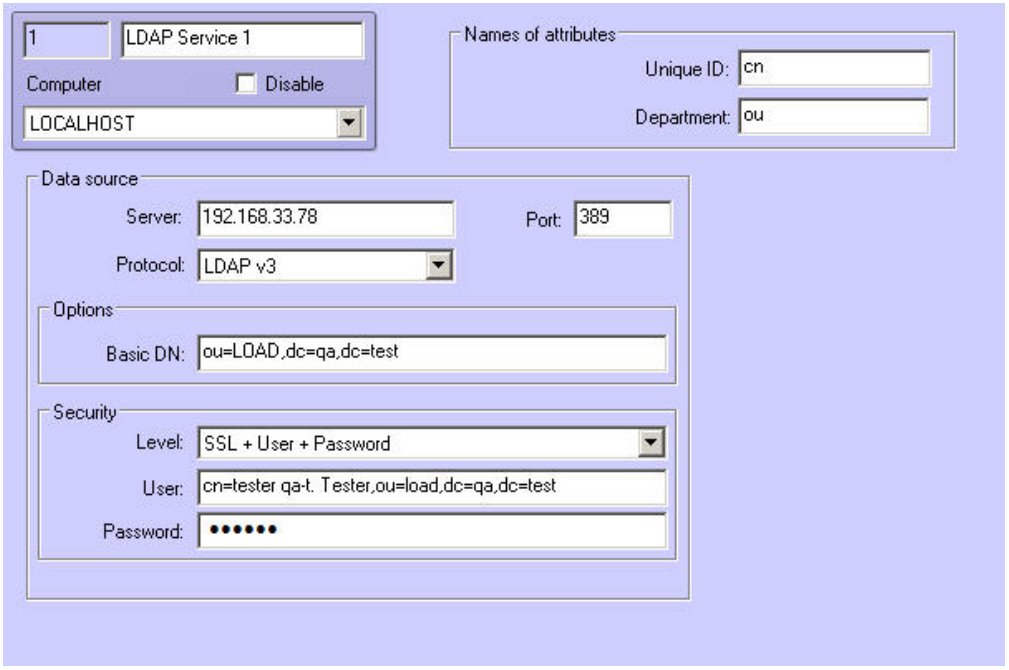
Find below some examples of the LDAP Service object configuration for use with different systems:



For LDAP address book



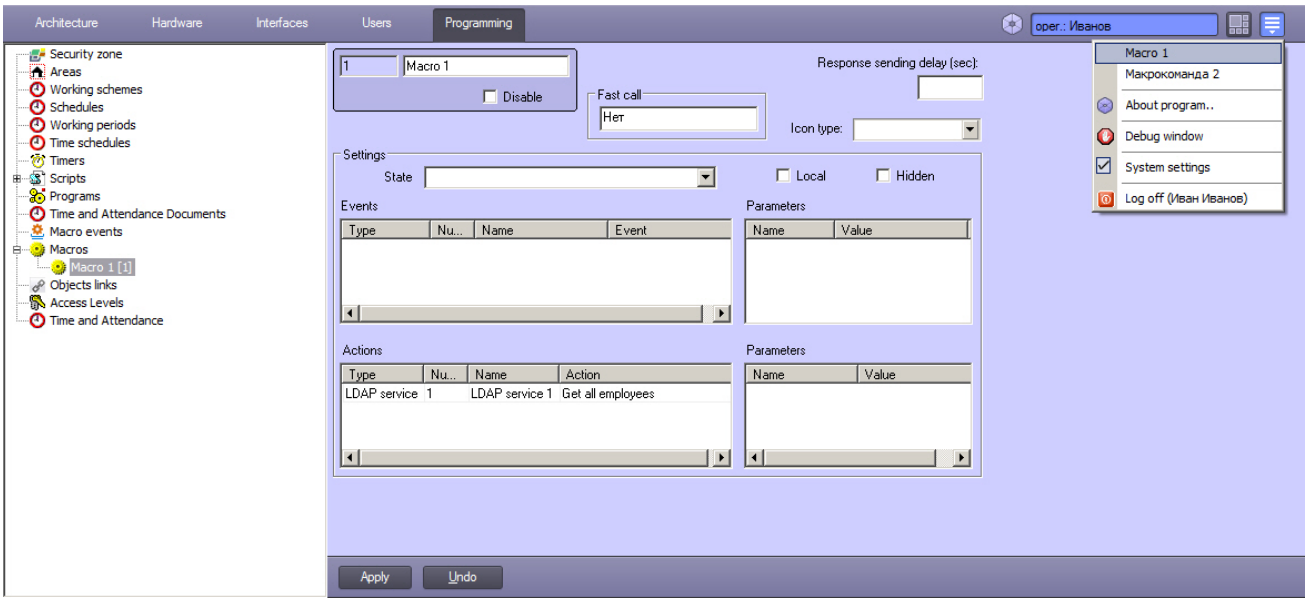
For OpenLdap



For Active Directory based on Windows Server 2012 R2

10.5.2.5 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.

10.5.3 Active Directory configuration

10.5.3.1 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.

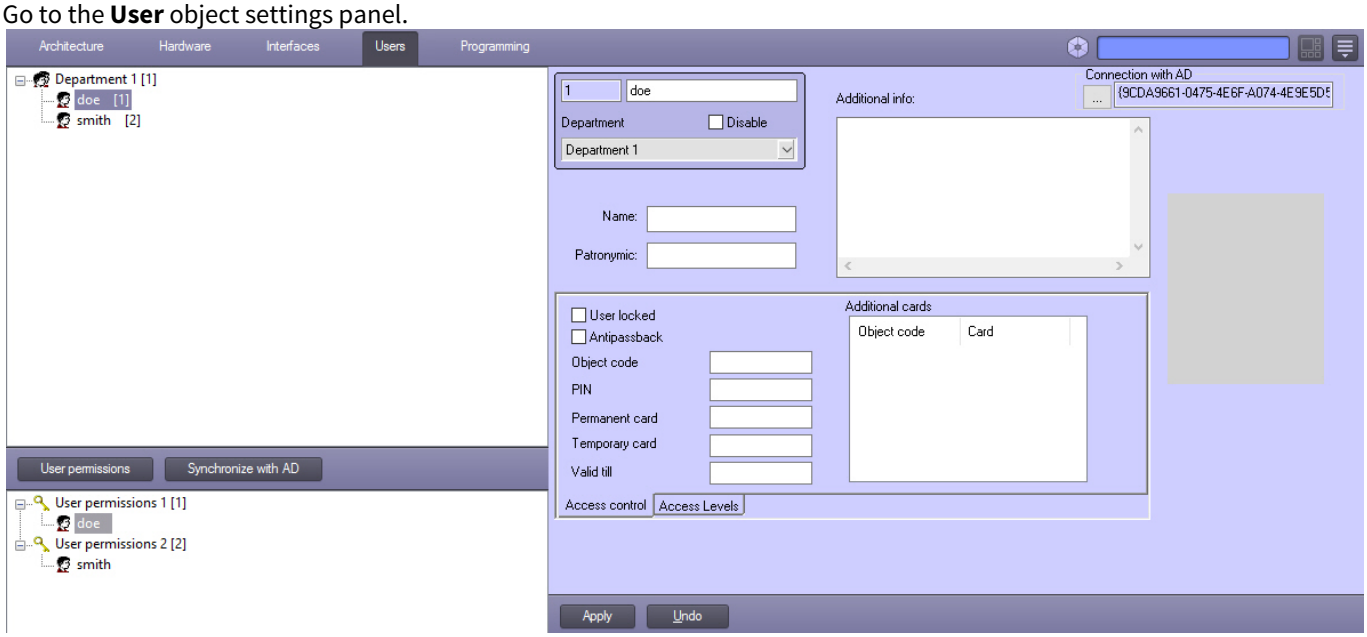
After the *Intellect* and Active Directory joint operation is configured, the Active Directory users are able to launch, use and configure *Intellect* using their Windows account in accordance with the *Intellect* user permissions. The Active Directory users which are connected with the *Intellect* users, but do not belong to any of the groups associated with the *Intellect* user permissions, will not be able to launch *Intellect*.

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*.

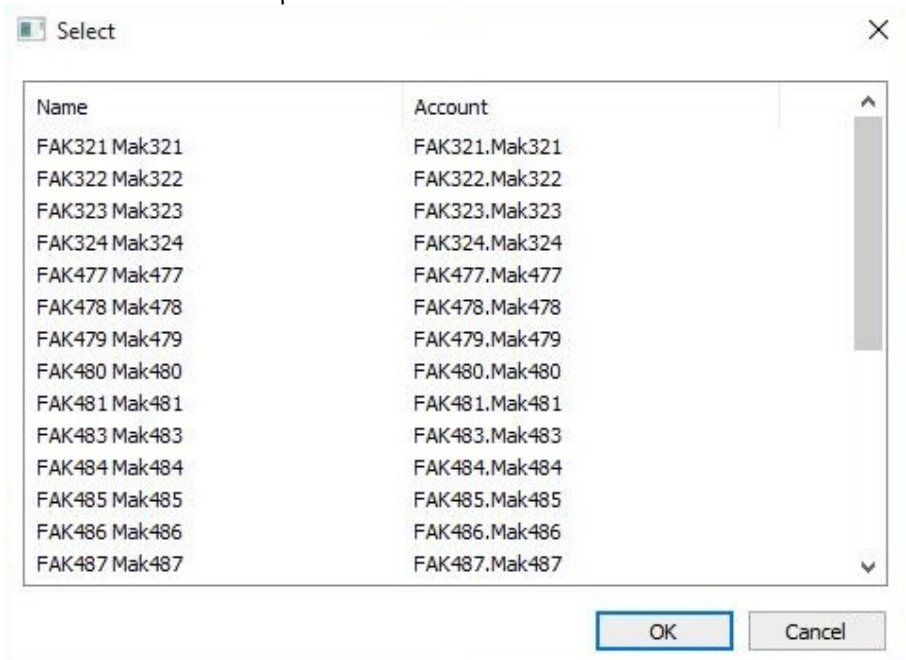
10.5.3.2 Connecting the Intellect and Active Directory users

Configure the connection between the Intellect users and the Active Directory users as follows:

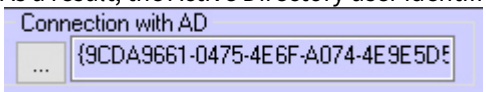
1. Go to the **User** object settings panel.



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 **OK**.
5. As a result, the Active Directory user identifier will be displayed in the **Connection with AD** field.



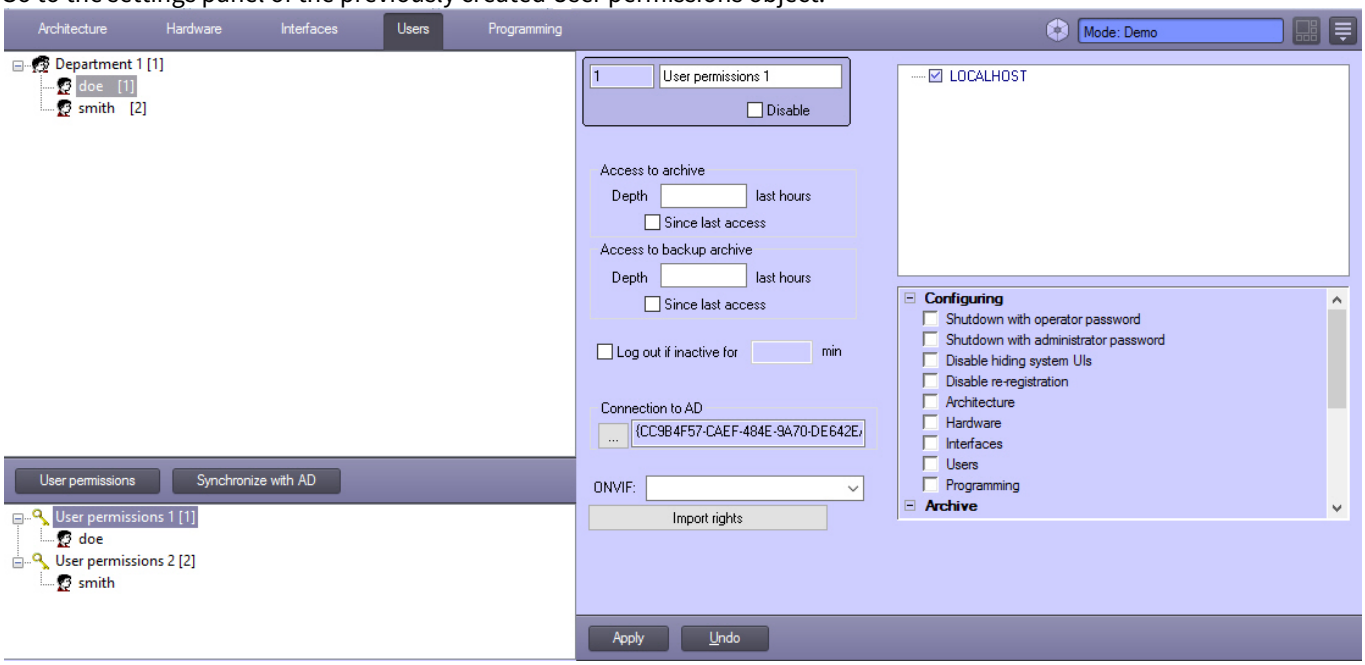
6. Click **Apply**.
7. Repeat steps 1-6 for all required users.

The connection between the Intellect users and the Active Directory users is configured.

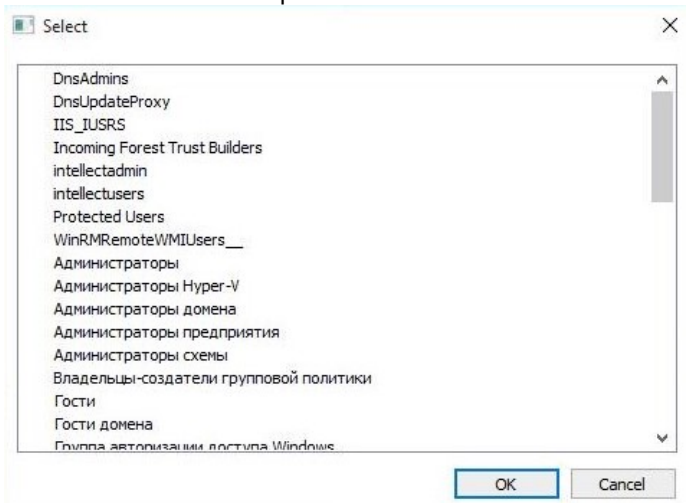
10.5.3.3 Connecting the Intellect user permissions to Active Directory groups

Configure the connection between the Intellect user permissions and Active Directory security groups as follows:

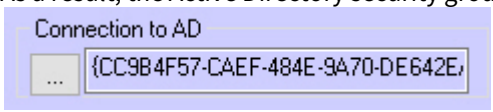
1. Go to the settings panel of the previously created User permissions object.



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.



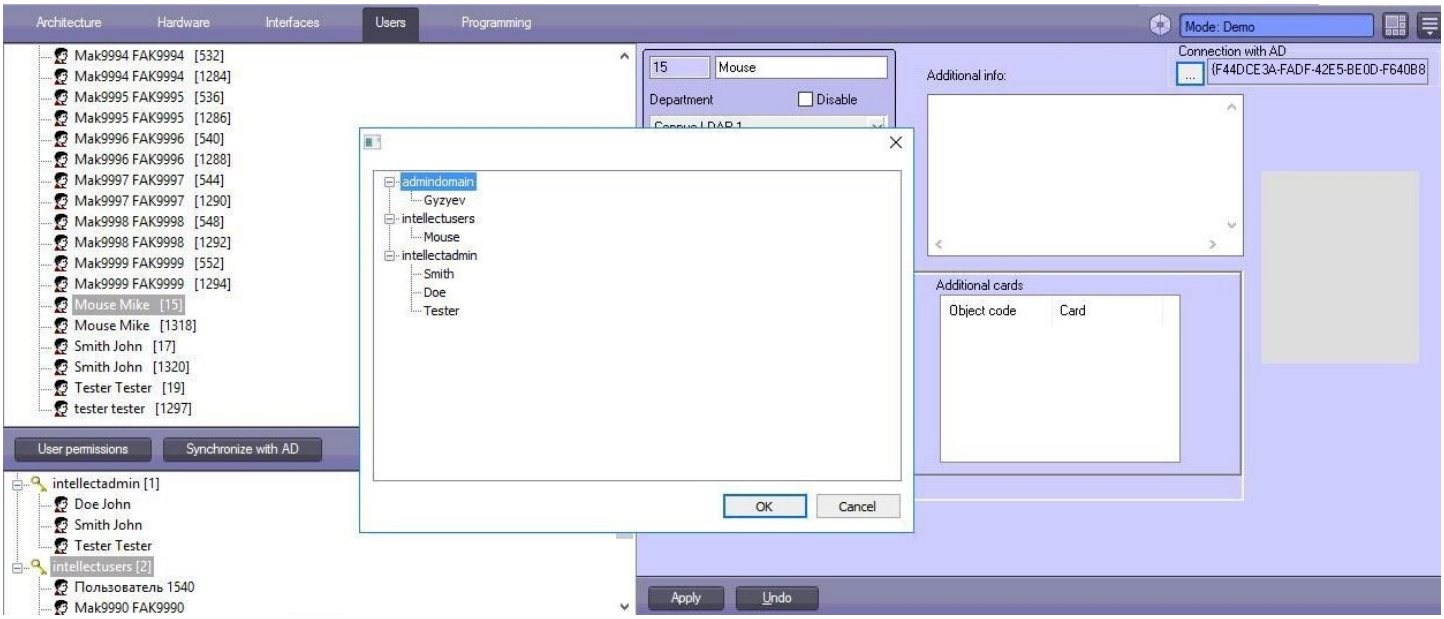
6. Click **Apply**.
7. Repeat steps 1-6 for all required user permissions.

The connection between the Intellect user permissions and Active Directory security groups is configured.

10.5.3.4 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.

To start the Active Directory synchronization, click the **Synchronize with AD** button. The updated structure of the *Intellect* users and user permissions will be displayed in the opened window.

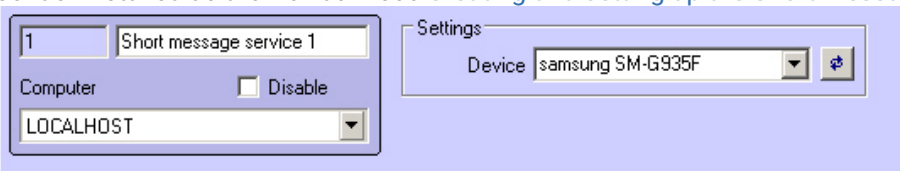


10.5.4 Configuring two-factor authentication

Intellect allows the use 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:

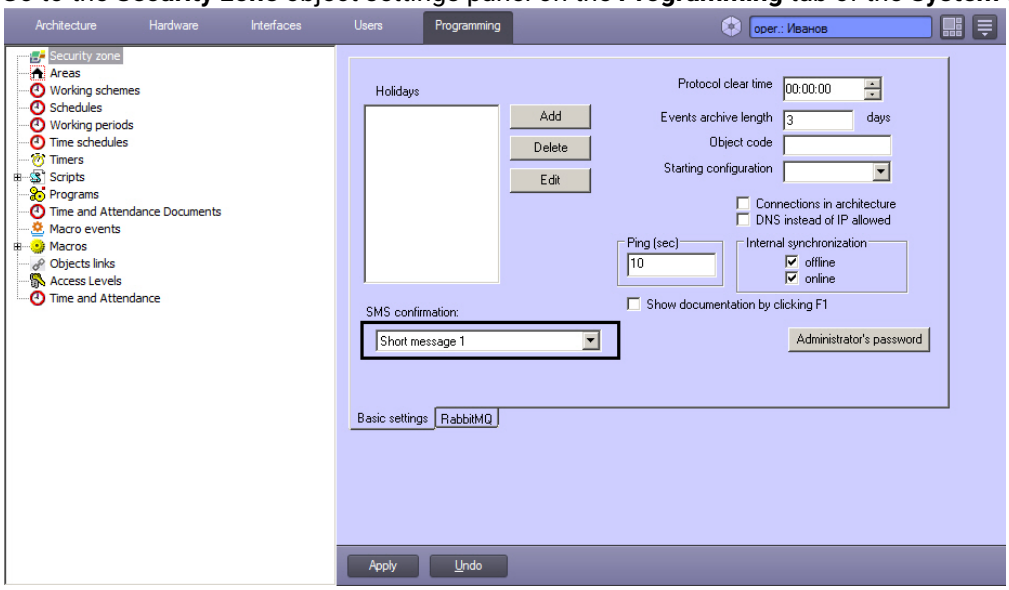
1. Install and configure the Axxon SMS-sender app on the smartphone – see Android-based Axxon SMS-sender Mobile Application. User Guide. This smartphone will be further used as modem, i.e. the short messages will be sent from its SIM card. Please notice that the mobile operator may charge for the SMS service.
2. Create and configure the **Short message service** object; make sure to select the smartphone with Axxon 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.

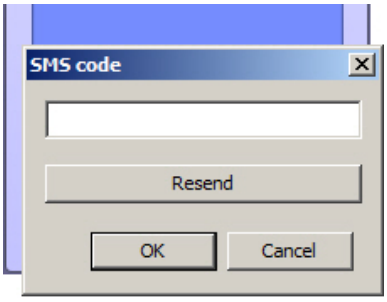


5. Go to the **Security zone** object settings panel on the **Programming** tab of the **System settings** dialog box.



6. From the **SMS confirmation** drop-down list, select the **Short message** object created on step 3.
7. Click **Apply**.

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.

10.6 System settings (the Programming tab)

10.6.1 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.

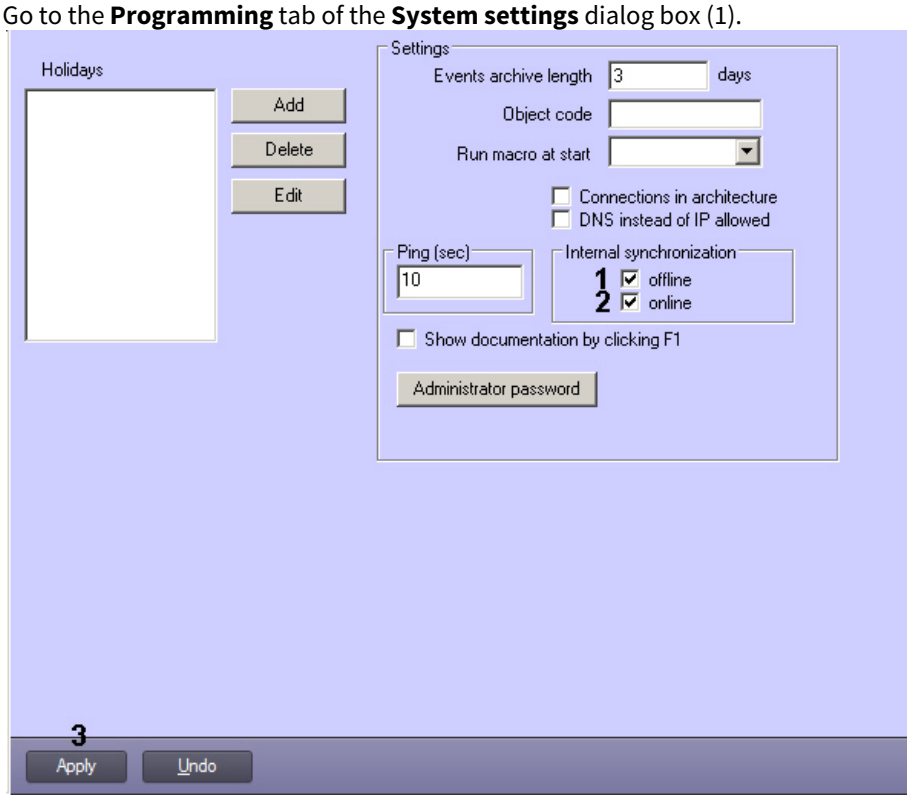
Internal synchronization, both offline and online, can be enabled and disabled for all computers in the distributed system.

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.

10.6.2 Connection of objects with cameras

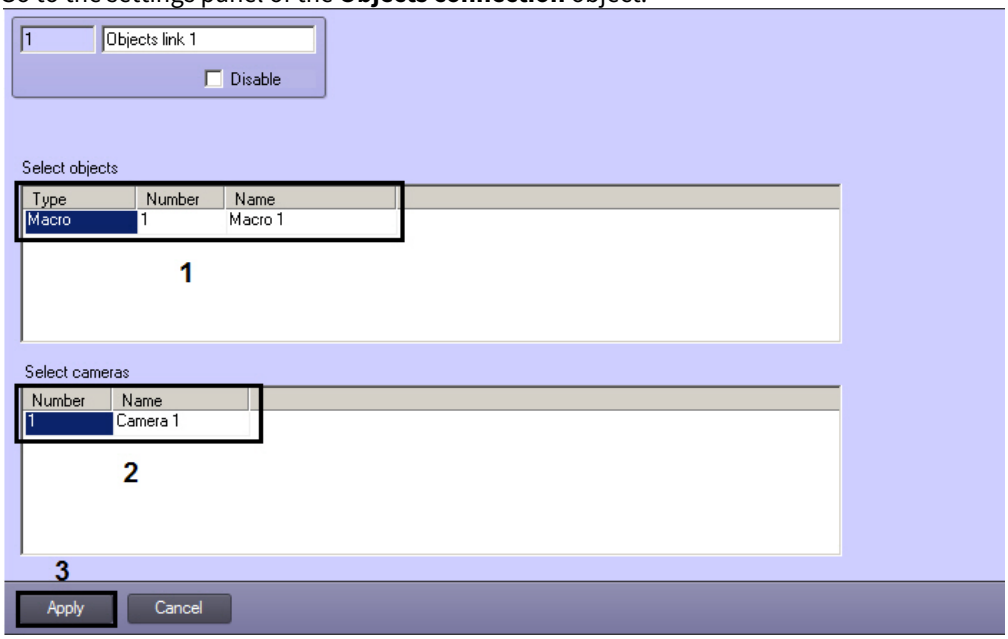
In the Intellect software package it is possible to link cameras to objects.

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.

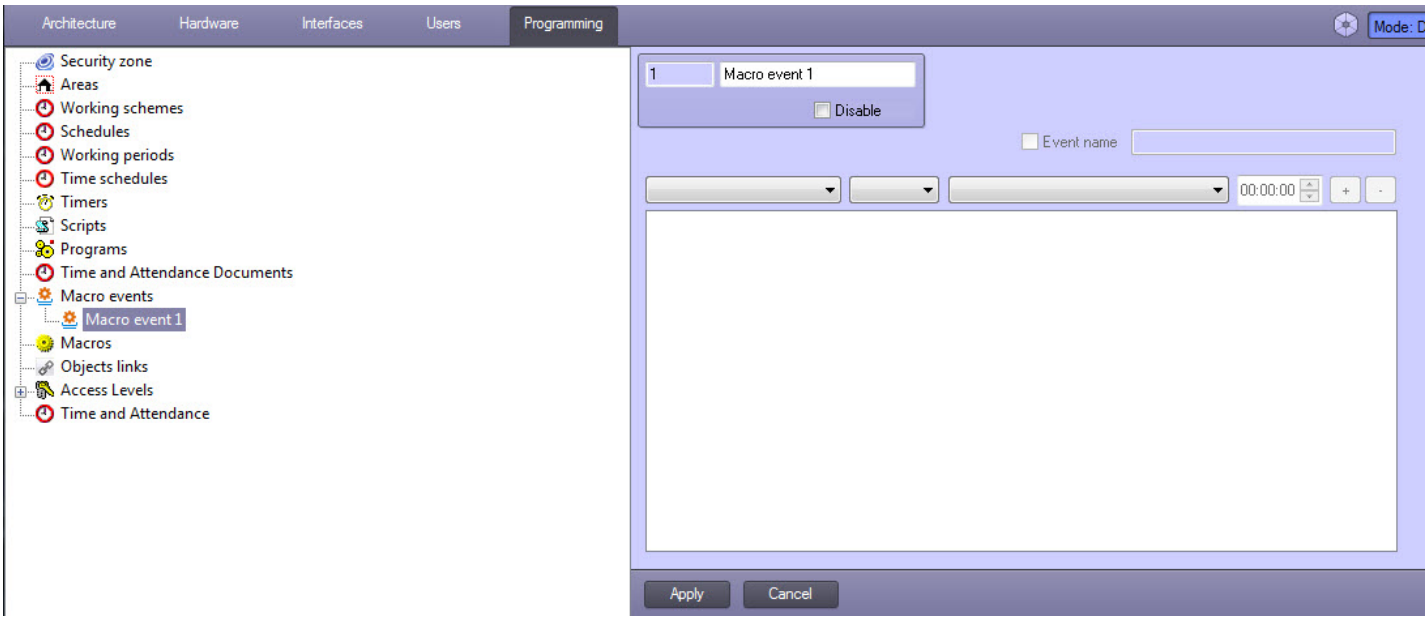
10.6.3 Creating and configuring Macro events

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.

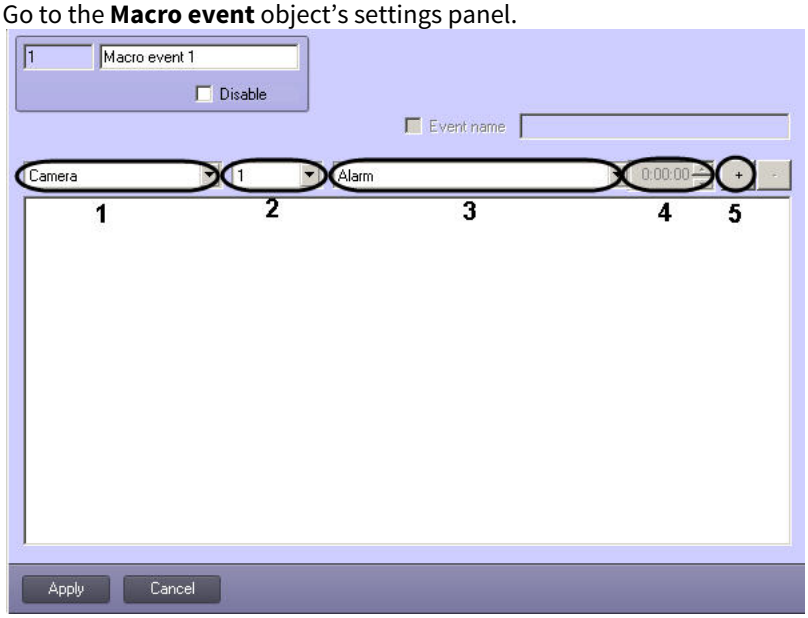
The **Macro event** object is created and configured on the basis of **Macro events** object on the **Programming** tab of the **System settings** dialog box.



10.6.3.1 Configuring the macro events

To configure macro events, do the following:

1. Go to the **Macro event** object's settings panel.



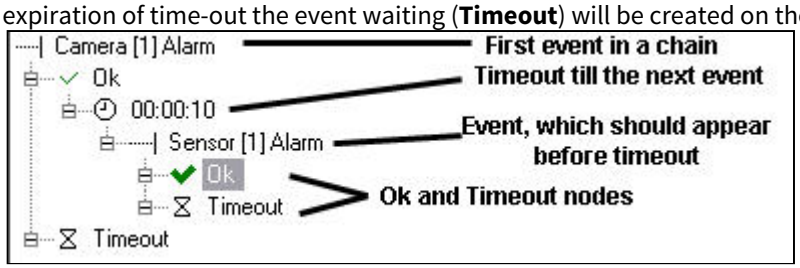
2. Select the object type from the drop-down list (1).
3. Select the object ID from the drop-down list (2) if it's required. If the object ID is not selected, then events from all objects of such type will be considered in.
4. Select the event type from the drop-down list (3). All events from the selected 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.

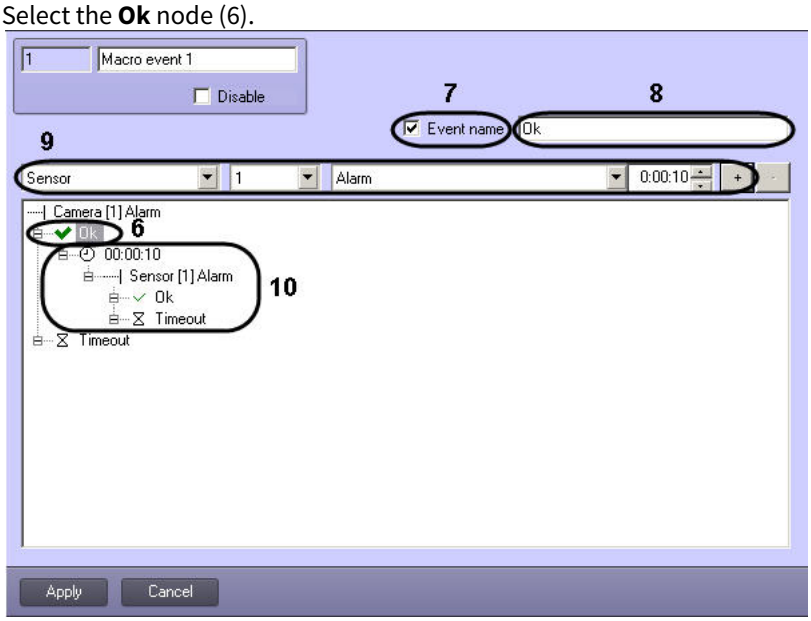
To edit the time-out period select the occurrence time of event in the chain and enter the time again in the text field.



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).



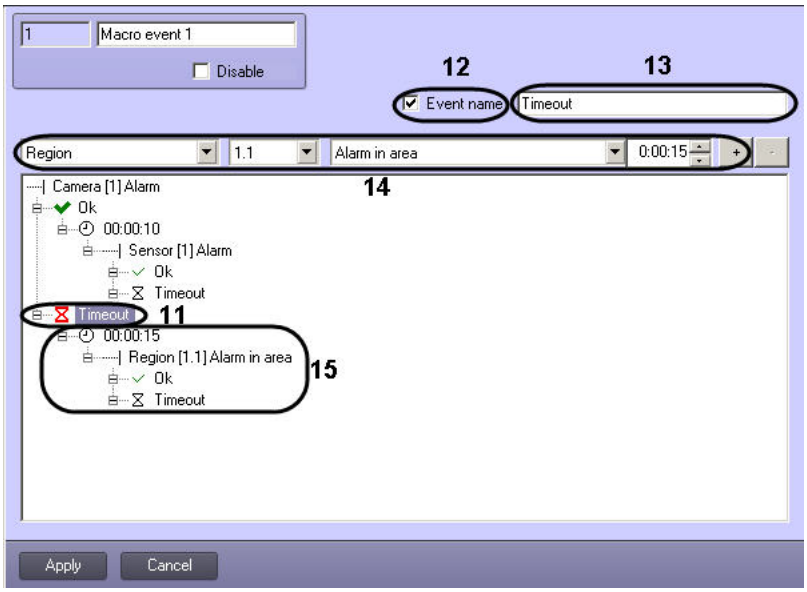
   b. Set the **Event name** (7) checkbox and enter the name of generated event in the text field (8) in case of macro event is to be generated when all previous events in the chain have occurred. The node will be marked by ✔ sign.

   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.

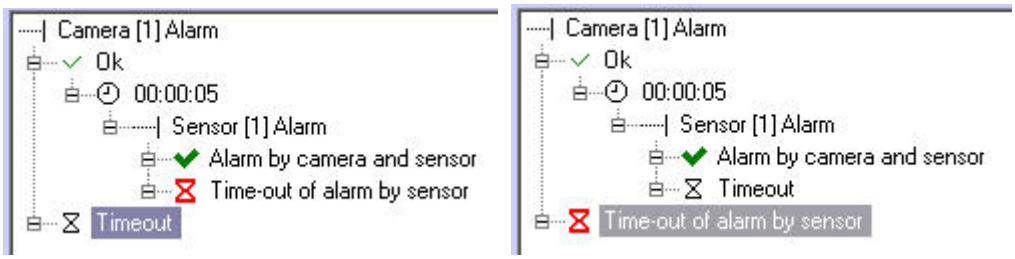
> **Note.**
>
> To delete the event from the chain select its name or occurrence time and click the **–** button. All underneath events in the chain will be also deleted.

Configuring the macro events is completed.

10.6.3.2 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:



10.6.4 Creating and using macros

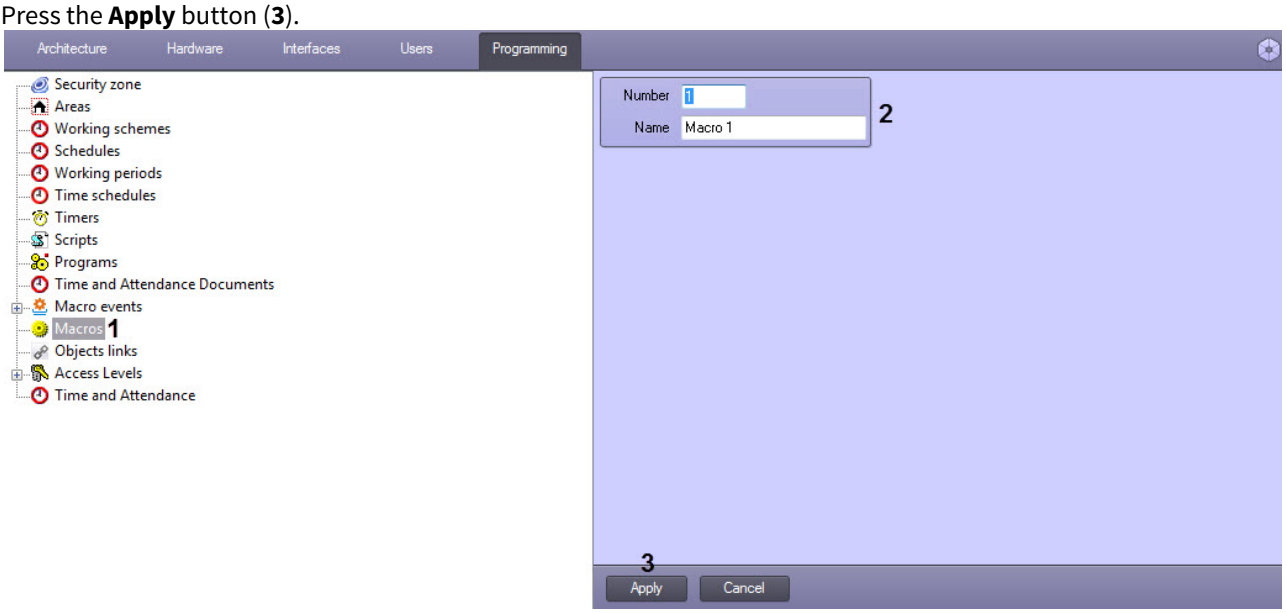
A macro in the *Intellect* system is a system object, designed to maintain logic interaction among other system objects. The **Macro** object settings define the conditions and the corresponding actions. The **Macro** objects are used for automatic controlling of the surveillance system.

An unlimited number of **Macro** objects can be created in the system.

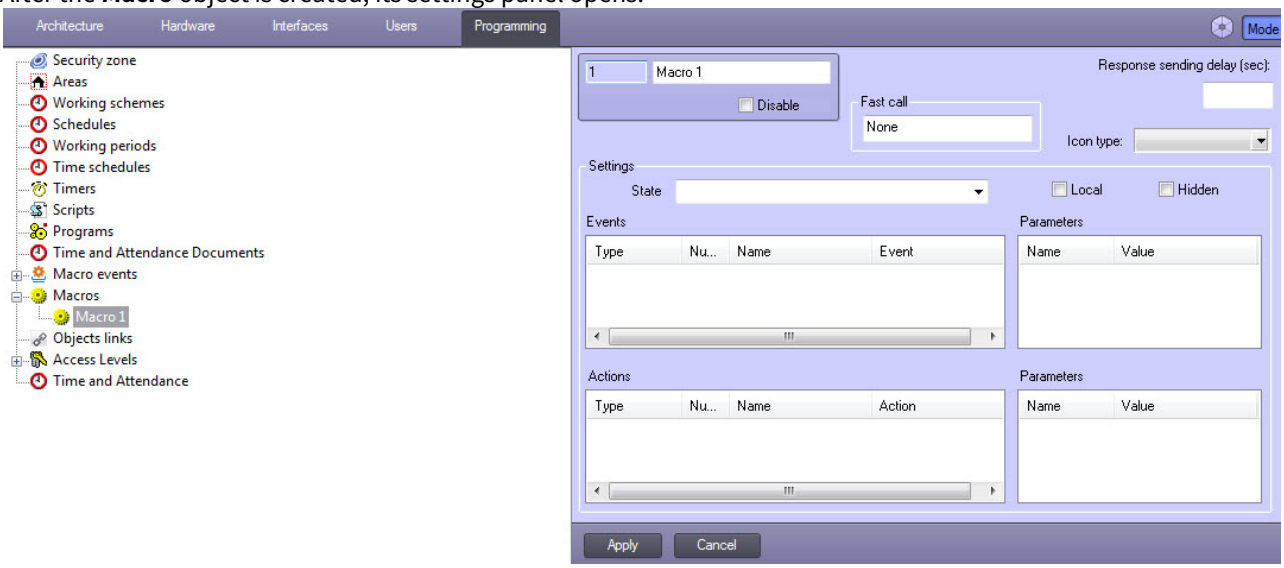
10.6.4.1 Creating macros

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.

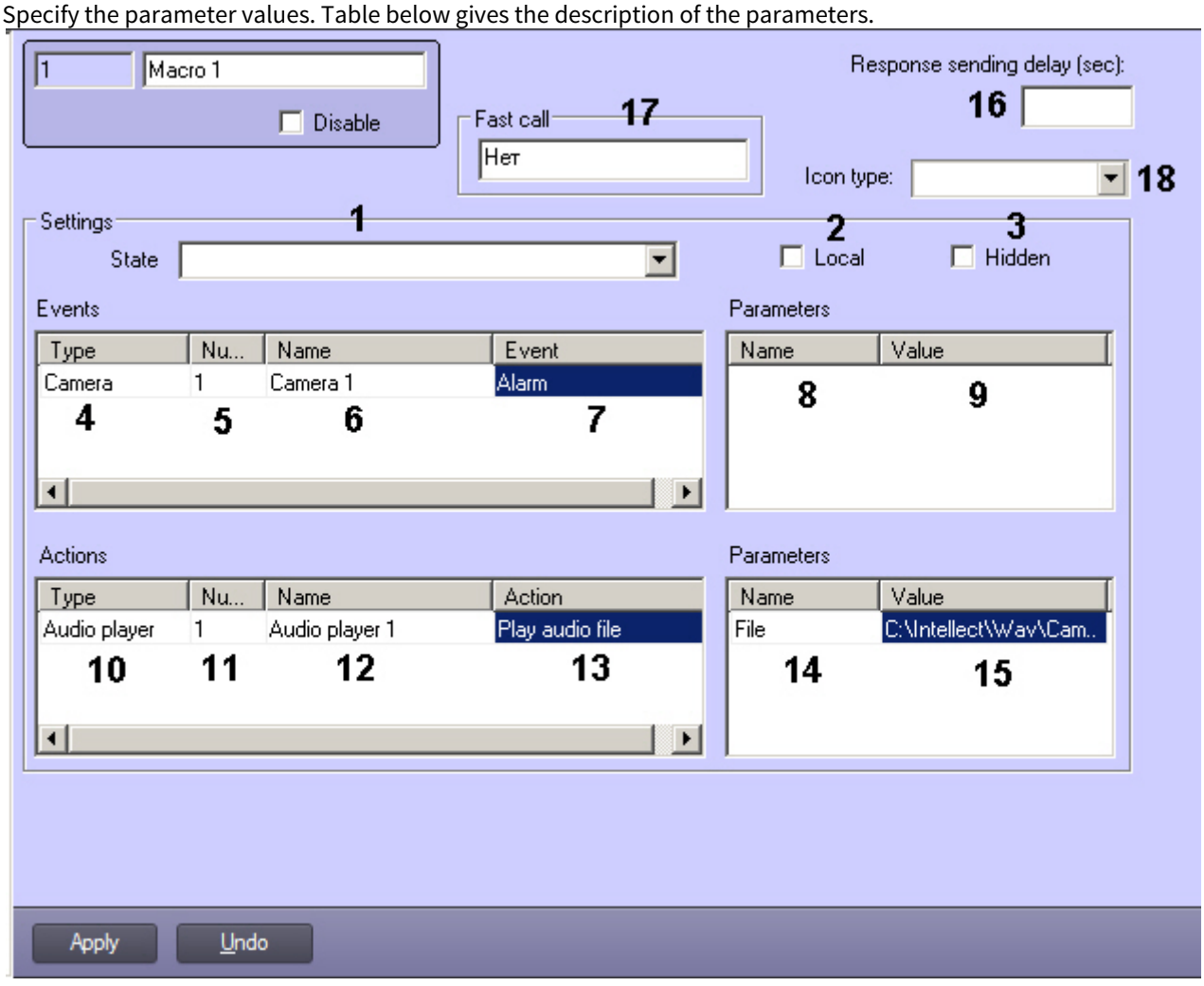


Table 8.23—1

№	Name	Field type	Description	Format	Default value	Value range
Settings group						
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

№	Name	Field type	Description	Format	Default value	Value range
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
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)						

№	Name	Field type	Description	Format	Default value	Value range
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 250.
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 events do not reoccur over the specified period.*	Integer number	-	>0
17	The **Fast call** field	Left-click in the field and click the required key combination	Sets a shortcut for a macro. *Note. If the same combination of hot keys is set for several macros, when clicking a key combination, all of these macros run.*	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 absend 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.

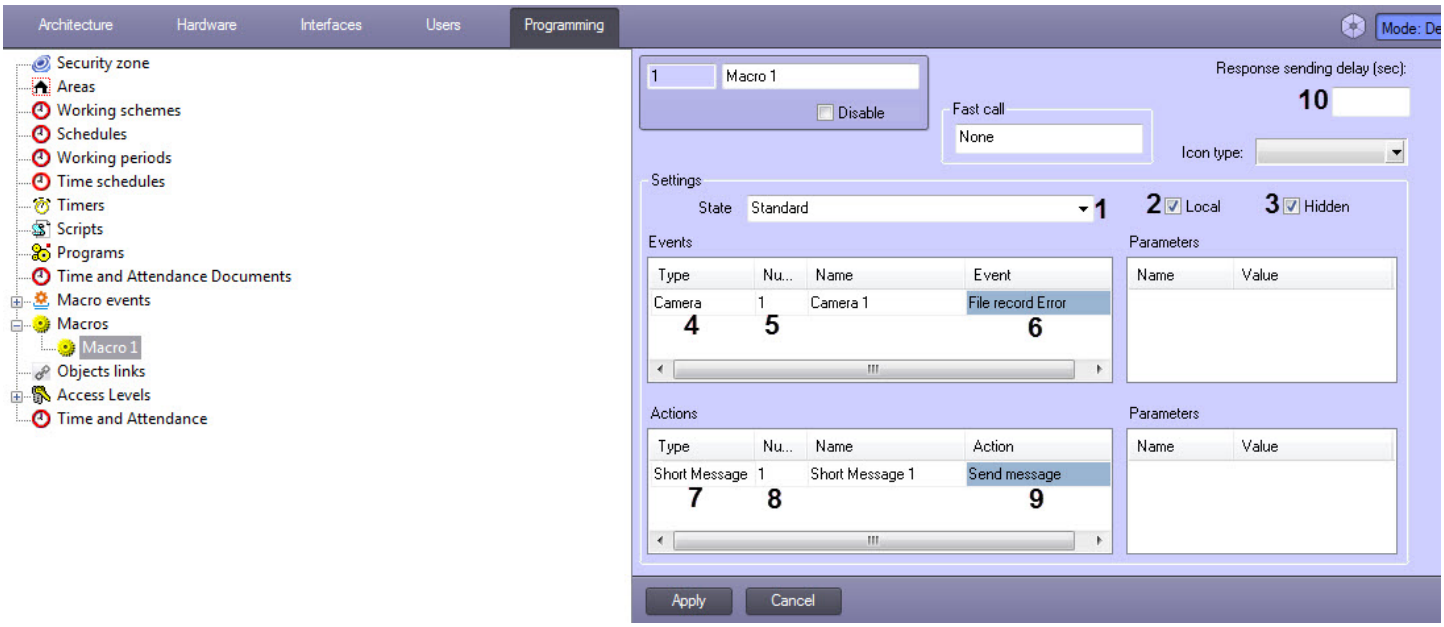
3. Click the **Apply** button to save the settings.

10.6.4.2 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 soma time later the event occurs, specify the **Response sending delay (sec.)** parameter value (10).
11. Press the **Apply** button.

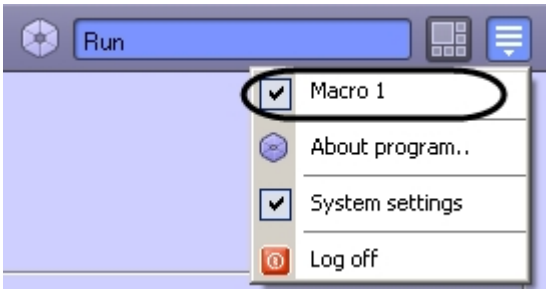
If the **Hidden** checkbox is not checked, the macro will need manual activation, which is done by clicking the **Run** button in the **Main control** menu and by selecting the macro in the list.



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 Macro commands operation and Running macros from the Surveillance window).

10.6.5 Creating and using the Timer object

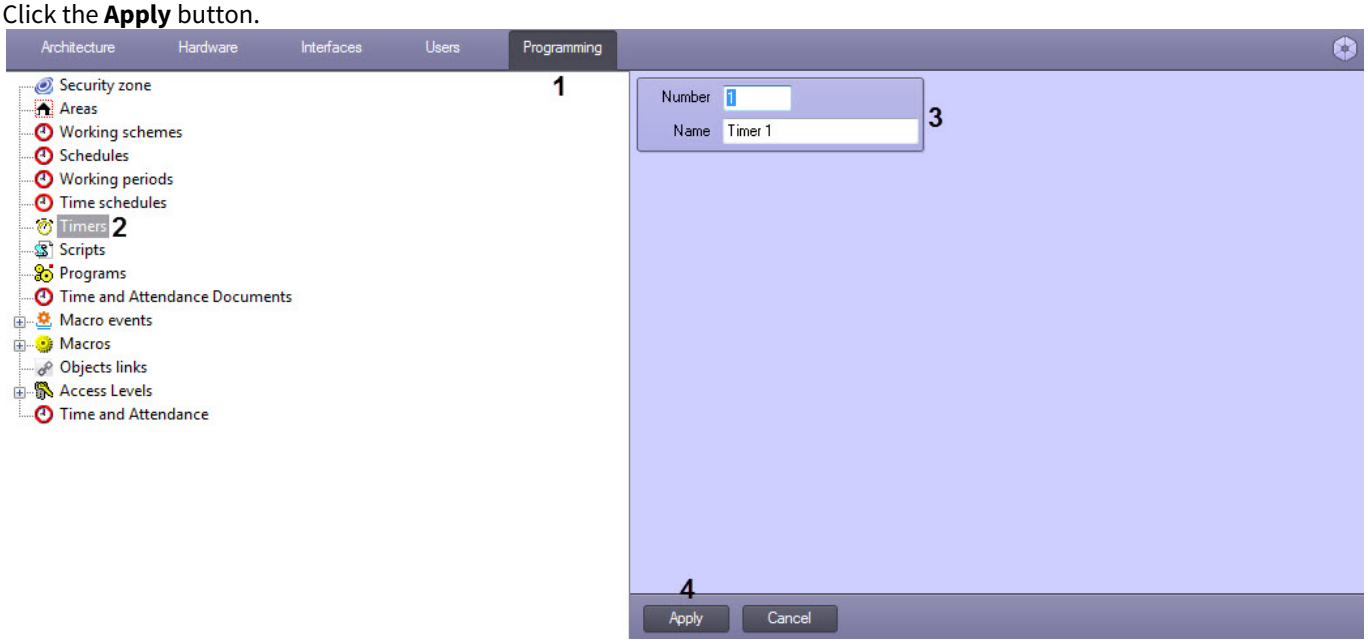
The **Timer** object sets a time point upon reaching which an action (a macro) is executed. Thus, the **Timer** object is used together with the **Macro** object and for other objects setup.

10.6.5.1 Creating and configuring the Timer object

To create a **Timer** object, do the following:

1. Open the **Programming** tab.
2. Create a **Timer** object under the **Timers** object in the objects tree.
3. Enter the number and name for the **Timer** object in the corresponding field of the settings panel.

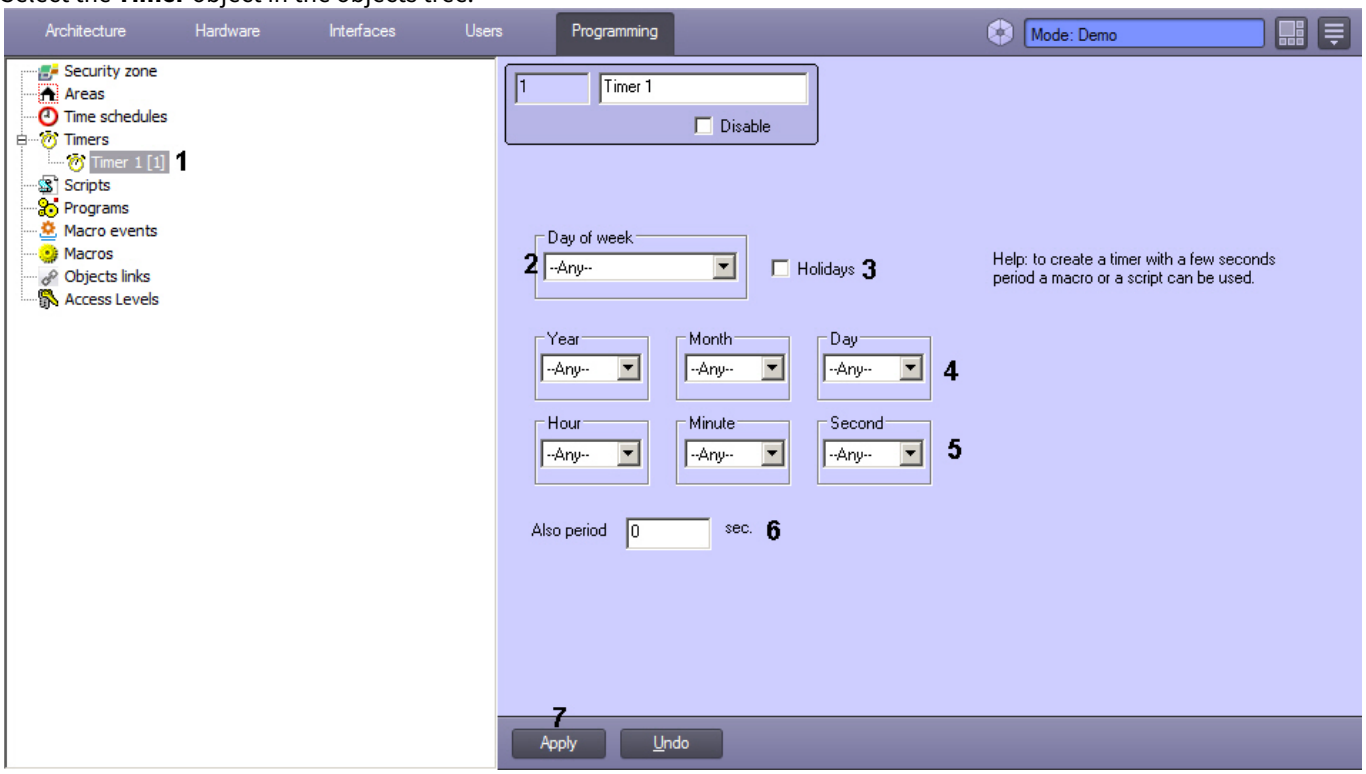
4. Click the **Apply** button.



The **Timer** object will appear in the objects tree.

To set up the **Timer** object, do the following:

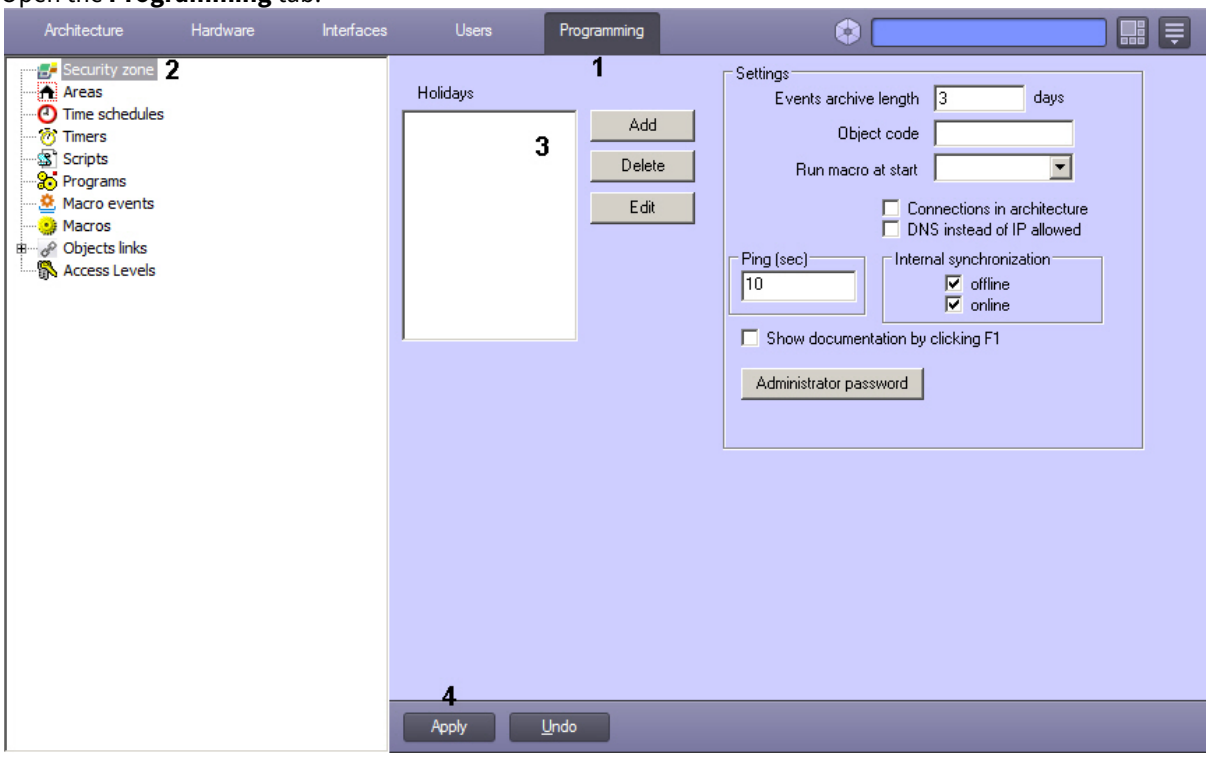
1. Select the **Timer** object in the objects tree.



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 (5);
   b. select the exact date (year, month, day) from the corresponding fields (4) and the exact time (hour, minute, second) in the corresponding fields (5).
3. To enable the timer triggering with a period in seconds after the first triggering of the timer, enter the required interval in seconds in the **Also period** field (6).
4. Check the **Holidays** checkbox to take into account the holidays set in the Common settings (3).
5. Click the **Apply** button (7).

To create the list of holidays, do the following:

1. Open the **Programming** tab.

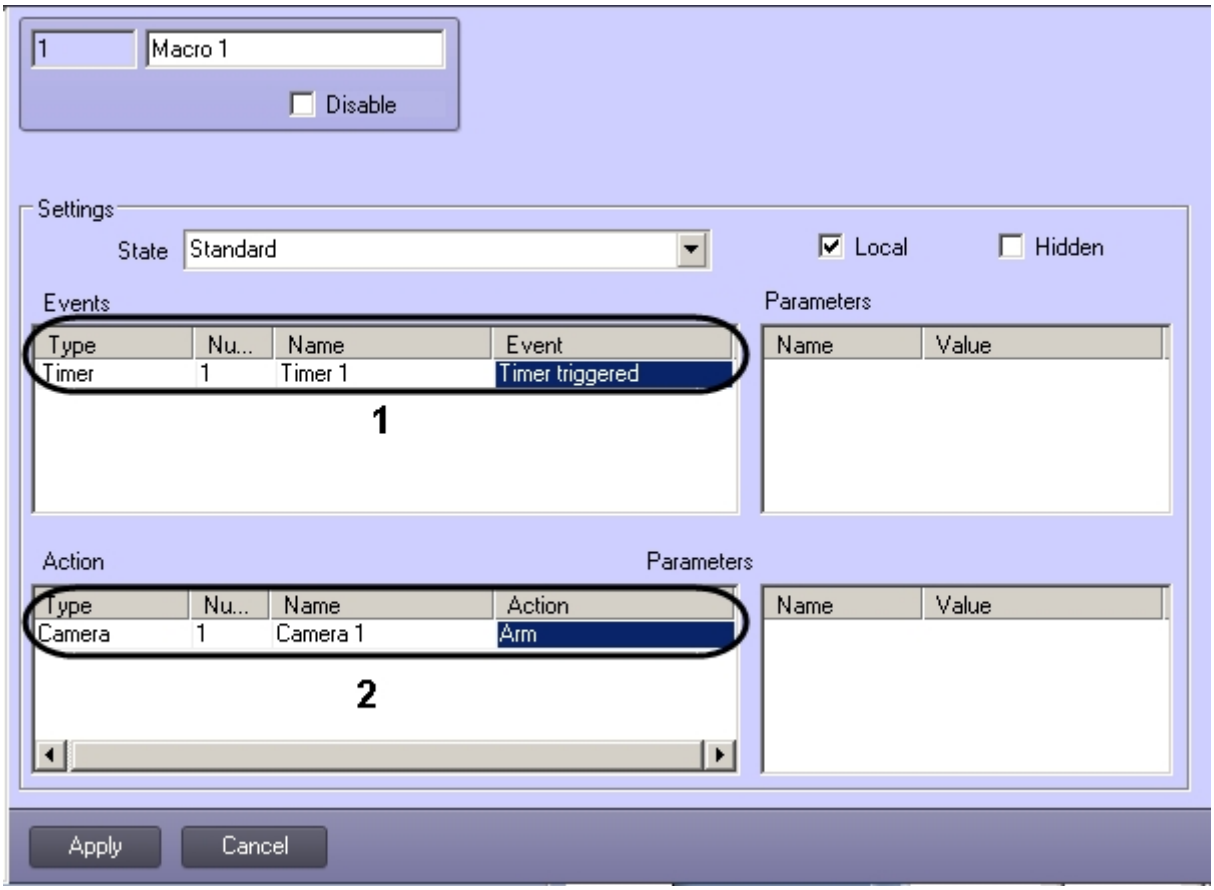


2. Select the **Security zone** object.
3. Enter a holiday date in the DD.MM.YYYY format.
4. Click the **Apply** button.

10.6.5.2 Using the Timer object

Example 1. Consider a macro that activate an arming mode in selected camera when the timer triggers.

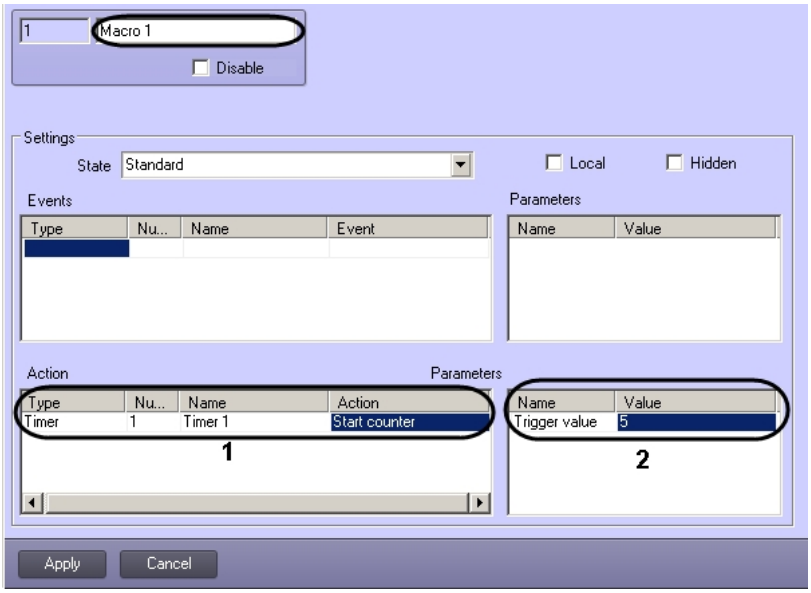
No	Event	Action
1	The timer triggered (1).	Activate an arming mode (2)



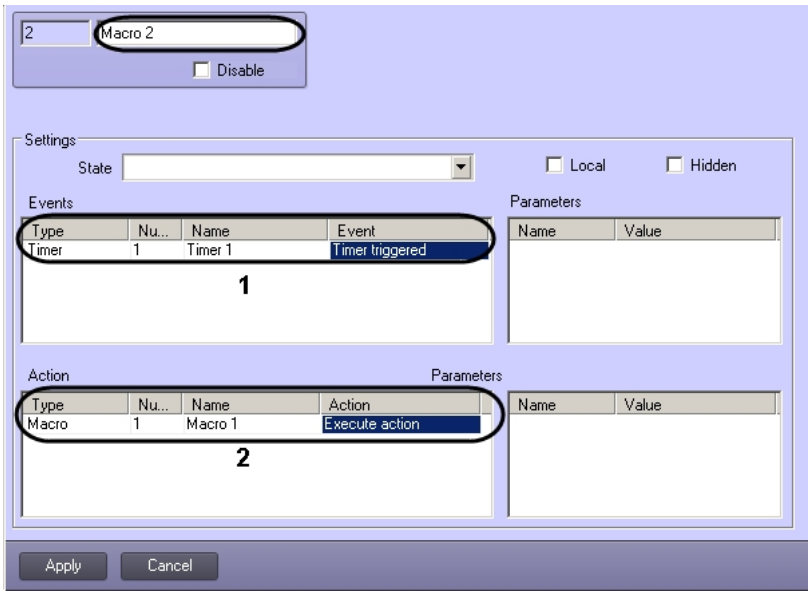
Example 2. Consider macros that allow to set the timer with trigger period of several seconds.

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.

10.6.6 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.

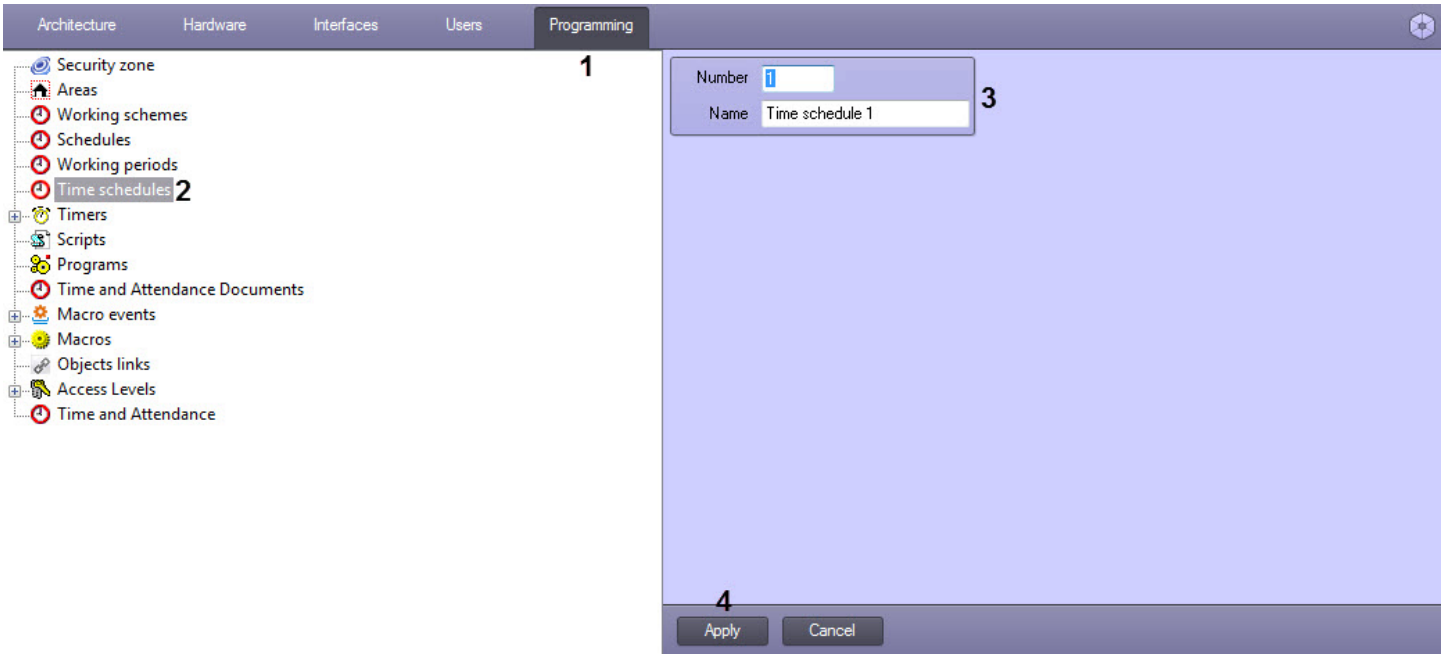
The **Time schedule** object is used in conjunction with the **Macro** object and for setting up other system objects.

An unlimited number of **Time schedule** objects can be created in the system.

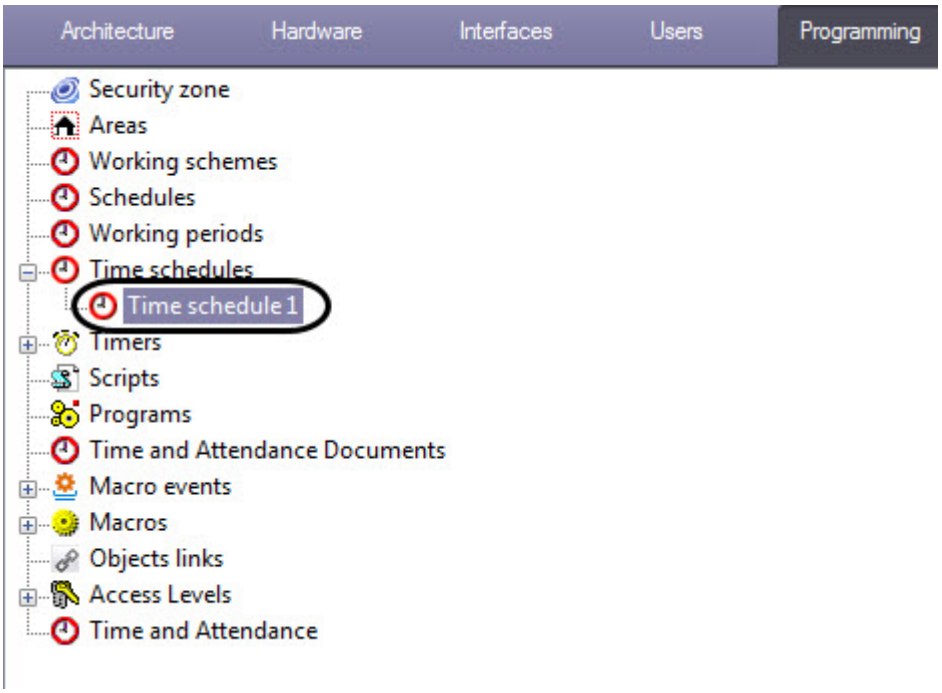
10.6.6.1 Creating and configuring time schedules

To create a **Time schedule** object, do the following:

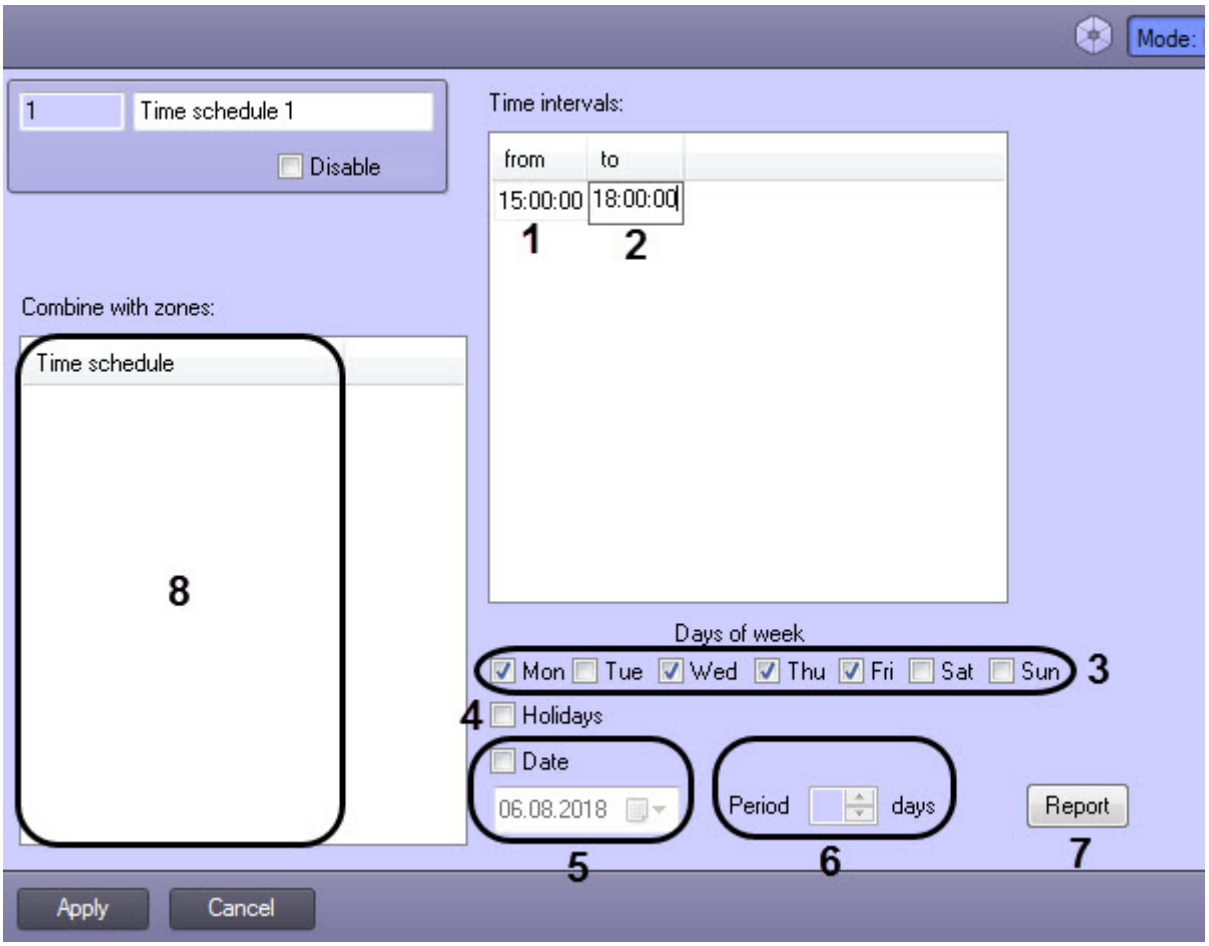
1. Open the **Programming** tab (1).
2. Create the **Time schedule** object under the **Time schedules** node in the objects tree (2).
3. Specify the number and name of the time schedule into the corresponding fields of the settings panel (3).
4. Click the **Apply** button (4).



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	Field type	Description	Format	Default value	Value range
The **Time intervals** group						
1	The from column	Enter the value	Exact time of starting the macro execution	HH:MM:SS	00:00:00	00:00:00 to 23:59:59
2	The to column	Enter the value	Exact time of ending the macro execution	HH:MM:SS	00:00:00	00:00:00 to 23:59:59
The **Days of week** group						
3	Checkboxes: Mon Tue Wed Thu Fri Sat Sun	Checkbox	Adds days to the timetable. The days of the week are added individually y for each time interval.	-	No	**Checked** – the day of the week is included in the timetable. **Not checked** – the day of the week is not included in the timetable.
The **Holidays** group*						

No	Parameter name		Field type	Description	Format	Default value	Value range
4	**Holidays**		Checkbox	Adds holidays to the timetable. The holidays are added individually for each time interval.	-	No	**Checked** – the list of holidays is included in the timetable. **Not checked** – the list of holidays is not included in the timetable.
The **Date** group							
5	**Date**	Check-box	Checkbox	Enables the **Period__days** field. If set, the Days of week group is disabled. The days are added individually for each time interval.	-	No	**Checked** – enable the **Period__days** field. **Not checked** – disable the **Period__days** field.
		Field	Enter the value	Specifies the exact date. The days are added individually for each time interval.	DD.MM.YYYY	Current date	00.00.0000 to 31.12.9999
6	**Period**		Enter the value	Sets the cyclicity in N-days, time schedule triggers from the specified date (i.e. time schedule responses every N-day)	Numeric value	Disabled	0 to 999999999999999. Cyclicity is set individually for every time interval
7	The **Report** button		-	Displays the box with the table of time schedule activity	-	-	-
The **Combine with schedule** table							
8	The **Time schedule** dropdown list		Selected from the list	Sets the time schedule with which the given time schedule is to be combined	Names of the registered **Time schedule** objects	-	Depends on the number of registered **Time schedule** objects

* The **Holidays** checkbox adds the list of the days specified in the **Security zone** object in the **Programming** tab.

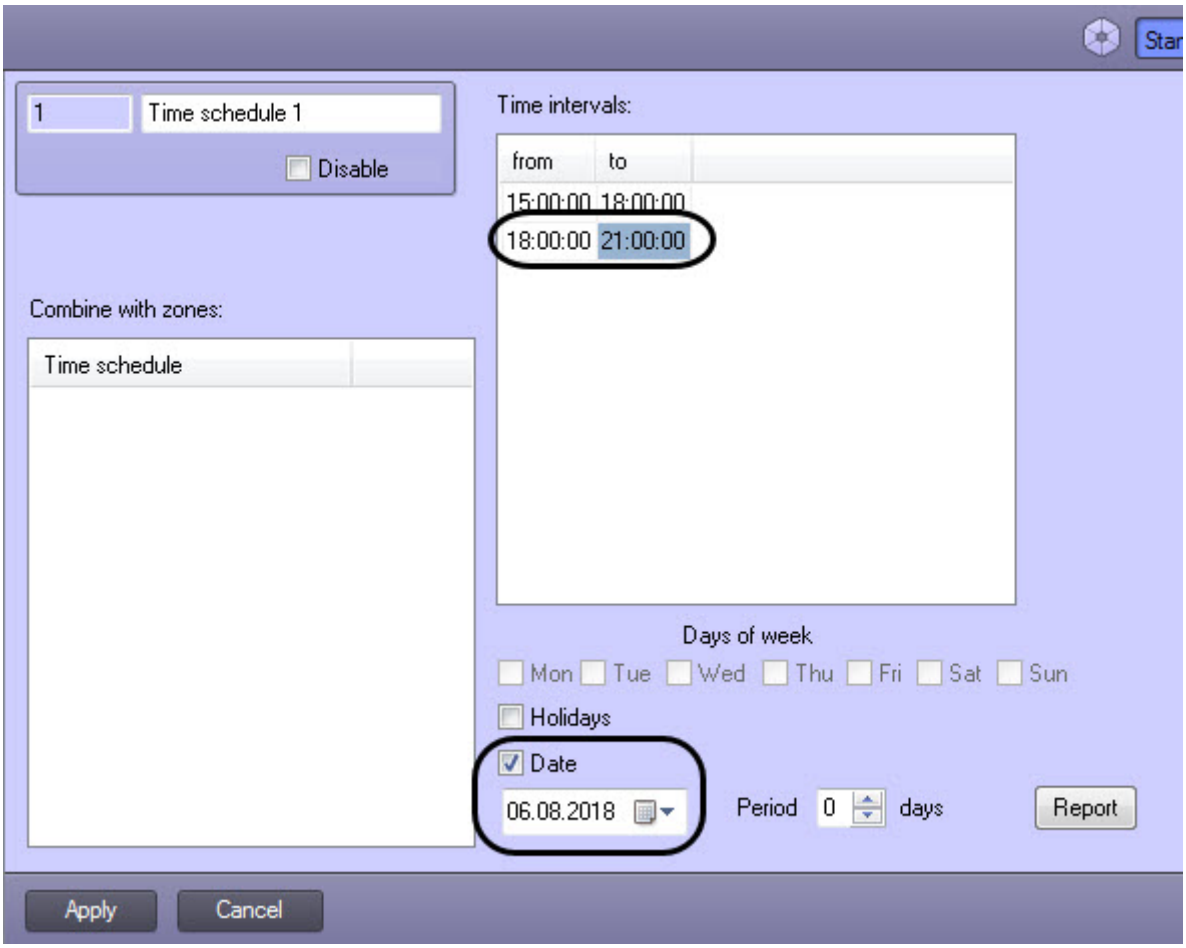
If the moment of time interval beginning is set later than the moment of ending, then time schedule will cover the present day (from the time interval beginning) and part of the following day (to the time interval ending) on conditions that the Time schedule is set for the present and following day. 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 into specia days, for example, days before holidays.The date of a special day and 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 .

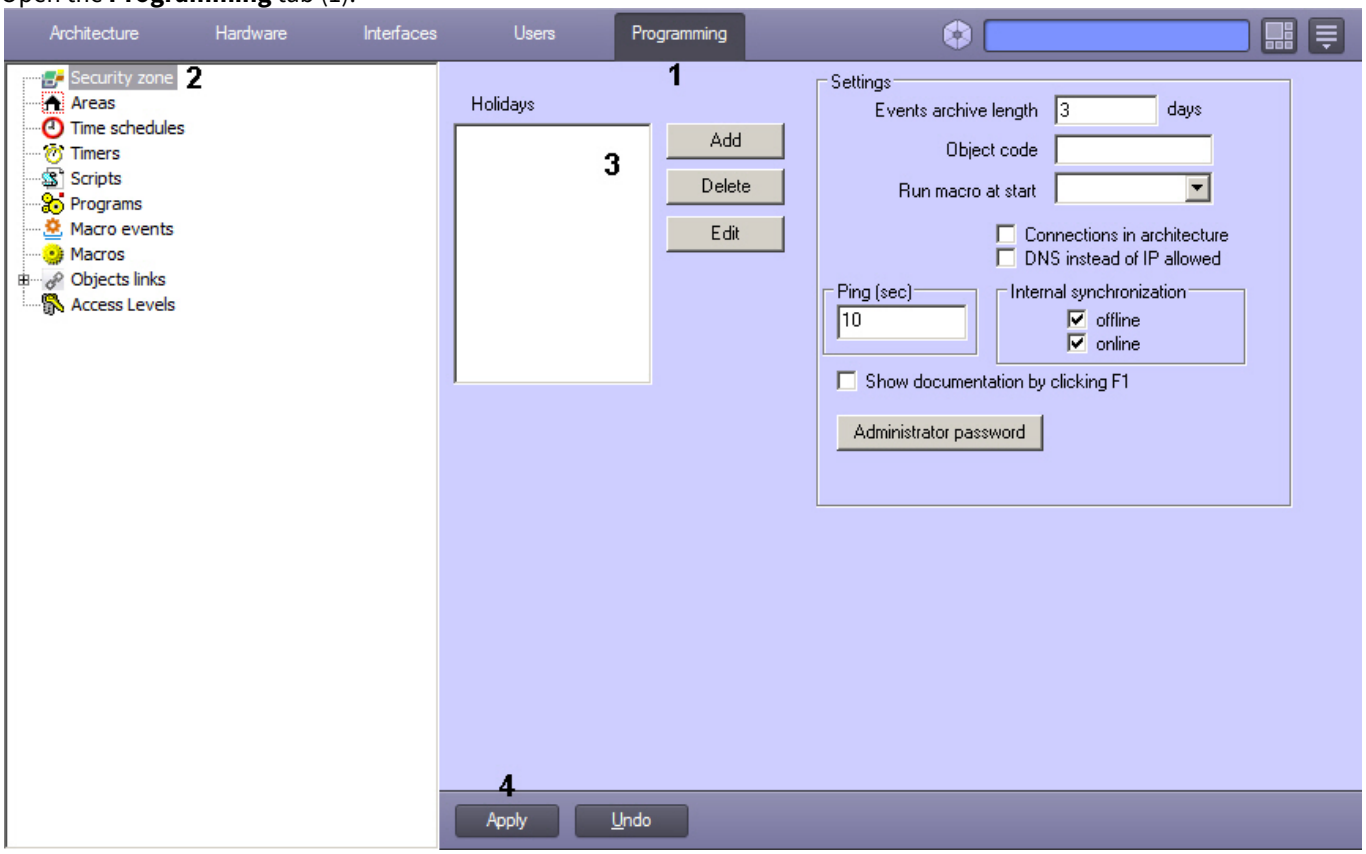
Attention!

The duaration of additional time schedule usage in days is not set on the settings panel. So, time schedule combining is to be disabled right after its application.



To create the list of holidays, do the following:

1. Open the **Programming** tab (1).



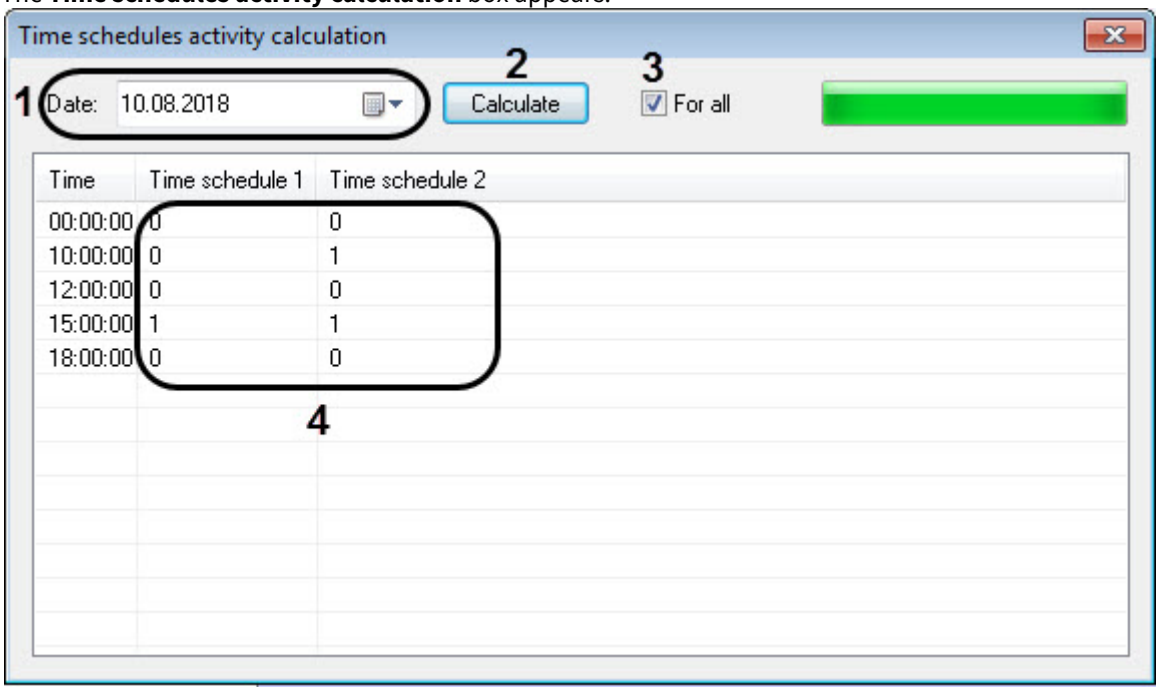
2. Select the **Security zone** object (2).
3. Specify the holiday date in the following format: DD.MM.YYYY (3).
4. Click the **Apply** button (4).

10.6.6.2 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).

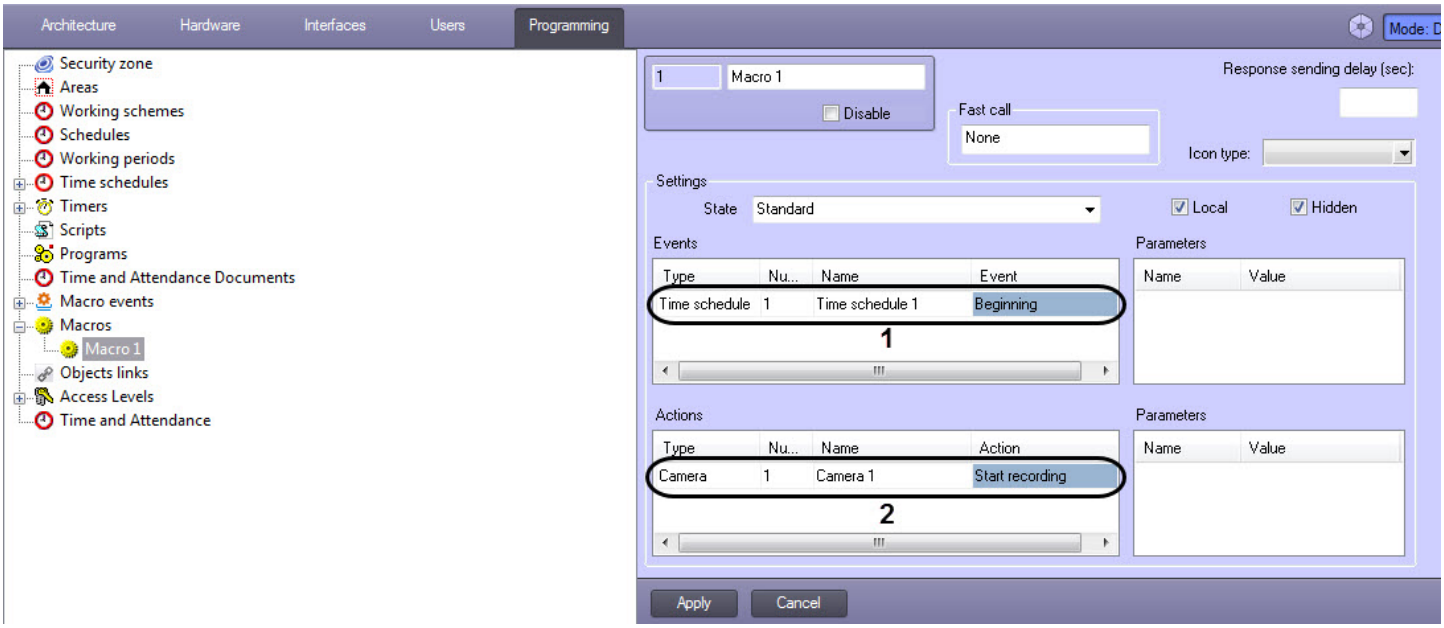
10.6.6.3 Examples of time schedules usage

Example 1. Consider two micros which work together and allow recording a video within the time schedule limits.

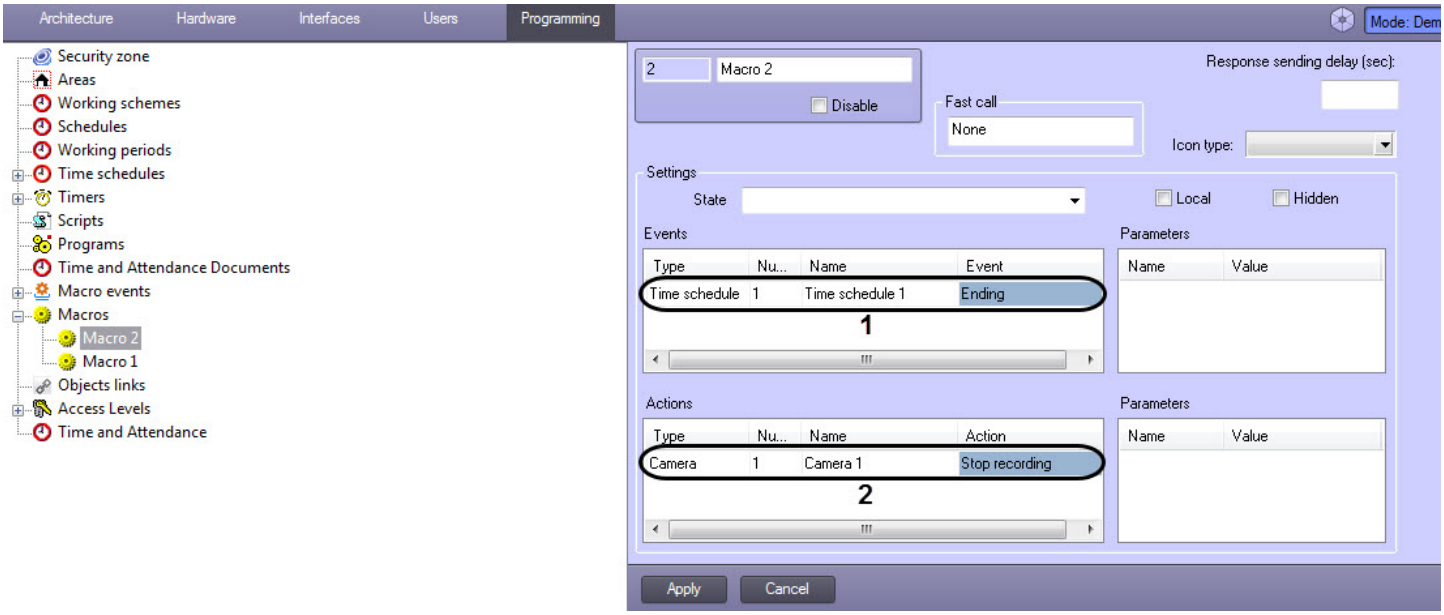
Set the events and actions values in **Macro** setting window that is given in the table.

№	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.



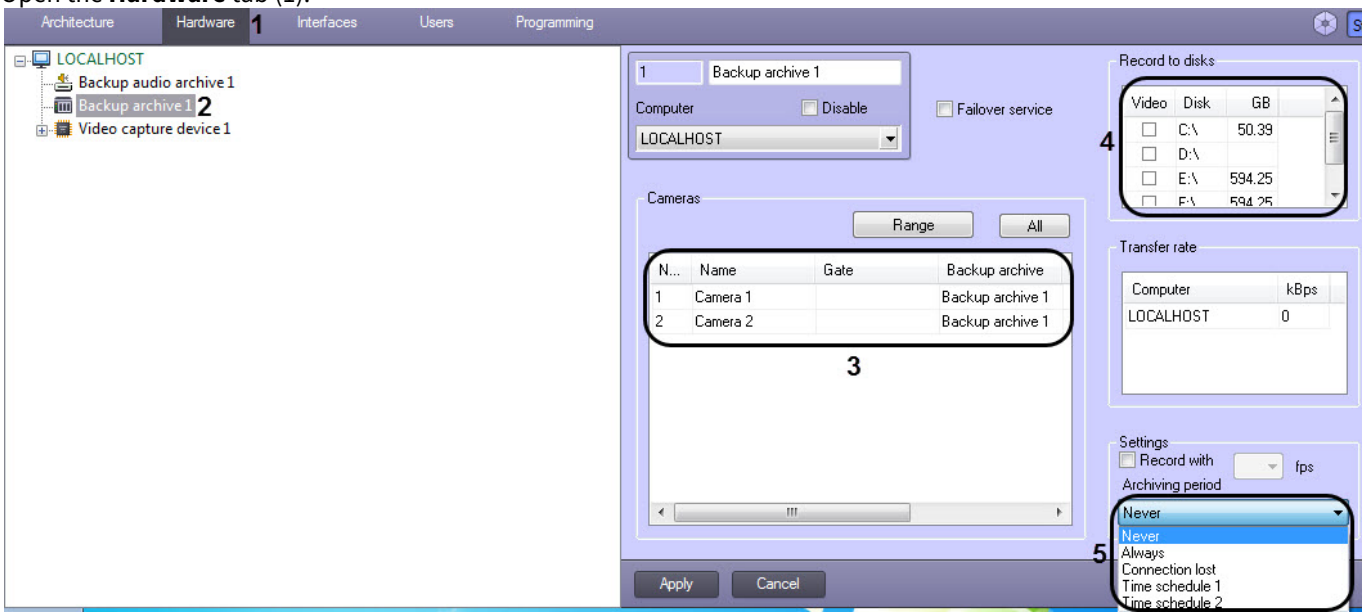
Example of a macro with a time schedule. Time schedule ending.



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).

10.6.7 Subdivision of the guarded location into areas and regions

10.6.7.1 About areas and regions

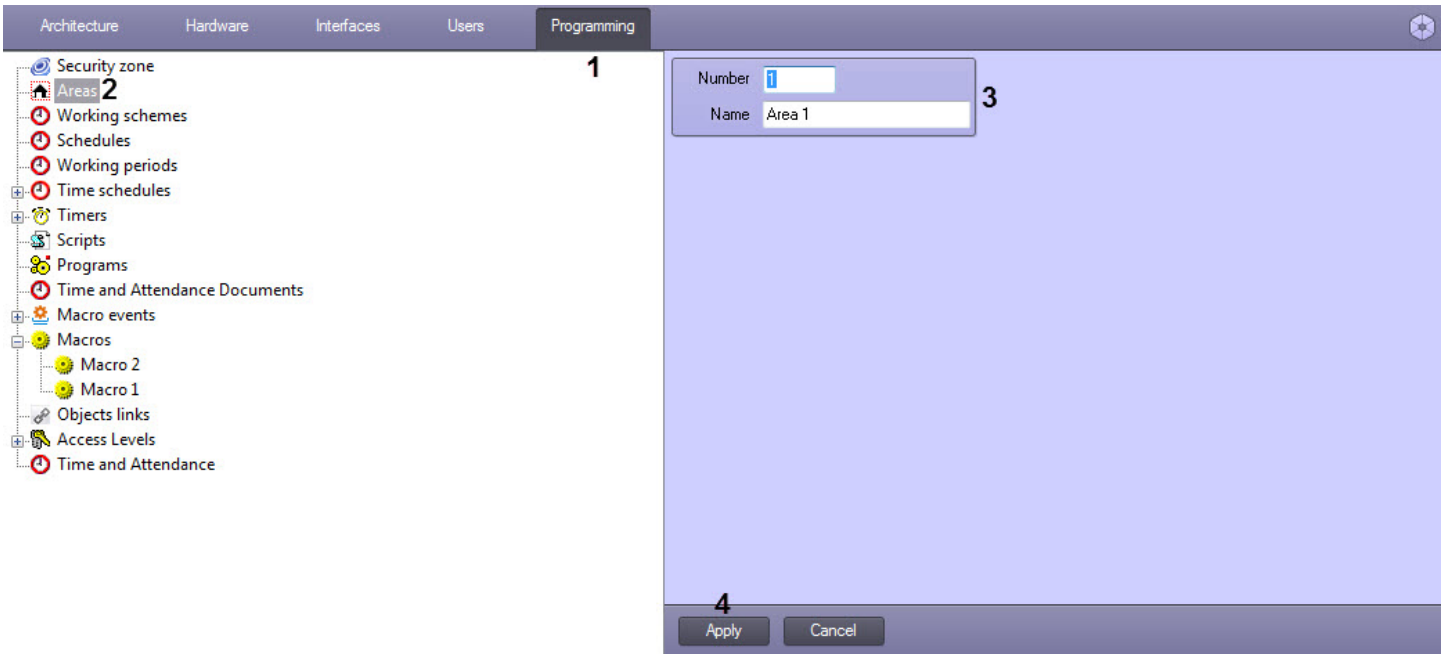
If the *Intellect* system is used to guard the large territory of complex topology (buildings, groups of buildings), we recommend to divide the whole territory into smaller zones. This allows to group relevant devices by location and makes it easier to view and control them, as well as to analyze the 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 guarded 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 guarded territory into areas and regions at the time of designing the video surveillance system, before the actual system configuration.

10.6.7.2 Creating areas

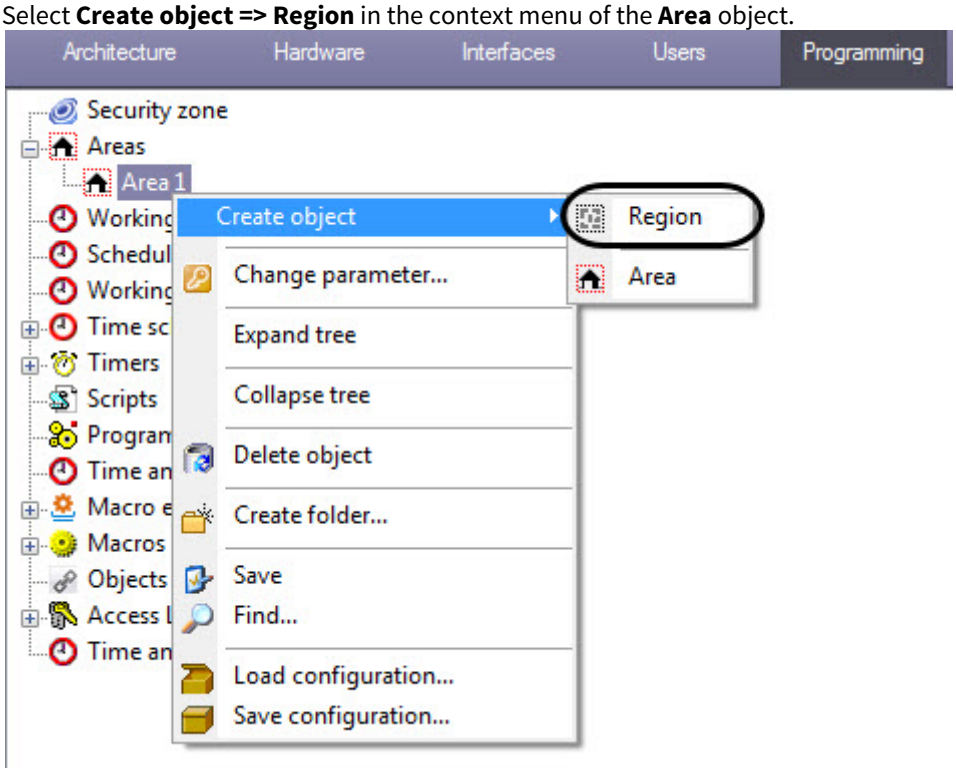
The areas are represented by **Areas** objects created in the **Programming** tab. The **Areas** object has no parameters of its own and is used to group the **Region** objects only. Figure below shows the process of creating an **Areas** object.



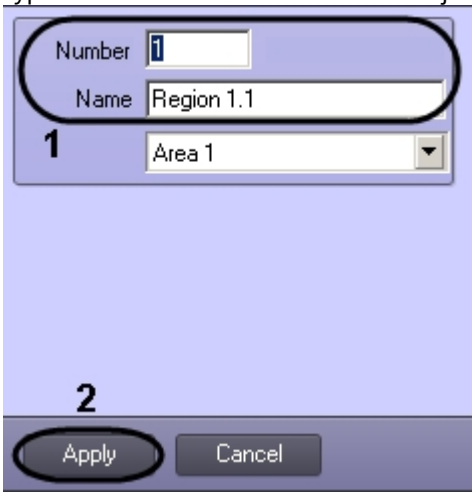
10.6.7.3 Creating regions

To create a region, do the following:

1. Create a **Region** object.
   a. Select **Create object => Region** in the context menu of the **Area** object.



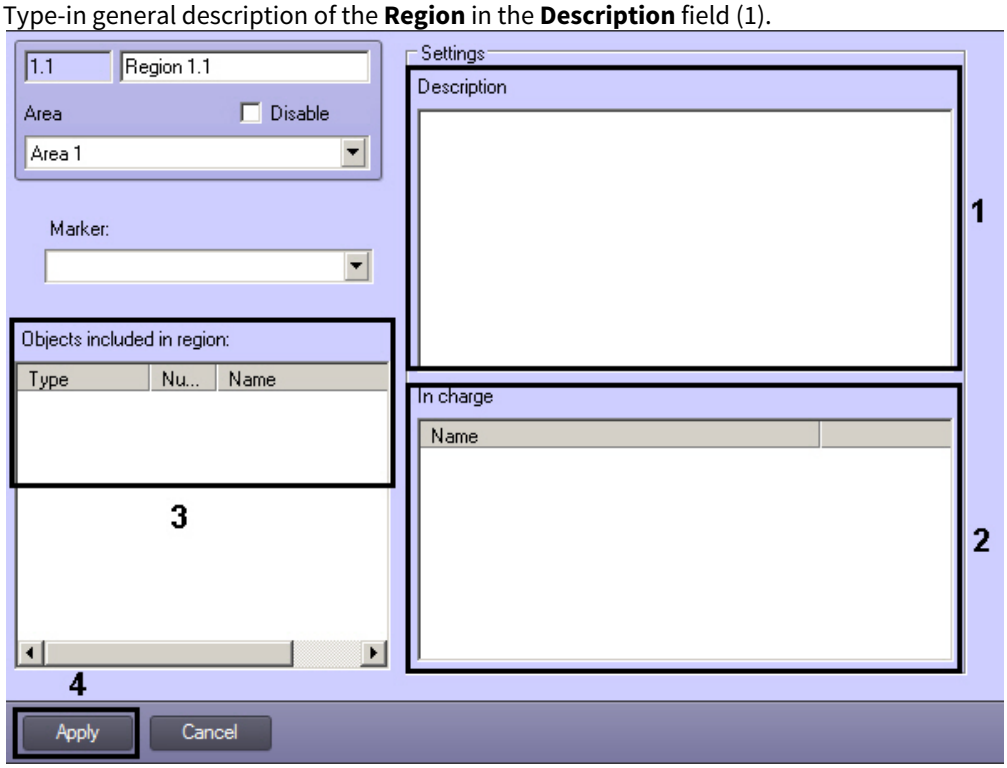
b. Type-in the number and name of the object in the corresponding fields (1).



c. Click the **Apply** button (2).

> **Note.**
>
> As a result the settings panel for the **Region** object appears.

2. Configure the created **Region** object.
   a. Type-in general description of the **Region** in the **Description** field (1).



   b. In the **Name** list of the **Responsible** table select the user responsible for this region (2).

> **Note.**
>
> The **Name** list consists of the usernames registered in the system (see User registration and removal section).

   c. To save the changes click the **Apply** button (4).

3. Create links between **the Region** object and objects in the **Hardware** tab that are to 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 section).

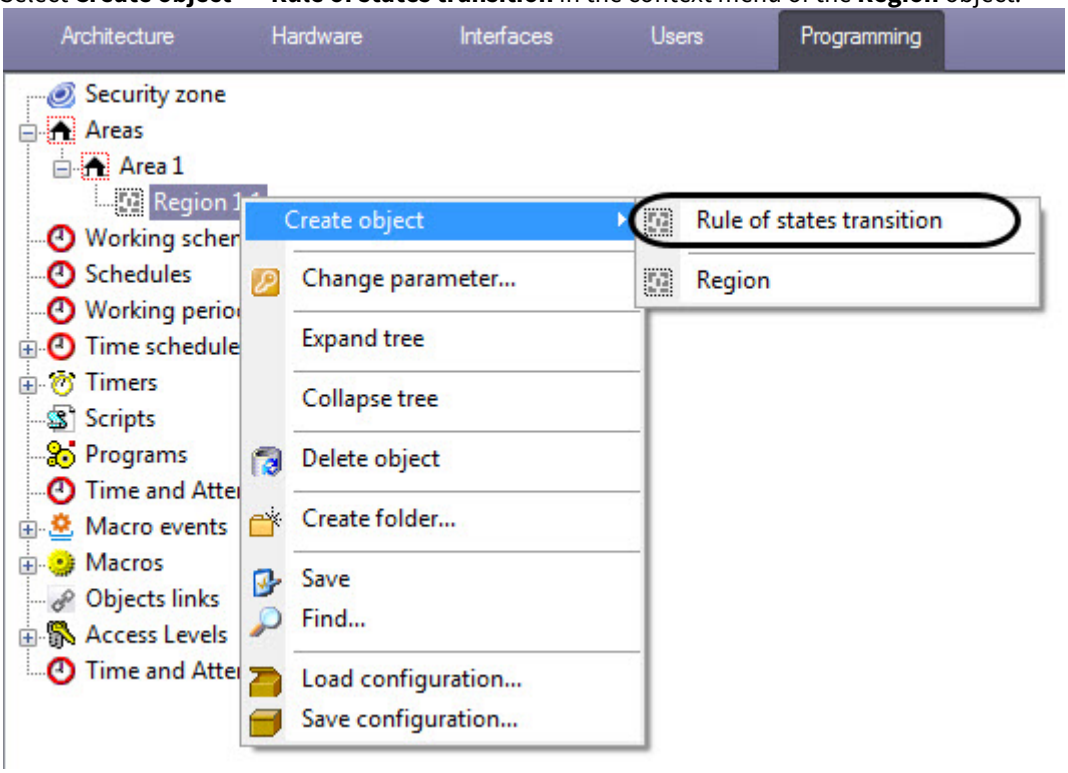
4. After creating the links listed above the list of objects added to the region is displayed in the **Objects included into region** table (3). This table cannot be edited.

The **Region** is now created.

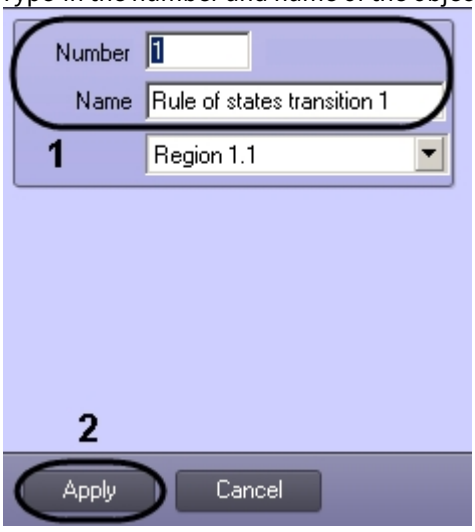
10.6.7.4 Creating rules of states transition

To create a rule of states transition, do the following:

1. Create a **Rule of states transition** object.
   a. Select **Create object => Rule of states transition** in the context menu of the **Region** object.



   b. Type-in the number and name of the object in the corresponding fields (1).

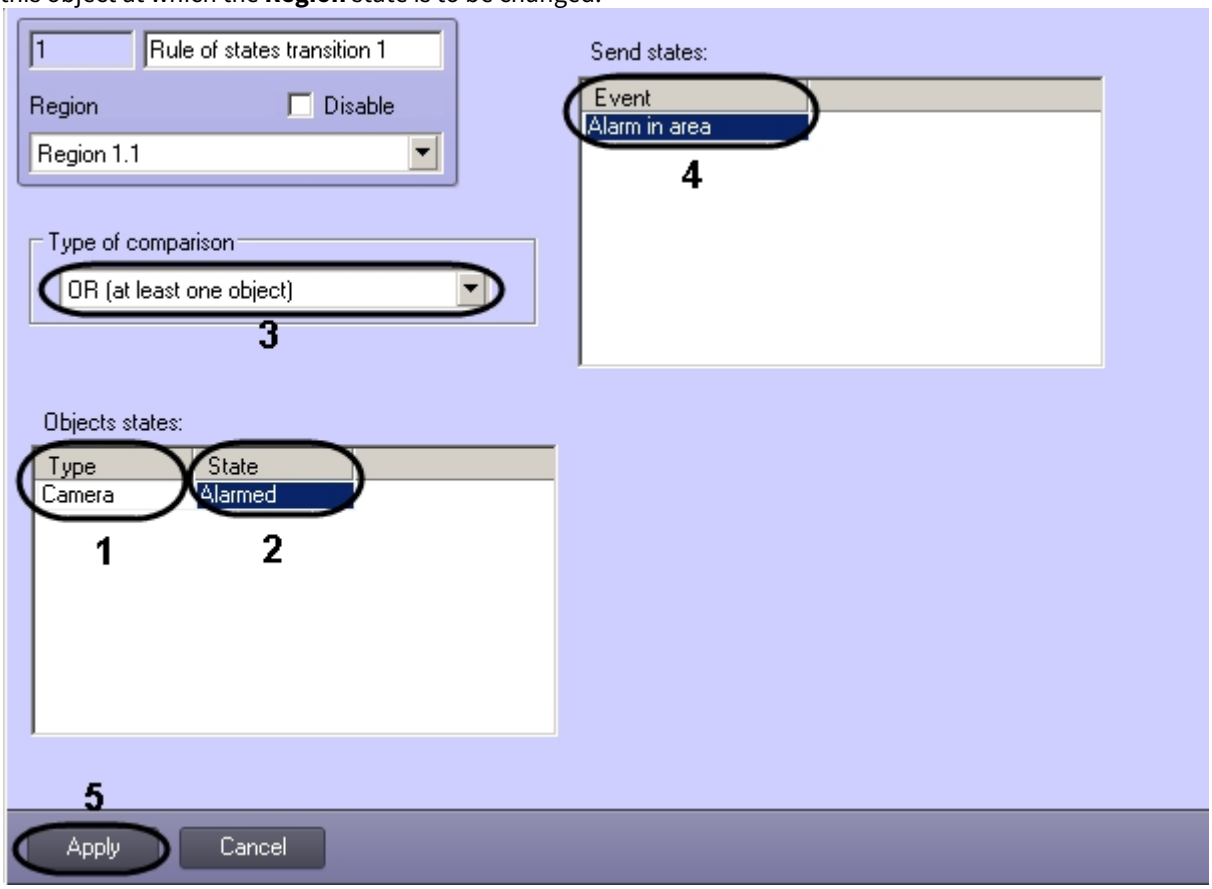


   c. Click the **Apply** button (2).

> **Note.**
>
> As a result the settings panel for the **Rule of states transition** object appears.

2. Set the condition of rule activation on the settings panel of the **Rule of states transition** object.

a. Select the object type in the **Type** list of the **Object's states** table (1) and in the **State** list (2) specify the state of this object at which the **Region** state is to be changed.



> **Note.**
>
> Repeat step 2.1 for all required object types.

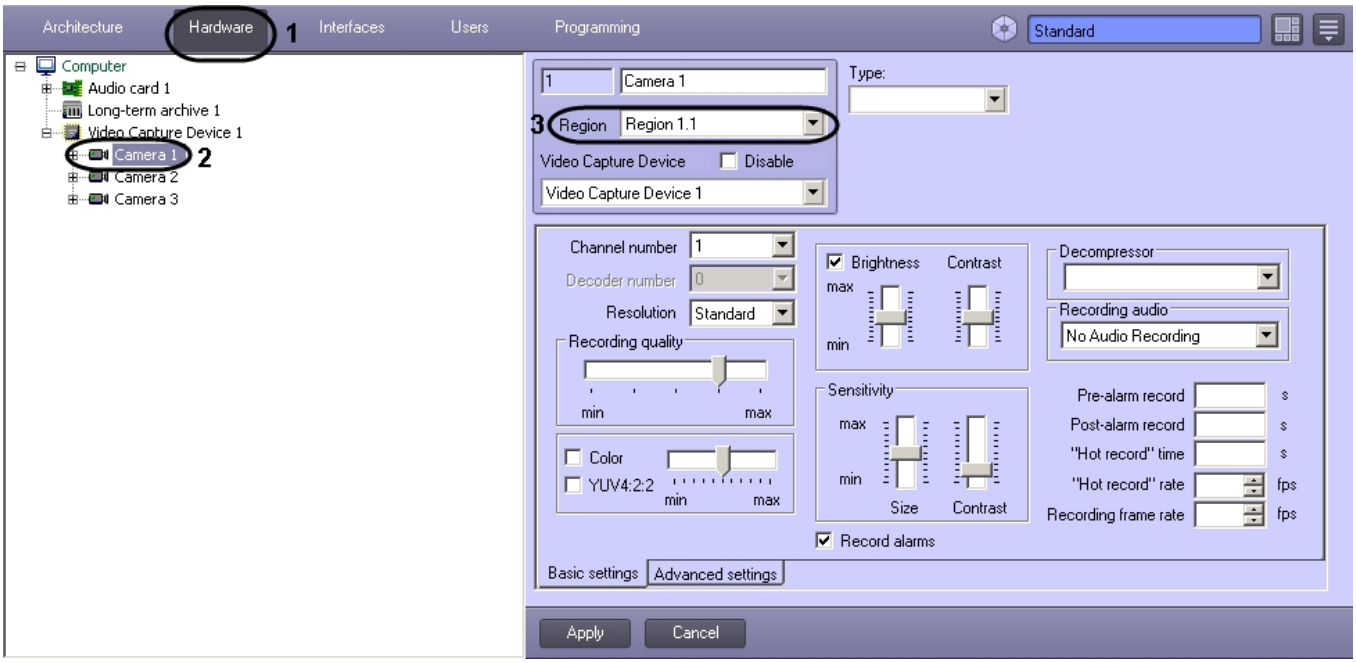
b. If the state of the **Region** is to be changed when all objects of types added to the **Object's states** table are in these states, select the **AND** (all objects) value in the **Type of comparison** list (3).
c. If the state of the **Region** is to be changed when at least one object of type added to the **Object's states** table is in this state, select the **OR** (at least one object) value in the **Type of comparison** list (3).
d. In the **Event list** of the **Send states:** table select the event generated by the **Region** object when the rule condition is met (4).
e. To save the changes click the **Apply** button (5).

The **Rule of states transition** is now created.

10.6.7.5 Examples of using areas and regions

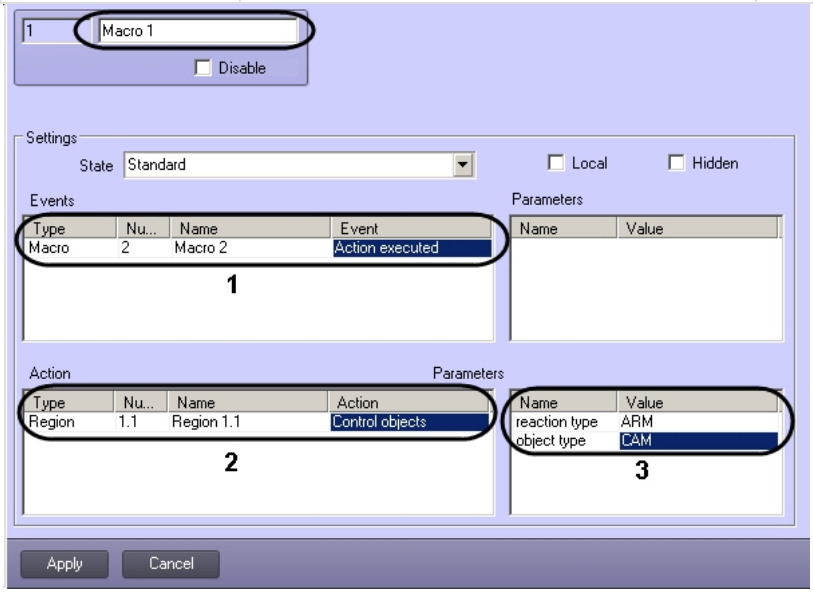
Example 1. The regions created in the system are used to group the system objects, representing the devices by their location on the secure territory.

To include a device into a Region, select an appropriate region in the **Region** field of the settings panel of the corresponding object.



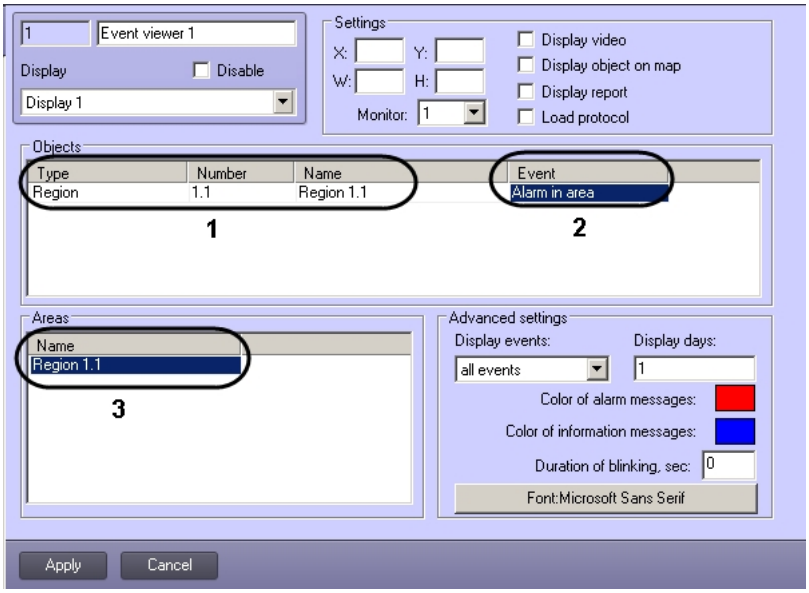
Example 2. Arming all cameras included into **Region** 1 when **Macro** 2 is run. Parameters of macro (**Macro** 1) essential for this operation are given in the table.

Event	Action	Parameters
Macro 2 is executed (1)	The **Control objects** action of **Region** 1 is executed (2)	Reaction type = «ARM» Object type = «CAM» (3)



Example 3. INTELLECT™ allows displaying reports about devices grouped in Regions.

Figure below shows the Event Viewer object configuration to display a report on the **Alarm in area** event on any of the devices in **Region 1**.


1
Event viewer 1
Display
Disable
Display 1
Settings
X:
Y:
W:
H:
Monitor:
1
Display video
Display object on map
Display report
Load protocol
Objects
Type
Number
Name
Event
Region
1.1
Region 1.1
Alarm in area
1
2
Areas
Name
Region 1.1
3
Advanced settings
Display events:
Display days:
all events
1
Color of alarm messages:
Color of information messages:
Duration of blinking, sec:
0
Font:Microsoft Sans Serif
Apply
Cancel

11 The Report System

11.1 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:

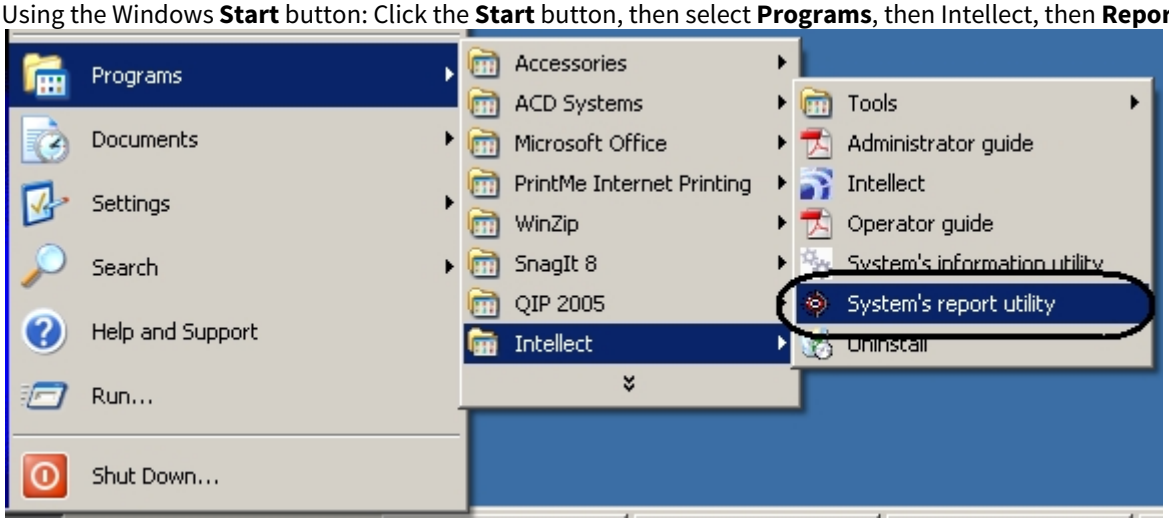
1. Selecting the objects (or groups of objects) from those available for reporting (objects include hardware and software modules).
2. Selecting the events to be included in the report for each object selected.
3. Creating the report templates.
4. Creating the screen reports.
5. Creating the printed 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.

11.2 Starting and shutting-down the Report system

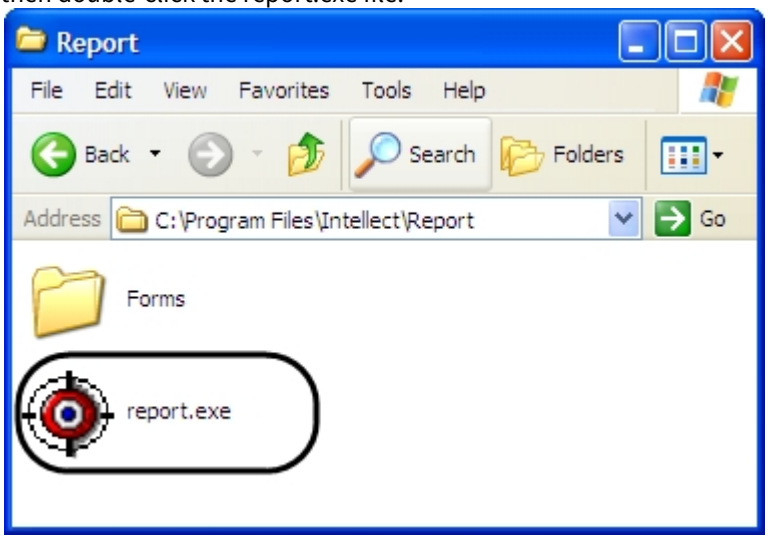
11.2.1 Starting the Report system

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**.

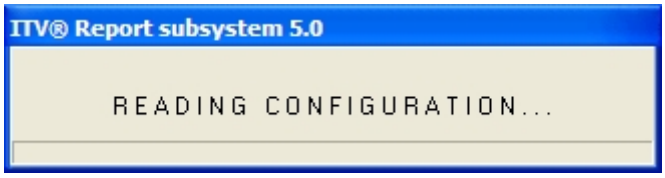


2. Using the program folder of the *Intellect* software: open the **Report** folder in the program folder of the *Intellect* system, then double-click the report.exe file.



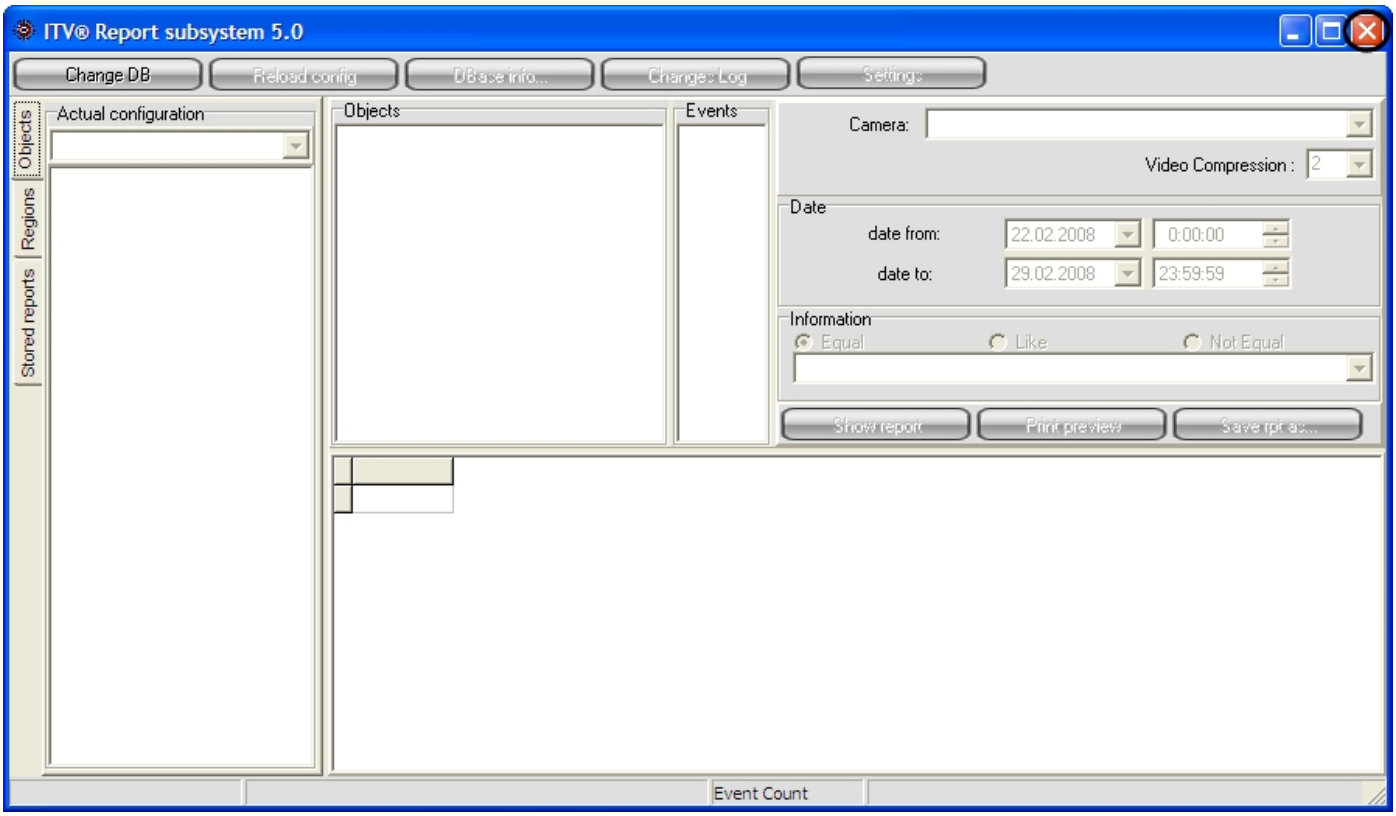
The Report system will start.

The notification window will appear, indicating that the system configuration is being read from the database.



11.2.2 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.

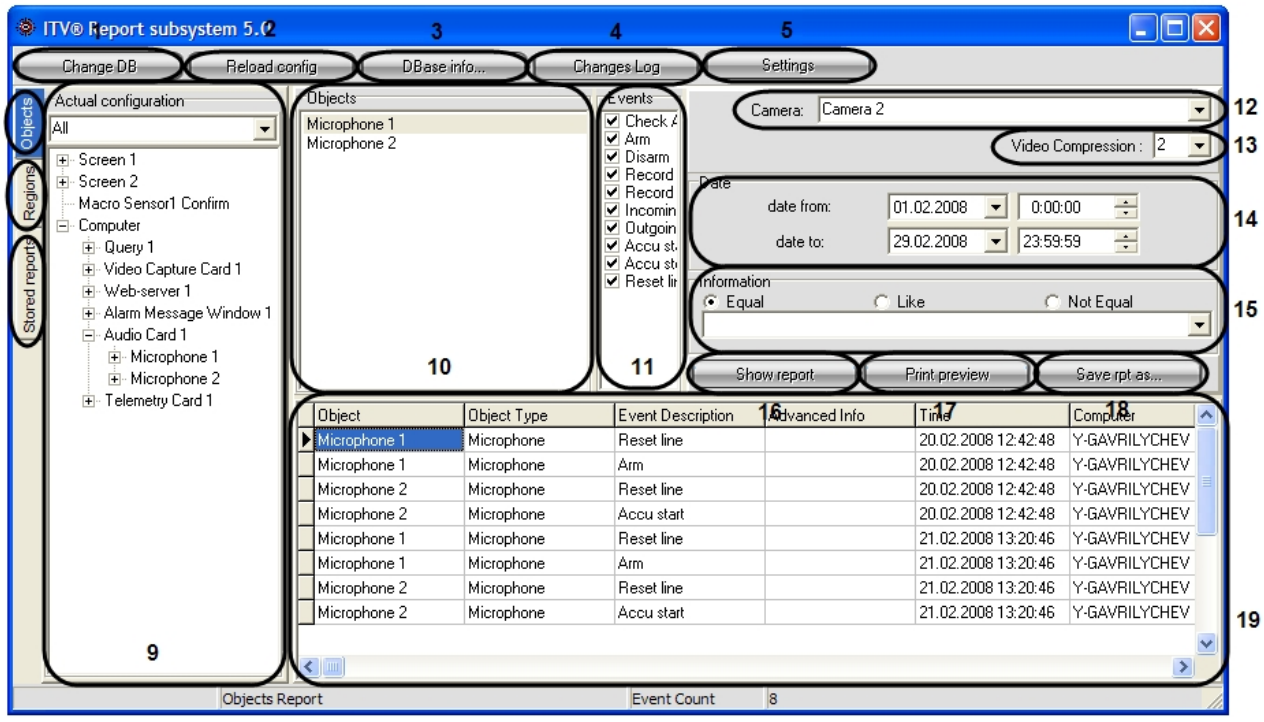


The Report system window will shutdown.

11.3 The Report window

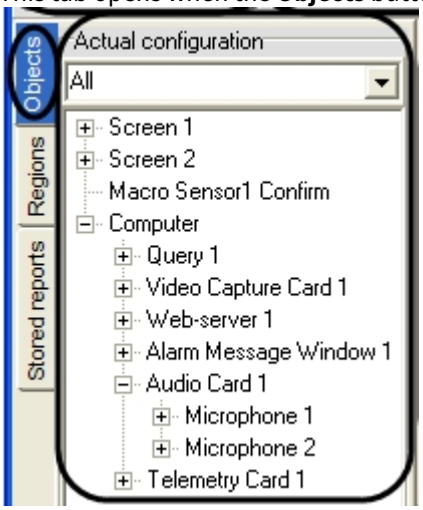
The Report system window contains the following sections: the main control panel, the report creation panel, and the report view panel.

Figure below shows an example of the Report window.

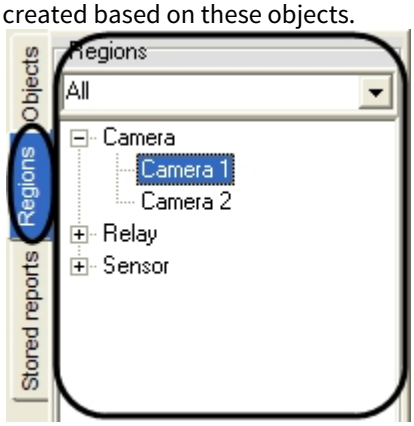


The Report window includes the following interface elements (numbered according to the screenshot on the figure):

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.

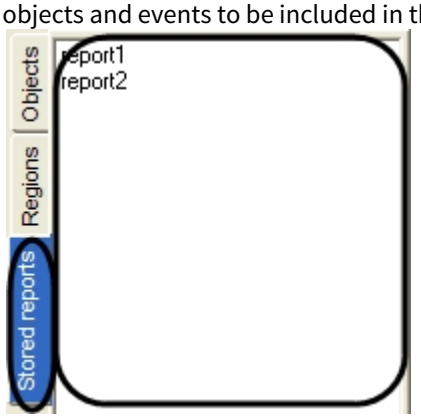


   The **Regions** button opens the **Regions tab** allowing to select the objects in the chosen region. The reports are then created based on these objects.



   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).

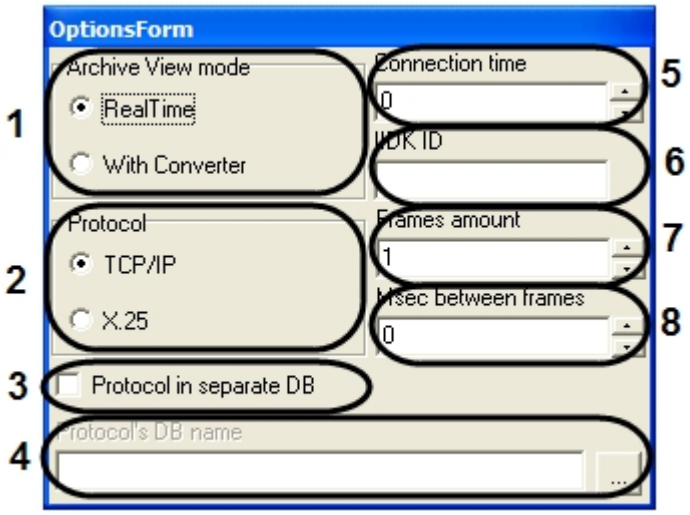
> **Note.**
>
> If the screen report has not been created before the printed report is activated, the screen report is automatically created.

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.

11.3.1 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.

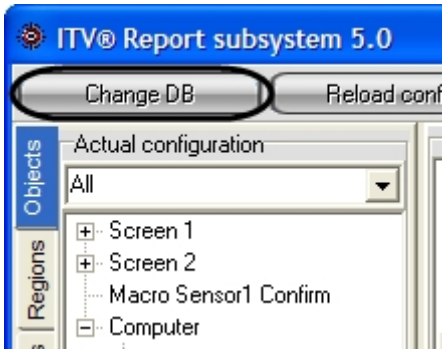
11.4 Connecting to databases

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.

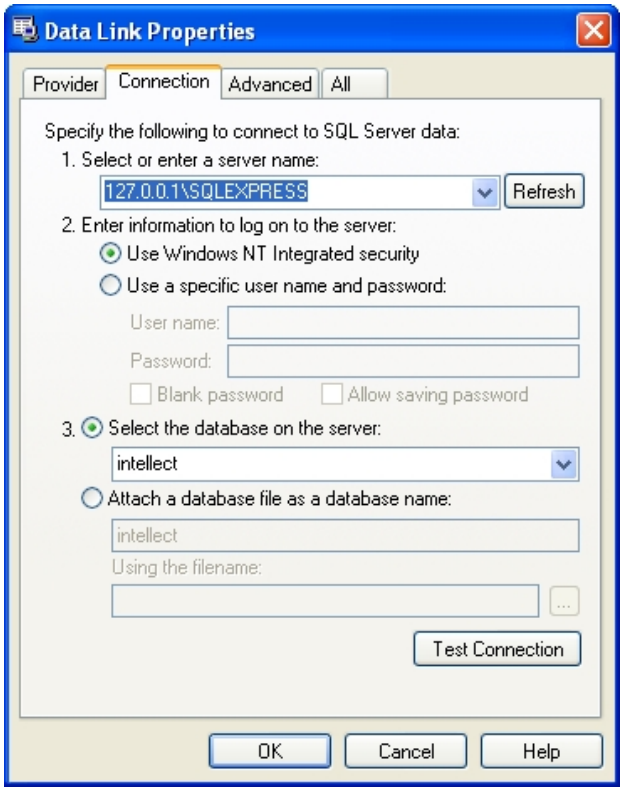
11.4.1 Connecting to the main database of the Intellect system

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.



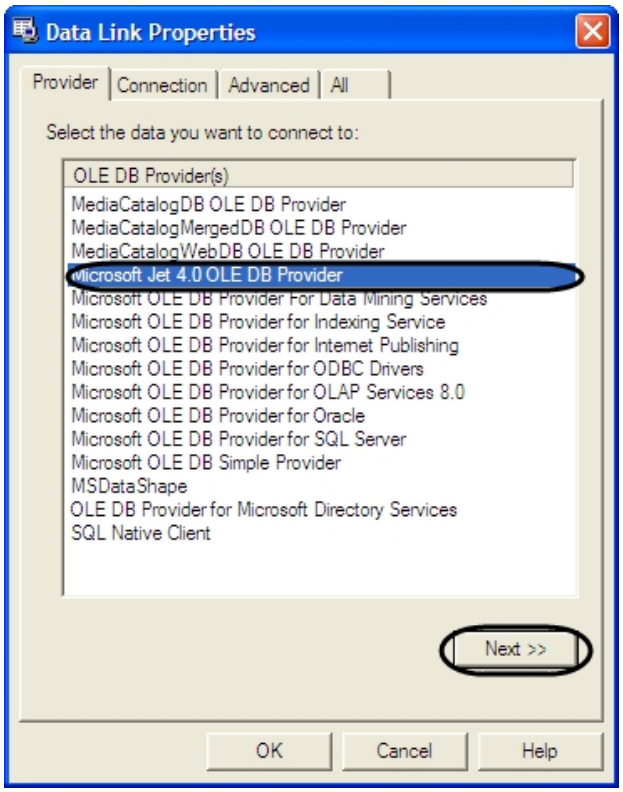
The *Intellect* system uses two types of database: SQL and Access. The connection procedure for each database type is described below.

11.4.1.1 Selecting an Access database and setting up the connection

This section describes the connection to an Access database as the main *Intellect* database.

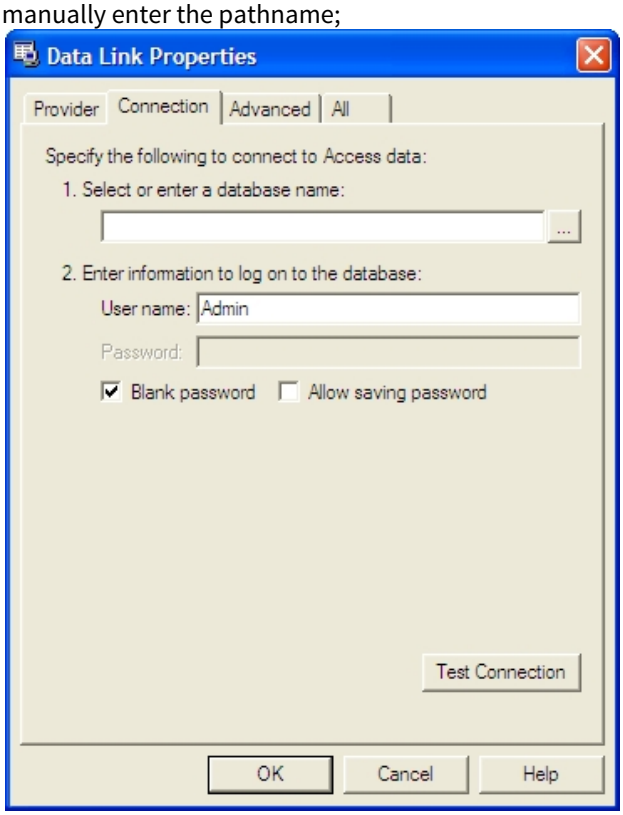
To connect to an Access database, open the **Data Link Properties** window. To set the main database in the Access format, do the following:

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.

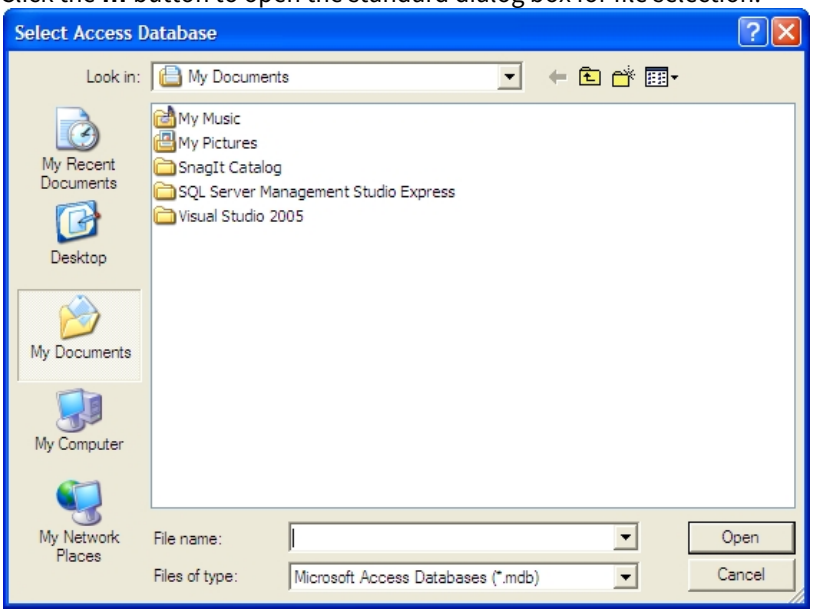


2. Select or enter the pathname of the database file in the **Select or Enter a Database Name** field of the **Connection** tab. To enter the pathname, do one of the following:

a. manually enter the pathname;

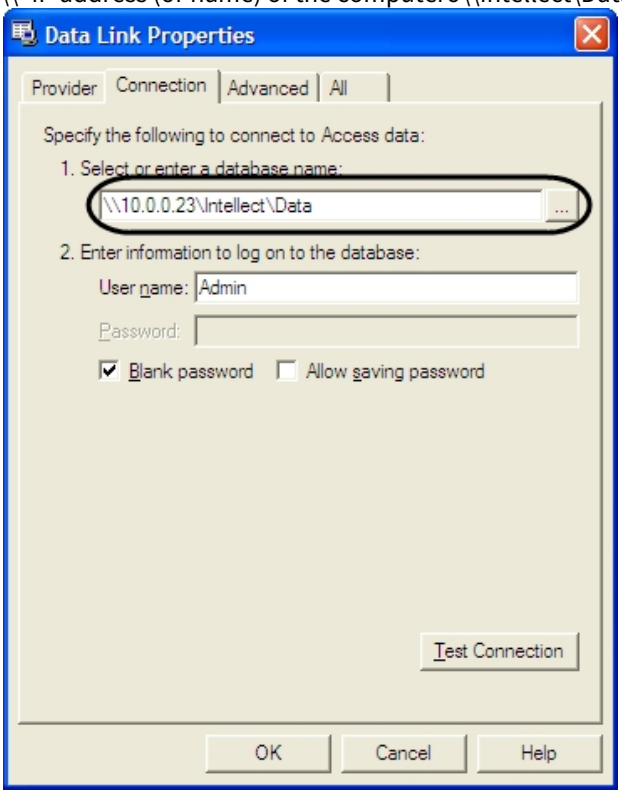


b. Click the **...** button to open the standard dialog box for file selection.

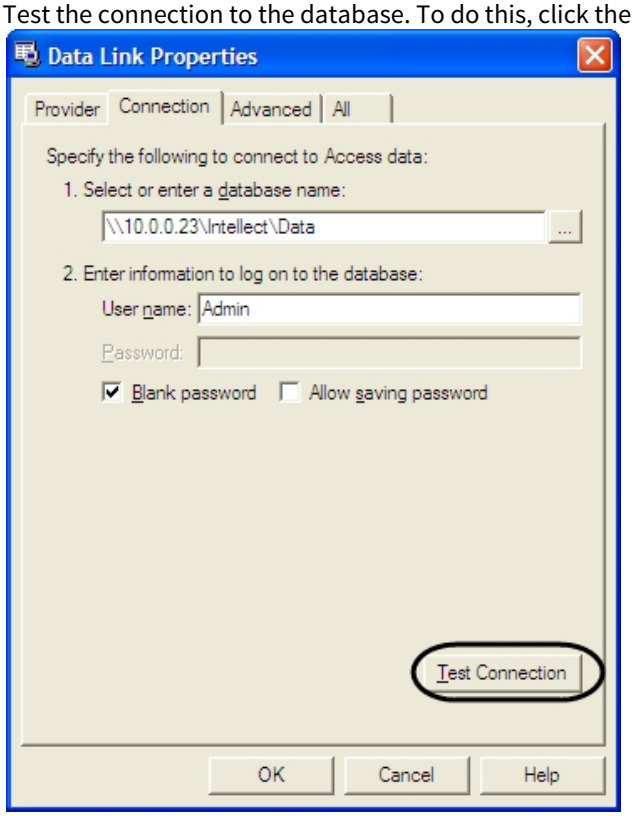


c. To connect to the main Access database located on the remote computer, the pathname should have the following format:

\\<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.

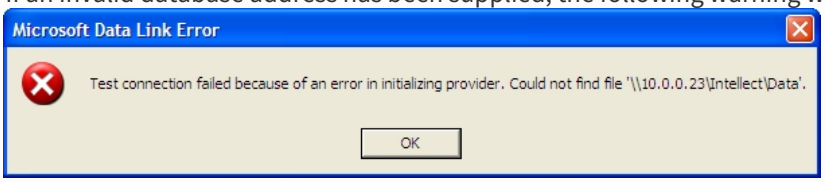


4. The information box with the text **Test connection succeeded** will appear in case of successful connection.



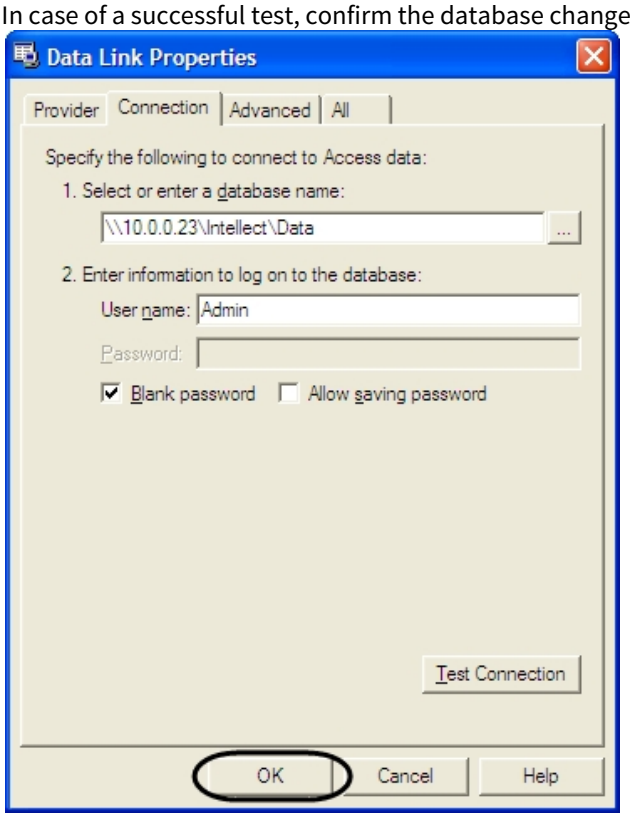
5. An information box with the error description will appear in case of a connection error.

> **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.



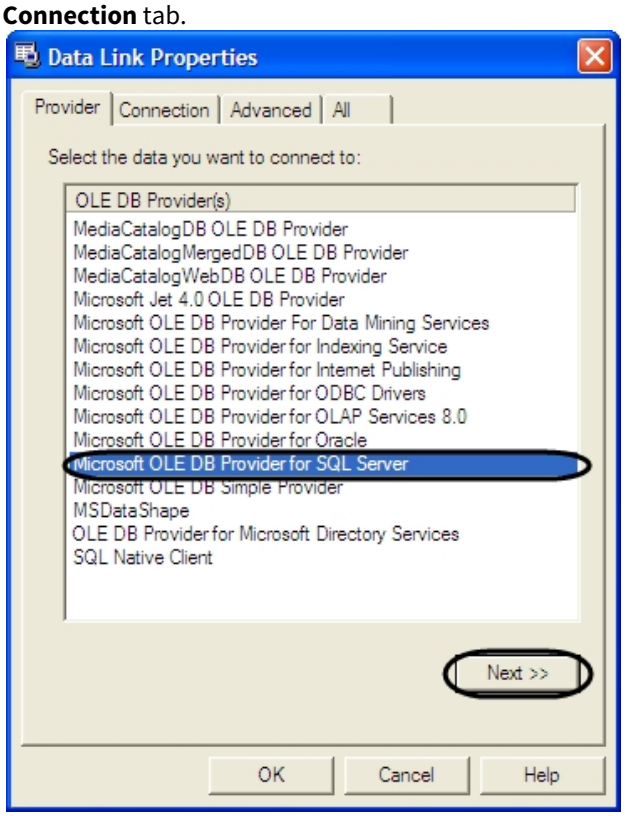
This completes the selection of the main database in Access format. The information from the selected database is now loaded into the Report system.

11.4.1.2 Selecting an SQL database and setting up its parameters

This section describes the connection to a Microsoft SQL database as the main *Intellect* database.

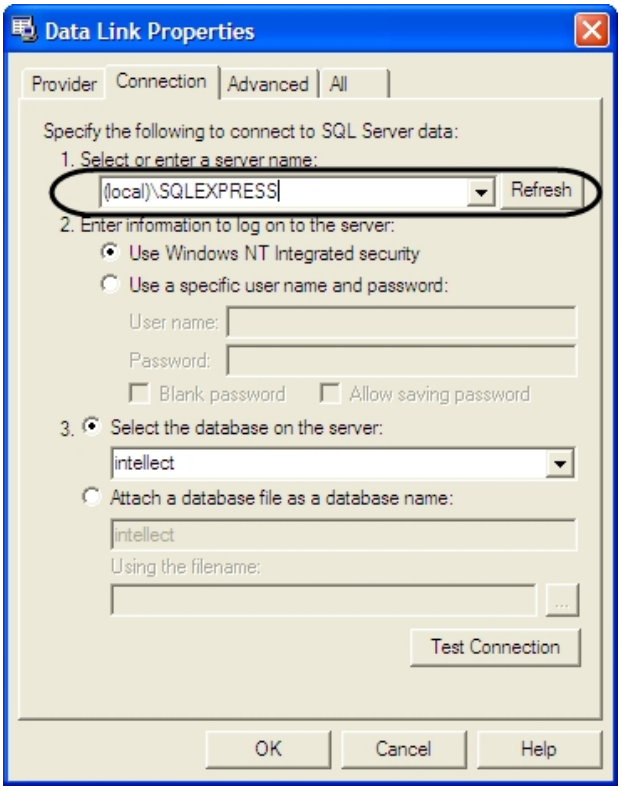
To connect a Microsoft SQL database, open the Data Link Properties window. To set the main database in Microsoft SQL format, do the following:

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.

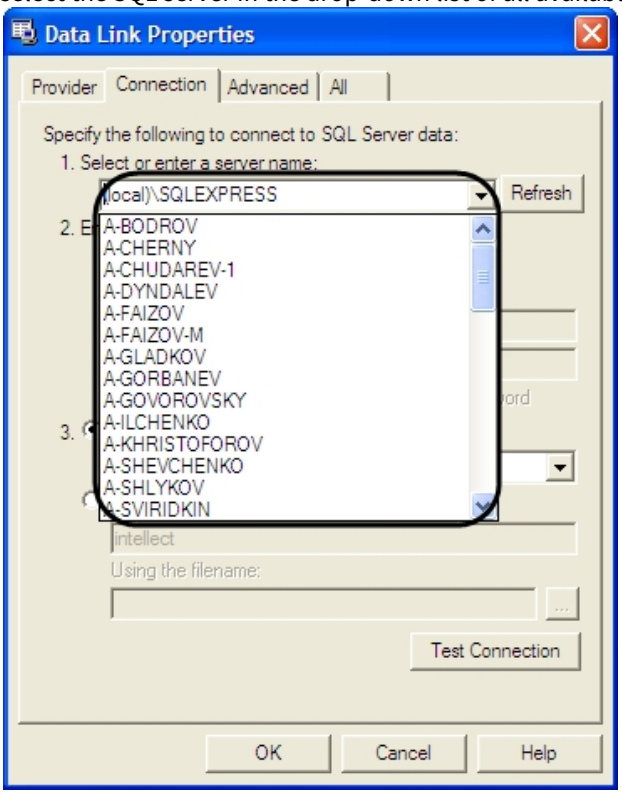


2. Specify the name of the database SQL server in the **Connection** tab. This can be done using the **Select or Enter a Server Name** field.
   To enter the SQL server name, do one of the following:

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.

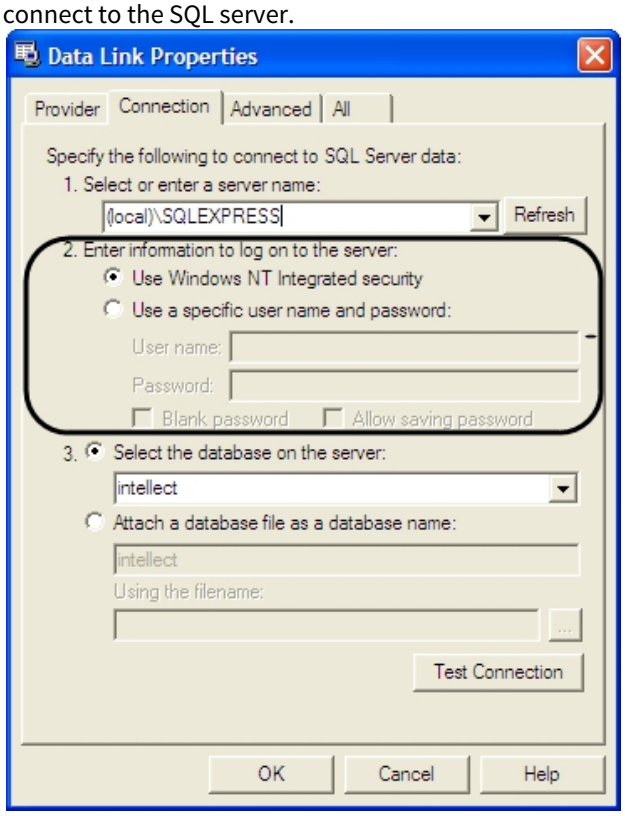
By default, the local server is selected named <local>\SQLEXPRESS.

> **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.

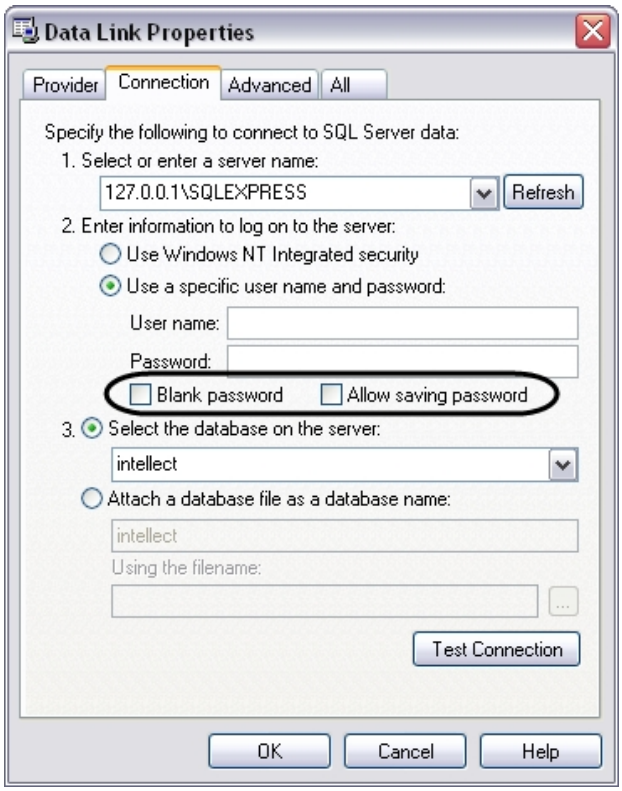


4. When the **Use Specific User name and Password** radio-button is selected, enter the information into the following fields: **User Name** and **Password**.

> **Note.**
>
> By default, the following information is set up during Intellect software installation: user name “sa”, password “axxonsoft” (see the Installing INTELLECT™ software section).

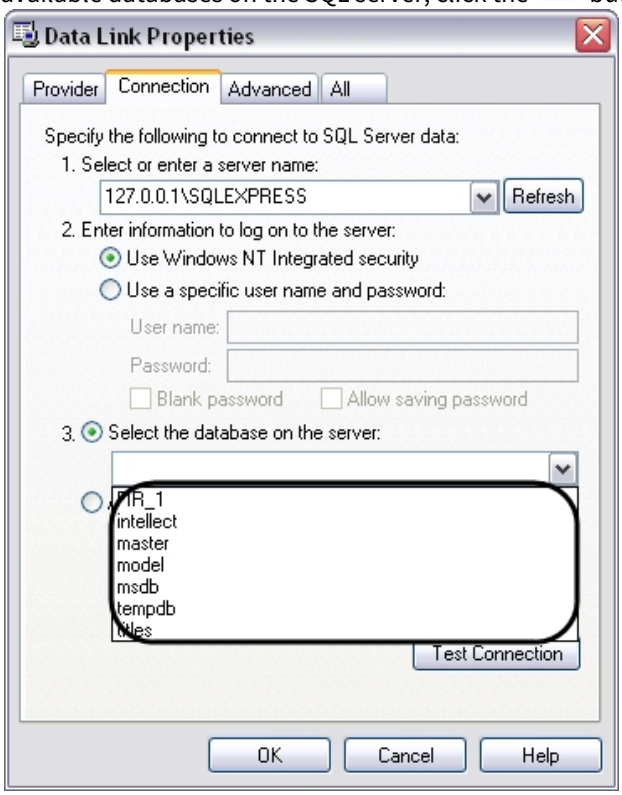
> **Note.**
>
> By default while installing the *Intellect* complex, the user(login) «sa» and Administrator password SQL Server (is registered while installing SQL Server, see Installing INTELLECT™ software) are set for authorization on SQL server

5. When the **Use Specific User name and Password** radio-button is selected, the **Blank Password** and **Allow Saving Password** checkboxes become enabled.



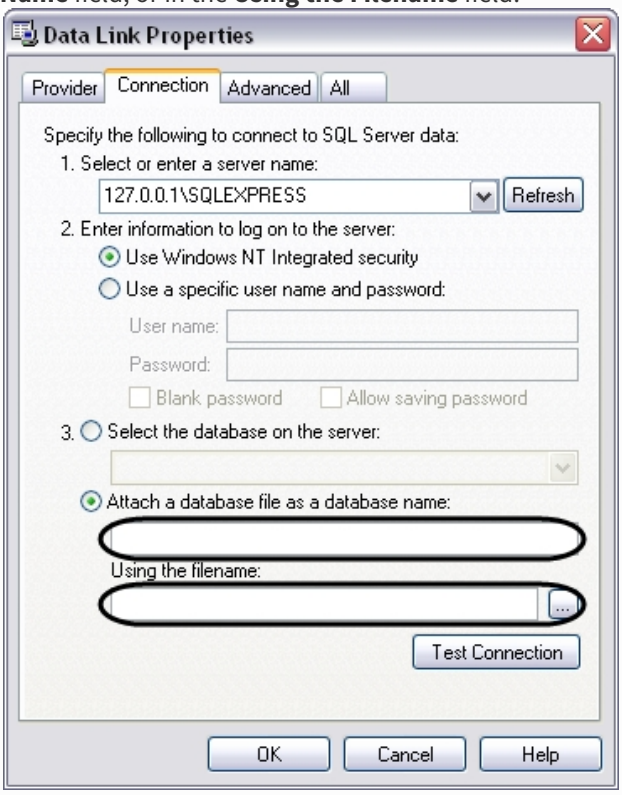
The **Blank Password** checkbox allows to enable connection to the SQL server with no password.
The **Allow Saving Password** button saves the password for the next connection to the SQL server.

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.

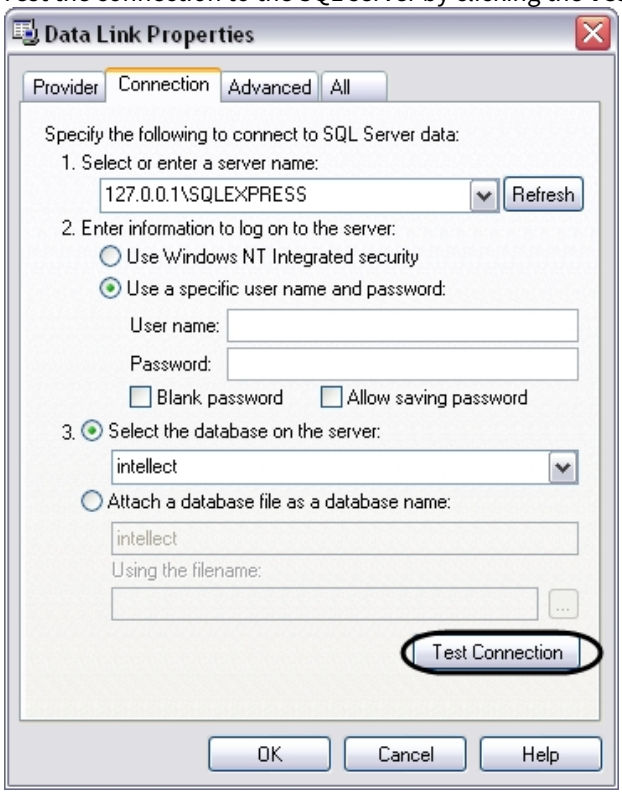


Note.

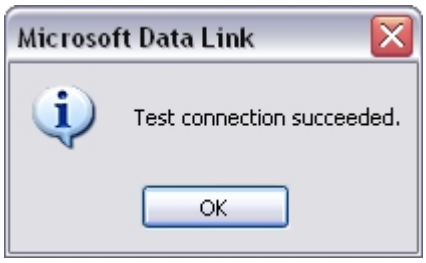
If necessary, the name of the database to connect to can be entered in the **Attach Database File** as **Database Name** field, or in the **Using the Filename** field.



7. Test the connection to the SQL server by clicking the **Test Connection** button.



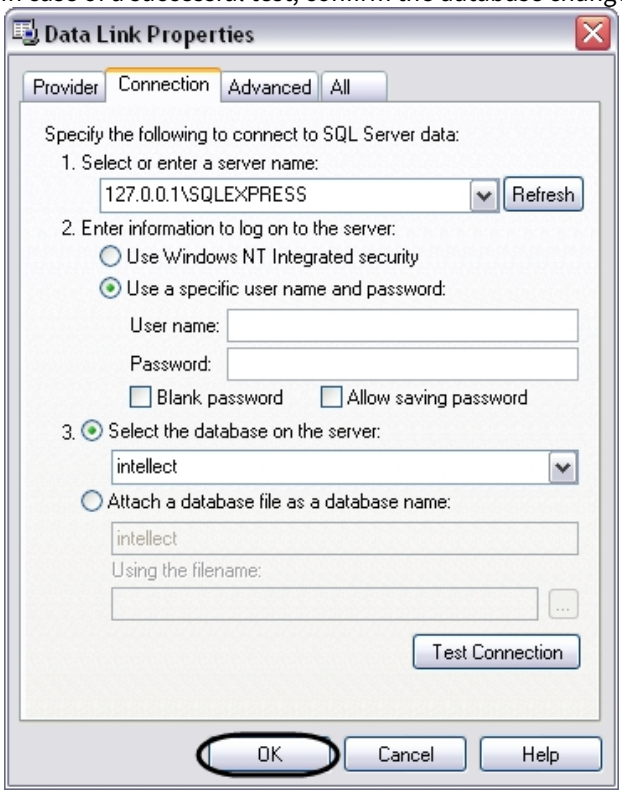
The information box showing the message "Test connection succeeded" will appear in case of successful connection.



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.



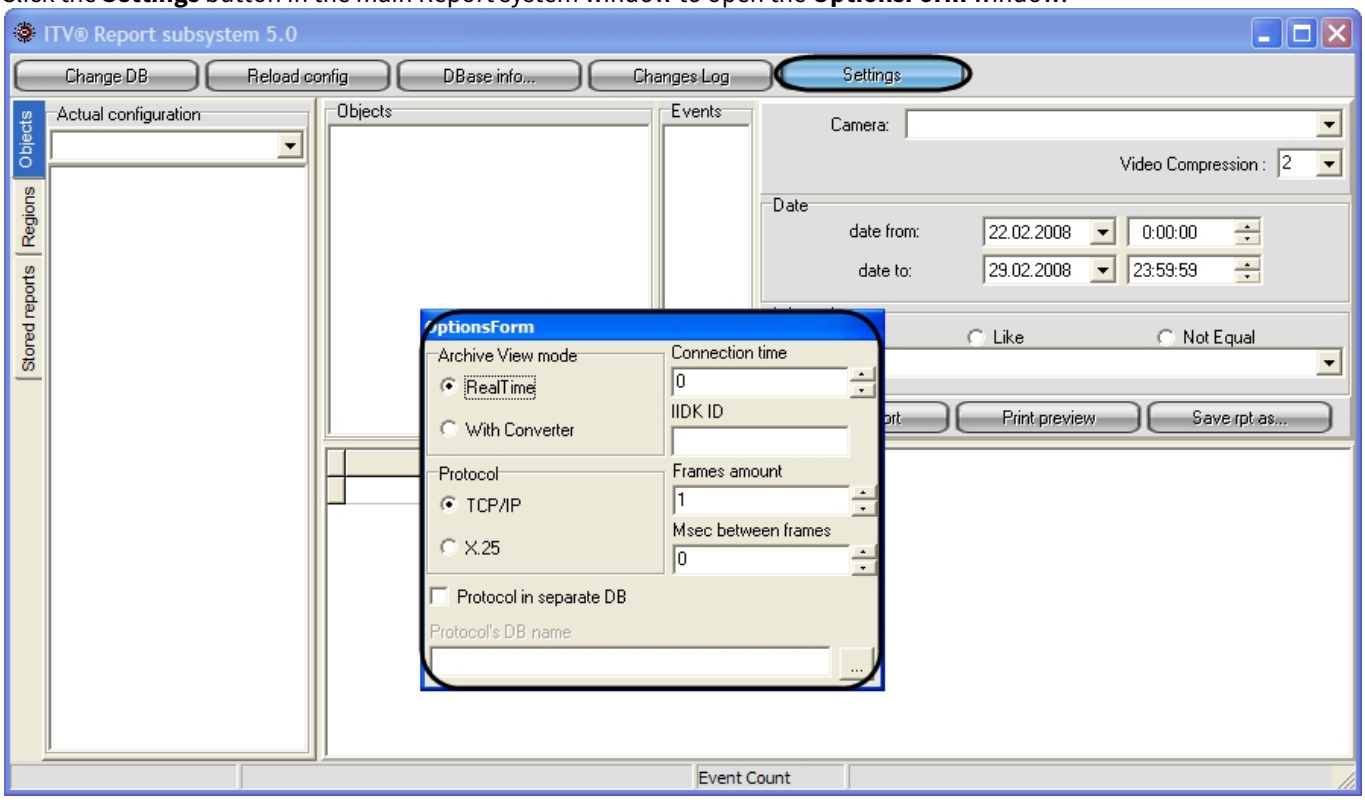
This completes the selection of the main database in Microsoft SQL format. The information from the selected database is now loaded into the Report system.

11.4.2 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).

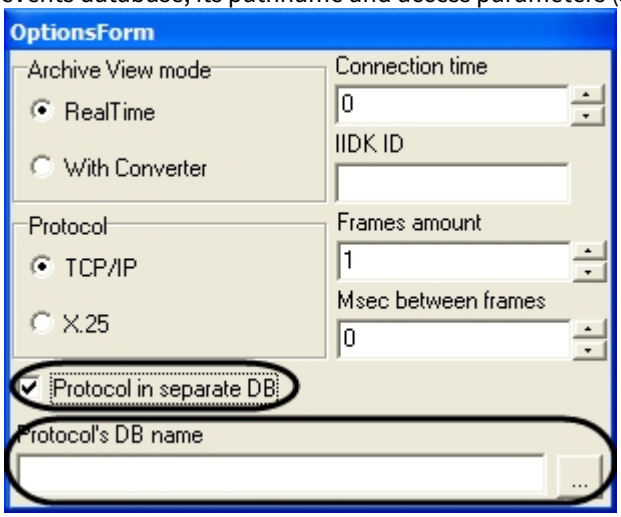
To connect the events database to the Report system, do the following:

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).



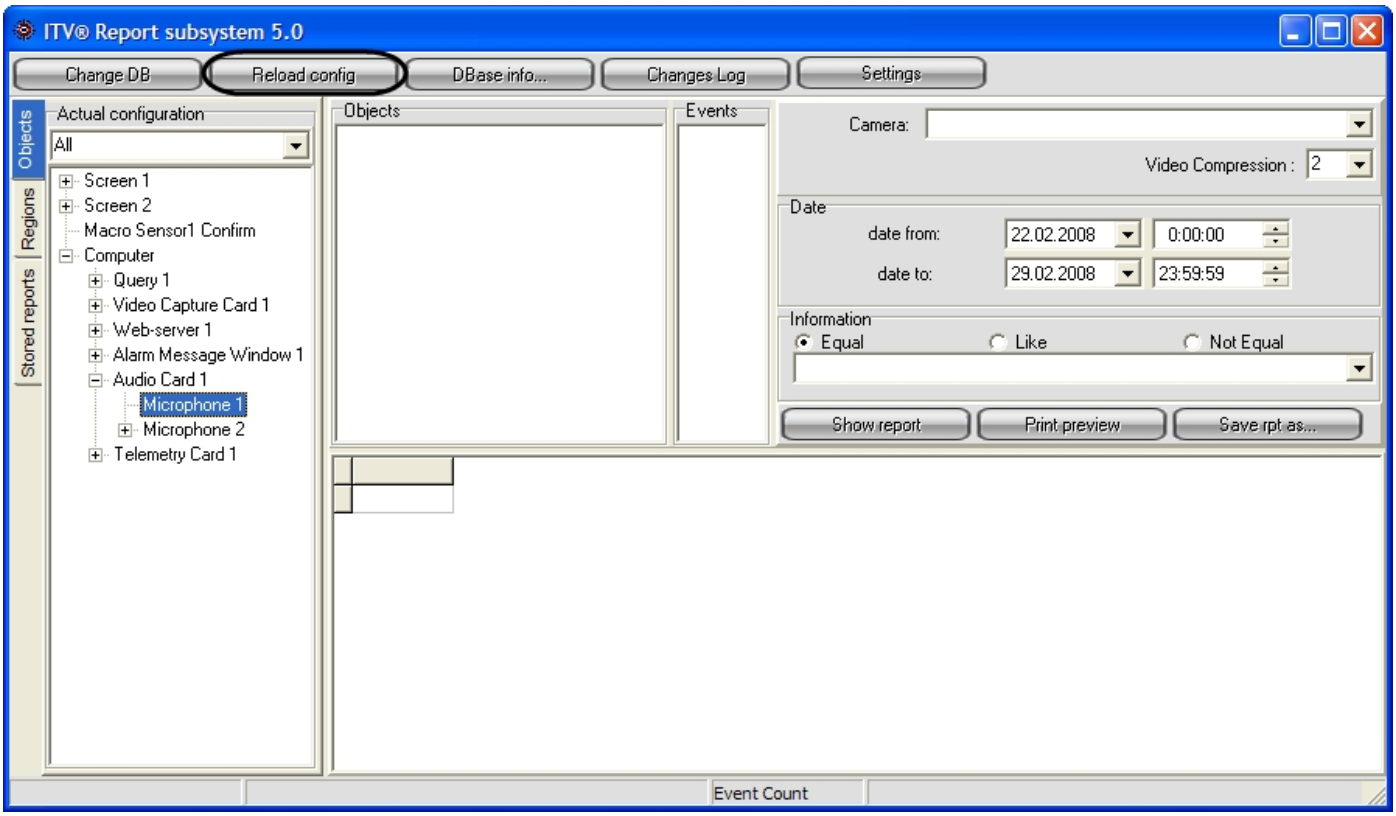
4. Press the **Escape** key on the keyboard to close the **OptionsForm** window.

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.

11.5 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.

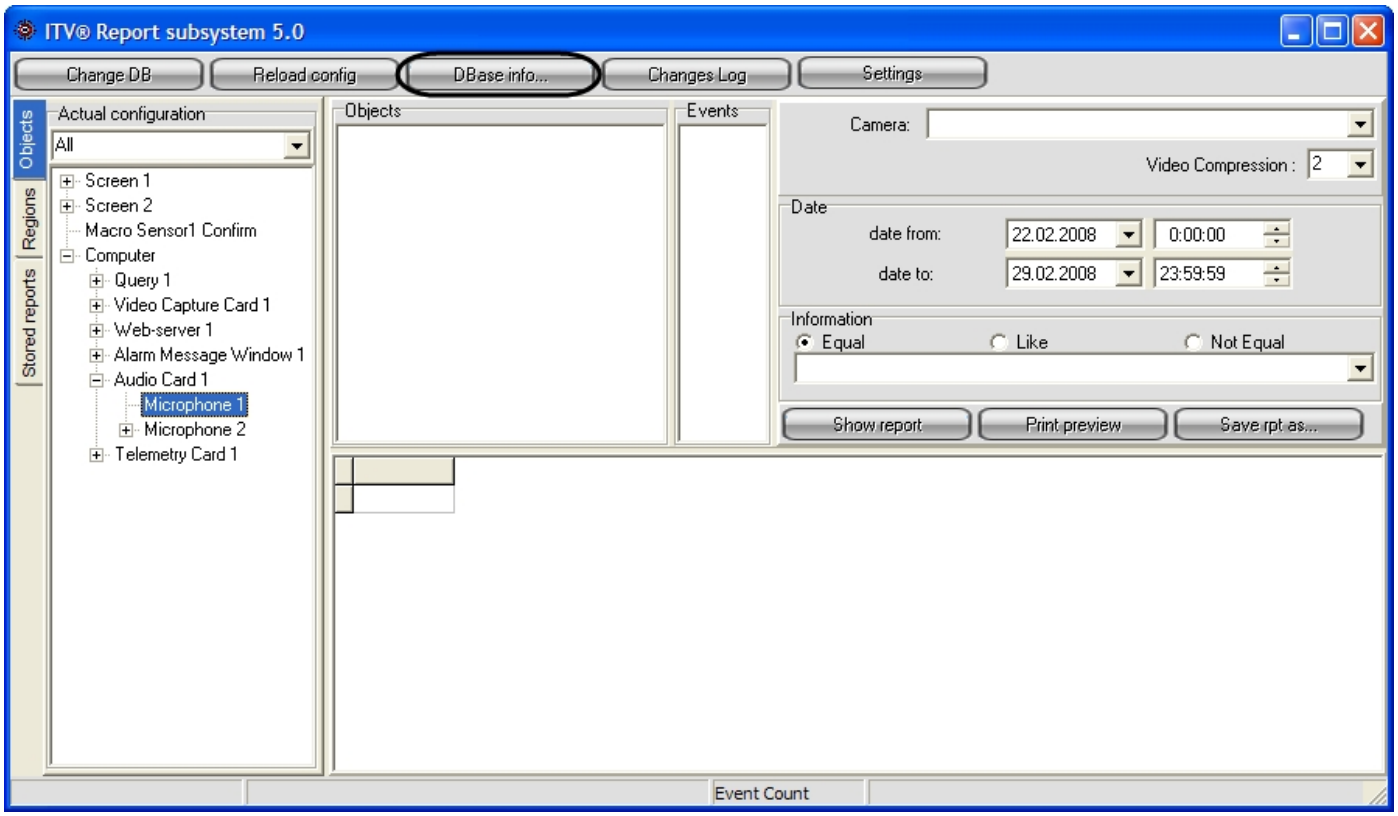
The configuration and events database can be loaded manually, as well. To reload the configuration and events database, click the **Reload Config** button on the main control panel of the Report window.



The objects tree, the regions list, the report templates list, and the registered events list will be refreshed according to the new system configuration.

11.6 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.



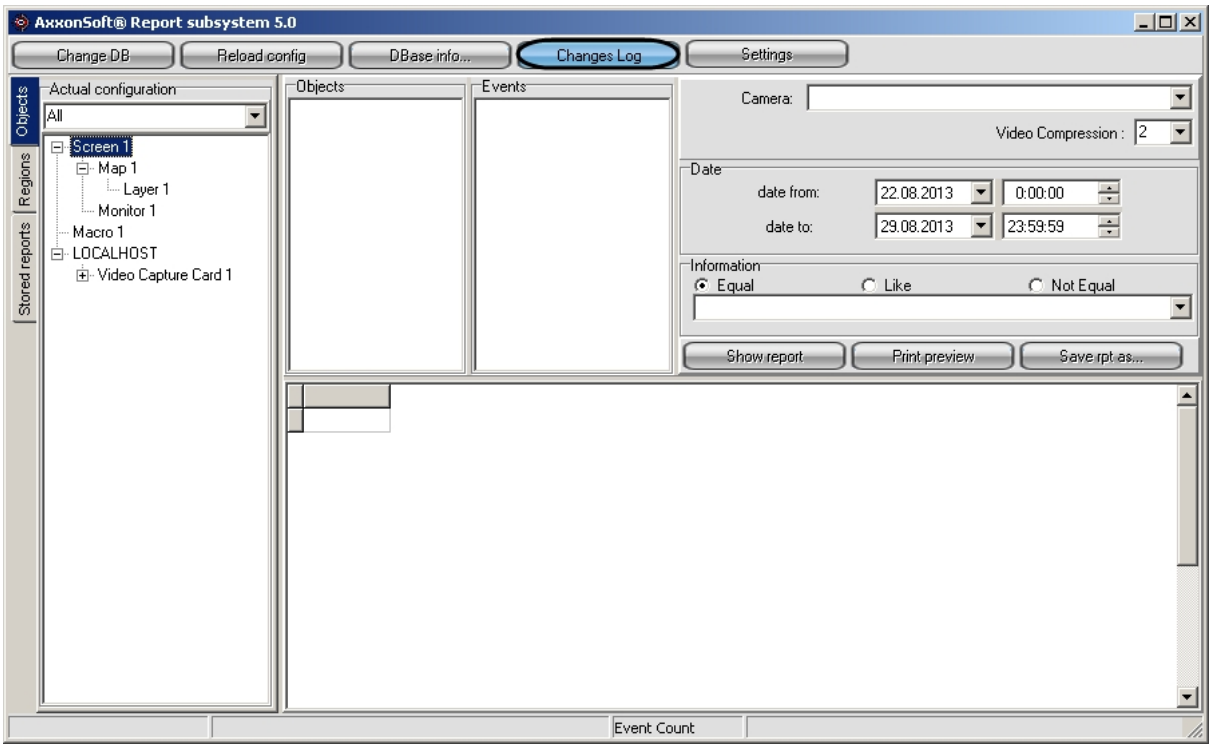
The following information is displayed:

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.

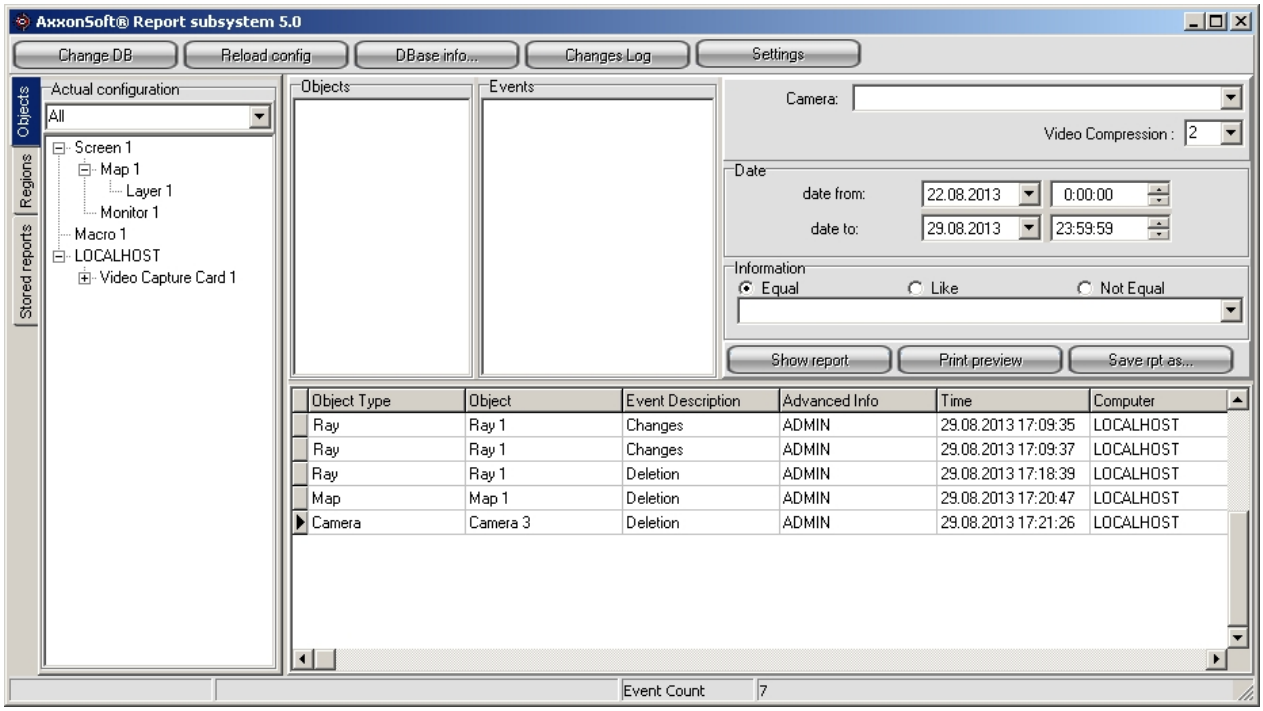
11.7 Creating the log of changes made to the system configuration

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.

11.8 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.

11.8.1 Recommendations for template creation

We do not recommend including too many objects in a template. If the template includes too many objects, the request on all events related to these objects, will take a very long time to execute, or will fail.

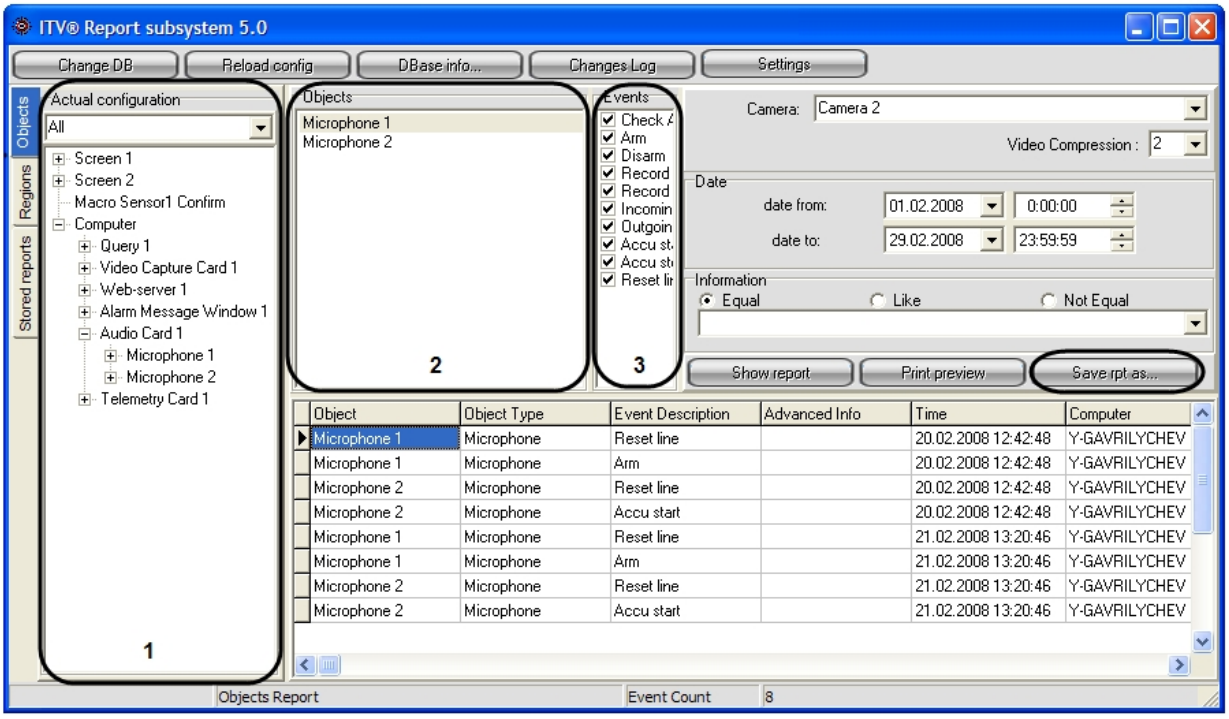
We recommend creating smaller templates that group the objects according to different regions of the guarded area.

We do not recommend including more than 200 objects in one template.

11.8.2 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.

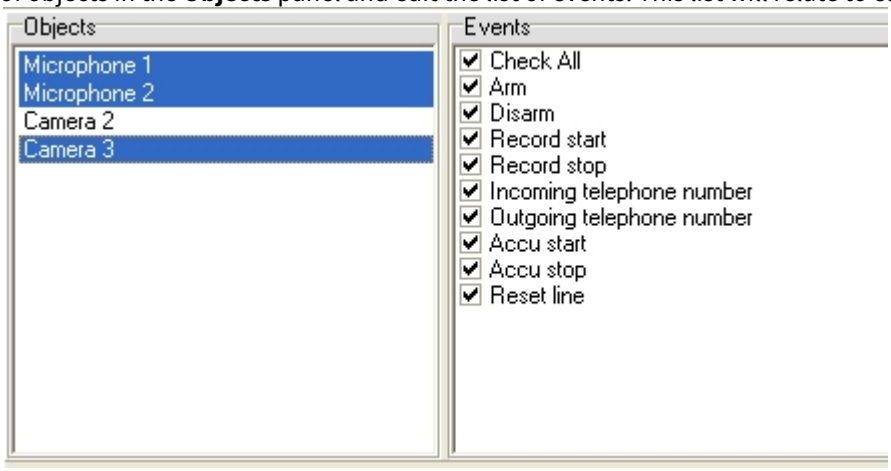
To select objects in regions, click the **Regions** tab and choose the required region type in the **Regions** drop-down list.

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.

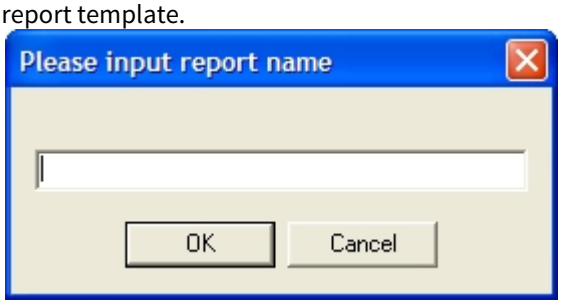
To remove the object from the report list, select the object in the **Objects** panel and press Delete on the keyboard.

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.

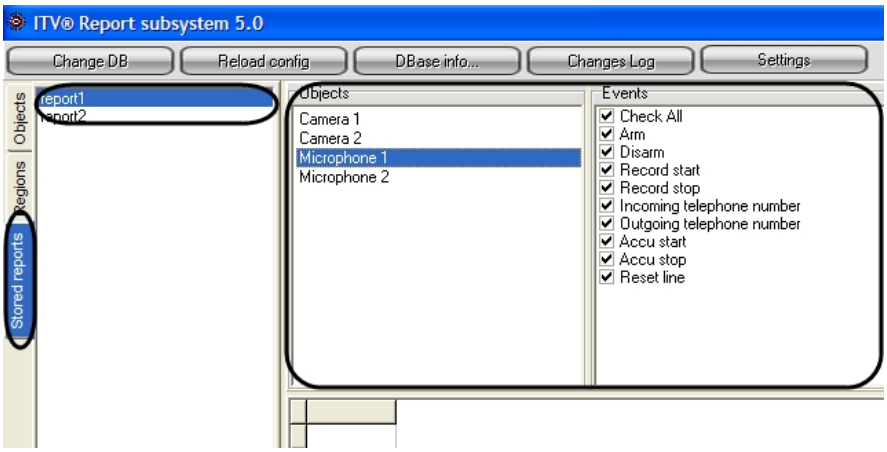
3. Click the **Save Rpt As** button. The **Please Input Report Name** dialog box will appear, allowing to specify the name of the report template.



   Type in the template name and click **OK**.

This completes the creation of the report template.

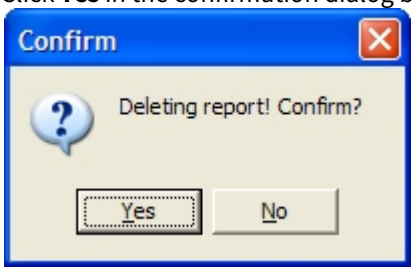
The template will appear in the objects tree of the **Shared Reports** tab. To view the template, use the **Objects** and **Events** panels. These panels are populated automatically upon template selection in the **Shared Reports** objects tree. These panels allow editing the events list and removing the objects from the list. The changes will be saved in the template.



11.8.3 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.

11.9 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.

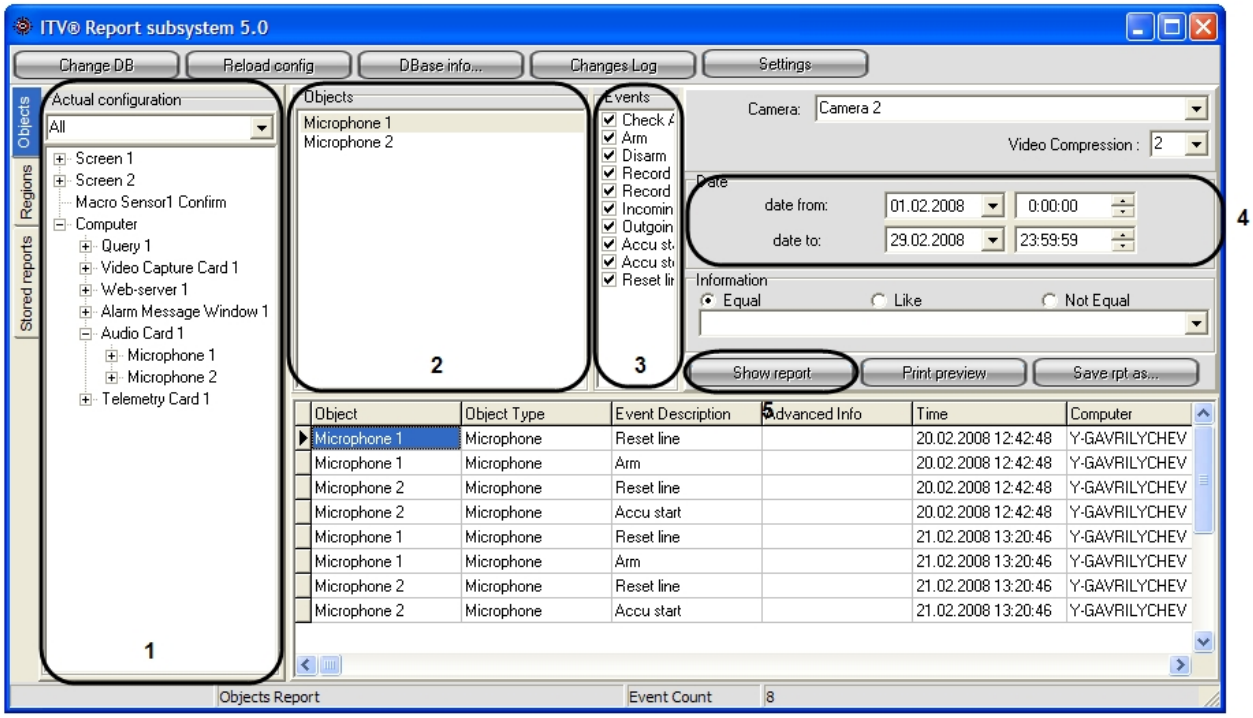
> **Note.**
>
> The playing of the recording in the surveillance window is possible if the *Intellect* software is running on the videoserver.

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.

11.9.1 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.



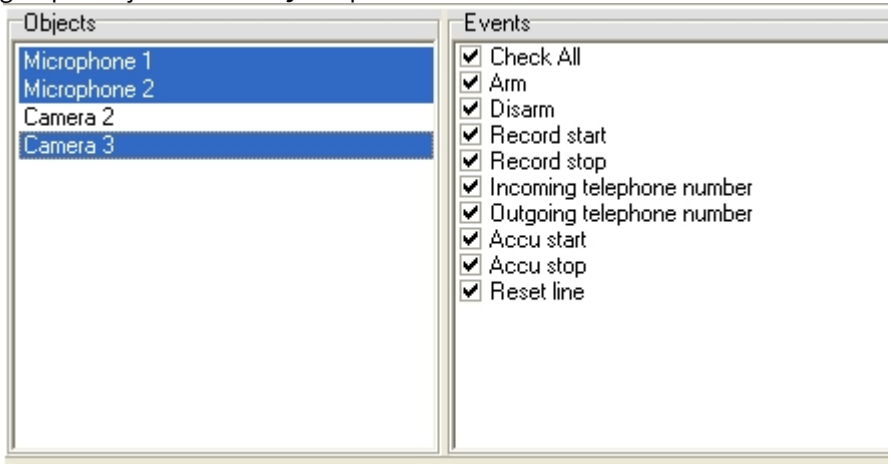
To create the screen report, do the following:

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.

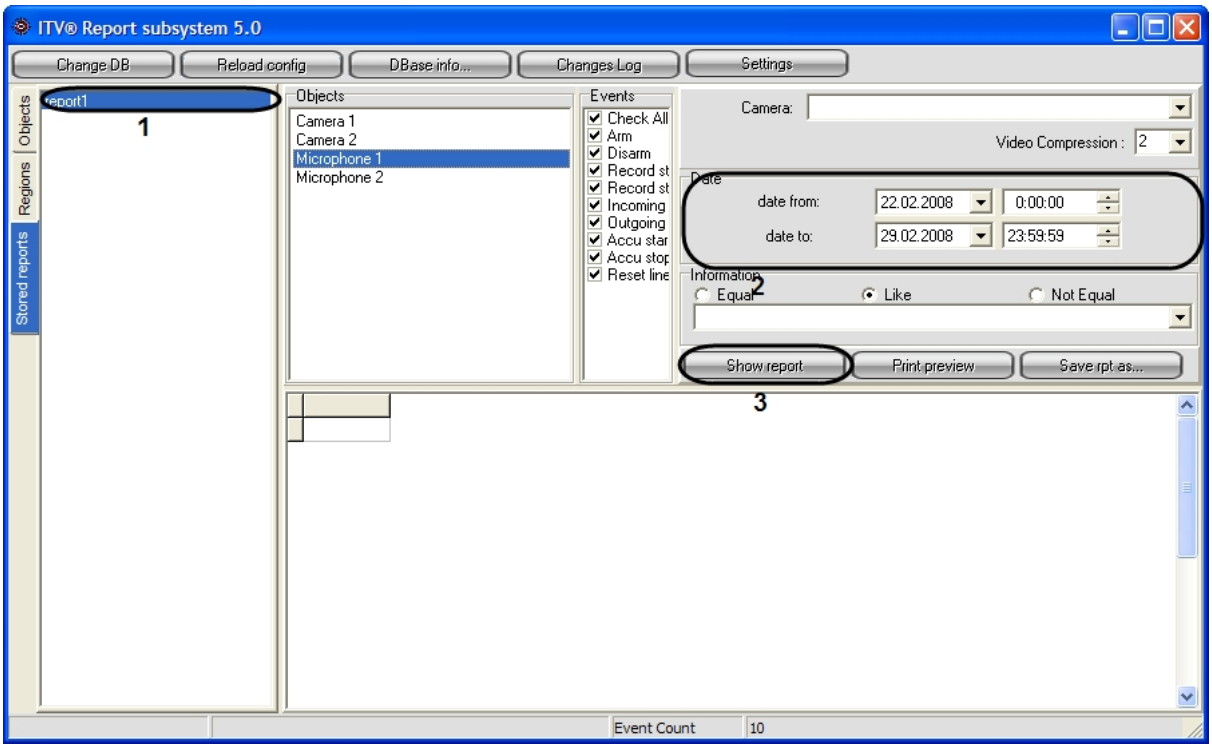
> **Note.**
>
> Clicking the **Show Report** button is equivalent to pressing F5 on the keyboard.

This completes the creation of the screen report. The screen report will be displayed in the lower part of the Report window.

11.9.1.1 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.

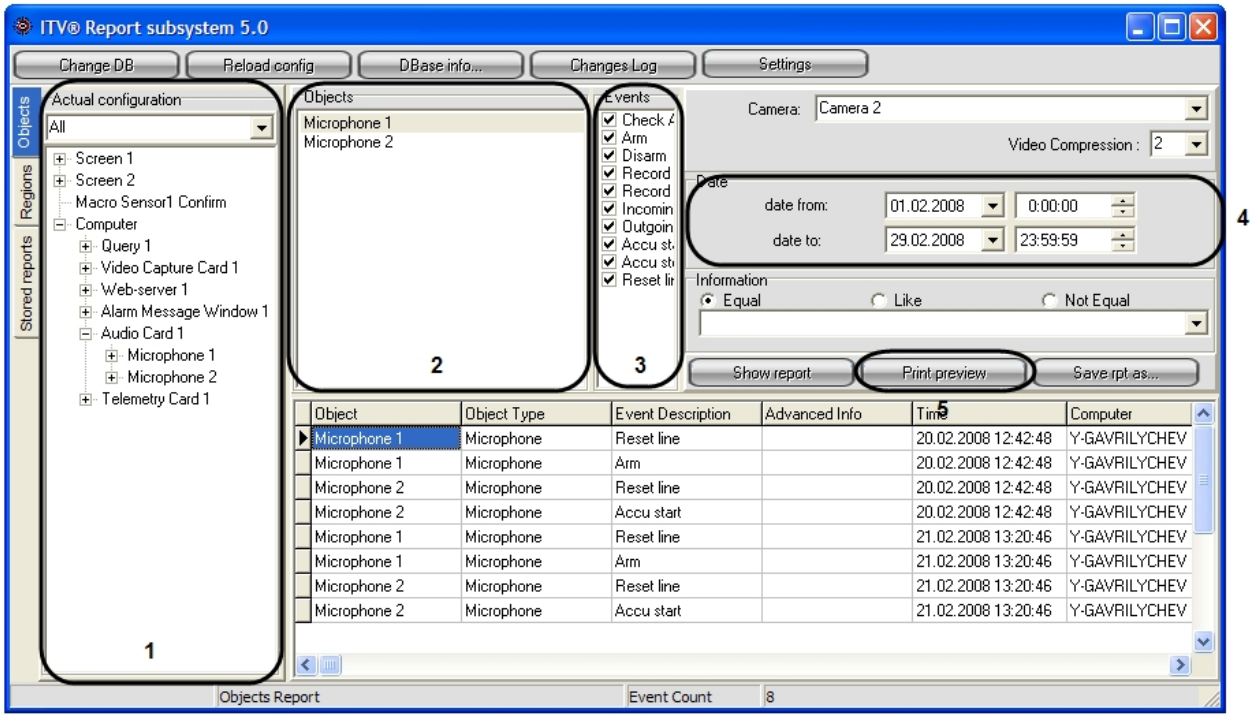
> **Note.**
>
> Clicking the **Show Report** button is equivalent to pressing F5 on the keyboard.

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.

11.9.2 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.

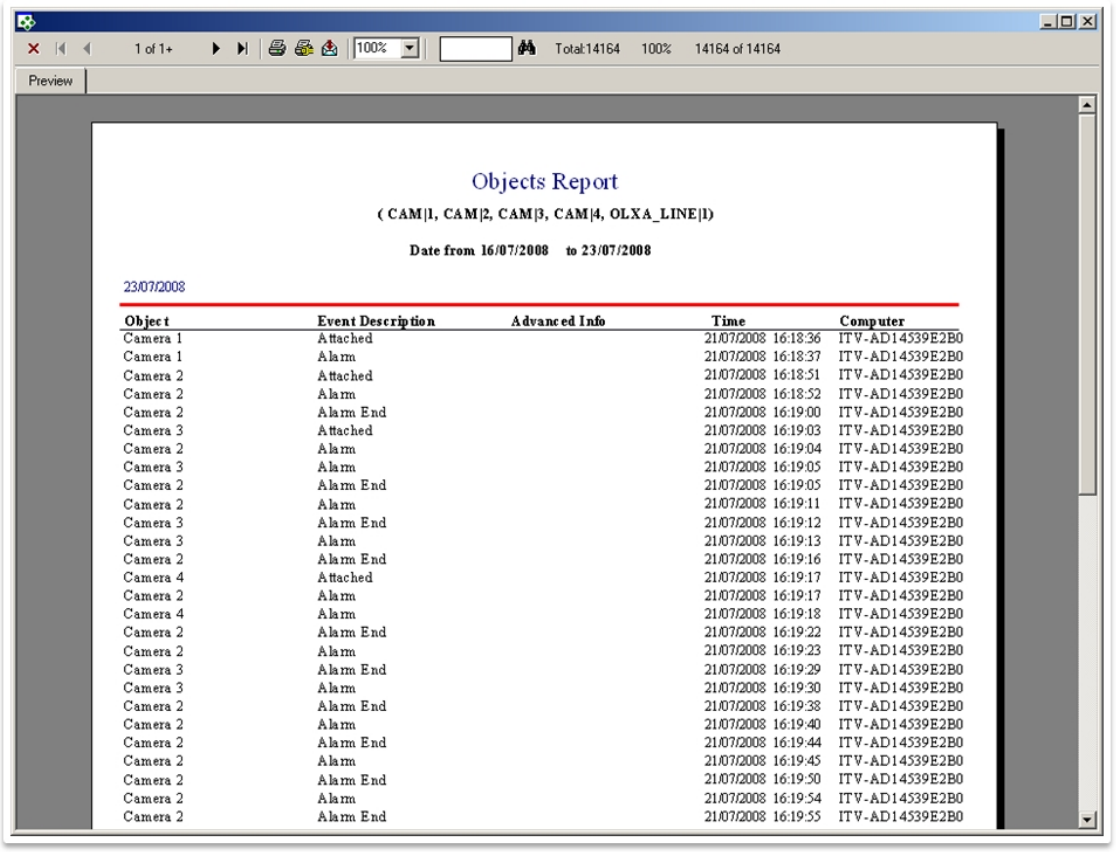


Creating a printed report is similar to the screen report creation procedure in p. 1 to 4 (see sections above).

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.

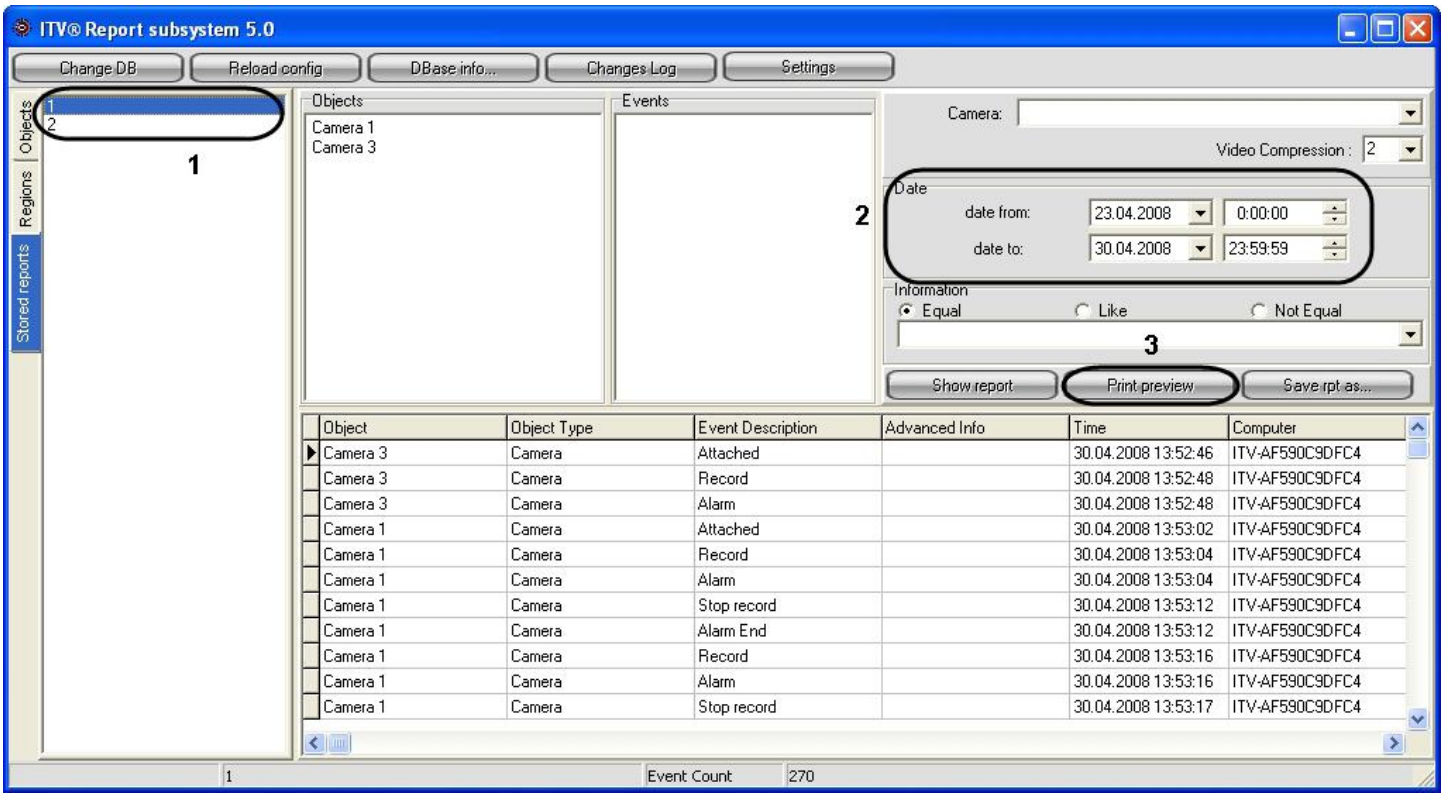
This completes the creation of the printed report. The report will open in a separate window.



11.9.2.1 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.

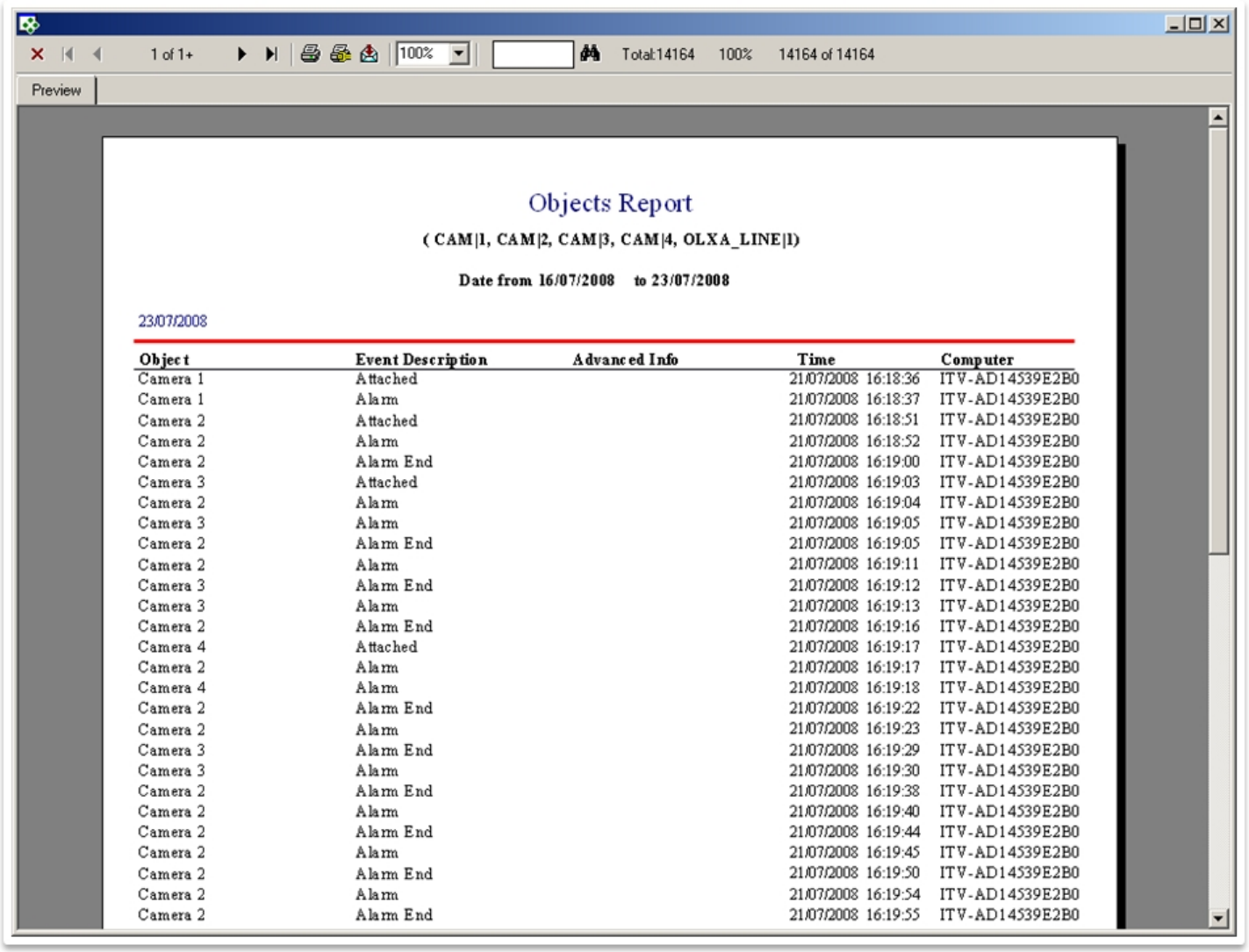


Creating a printed report is similar to the screen report creation procedure in p. 1 to 2 (see the Creating a screen report from the report template section above).

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.

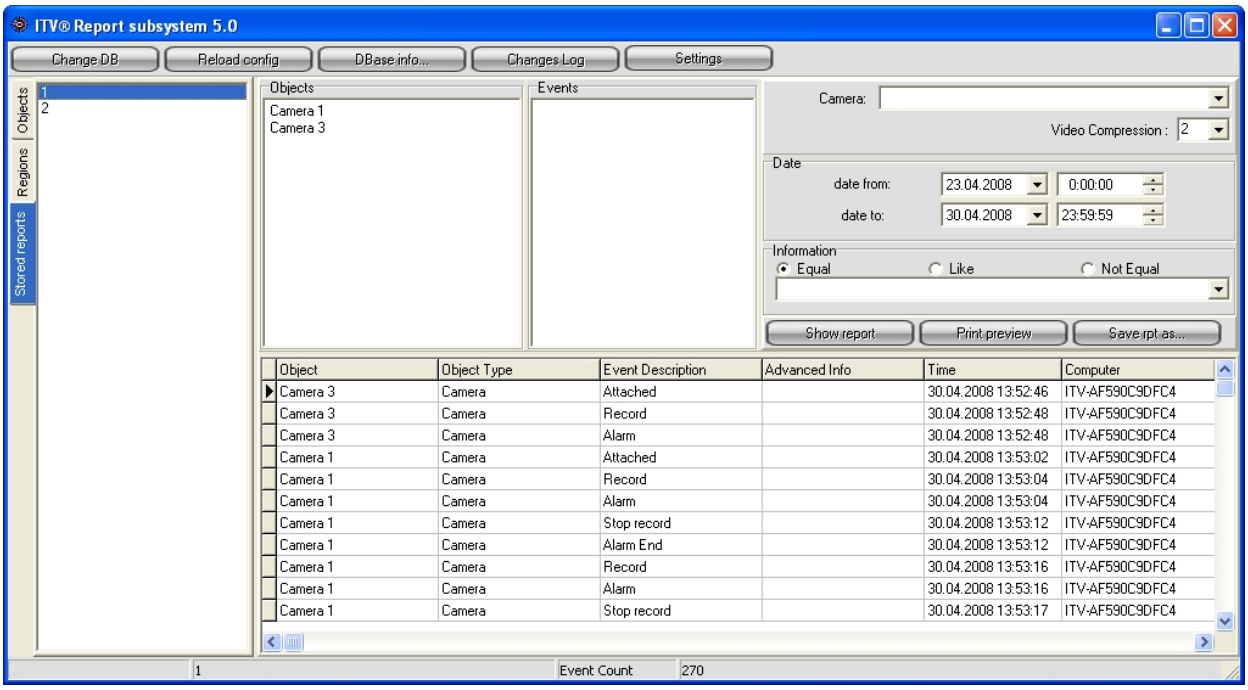
This completes the creation of the printed report from the template. The report will open in a separate window.



11.9.3 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.

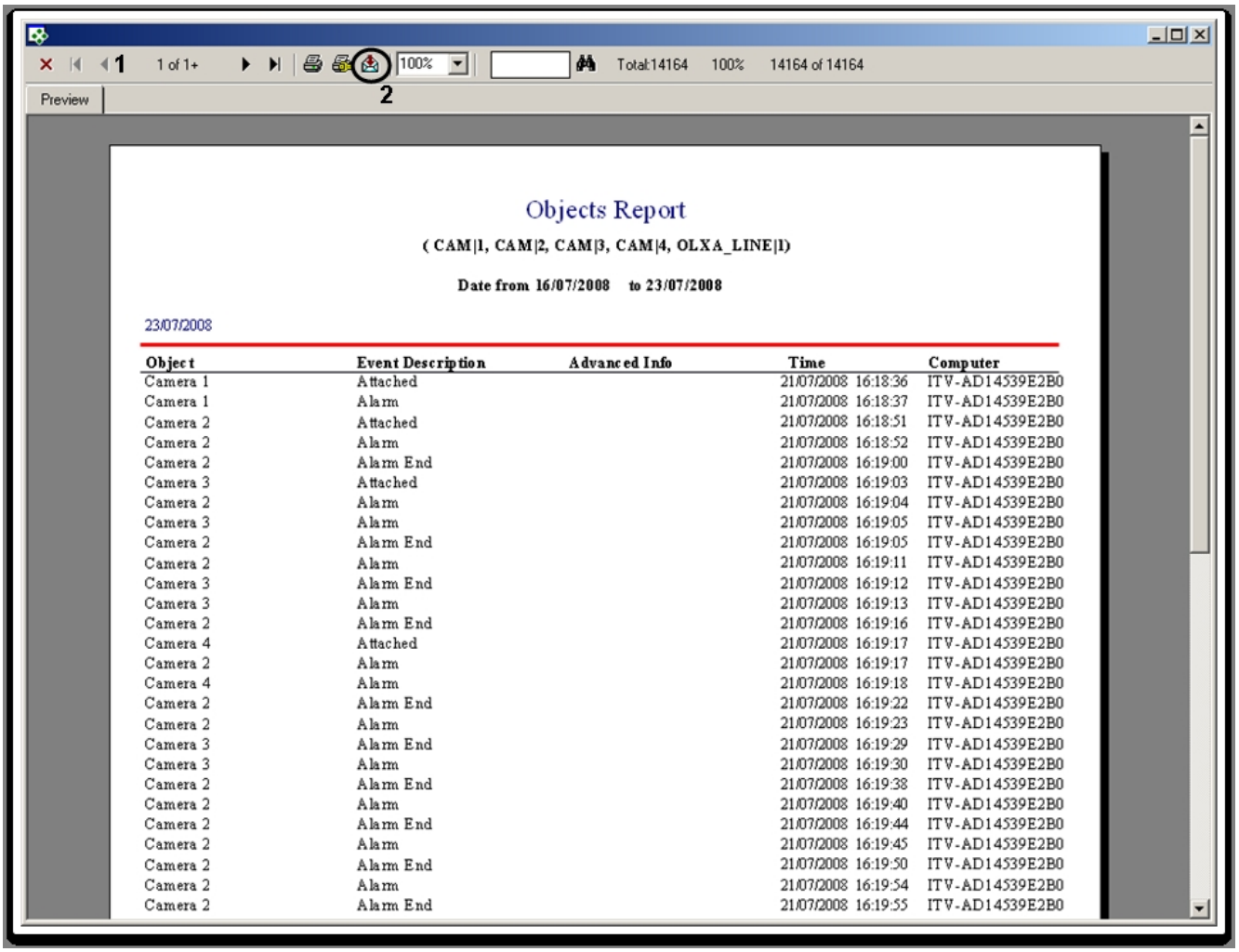
> **Note.**
>
> Clicking the **Print Preview** button is equivalent to pressing F6 on the keyboard.

This completes the creation of the printed report from the template. The report will open in a separate window.

11.9.4 Exporting the report to a file

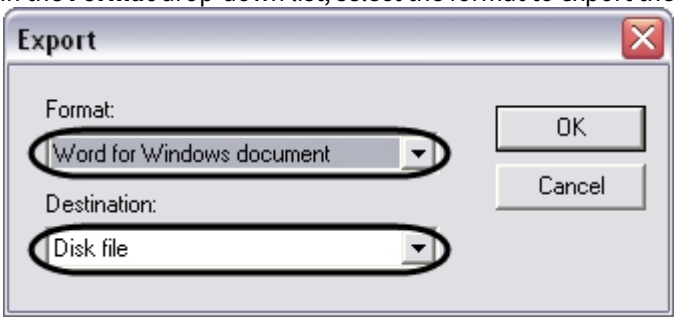
The Report system allows exporting the created report into one of the commonly used file formats.

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:

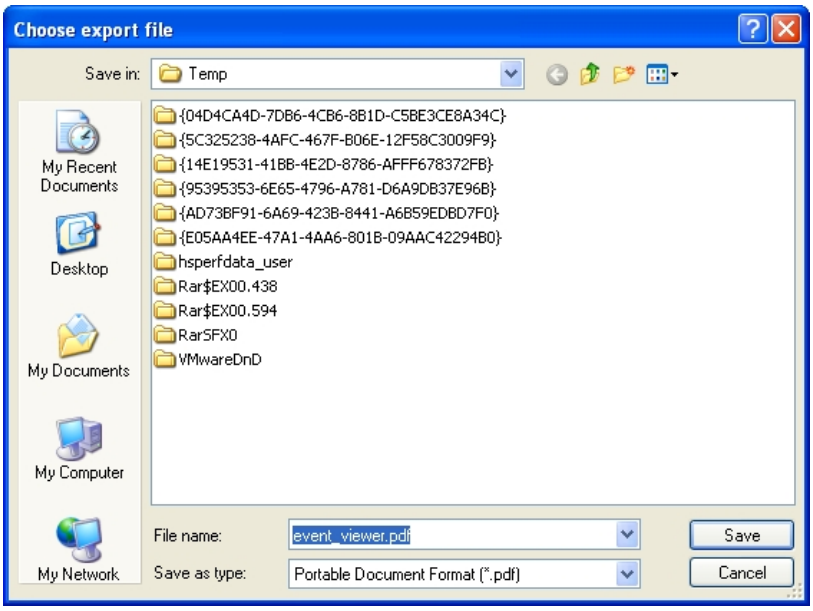
1. Create the printed report (see the Creating a Printed Report section).
2. Click the **Export** button in the window showing the report.
3. Specify the following in the **Export** dialog box:
    a. in the **Format** drop-down list, select the format to export the report to



    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.

11.10 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.

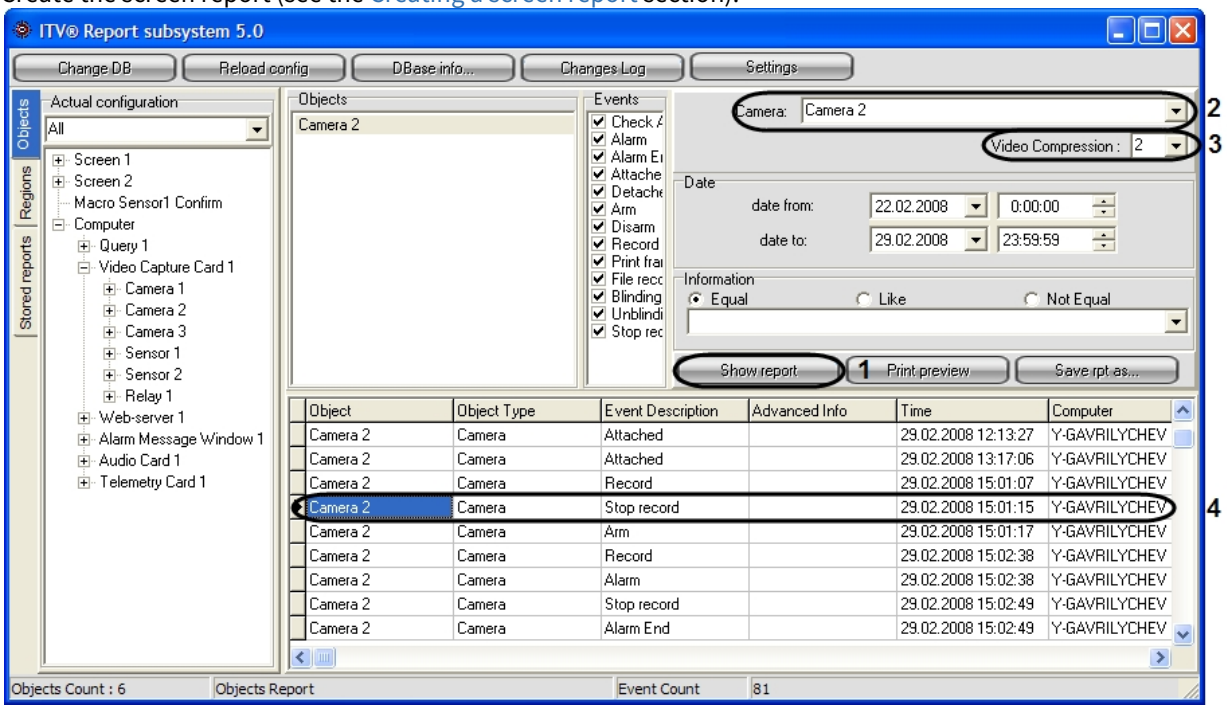
The recordings are played using the Converter.exe utility or the surveillance window of the corresponding camera. The playback option is selected in the Report system settings window (See the OptionsForm Window section).

> **Note.**
>
> To play the video recordings directly in the surveillance window, start the *Intellect* software, and create and set up the surveillance window.

11.10.1 Playback of the video recordings from the Report system

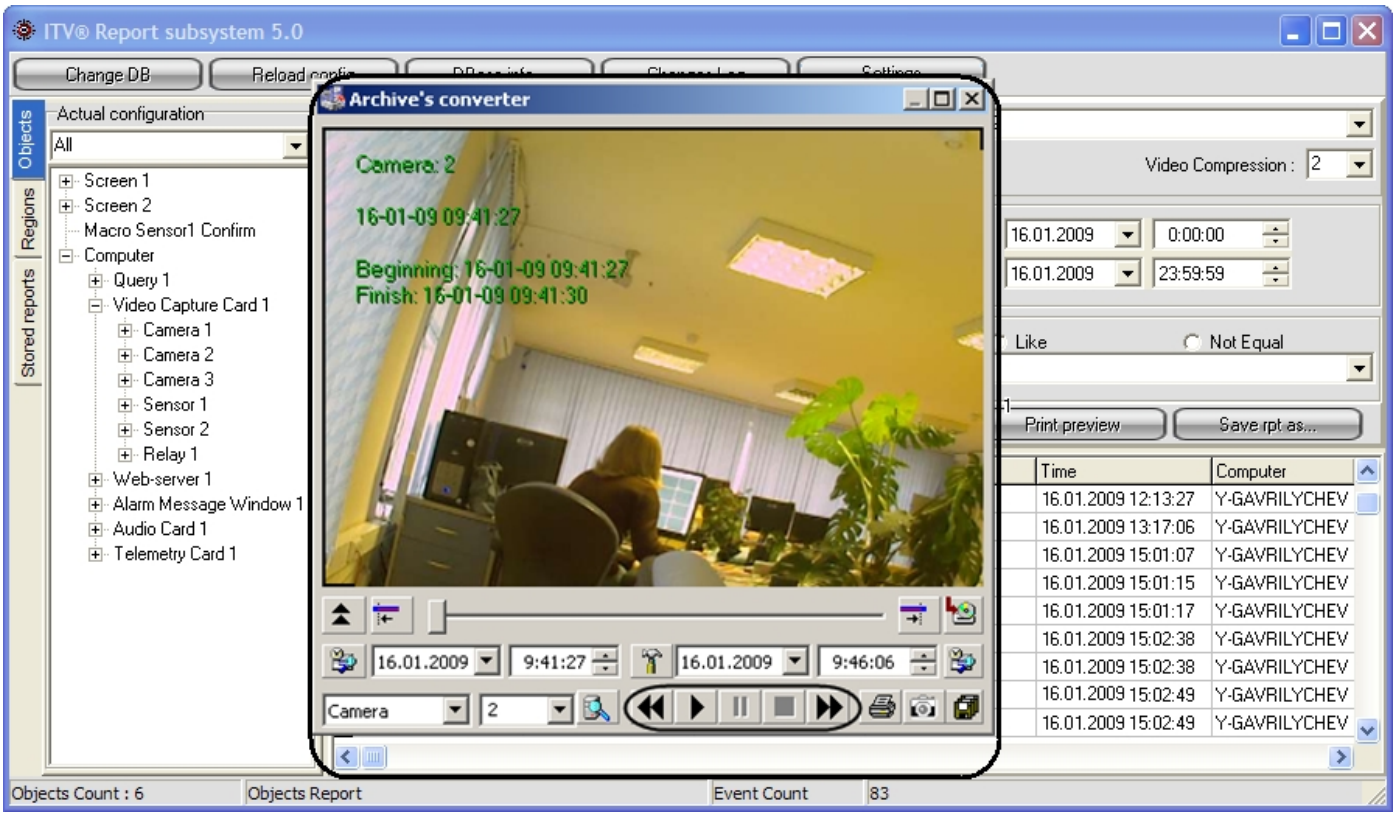
To play the video recordings from the Report system, do the following:

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.

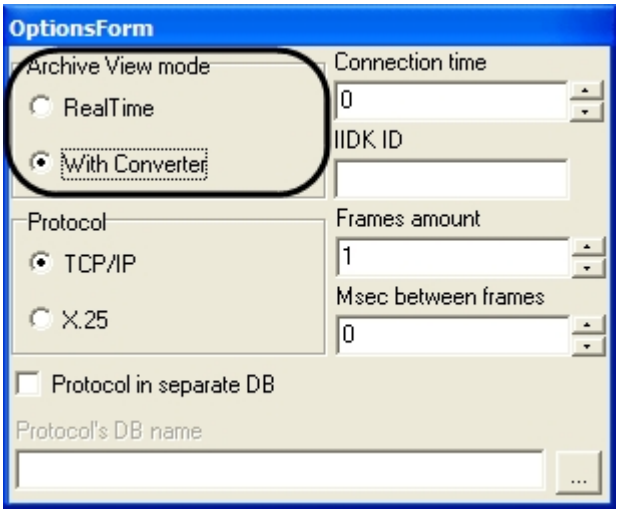
The converter.exe utility or the surveillance window will open, showing the recording for the time specified in the **Data** column of the screen report for the selected event.



11.10.2 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.

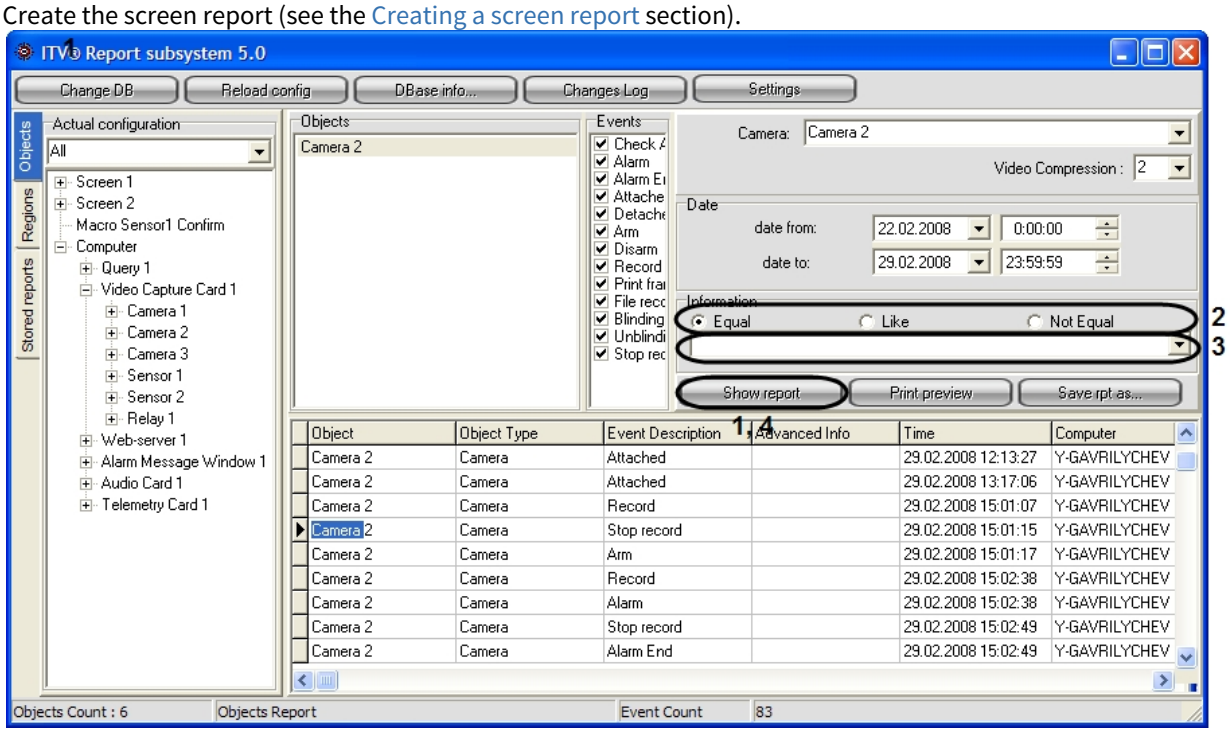
11.11 Filtering the events in the screen report according to the additional information

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.

11.12 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.

12 Administrator's Guide. Conclusion

More detailed information on the Intellect software package is presented in the documents titled:

1. Operator’s Guide;
2. Programming Guide (JScript).
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 occurr 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.

Please send your comments or requests concerning this Guide to the AxxonSoft Training and documentation development division at (documentation@itv.ru).

13 Appendices

13.1 Appendix 1. Interface

13.1.1 Description of the Main Control Panel Interface

The Main control panel as part of the **System settings** interface box has a fixed position and is located in the upper right corner of the **System settings** interface box.



The INTELLECT™ Main control panel has been designed to be small (to save on the usable monitor area) and contains only the information window and two menu buttons to the right of it.

INTELLECT™ Main control panel elements and descriptions thereof are given below:

1. 

Information windows or help window. This window displays comments (brief information) to the UI elements, and system error information, when pointed at with the mouse. If *Intellect* is running in demo mode, the text in the window says "Mode: Demo".
2.  The **Screens** button. The button is designed for control of virtual screens.
3.  The **Execute** button. Designed to display the **System settings** dialog box on the monitor, manually execute the macros, open the "about" info and quit system operation.

13.1.2 Description of the System settings dialog box

13.1.2.1 Tabs panel

The Tabs panel is displayed in the upper left corner of the **System settings** dialog box and is designed for shifting between INTELLECT™ software groups of objects. The Tabs panel is shown in figure.



A list and brief description of tabs comprising the **System settings** dialog box are given in table.

№	Section (Tab) of the System settings dialog box	Key functionalities of the section (tab)
1	**Hardware**	The tab is designed for connection and configuration of hardware and program modules. Also, this tab is used for connection and configuration of customer-tailored components of the Operator UI, i.e., such objects as the **Operator query panel** and **Alarm message window**.
2	**Interfaces**	The tab is designed for the creation and configuration of virtual screens and UI components in them, i.e., Video Monitor, audio players and control panels of various devices and modules.
3	**Architecture**	The tab is designed for describing the system structure, network settings defining PC links and parameters for data exchange between the PCs of the distributed network.

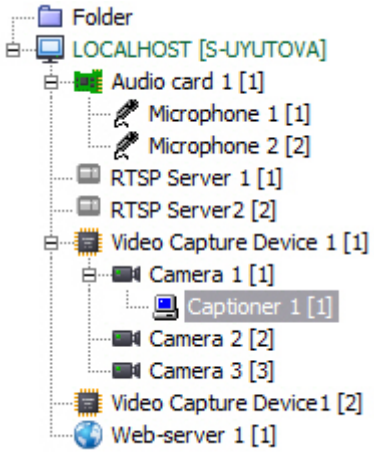
№	Section (Tab) of the System settings dialog box	Key functionalities of the section (tab)
4	**Programming**	This tab is designed for the creation of macro commands and scripts, as well as for the creation of time zones, shift timetables, delineation of secured object areas, access levels for the access points, which are equipped with readers.
5	**Users**	The tab is designed for the creation of user accounts (registration) of the digital video surveillance and audio monitoring system, classification of the levels (rights) of their access to the system resources and assigning passwords to the users.

To transfer from one tab to another, use the mouse. For the above purpose, follow the next steps:

1. Drag the mouse cursor to the tab.
2. Click the left mouse button.

13.1.2.2 Object tree

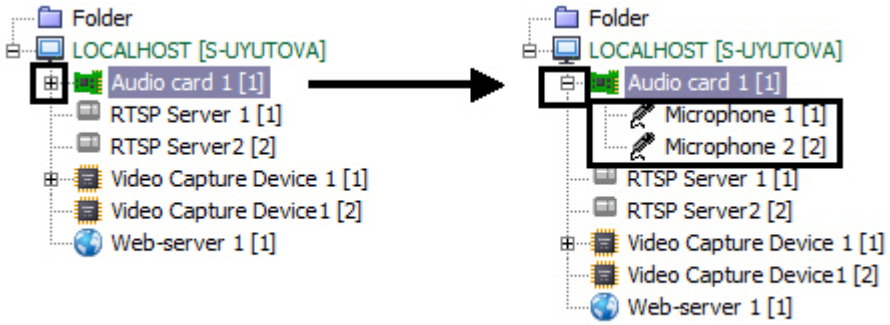
The system is based on the tree-like structure of the objects layout (object tree). The object tree is arranged as a multi-level list of embedded objects.



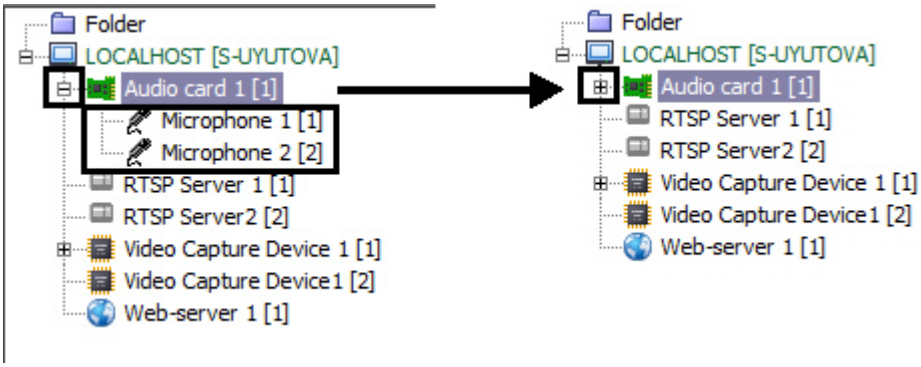
The objects structure is configured as a hierarchy, where low-order (daughter) objects can only be created on the basis of the higher-order (parent) object. Objects in the tree are sorted by name in the following order: Cyrillic characters, spaces, symbols, numbers, Latin characters. If folders are created in the object 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 object tree can be viewed in expanded form, embedded groups (branches) can be viewed or hidden, if not required to be controlled currently.

To get down the branch of the object tree, containing daughter objects, click the left mouse button pointing at«-» symbol appearing to the left of the parent object.

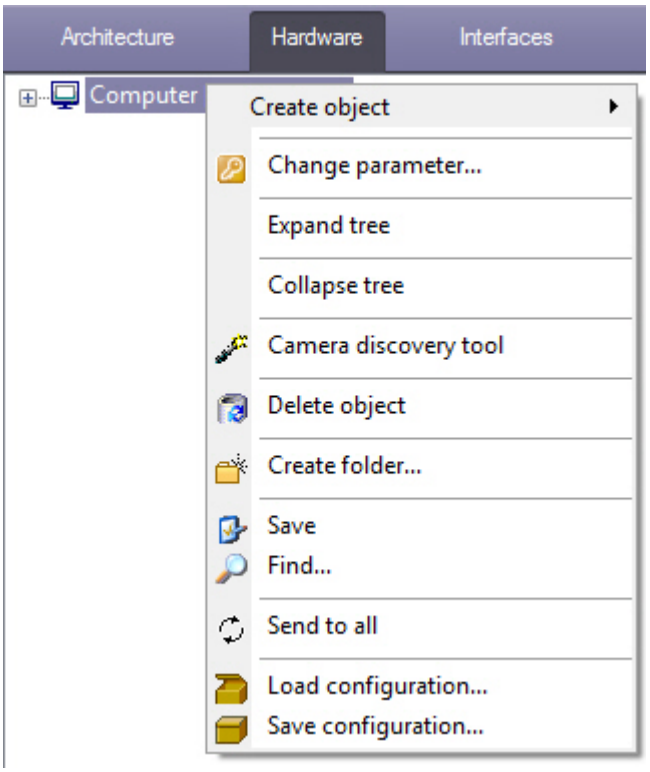


To collapse the daughter objects, click the left mouse button pointing the cursor at the minus symbol.



13.1.2.3 Context menu of the system object

The context menu is displayed within the objects tree. To display the menu on the monitor, click the right mouse button, pointing the cursor at the system object in the objects tree.

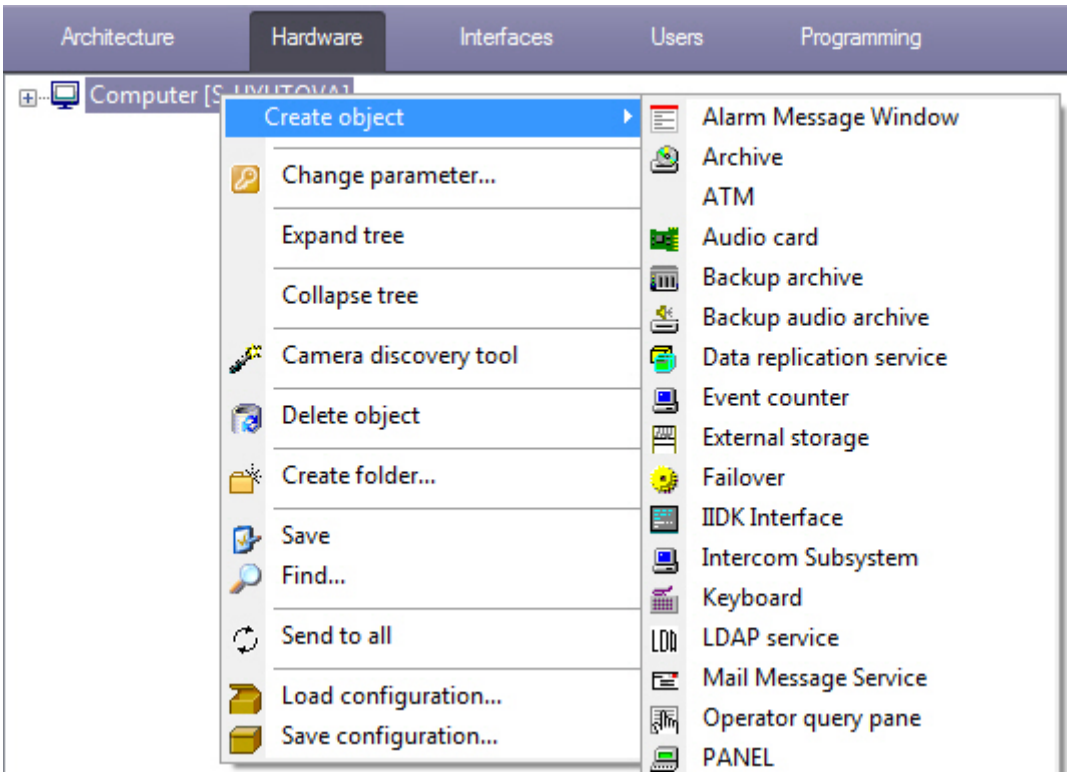


The number of menu lines depends on the video surveillance system configuration and object tasks. The context menu of a system object is described below.

> **Note**
>
> If the Settings panel of any object is open (see Object Setting Panel), and you right-click on an empty place in the object tree area, this panel will close and the Context menu will open, and the object will be deselected in the object tree.

13.1.2.3.1 The Create object function

The **Create object** function, which is used to create a new system object in the Hardware objects tree, is selected from the context menu of the parent system object.

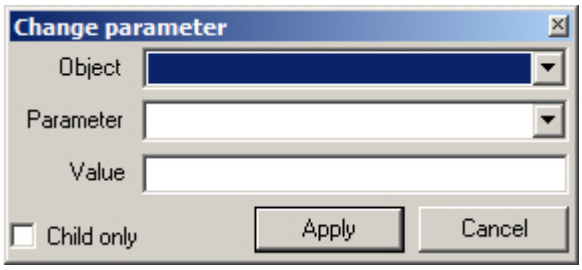


When the **Create object** function is selected, the menu will display a list of embedded objects. Figure shows an example of a list of objects which can be created on the basis of a **Computer** object.

13.1.2.3.2 The Change parameter function

The **Change parameter** function is to edit the parameters of INTELLECT™ objects in the database. This function is not recommended to be used by new users.

When the **Change parameter** function is selected in the context menu of the system object, the **Change parameter** box appears.



In the **Object** dropdown list select the type of system objects the parameter of which is to be edited. This list contains only objects that are child objects of that one the context menu of which was used to call the box. To change parameters of the **Computer** object, select the **Change parameter** item in the context menu that appears when the area with no objects of INTELLECT™ objects tree is right-clicked.

In the **Parameter** dropdown list select the object parameter that is to be changed in the INTELLECT™ database.

> **Attention!**
>
> The parameter will be changed for all objects of selected type in the distributed configuration.

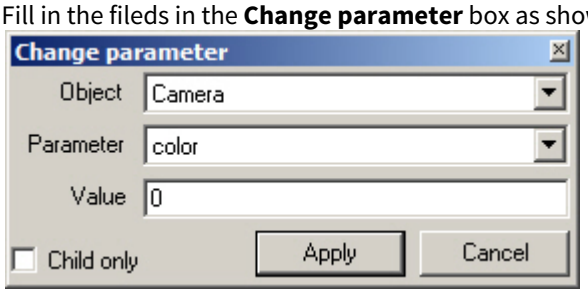
In the **Value** field specify a new value for the parameter in the format in which it will be stored in the database. One can learn about the type of parameter using the ddi.exe utility (see Editing intellect.dbi and intellect.ext.dbi database templates using the ddi.exe utility section). One can learn about the format of parameter while viewing INTELLECT™ database (see Viewing INTELLECT™ software database section).

If the parameter is to be changed for child objects only then set the **Only child objects** checkbox checked. For instance, this checkbox allows changing the parameter only on the computer selected in the tree.

Example. All cameras in the system are to be set for displaying black-and-white video.

For this do the following:

1. Call the **Change parameter** box in the context menu of the **Video Capture Device** or **Camera** object.
2. Fill in the fileds in the **Change parameter** box as shown in the figure.



3. Click the **Apply** button.

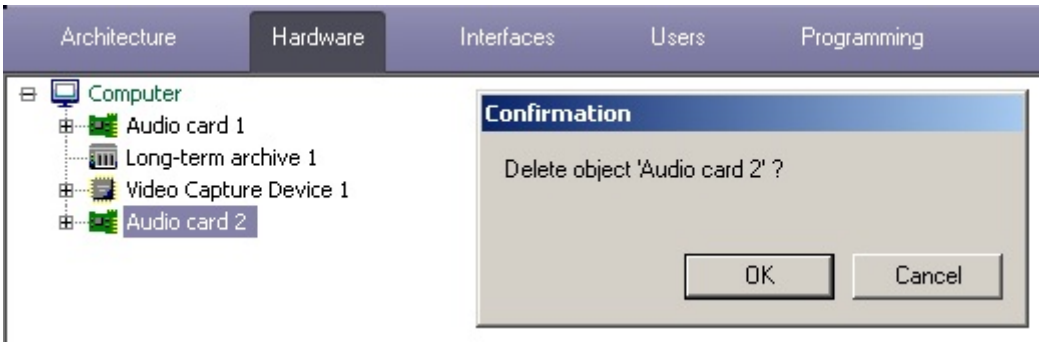
As a result the black-and-white mode of displaying video is set for all cameras in the system.

13.1.2.3.3 The Camera discovery tool function

When the **Camera discovery tool** function is selected in the context menu of the **Computer** system object, *Camera discovery tool* starts. Its operation is described in INTELLECT™ Software Package. Installing and configuring security system components guide in the section of the same name.

13.1.2.3.4 The Delete object function

To delete an object from the tree, drag the cursor pointer to the object and, with the context menu opened, select the **Delete object** option. Now the PC monitor will show a dialog box requesting to confirm that the system object be deleted.



To confirm that the object should be deleted, click **OK** or, if you want to quit the delete function, click **Cancel**. As soon as deletion is confirmed, the object, as well as its daughter objects, will be removed.

The function **Delete** system object applies to all objects, including the **Computer** object, created by default when Intellect™ system is installed.

> **Note**
>
> Please be aware, that, a deleted **Computer**- local computer parent object can hardly be restored. That is why the developer does not recommend deleting objects such as **Computer**, created by Intellect™ system.

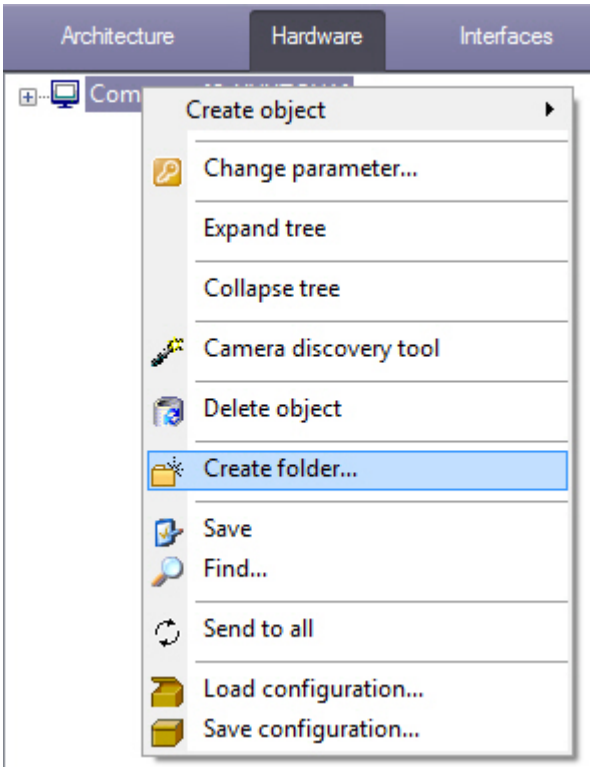
13.1.2.3.5 The Create folder function

The **Create folder** function is used to properly arrange the system objects displayed in the objects tree, in cases when there are many types of objects. Objects are grouped into folders at the user's discretion. The function is available on all tabs of the System settings dialog box except the **Architecture** tab.

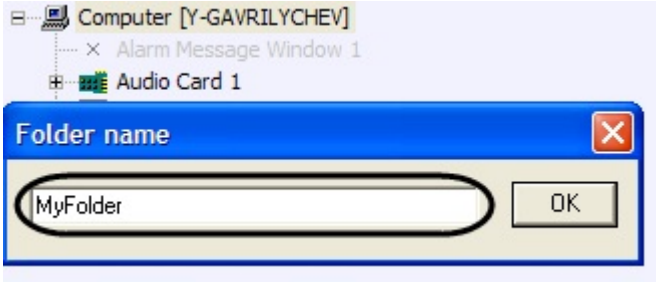
To create a folder, display the object context menu in the monitor and select the **Create folder** option.

Note.

A folder can be created on the base of the object that has child objects. For instance, a folder can be created on the base of the **Computer** or **Video Capture Device** object, but it is not possible to create a folder on the base of the **Captioner** or **Detection zone** object.



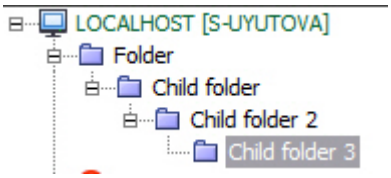
Now the PC monitor will show a dialog box requesting to enter a **Folder name**. Having entered the folder name in the dialog box, click **OK**.



As a result the folder is created in the objects tree.



To create a folder located in another folder, select the **Create folder** item in the functional menu that opens by right-clicking a previously created folder.

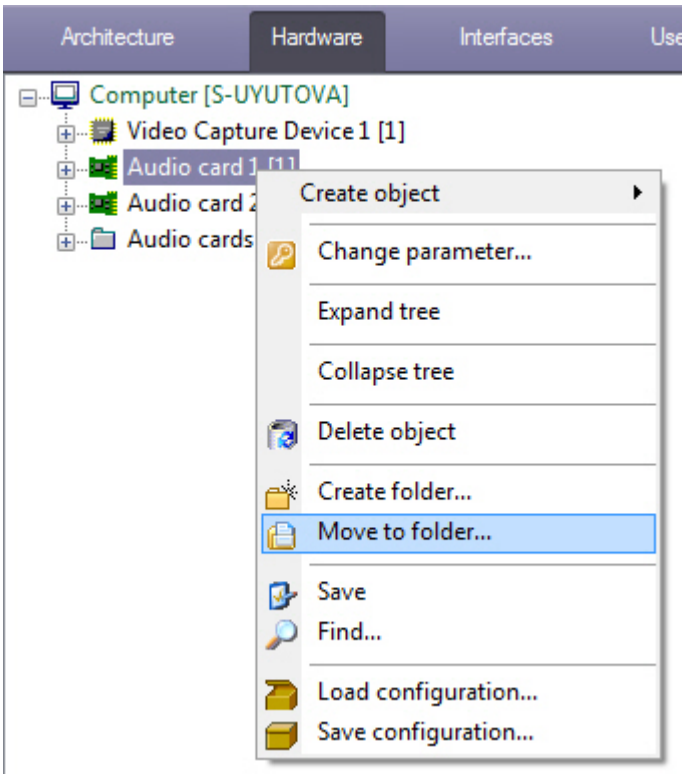


13.1.2.3.6 The Move to folder function

This function allows moving system objects to the objects tree folder.

> **Important!**
>
> Objects are grouped into folders separately on each Server/RAW in the distributed architecture. Grouping created on one Server/RAW will not be available on other Servers/RAWs. The folders themselves are synchronized between Servers/RAWs.
>
> Set up database synchronization to equalize folders content on all Servers/RAWs.

To move objects to the folder, select the object, which you need to move, display the context menu and select the **Move to folder** option.



The monitor will display a window for selecting a folder, where you will move the selected system object.



To confirm the selected folder, click **OK**. The object will be moved to the given folder.



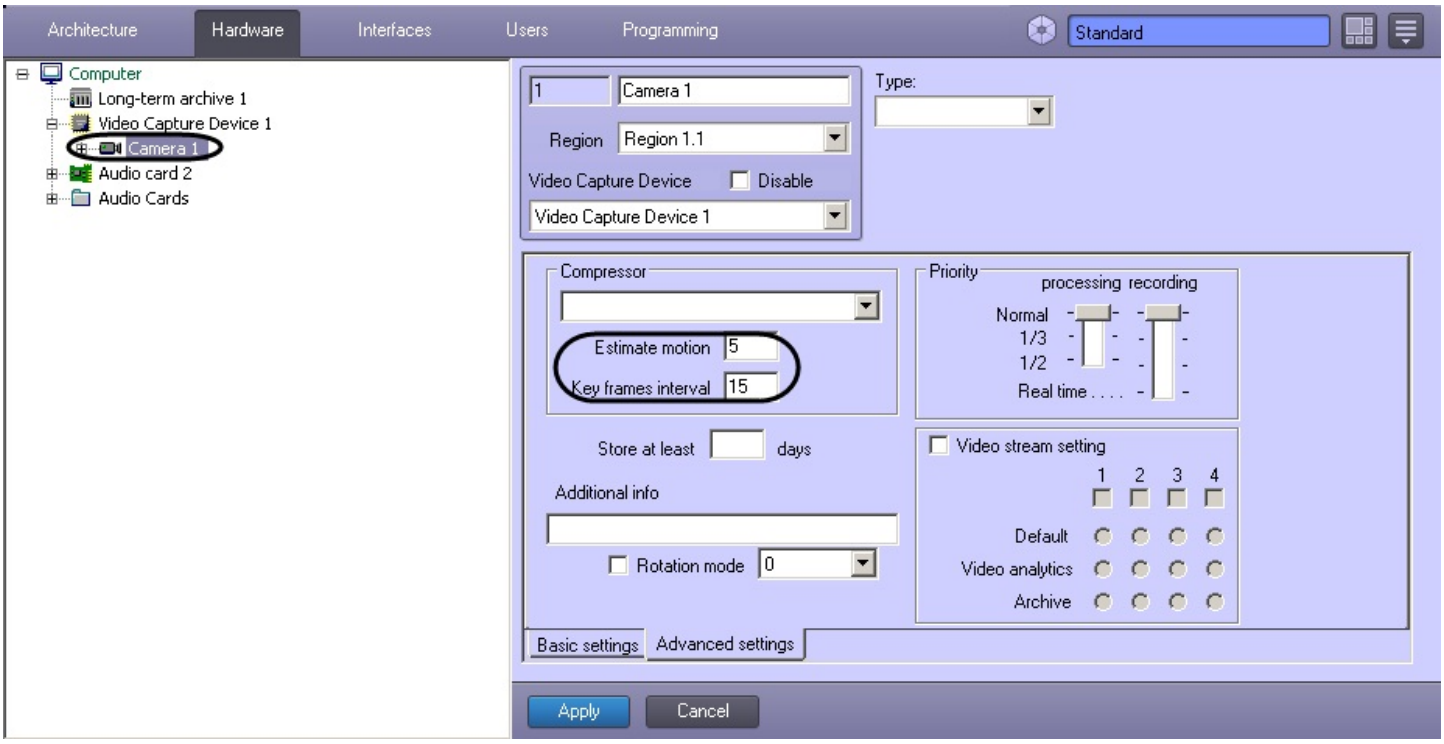
13.1.2.3.7 The Save function

INTELLECT™ system allows creating objects based on a template. A template is created using the **Save** function accessible in the main functional menu.

> **Note.**
>
> Objects can also be copied and pasted using the Ctrl+C and Ctrl+V keys.

Below we describe how to create the **Camera** object on the basis of a template using the **Save** function.

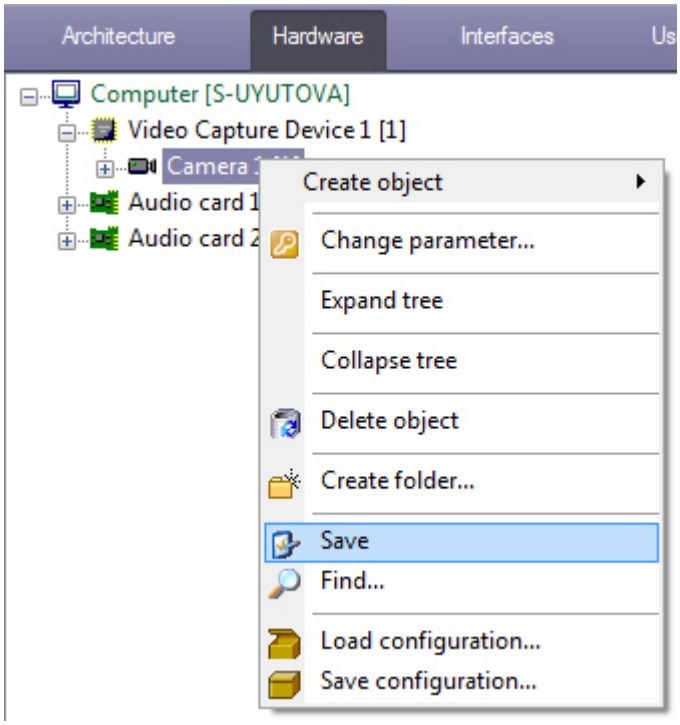
First of all select an object that has already been created and configured, for instance, the **Camera 1** object. Figure shows a setting panel with highlighted parameters of the **Camera 1** object which have been modified (differ from the default settings).



To create a template based on this object, do the following:

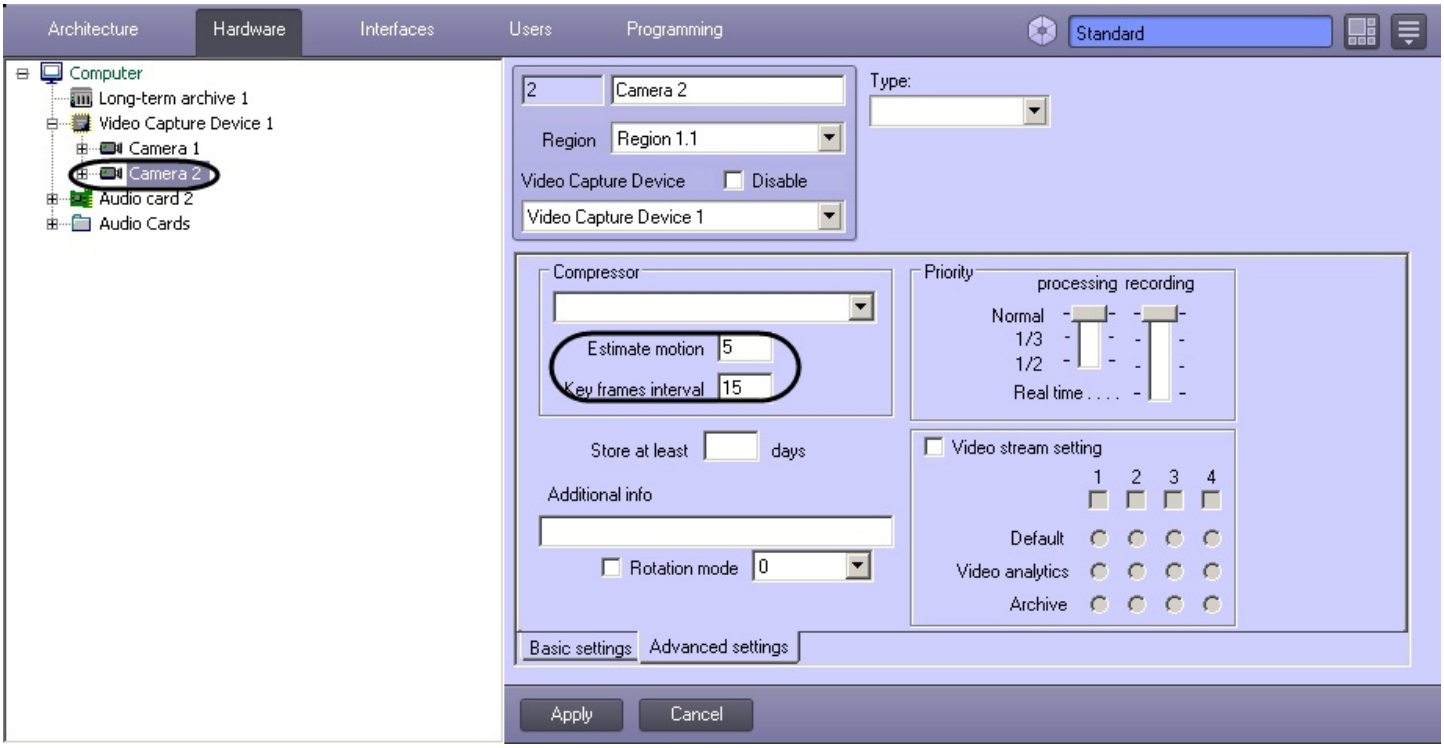
1. Call the context menu of the **Camera 1** object.

2. Select the **Save** menu item.



The template of the **Camera** object (with the settings of the **Camera 1** object) has been created.

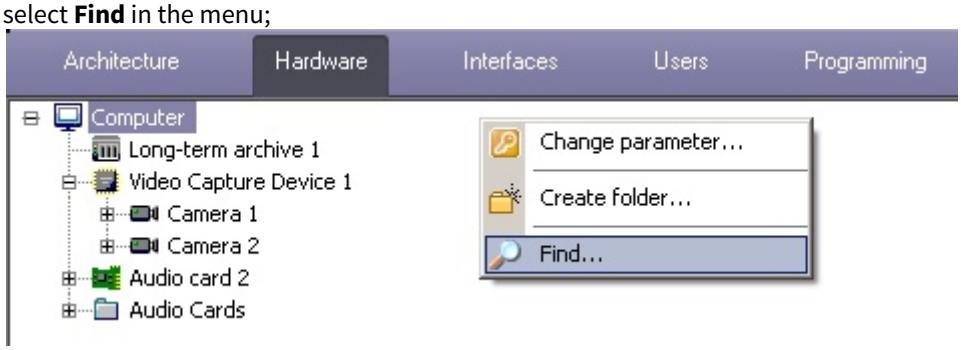
Now create the **Camera 2** object based on the **Video Capture Device 1** object (see The Create object function section). By default the **Camera 2** object will have the same settings as the **Camera 1** object.



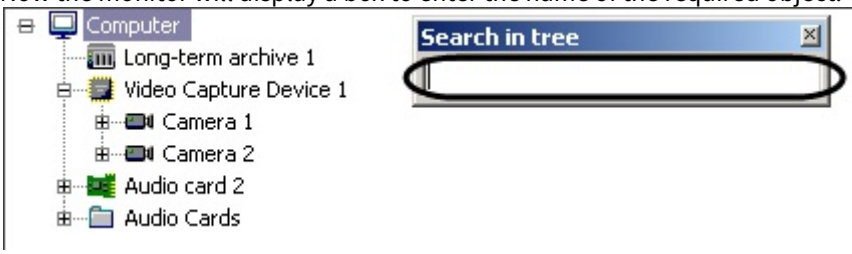
13.1.2.3.8 The Find function

The **Find** option of the menu is designed to search for an object in a tree. Intellect™ system uses two methods of searching for an object:

1. Searching within a tree. This method is used when only an object name (type) is known. In this case, to find an object, follow the next steps:
   a. display the context menu for the objects tree on the monitor;
   b. select **Find** in the menu;



Now the monitor will display a box to enter the name of the required object.

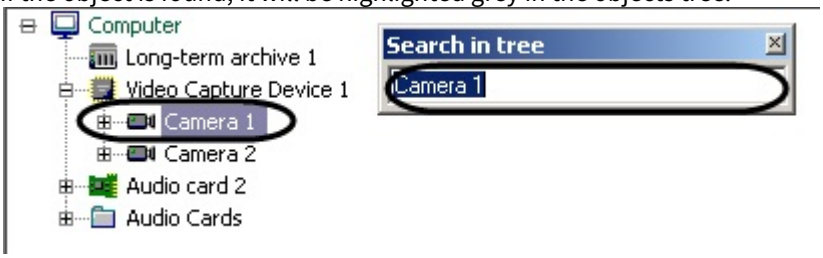


> **Note.**
>
> It is possible to open this window using Ctrl+F hotkeys combination.

   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.

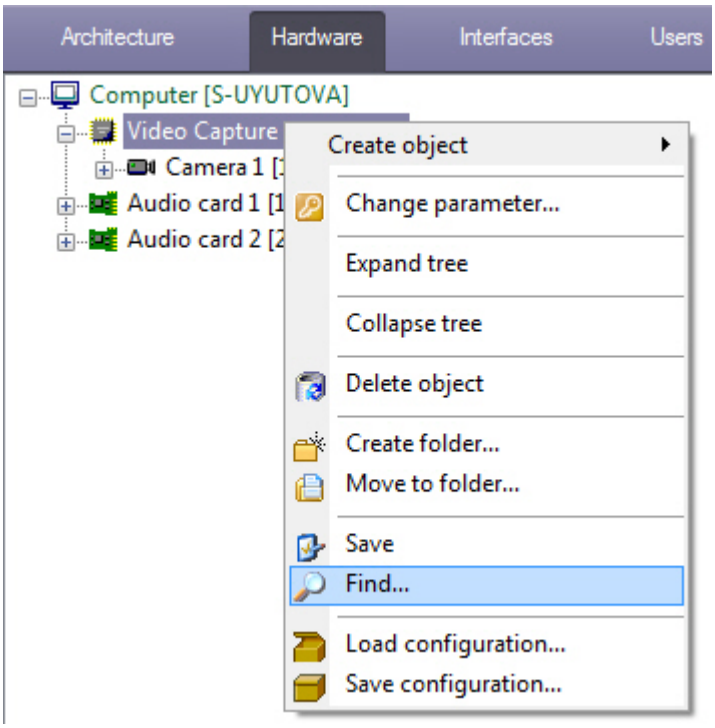


   To close the window for entering the object name, when the search is complete, click the left mouse button, pointing at the window field displaying the objects tree.

2. Search from a selected object.
   To find an object, whose location in the objects tree is approximately known, the next steps can be followed:
   a. select an object, located above of the search field.

> **Note**
>
> Object search across the tree is more effective, if the required object is a daughter object of the **Computer** object. Otherwise, the search will go down the branch of the selected object

   b. display the context menu for the objects tree field on the monitor;
   c. select **Find** in the menu.

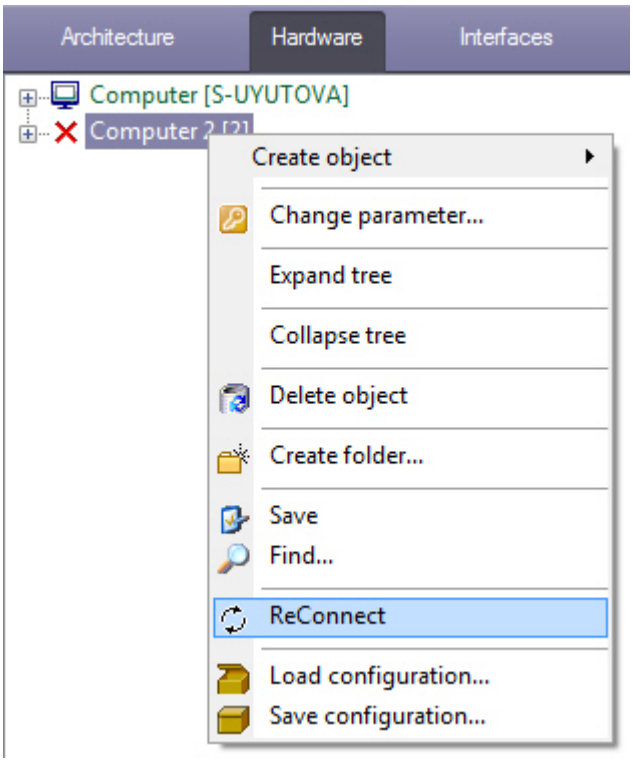


To proceed further follow method 1 (described above).

13.1.2.3.9 The Reconnect function

This line is displayed on the monitor in cases, when, apart from the base **Computer**, there is at least one (additional) **Computer** object, available for connection to the base **Computer**, communication with which fails, due to unknown reasons.

To install a link between two **Computer** objects, display the context menu of the additional **Computer** object, available for connection to the network and select **Reconnect** from the menu.



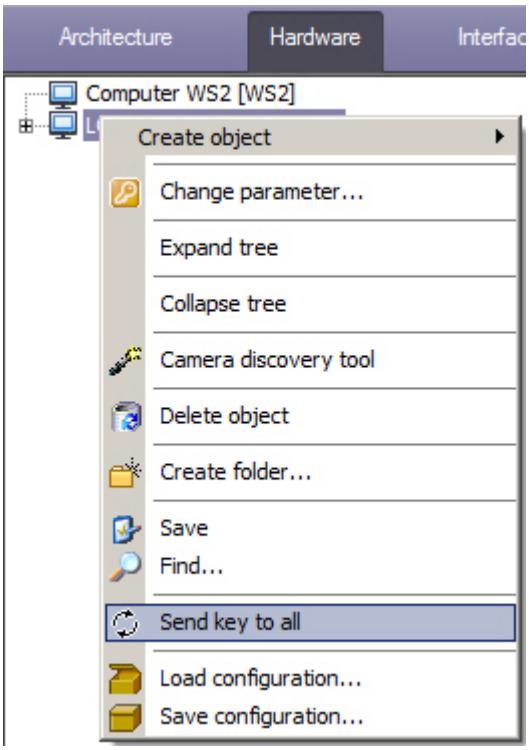
Now the object of the base and remote computer will be connected to the network.



13.1.2.3.10 The Send key to all function

This function allows broadcasting intellect.sec, the key file, governing the system configuration, to all PCs which have the distributed digital video surveillance and audio monitoring system. If the system functional has been updated and a new key file was received, it should be updated in all system PCs, using the **Send key to all** function.

This function is accessible only from the context menu of the **Computer** object, corresponding to the given local computer, which performs administrator functions.

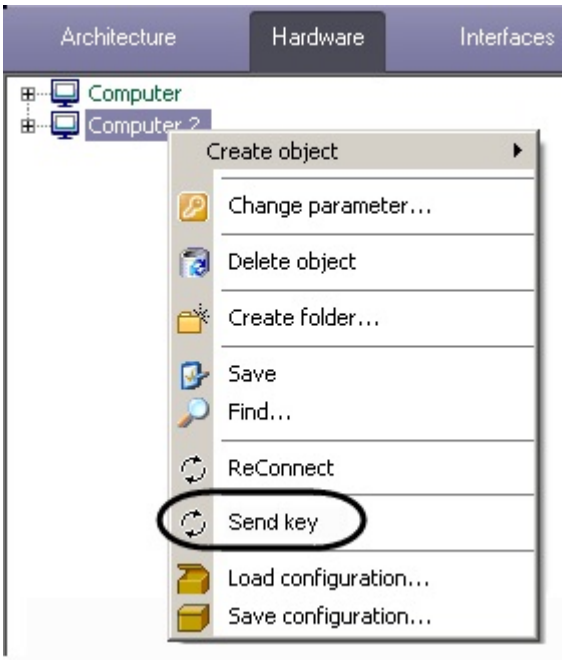


Note

If an updated key file is not broadcast in due time to all system computers, the Intellect™ system will not get started, when the PC is switched on, since the key file data will not match the information contained in the database.

13.1.2.3.11 The Send key function

This function allows updating the key file in the remote computer of the system and can be accessed only from the Main menu of the object, such as **Computer**, corresponding to the remote computer.

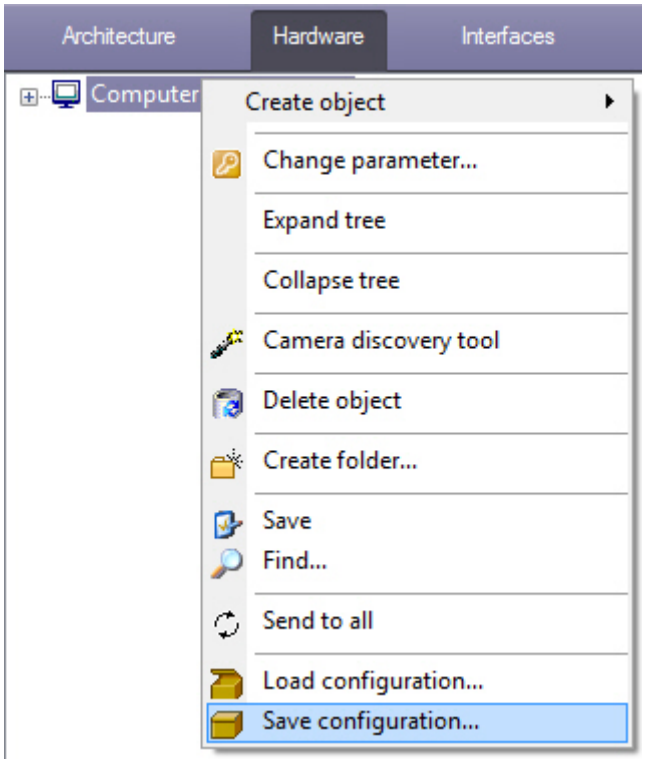


Note

If an updated key file is not broadcast in due time to the given computer, the Intellect system will not get started, when the PC is switched on, since the key file data will not match the information contained in the database.

13.1.2.3.12 The Save configuration function

The **Save configuration** function allows saving the current configuration parameters of an object to a file with the extension .cfg, so that the parameters can be re-used to configure other objects or to restore configuration parameters after unexpected loss (for example, if an object is accidentally deleted).

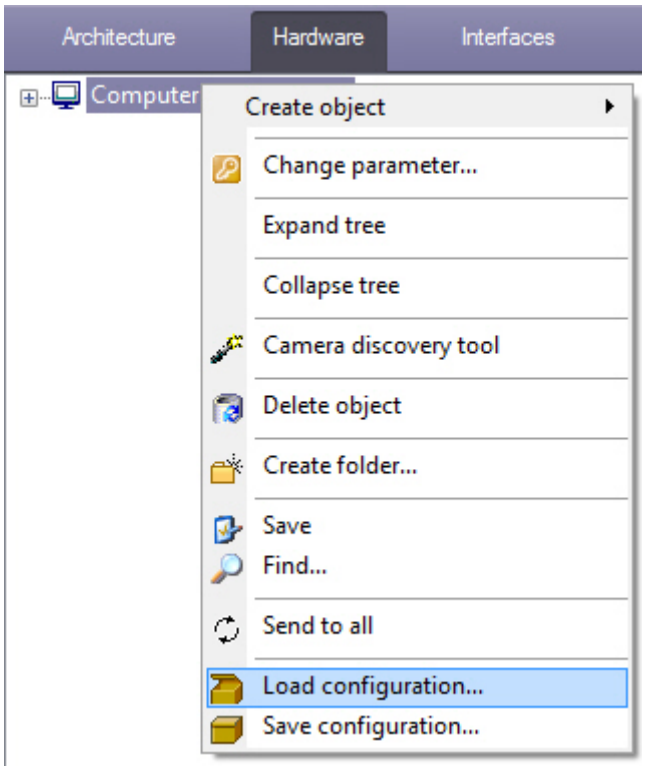


After **Save configuration** is selected in the menu, a standard Windows dialog box appears, in which you can specify the name of the configuration file and location in which you want to save it. By default, the file name includes the name of the object type and its number, for example **CAM.1.cfg** or **GRABBER.3.cfg**.

The saved configuration can be applied to any object of the type used to create the configuration file. To do so, use the **Load configuration** function (see the section The Load configuration function).

13.1.2.3.13 The Load configuration function

The **Load configuration** function allows loading configuration parameters from a file with the .cfg extension that has been created using the **Save configuration** function (see the section Save configuration function). Configuration parameters can be applied only for objects of the type used to create the configuration file.

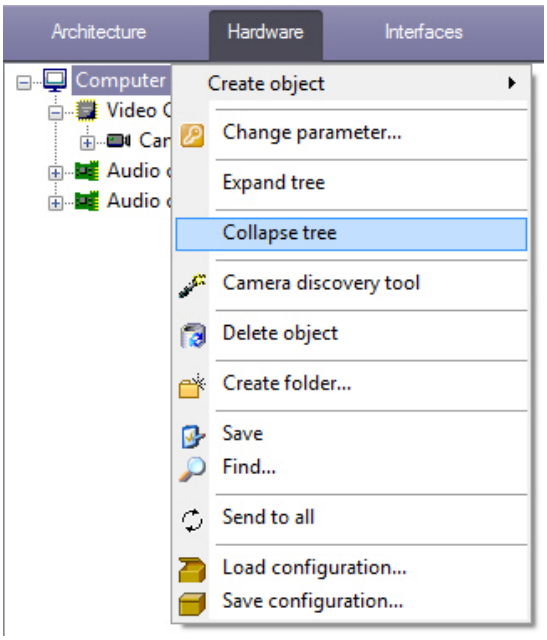


After **Load configuration** is selected in the menu, a standard Windows dialog box appears, in which you can navigate to the necessary configuration file.

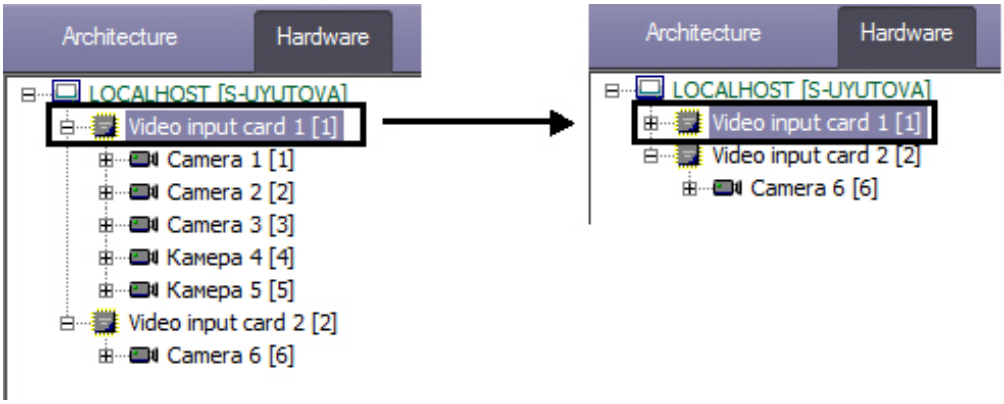
> **Note.**
>
> Some configuration parameters that must be unique for objects of the given type are not applied when a configuration is loaded.
>
> For example, the **PCI channel** parameter for the **Video Capture Device** object is not changed to the value given in a configuration file if an existing **Video Capture Device** object in the device tree already has the same **PCI channel** value. For more information on allocation of PCI channels between **Video Capture Device** objects, go to the section Creating and configuring the Video Capture Device object in the Installing and configuring security system components guide.

13.1.2.3.14 Collapsing the tree

The **Collapse tree** feature allows collapsing the object tree (see Object tree).



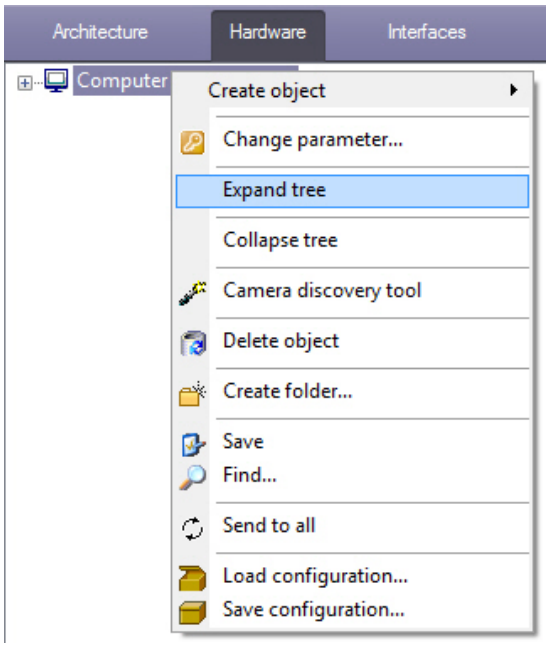
Only branch of the object tree under the object from functional menu of which the function is triggered will be collapsed using this function.



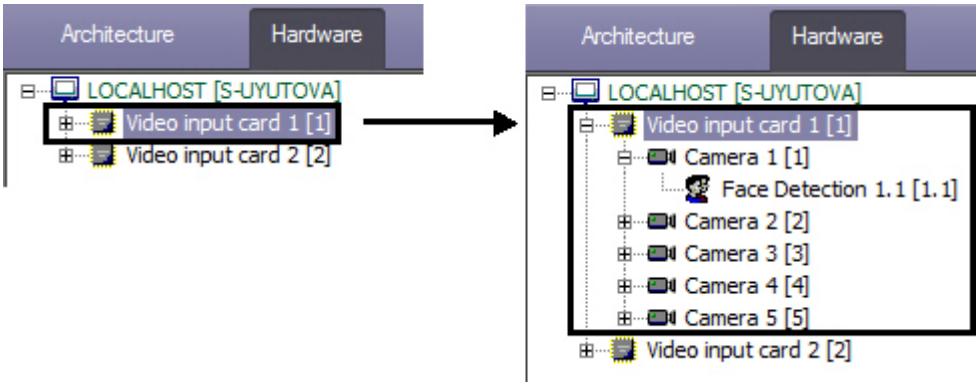
To collapse all object tree branches, select the **Collapse tree** menu item holding down the Shift key.

13.1.2.3.15 Expanding the tree

The **Expand tree** feature allows expanding the object tree (see Object tree).



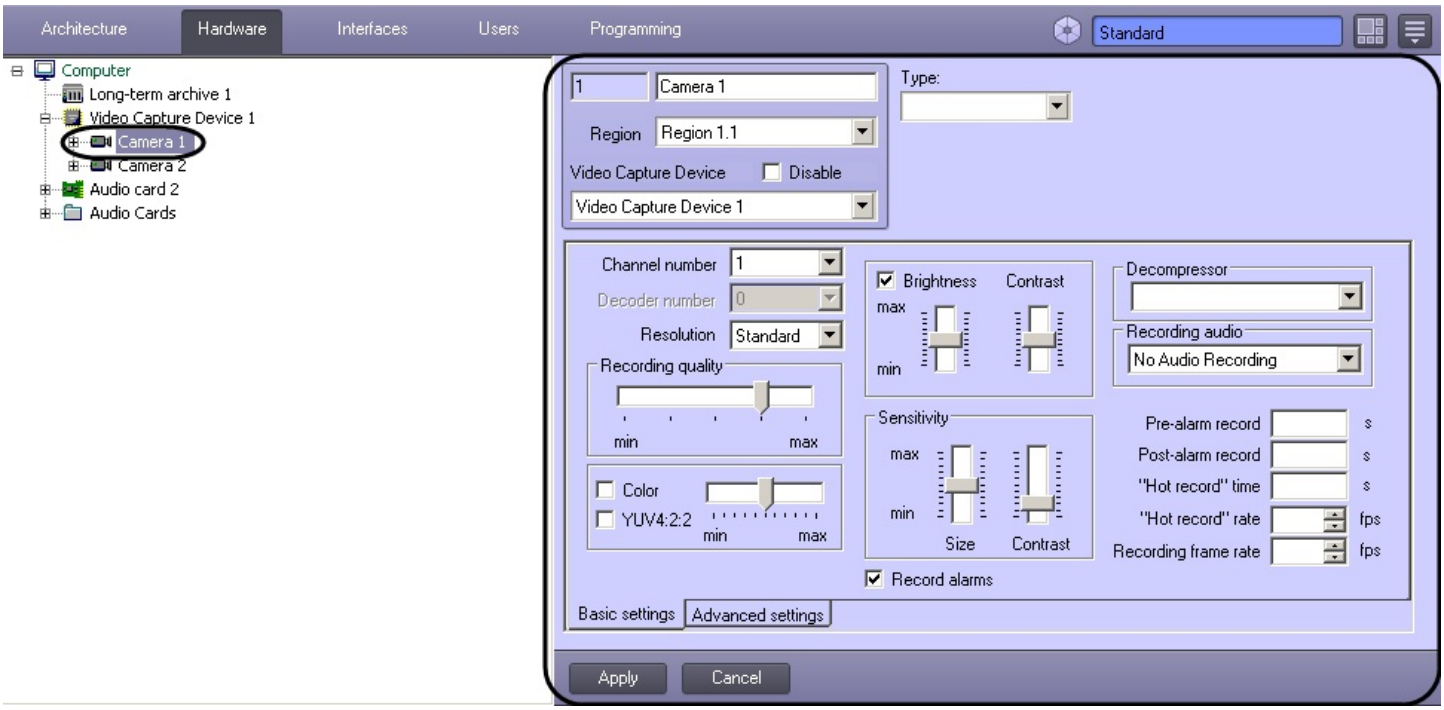
Only branch of the object tree under the object from functional menu of which the function is triggered will be expanded using this function.



To expand all object tree branches, select the **Expand tree** menu item holding down the Shift key.

13.1.2.4 The Object setting panel

The setup panel of the system object can be found in the right hand side of the **System settings** dialog box and is designed to displayed and configure the object selected in the tree.



Depending on the type of object selected, the settings panel of the given object displays the field for entering certain parameters – the elements of the settings panel.

Elements of the settings panel are given below:

1. 
   The field for entering the numerical value of the parameter
2. 
   The field for entering the line value of the parameter
3. 
   Check mark
4. 

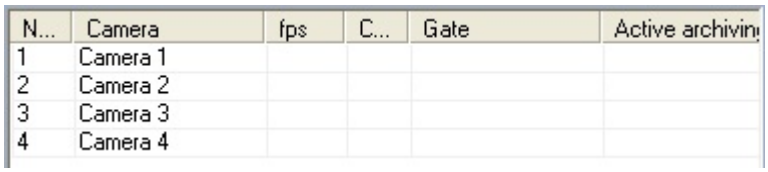
   Selector
5. 

   Slide
6. 

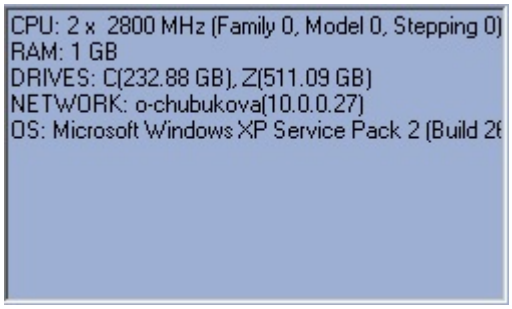
   Dropdown list

7. 

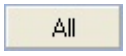
Data table

8. 

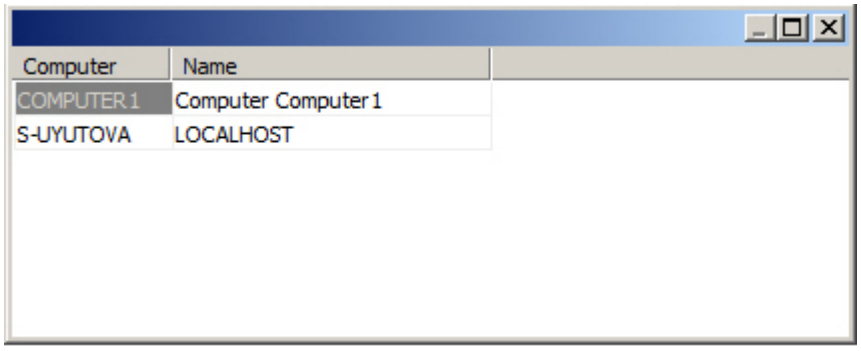
Table

9. 

Data field

10. 

Button

11. 

Extended data table

Element name	**Options for using the element**
The field for entering the numerical value of the parameter	Enter the numerical value of the parameter Drag the mouse cursor to the field, click the left button and enter the required number in the keyboard
The field for entering the line value of the parameter	Enter the line value of the parameter Drag the mouse cursor to the field and enter the required number in the keyboard
Check mark	Check/un- check the box To check the box, click on it with the left mouse button, to remove the check mark – click it again.
Selector	Set the selector in the required position To select the required option, click on it with the left mouse button. All other fields in this case get cleared automatically.

Element name	Options for using the element
Slide	Set the slide in the required position. Drag the pointer along the scale with the mouse.
Dropdown list	Select the required line in the dropdown list. The list drops down as soon as you click the down arrow, which, as a rule, is displayed in the right hand side of the element and is configured as a triangle. To select a line, click on it with the left mouse button.
Data table	The table displays the fields, which have been automatically filled in previously. To use the table, check the box corresponding to the required line (column). The fields containing text may not be edited. The number of lines may not be edited. *Note. The table for archive storage selection is an exception – new lines can be added to this table when configuring storing to network disks.* When right-clicking on any area of the information table an advanced window with information appears (see item 11 above). This window is designed to ease dealing with small tables. In order to set all the checkboxes checked in the data table select a checkbox in the column and click Ctrl+A. In order to set all the checkboxes unchecked in the data table select a checkbox and click Shift +A.
Table	The data is entered as follows: 1. Drag the cursor to the table cell. 2. Enter/select the required value in the field/from the list in the column lines of the table. As you move to the next cell, the data you have entered is retained in the table. 3. To add new lines in the table, select any field in any filled out line available and press the down arrow on the keyboard. 4. To delete a line from the table, press the Ctrl+Delete key combination.
Data field	The data field allows displaying various information messages. It cannot be edited.
Button	The start up function button. To click the button with the mouse, drag the mouse cursor to the button, then click on it with the left mouse button.
Extended data table	See Data table.

13.1.2.5 The Apply and Cancel buttons

The **Apply** and **Cancel** buttons are displayed at the bottom part of the **System settings** dialog box and are used to confirm or cancel the entry of values for the object settings.



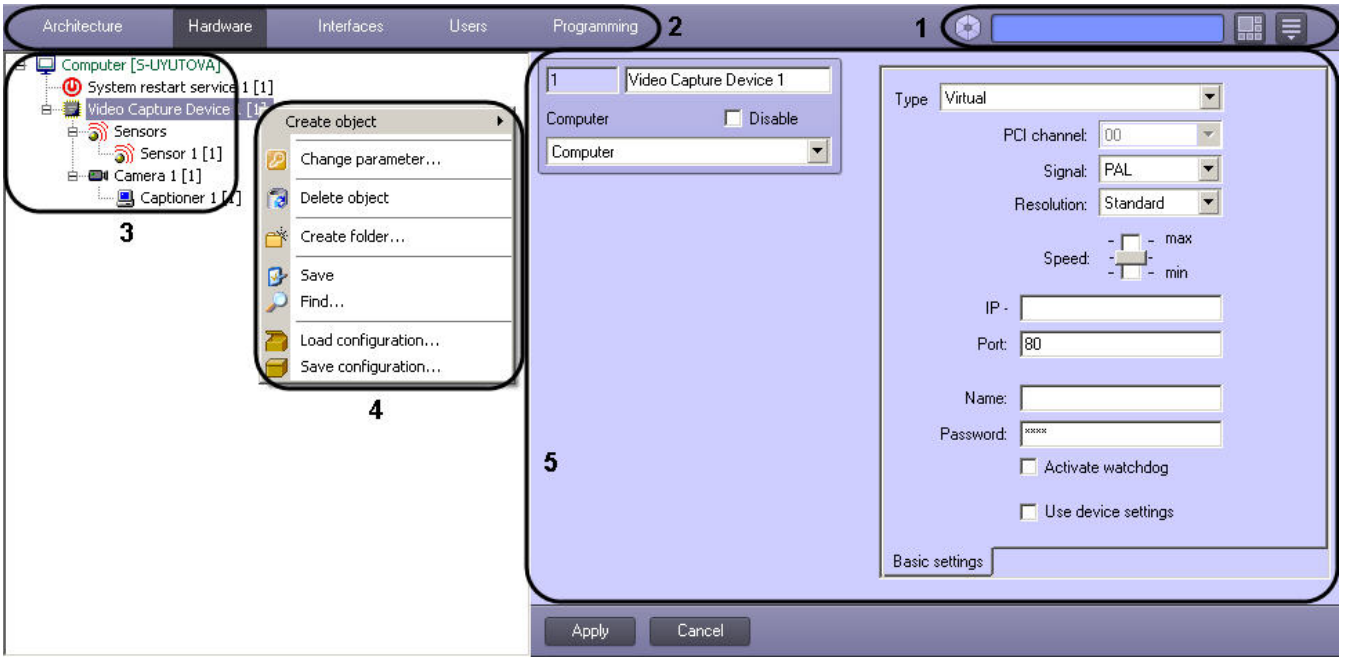
The **Apply** button is used to save the assigned object identification and setting parameters. The **Cancel** button is used to return to the previous object identification and setting parameters.

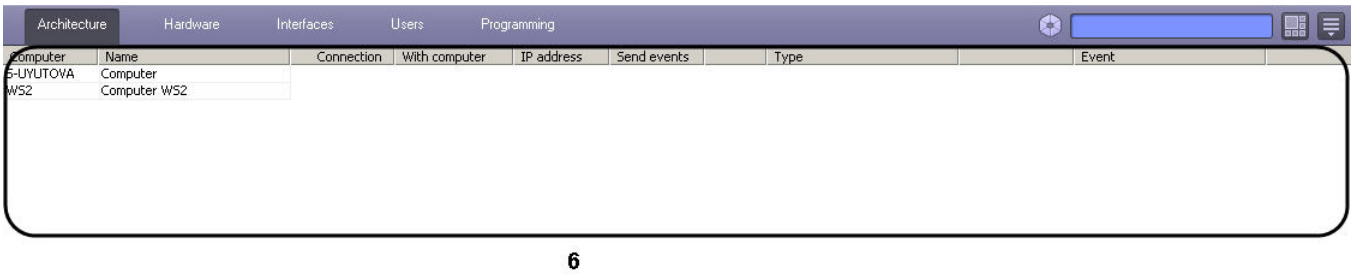
> **Note**
>
> The parameters entered with the **Apply** button cannot be cancelled with the **Cancel** button.

13.1.2.6 The elements of the System settings dialog box

The **System settings** dialog box interface contains the following elements:

1. Main Control Panel.
2. Tabs panel.
3. Objects Tree.
4. Context menu of the system object.
5. Settings panel of the objects.
6. Connection settings table.
7. **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 and audio surveillance system.

13.1.2.7 The Architecture tab

The **Architecture** tab allows creating a distributed video surveillance and audio monitoring system and is used to configure connections and data exchange between various system components.

13.1.2.7.1 Connection settings table

The Connection settings table can be accessed from the **Architecture** tab. This table is used to configure connections between computers of the distributed system and distribute the information about the events registered by the system. The connection settings table is shown in the figure.

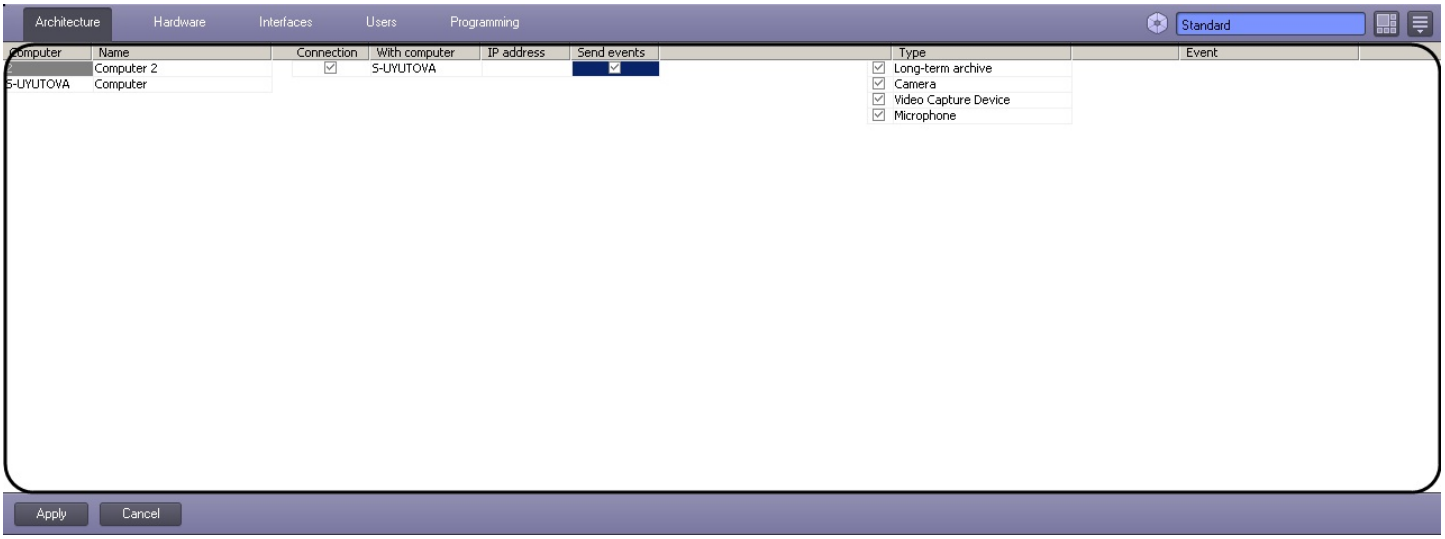


Table describes the elements of the connection settings table.

№	Column	Description	Value
1	**Computer**	Network name of the computer	Is defined by the OS
2	**Name**	Computer name in the system	Is defined in the Hardware settings tab
3	**Connection**	Check mark	If the box is checked, it means that the computer is connected. If the box is not checked, it means that connection was not established.
4	**With computer**	List of names of the network computers	Is 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)	Is either defined by the OS or assigned manually. When IP-address of the Server/RAW is edited, then IP-address only for the current Server/RAW is changed. For other Servers/RAWs IP-addresses are to be changed individually. In case of the entered address is already specified to a computer in the system, the address will be set to the configured computer and the corresponding warning message will be displayed. Address of the computer which previously had this address will be discarded.
6	**Send messages**	Checkbox	A checked box means there is permission for sending the messages to the computer it is connected to. A non-checked box means there is no permission for sending the messages.

№	Column	Description	Value
7	**Type**	List of the system objects, from which the events will be broadcast to the selected computers.	Is defined by the list of the registered objects.
8	**Event**	A check mark in the list across each point of the event list, corresponding to the hardware selected in the Type column.	A checked box means that the given event will be broadcast. A non-checked box means that the given event will not be broadcast.

13.1.2.8 The Hardware tab

The **Hardware** tab is used to create and configure the system objects corresponding to different hardware types, used as components of the video surveillance and audio monitoring system, which will be created.

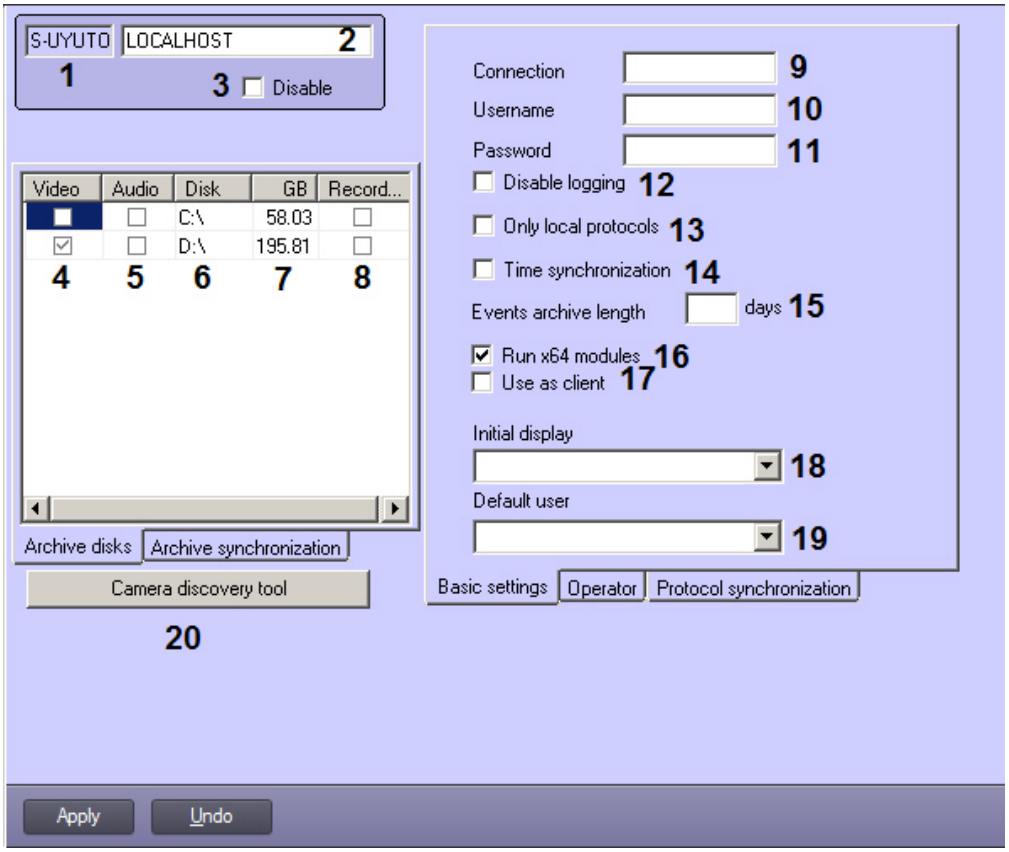
13.1.2.8.1 Hardware tab components

The **Hardware** tab displays the tree of system objects referred 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 monitoring system are described in the following sections.

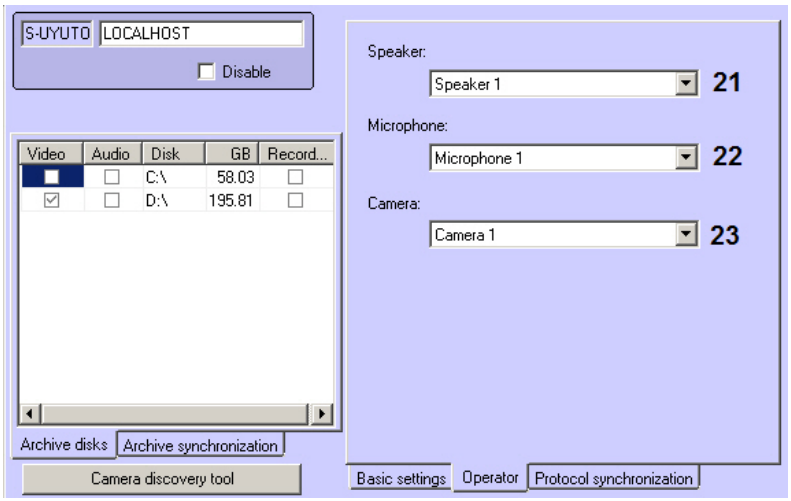
13.1.2.8.2 The Settings panel of the Computer object

The settings panel of the **Computer** object is shown in the figures.

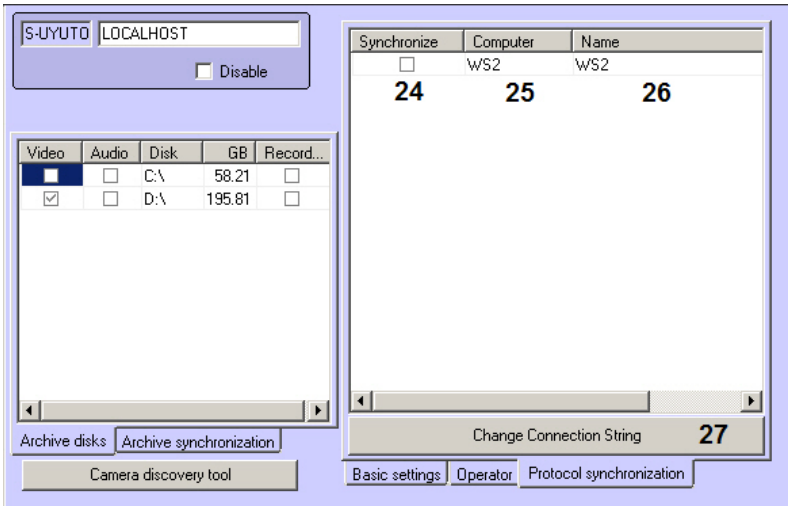
The **Basic settings** tab:



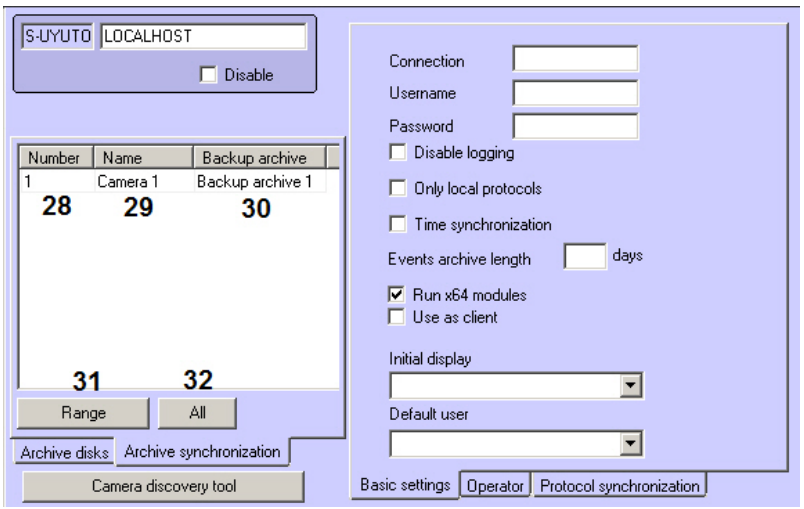
The **Operator** tab:



The **Protocol synchronization** tab:



The **Archive synchronization** tab



The table describes the parameters of the **Computer** object settings.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	**Network name***	Automatically	Displays the computer name in the local network	Latin characters and digits 0..9	-	Depends on the number of **Computer** objects registered in the system Number of symbols – from 1 to 15.
2	**Name***	Enter the value in the field	Set the name of the **Computer** object in the system	Latin, Cyrillic and service characters	Compute r	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	**Disable**	Is identified by the check mark	Defines the condition of the Computer object (enabled or disabled) in the system	Boolean type	No	Yes – the Computer is disabled and is not in use No – the Computer is enabled and is in use.
Disks for Archive Storage						
4	**Video**	Is identified by the check mark	Set the disk for storing video archive from cameras and also audio archive during synchronous audio and video recording	Boolean type	No	Yes – the disk is used for video archive storing No- the disk is not used for video archive storing
5	**Audio**	Is identified by the check mark	Set the disk for storing audio archive from microphones	Boolean type	No	Yes – the disk is used for video archive storing No- the disk is not used for video archive storing
6	**Disk**	Automatically, specify the value in the field	Displays the names of local disks, accessible for storing video and audio archive, and also used to specify the network disks used for archive storing.	Names of local disks (Latin characters), names of network disks (UNC-pathes)	-	Depends on the total number of local and network disks
7	**GB**	Automatically	Contains information about free space on the every accessible disk	Disk space in GB	-	Depends on the total free disk space
8	**Recording**	Automatically, set the checkbox checked	Show current disk for storing archive	Boolean type	No	**Yes** – the archive is currently stored on the specified disk. **No** – the archive is not currently stored on the specified disk.
Settings Group						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
9	**Connection**	Enter the value in the field	Gives the name to the modem connection used in the Windows OS.	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols (letters, digits, service characters) Number of symbols – from 1 to 30.
10	**Username**	Enter the value in the field	Sets the login name for the existing Windows modem connection.	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols (letters, digits, service characters), case-sensitive. Number of symbols – from 1 to 30.
11	**Password**	Enter the value in the field	Sets the password for the existing Windows modem connection	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols (letters, digits, service characters), case-sensitive. Number of symbols – from 1 to 30.
12	**Disable record-keeping**	Is identified by the check mark	Switches off storing of events to the Event viewer database on the local computer.	Boolean type	No	Yes - events are not stored to the Event viewer database No - events are stored to the Event viewer database
13	**Only local protocols**	Is identified by the check mark	Activates logging to the database the Events viewer only information about events, registered on the given computer	Boolean type	No	Yes – only events, registered at this computer are logged to the database the Events viewer No – events, registered at this computer are not logged to the database the Events viewer
14	**Time synchronization**	Checkbox	Set time synchronization of all computers in the distributed system with 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 time synchronization.	Boolean type	No	Yes – time is synchronized No – time is not synchronized
15	**Events archive length**	Type-in the value in the field	Sets the period of time for the events to be stored in the Event viewer database	Days	-	More than 1

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
16	**Run x64 modules checkbox**	Setting checkbox	Specifies the way of launch of 64-bits modules	Boolean type	Up to 4.10.2 – No From 4.10.3 – Yes	**Yes** - 64-bits module launches when the module launch attempt. If such variant is not found the 32-bits module launches. **No** - 64-bits modules are not launch
17	**Use as client** checkbox	Checkbox	Computer is used as the Client in the distributed video surveillance system	Boolean type	No	**Yes** – computer is used as Client. **No** – computer is used as Server or RAW.
18	**Initial display**	Is selected from the list	Set the screen to be displayed on default after starting of the Intellect digital video surveillance system. The last active **Display** is displayed after the Intellect restart if no one screen is selected.	Names of the **Display** objects registered in the system	-	Depends on total number of **Display** objects registered in the system.
19	**Default user**	Is selected from the list	Defines a default user, i.e., the user, the rights and authorities of which will be used to launch Intellect™ software without a password.	Names of the users registered in the system.	-	List of users registered in the Intellect™ system.
20	**Camera discovery tool**	Press the button	Access to creating, settings and editing of IP devices.	-	-	-
Operator						
21	**Speaker**	Is selected from the list	Allows selecting the speaker that is to be in use for audio playback (use when SIP devices are installed in video surveillance system – see Configuring SIP-devices).	Names of the **Speaker** objects registered in the system	-	Depends on number of the **Speaker** objects registered in the system
22	**Microphone**	Is selected from the list	Allows selecting the microphone that is to be in use for audio transmission (use when SIP devices are installed in video surveillance system – see Configuring SIP-devices).	Names of the **Microphone** objects registered in the system	-	Depends on number of the **Microphone** objects registered in the system
23	**Camera**	Is selected from the list	Allows selecting the camera that is to be in use for video transmission (use when SIP devices are installed in video surveillance system – see Configuring SIP-devices).	Names of the **Camera** objects registered in the system	-	Depends on number of the **Camera** objects registered in the system
Protocol synchronization						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
24	**Synchronize**	Is identified by the check mark	Set the synchronization of database The Events viewer of local and remote computers	Boolean type	No	Yes– database the Events viewer of local and remote computers are synchronized No– database the Events viewer of local and remote computers are not synchronized
25	**Computer**	Automatically	Displays the net name of remote computer with which database the Events viewer must be synchronized	Latin alphabet and service characters	-	Depends on the number of computers, registered in the system
26	**Name**	Automatically	Displays the name of remote computer in the net	Latin, Cyrillic and service characters		A line containing a sequence of any symbols (letters, digits, service characters), case-sensitive. Number of symbols – from 1 to 60.
27	**Change connection string**	Press the button	Access to settings and editing the parameters of connection to the database the Events viewer of remote computer	-	-	-
The **Archive synchronization** tab						
28	**Number**	Select in the list	Sets the ID of camera the archive of which is to 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 object tree of the main Server	-	Depends on the number of the **Camera** objects registered in the system
29	**Name**	Select in the list	Sets the name of camera the archive of which is to 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 object tree of the main Server	-	Depends on the number of the **Camera** objects registered in the system
30	**Backup archive**	Select in the list	Sets the **Backup archive** object configured to cooperate with the Failover service and used for synchronization of archive of the 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
31	**Range**	Click the button	Opens a dialog box for bulk camera selection	-	-	-
32	**All**	Click the button	Adds all created cameras to the table	-	-	-

13.1.2.8.3 The Settings panel of the Video Capture Device object

The settings panel of the **Video Capture Device** object is shown in figure.

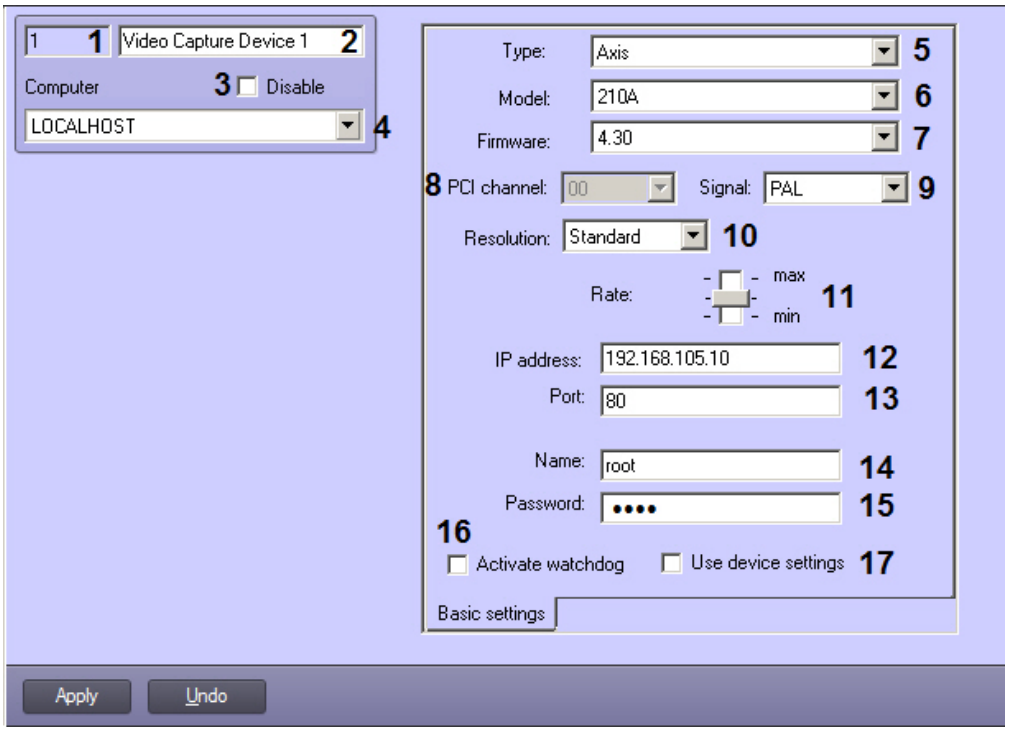


Table describes the parameters of the **Video Capture Device** settings panel.

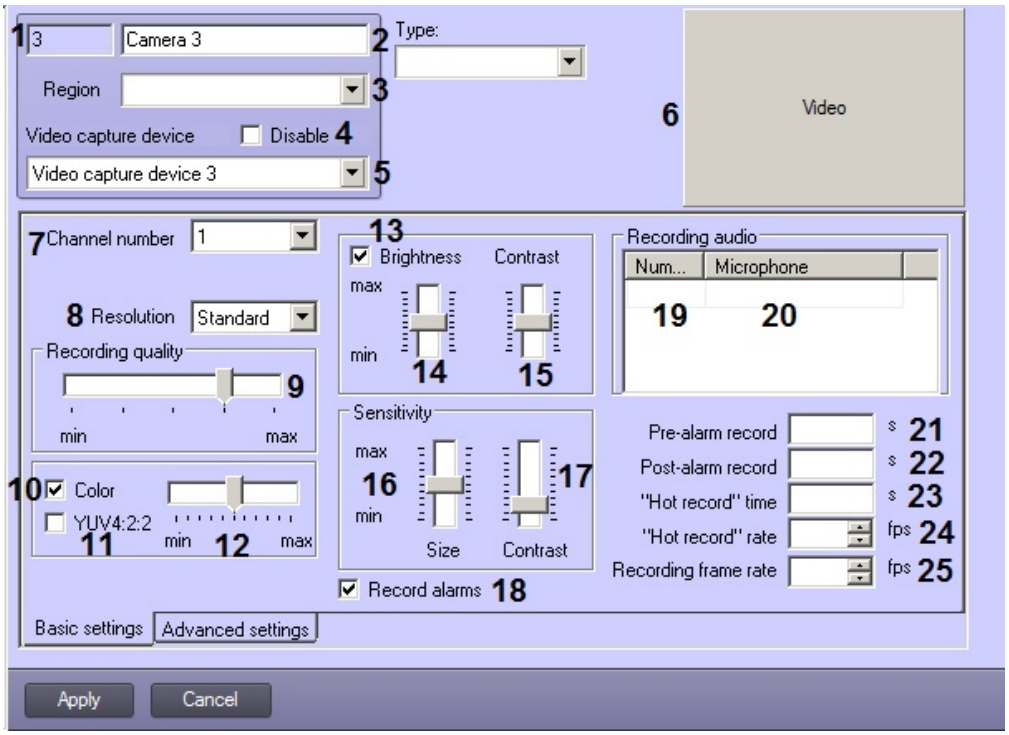
№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
1	The **Identification number** field	Automatically	Shows the identification number of the **Video Capture Device** object in the system.	Sequence of numbers	-	Depends on the number of the **Video Capture Device** objects in the system.
2	The **Name** field	Enter the value in the field	Assigns a name to the **Video Capture Device** object in the system.	Latin, Cyrillic letters and service characters	Video Capture Device	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Is set with a checkbox	Shows the status (enabled or disabled) of the **Video Capture Device** object in the system.	Boolean type	-	Yes – the **Video Capture Device** object is disabled and is not in use. No – the **Video Capture Device object** is enabled and is in use.
4	The **Computer** dropdown list	Is selected in the list	Assigns the parent **Computer** object for the **Video Capture Device** object.	Name of the **Computer** objects registered in the system.	Name of the parent **Computer** object	Depends on the number of the **Computer** objects in the system.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
The Basic settings group						
5	The **Type** dropdown list	Is selected in the list	Sets the type of the Video Capture Device or vendor of the IP device	Types of Video Capture Devices	Is not defined	Video capture cards (FS-3, FS-5, FS-6, FS-8, WS–4, WS-7/17, etc.). Network video hubs (WaveHub, LinuxHub) Network devices (Axis, Panasonic, etc.) Virtual
6	The **Model** dropdown list	Is selected in the list	Sets the model of IP device	Names of models of IP devices		Integrated models of IP devices by selected vendor
7	The **Firmware** dropdown list	Is selected in the list	Sets the firmware of the IP device	Numbers of integrated firmware of the IP device		Integrated firmware of the selected IP device
8	The **PCI channel** dropdown list	Is selected in the list	Assigns the PCI channel number of the video capture card's ADC.	List of active channels available for video input.	-	From 0 to 31, depending on the number of PCI channels in the video server and the number of installed ADCs.
9	The **Signal** dropdown list	Is selected in the list	Sets the format of the incoming video signal.	List of video signal formats	PAL	PAL, NTSC
10	The **Resolution** dropdown list	Is selected in the list	Sets resolution of the video frames.	List of available video frame resolutions	Standard	**Standard** **High**. **Full** Specific values depend on camera model.
11	The **Speed** slider	Is set in the required position.	Sets the frame rate of the video stream	Permitted deviations of the total video signal frame rate transmission.	Average	Depends on possibilities of used IP-camera or video capture card. For cards with program compression: **Max** – maximum permitted total video signal frame rate. **Average** – half of the maximum permitted total video signal frame rate. **Min** – one third of the maximum permitted total video signal frame rate.

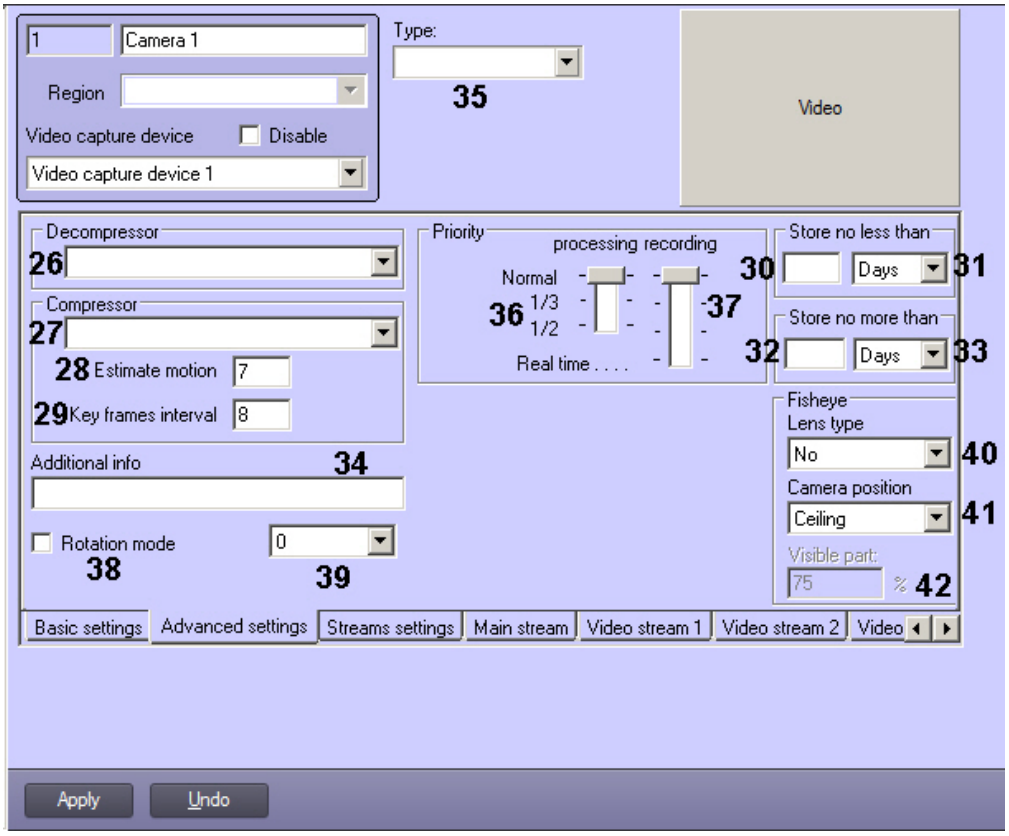
№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
12	The **IP** field	Enter the value in the field	Sets the IP address of a network device.	IP address	-	A line presented as xxx.xxx.xxx.xxx Contains the values: 0.0.0.0 – 255.255.255.255 Depends on network settings of IP devices registered in the system. When configuring getting live video from ECHD Server the *<ECHD Server address>:<camera GUID>:<external account>* line is specified.
13	The **Port** field	Enter the value in the field	Sets the connection port of IP-device	Nonnegative integer		From 0 to 65535 Depends on net settings of IP devices
14	The **Name** field	Enter the value in the field	Set the user's name for connection to the net IP-device	-	-	Depends on net settings of IP-device
15	The **Password** field	Enter the value in the field	Sets the password required for connection to the network device.	-	-	Depends on net settings of IP devices
16	The **Activate WatchDog** checkbox	Is set with a checkbox	Activate Windows OS reset, if the main modules of the Intellect video surveillance system hang up	Boolean type	-	Yes – reset of Windows OS is activated No - reset of Windows OS is not activated
17	The **Use device settings** checkbox	Is set with a checkbox	Allows using settings specified in Web server or another software of IP device	Boolean type	No *Note. Value of checkbox depends on settings performed in the wizard while creating the **Video input card** object using the* Camera discovery tool.	Yes – settings of IP device are in use. No – settings of INTELLECT™ are in use

13.1.2.8.4 The Settings panel of the Camera object

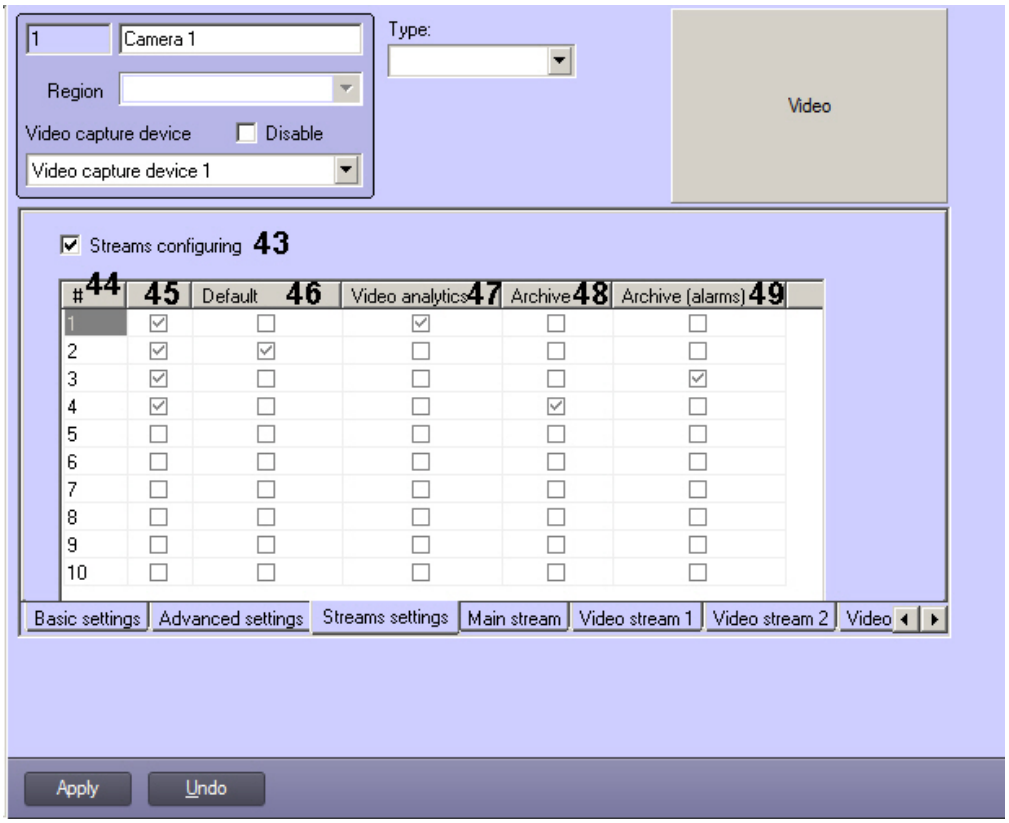
The settings panel of the **Camera** object is shown in figures.



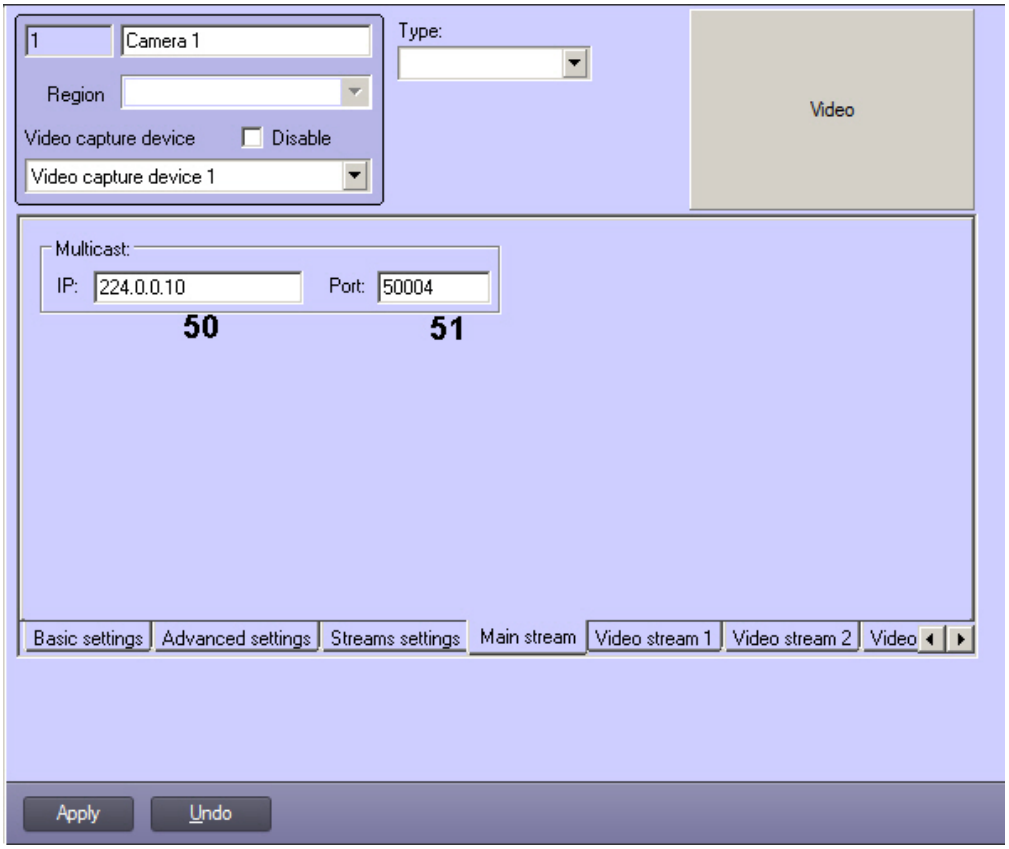
The **Basic settings** tab.



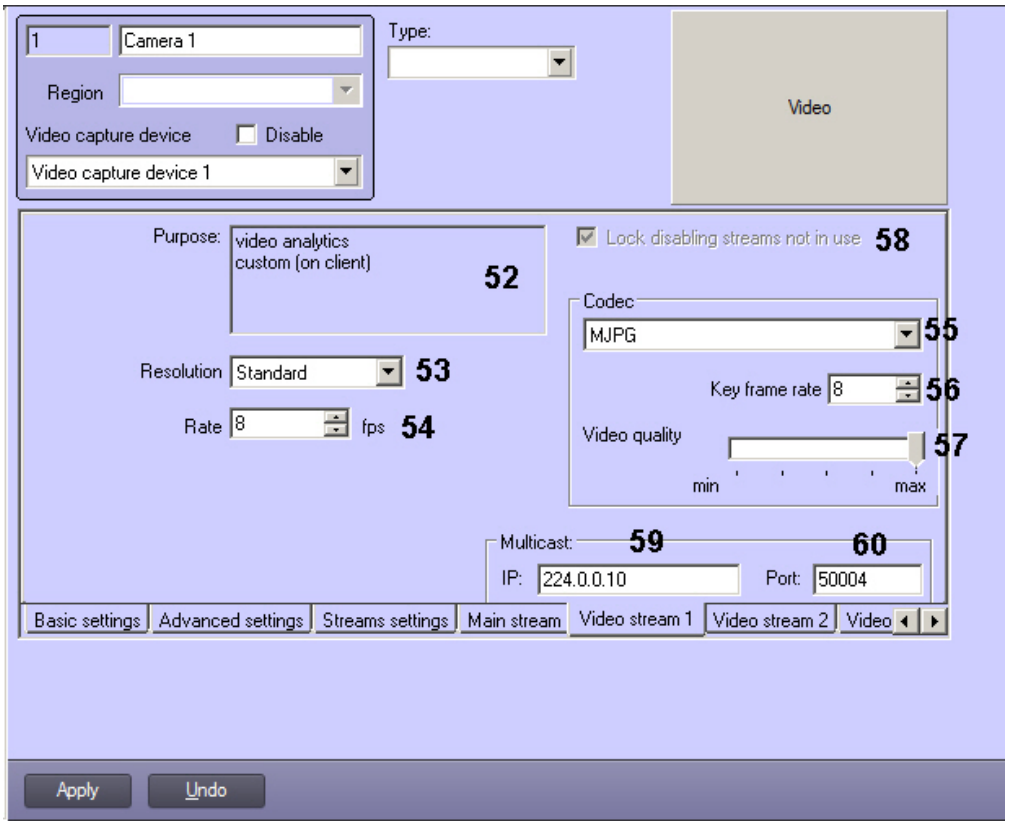
The **Advanced settings** tab.



The **Streams settings** tab.



The **Main stream** tab.



The **Video stream** tab.

Table describes the settings parameters of the **Camera** object.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
1	The **Identification number** field *	Automatically	Shows the identification number of the **Camera** system object in the system.	Sequence of numbers	-	From **1** to **FaceCamOffset,** by default FaceCamOffset = 50000. FaceCamOffset value is set with the help of the registry key of the same name (see Registry keys reference guide).
2	The **Name** field *	Enter the value in the field	Set the name of the **Camera** object in the system	Latin, Cyrillic letters and service characters	Camera	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Region drop-down** list	Is selected from the list	Assigns the **Section** structural element, to which the given **Camera** object refers.	Name of the **Section** objects registered in the system.	Section	Depends on the number of created **Section** objects registered in the system.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
4	The **Disable** checkbox	Is set with a checkbox	Set the status (enabled or disabled) of the **Camera** object in the system.	Boolean type	No	**Yes** – the **Camera** object is disabled and is not in use. **No** – the **Camera** object is enabled and is in use.
5	The **Video Capture Device** drop-down list	Is selected from the list	Set the parent **Video Capture Device** object for the given **Camera** object.	Name of the **Video Capture Device** objects registered in the system.	Name of the parent **Video Capture Device** object.	Depends on the number of the **Video Capture Device** objects in the system.
6	The **Video** box	Left-click	Displays video with settings. A webpage of *Web server* of IP device appears in default browser when pressing and holding Shift (not available in Internet Explorer).	Video	-	-
The **Basic settings** tab						
7	The **Channel number** drop-down list	Is selected from the list	Defines the number of the channel used to connect a video camera to the video capture card. Corresponds to the BNC-adapter number.	Sequence of numbers	1	Depends on the type of the video capture card. Maximum 16 channels.
8	The **Resolution** drop-down list	Is selected from the list	Set the resolution of the frame.	List of available resolutions of the frames.	Standard	**Standard**. **High**. **Full**. Particular values depend on the camera model.
9	The **Recording quality** slider	The slider is set in the required position	Set the quality of the recorded frame. Is a value reciprocal to the level of video signal compression.	-	Above average	**Min** – maximum compression level and the lowest video signal quality. **Max** – the lowest compression level and the highest video signal quality.
10	The **Color** checkbox	Is set with a checkbox	Set the type of video image received from the camera (color or black and white)	Boolean type	Yes	**Yes** – the video will be color. **No** – the video will be black and white.
11	The **YUV 4:2:2** checkbox	Is set with a checkbox	Set the format of the video signal color image.	Boolean type	No	**Yes** – the video signal will be displayed in the YUV 4:2:2 format. **No** – the video signal will be displayed in the YUV 4:2:0 format.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
12	The **Color** slider	The slider is set in the required position	Set the color saturation of the colored video	From maximum color saturation to a black and white video.	Average	**Max** – corresponds to the maximum color saturation of the video. **Min** – corresponds to the black and white video.
13	The **Brightness-Contrast** checkbox	Is set with a checkbox	Set the mode for setting brightness and contrast of the video	Types of modes for setting brightness and contrast of the video	Automatic	**Automatic** (Position 1***) - brightness and contrast are set automatically. **Manual** (Position 2***) - brightness and contrast are set manually. **Manual setting with automatic optimization** (Position 3***) - brightness and contrast are set manually and followed by automatic optimization.
14	The **Brightness** slider	The slider is set in the required position	Set the video brightness	From maximum brightness (white video) to minimum brightness (black video)	Average	**Max** – corresponds to the maximum brightness of the video. **Min** – corresponds to the minimum brightness of the video.
15	The **Contrast** slider	The slider is set in the required position	Set the video contrast	-	Average	**Max** – corresponds to the maximum contrast of the video. **Min** – corresponds to the minimum contrast of the video.
16	The **Size** slider	The slider is set in the required position	Set the minimum object size triggering the main motion detector.	% in relation to the screen elevation	Average	**Minimal** – 0% of the video surveillance box size. **Maximum** – 100% of the video surveillance box size
17	The **Contrast** slider	The slider is set in the required position	Set the minimal contrast of the object triggering the main motion detector	-	Less than average	**Max** – correspond to maximal contrast of the object **Min** – corresponds to the minimal contrast of the object

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
18	The **Record alarms** checkbox	Is set with a checkbox	Starts automatic video recording on the alarm from the camera	Boolean type	Yes	**Yes** – automatic video recording on the alarm from the camera is active. **No** – automatic video recording on the alarm from the camera is not active.
19	The **Number** drop-down list	Is selected from the list	Sets the number of Microphone audio from which is recorded simultaneously with video from the camera.	Number of the **Microphone** objects registered in the system.	-	Depends on the number of the **Microphone** objects in the system.
20	The **Microphone** drop-down list	Is selected from the list	Sets the name of Microphone audio from which is recorded simultaneously with video from the camera.	Name of the **Microphone** objects registered in the system.	-	Depends on the number of the **Microphone** objects in the system.
21	The **Pre-alarm record** field	Enter the value in the field	Set the pre-alarm time period for video recording, during which there is pre-event recording	Time (in sec)	-	Recommended time – from 0 to 20
22	The **Post-alarm record** field	Enter the value in the field	Set the time period for video recording after alarm registration.	Time (in sec)	-	Recommended time – from 0 to 20
23	The **Hot-record time** field	Enter the value in the field	Set the time period from the alarm registration or the start of record, during which the frame rate of recording will comply with the value entered in the Hot record rate field	Time (in sec)	-	Recommended time – from 0 to 30
24	The **Hot-record rate** field	Enter the value in the field / select from the list	Set the frame rate of alarm's hot recording	fps	-	Depends on the capabilities of the camera. Recommended time – from 0 to 20
25	The **Recording frame rate** field	Enter the value in the field/ select from the list	Set the frame rate for video recording	fps	-	Depends on the capabilities of the camera Recommended time – from 1 to 25 for PAL From 1 to 30 for NTSC

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
The **Advanced settings** tab						
26	The **Decompressor** drop-down list	Is selected from the list	Set the technology using which the compressed video stream will be decompressed while displaying 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 parameter (see Registry keys reference guide).*	The 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	The **Compressor** drop-down list	Is selected from the list	Set the algorithm of 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 parameter (see Registry keys reference guide).*	The list of available algorithms	No	Depends on the camera model
28	The **Estimate motion** field	Enter the value in the field	Set threshold of camera's sensivity to motion depending on the change of object's brightness. Delta frame of video signal is created by this criterion.	Sequence of numbers	7	From 2 to 255
29	The **Key frames interval** field	Enter the value in the field	Set the key frames rate.	Sequence of numbers	8	Depends on the capabilities of the camera
The **Store at least** group						

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
30	The **Store at least** field	Enter the value in the field	Set the time period for keeping the video archive from the camera and also audio archive(with the synchro records) on the Server. Parameter allows saving the large archive for selected camera due to size of other cameras archive. *Note. It is better to set the **Store at least** parameter not for more than 30% of cameras as this setting is a RECOMMENDED one. If there is not enough space for recording the archive, the setting is ignored and recording is not stopped anyway.* *If more than 10 cameras are created in the system, then while attempting to set this parameter for more than 30% of cameras in the system, the corresponding warning appears after the **Apply** button is pressed. It can be disabled using the NotifyAbout_arch_days registry key (*see Registry keys reference guide*).*	Day	-	More than 1
31	The **Store at least** dropdown list	Select value from the list	Sets units for time period specified in the **Store at least** field	The list of available time units	Days	Days Hours
The **Store no longer** group						
32	The **Store no longer** field	Enter the value in the field	Sets the time period for storing the archive – when it is expired, the archive is removed. *Note. The archive can be removed before the specified time if it is required for loop recording.*	Day or hour depending on the value selected in the dropdown list	-	More than 1
33	The **Store no longer** dropdown list	Select value from the list	Sets units for time period specified in the **Store no longer** field	The list of available time units	Days	Days Hours
Not in groups						
34	The **Additional info** field	Enter the value in the field	Set the information displayed on the monitor above the camera name. This information is added to the export file and when the frame is printed, as to the event log	The line not longer than 100 characters	Blank line	Latin, Cyrillic letters and service characters
35	The **Type** drop-down list	Is selected from the list	Set the type of the camera. The setting affects the type of the icons used to represent the camera on the map	The list of available camera types	-	Fisheye PTZ Standard
36	The **Processing priority** slider	The slider is set in the required position	Set the priority of video processing	The order of video processing	Normal	Normal – normal video procession order 1/3 – 1/3 procession order 1/2 – 1/2 procession order

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
37	The **Recording priority** slider	The slider is set in the required position	Set the priority of video processing in the recording mode	The order of video processing in the recording mode	Normal	Normal – normal video record order 1/3 – 1/3 procession order 1/2 – 1/2 procession order All resources – all ADC resourses are in use for video recording
38	**Rotation mode** checkbox	Setting checkbox	Enables a function of rotation the video image displayed on the Video surveillance monitor	Boolean type	No	**Yes -** rotation mode is enabled **No** - rotation mode is disabled
39	**Rotate on** drop-down list	Select value from the list	Specifies an angle of video image rotation when the rotation mode is enabled	Numbers	0	0, 90, 180, 270
40	The **Lens type** dropdown list	Select value in the list	Sets the type of lens in use	Supported lens types	No	**No** – select if there are no fisheye or anamorphic lenses 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 auto detection of video conversion parameters in order to eliminate artifacts is to be performed. **A0*V, A1UST, A8TRT, B0QQV, B4QQV, B5SST, B6SST** – types of panomorph lens.
41	The **Camera location** dropdown list	Select value in the list	Sets the camera location	Supported camera location modes	Ceiling	**Ceiling** **Wall** **Floor**
42	The **Visible part** field	Entered into the field	Defines the visible part of the frame on the Video Surveillance Monitor after the dewarp.	Percentage	75% for **Ceiling** position 66% for **Wall** position *Note. The default value may be not displayed.*	0-100

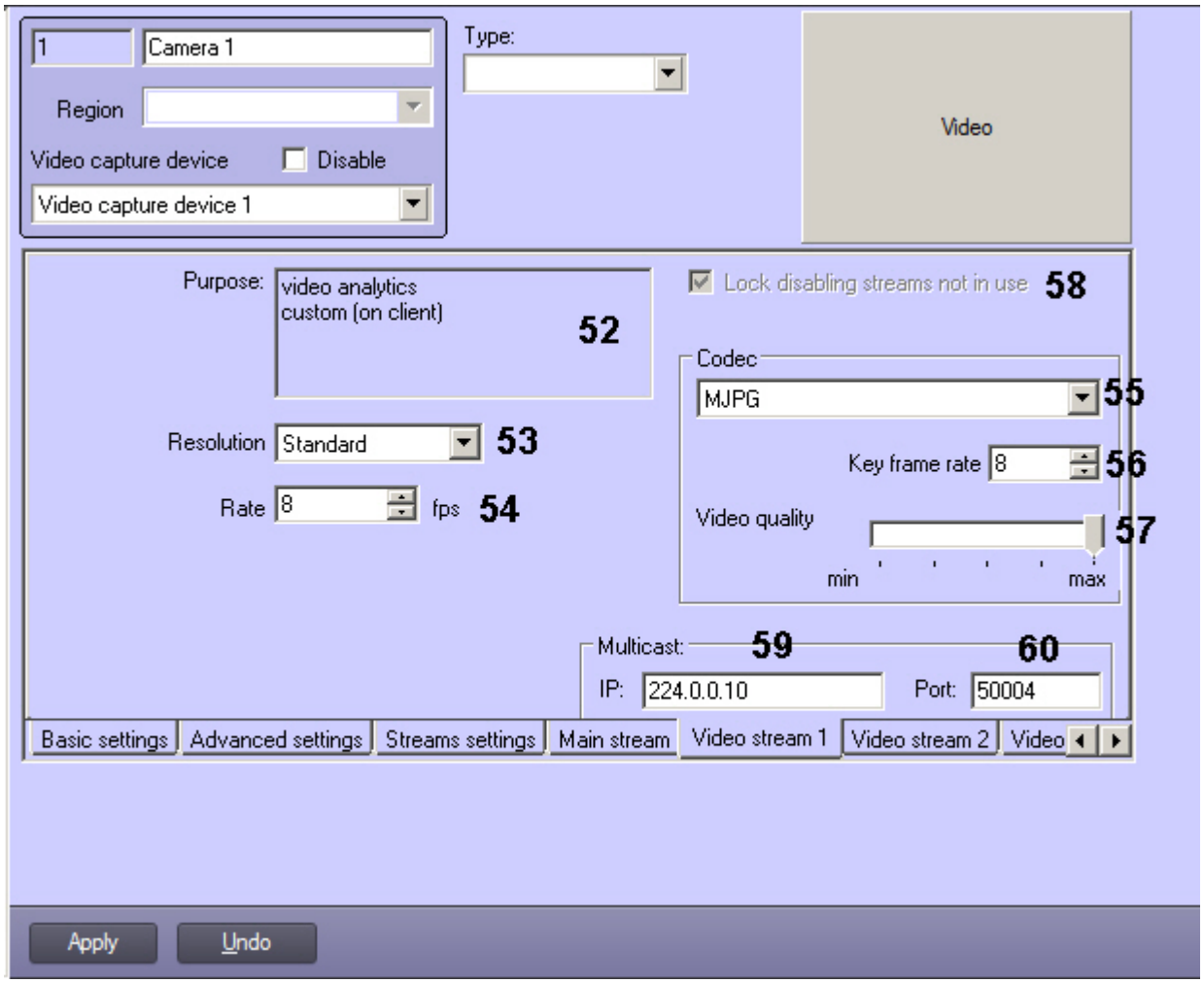
№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
Streams settings tab						
43	**Streams configuring** checkbox	Checking the box	Enables the multistream feature	Boolean	No	**True** – multistreaming is enabled; different streams can be used for analytics, archiving, and display. **False** – multistreaming is disabled; a single stream is used for analytics, archiving, and display.
44	**#** field	Automatically	Shows the stream number	Integer	-	1-10
45	**Enabled** checkbox	Checking the box	Sets the enabled streams	Boolean	No	**Yes** – the stream is in use **No** – the stream is not in use
46	**Default** checkbox	Checking the box	Assigns the video stream to be displayed both as locally and on remote clients	List of available streams	No	**Yes** – the stream is in use by default **No** – the stream is not in use by default
47	**Video analytics** checkbox	Checking the box	Assigns the video stream used for video analytics (including main motion detection tool). This stream is used by all *Intellect* detection tools (except embedded video camera detection tools) – including tracking detection tools, motion detection tool, face detection tool, facial recognition tools and detection tools that are the part of *Detector Pack.*	List of available streams	No	**Yes** – the stream is in use for video analytics **No** – the stream is not in use for video analytics
48	**Archive** checkbox	Checking the box	Sets video stream recorded to the archive not upon alarm – the continuous recording is performed.	List of available streams	No	**Yes** – the stream is in use for archive recording **No** – the stream is not in use for archive recording
49	**Archive (alarms)** checkbox	Checking the box	Sets video stream recorded to the archive upon alarm.	List of available streams	No	**Yes** – the stream is in use for archive recording by alarm **No** – the stream is not in use for archive recording by alarm
Main stream tab						
50	**IP** field	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

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
51	**Port** field	Enter the value in the field	Sets the port for transmitting the video data in the **Multicast** mode.	Numbers	Depends on the number of cameras and streams in the system	Any valid non-busy port numbers. The number of ports is determined by the system administrator.
Video stream tab						
52	**Purpose** field	-	Displays a description of how the video stream is used	String	Depends on the video stream's designated purpose	Most Latin and Russian characters, numbers
53	**Resolution** dropdown list**	Selected from a list	Assigns the video stream's resolution	List of - supported video resolutions	Standard	**Standard** **High** **Full** Particular values depend on the camera model.
54	**Speed** spinbox**	Typed into a field	Assigns the frame rate of the video stream	Frame rate (fps)	25	Depends on the capabilities of the camera
55	**Codec** dropdown list**	Selected from a list	Assigns the technology to be 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** spinbox**	Typed into a field	Assigns the key frames rate.	Set of natural numbers	8	Depends on the capabilities of the camera
57	**Video quality** slider**	Moving it to a position	Assigns the frame quality	-	Maximum	**Min** – maximum compression and minimum video quality **Max** – minimum compression and maximum video quality

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
58	Lock disabling streams not in use checkbox	Setting a checkbox	This checkbox is to be set checked if the purpose is not specified for the configured stream but is is in use for recording on command or script.	Boolean	No	**Yes** – if the stream value is not selected, then the stream is in the sleep mode and it cannot be in use for recording on command or script. **No** – if the stream purpose is not selected, then it can be in use for recording on command or script.
59	**IP** field	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** field	Enter the value in the field	Sets the port for transmitting the video data in the **Multicast** mode.	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 is not shown on the setting panel

Equivalent settings on the **Basic Settings and **Advanced settings** tabs, as well as on the settings panel of the **Video Capture Device** object, are ignored.



*** Position 1 -

Position 2 -

Position 3 -

13.1.2.8.5 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 figure.

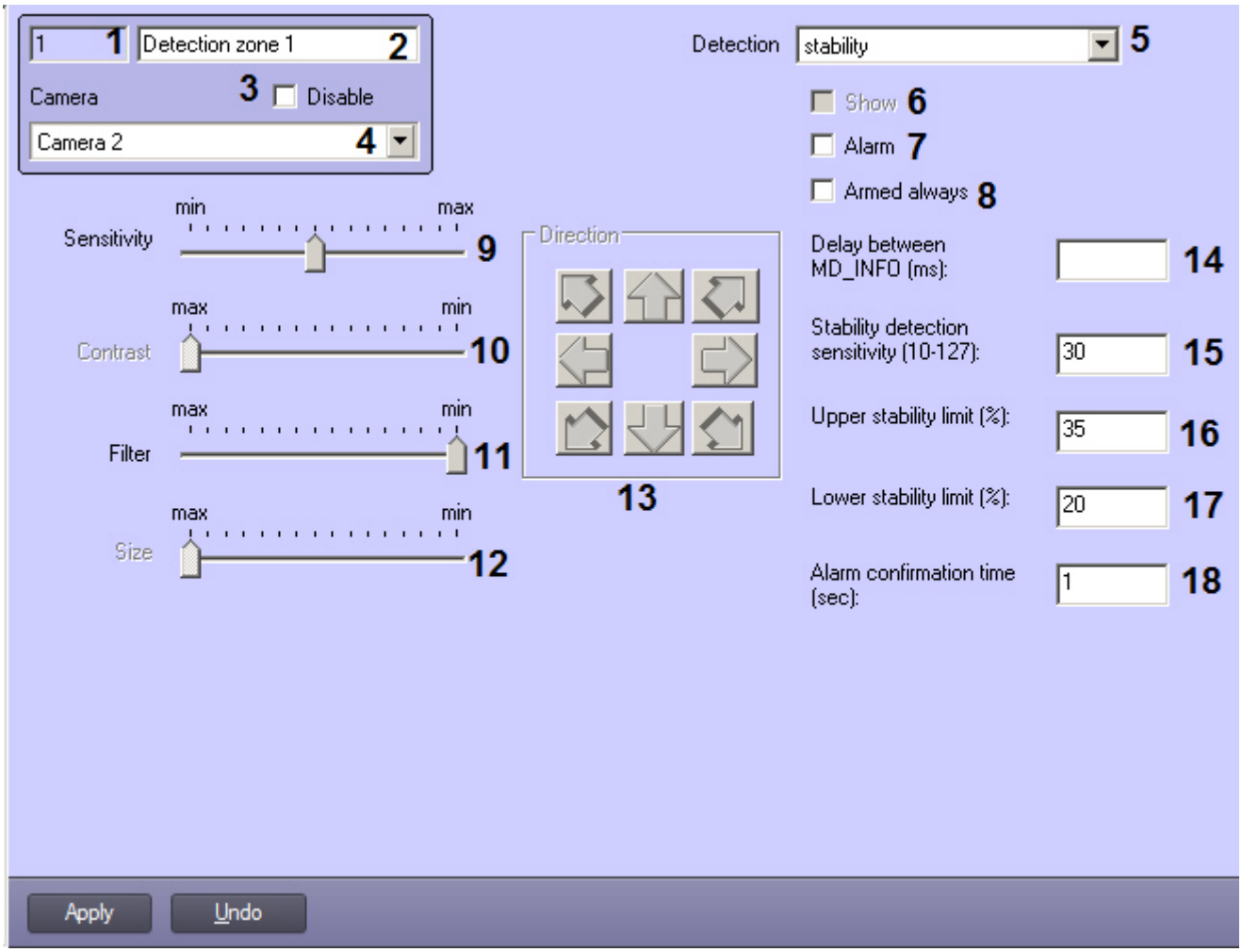


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Detection zone** object.

№	Parameter	Method for setting the parameter value	Parameter description
1	Identification number*	Automatically	Displays the identification number of the **Detection zone** object in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the name of the **Detection zone** object in the digital distributed video surveillance system.
3	Disable	Is identified by the check mark	Defines the condition of the **Detection zone** object (enabled or disabled) in the digital distributed video surveillance system.
4	Camera	Is selected from the list	Defines the parent **Camera** object of the digital distributed video surveillance system, to which the given **Detection zone** object refers.

№	Parameter	Method for setting the parameter value	Parameter description
5	Detection	Is selected from the list	Is used to define the type of the detector in use.
6	Show	Is identified by the check mark	Defines the frame border in the observed scene. This parameter is active only with the following detectors selected from the **Detector** list: motion, infrared.
7	Alarm	Is identified by the check mark	Enables alarm generation on camera and automated recording of the video signal from the camera with the alarm received from the selected detector.
8	Armed always	Is identified by the check mark.	Defines the condition of the selected detector as Always armed.
9	Sensitivity	Set the slide in the required position.	The function 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 act at its motion, and not at the video signal noise (including snow, rain, etc.). The HIGHER the sensitivity 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. **Video signal 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. **Camera blinding 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.

№	Parameter	Method for setting the parameter value	Parameter description
10	Contrast	Set the slide in the required position.	Specifies 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 pixels should be, so that the detection tool considers them as different objects. Is not applicable for all detector types.
11	Filter	Set the slide in the required position.	**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 pixels should be, so that the detection tool considers them as different objects. **Background change detection tool, video signal stability detection tool** The value of this parameter corresponds to the contrast threshold of the detected object. Is not applicable for all detector types.
12	Size	Set the slide in the required position.	The value of this parameter corresponds to the minimum size of the detection object relatively to the frame sizes. Is not applicable for all detector types.
13	Direction of search*	Press the arrow buttons.	Defines the direction of search for the motion detector.
14	Delay between MD_INFO (ms)	Enter value in the field	Sets the delay in milliseconds between MD_INFO events from the CAM_ZONE object in the Event Viewer (if MD_INFO event is enabled in ddi).
15	Stability detection sensitivity (10-127)	Enter value in the field	**Video signal stability detection tool** Sets 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
16	Upper stability limit (%)	Enter value in the field	**Video signal 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**. When exceeded, the alarm verification process starts.
17	Lower stability limit (%)	Enter value in the field	**Video signal 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.** When exceeded, the frame ceases to be used for background model.
18	Alarm confirmation time (sec)	Enter value in the field	**Video signal stability detection tool** Sets the time period in seconds during which the **Upper stability limit** must be exceeded to generate an alarm

*Name of the element is not displayed in the settings panel of the given object.

13.1.2.8.6 The Settings panel of the Audio card object

The **Audio card** object is designed to register and configure audio signal digitization devices installed on the videoserver of the Intellect™ system.

The settings panel of the **Audio card** object is shown in figure.

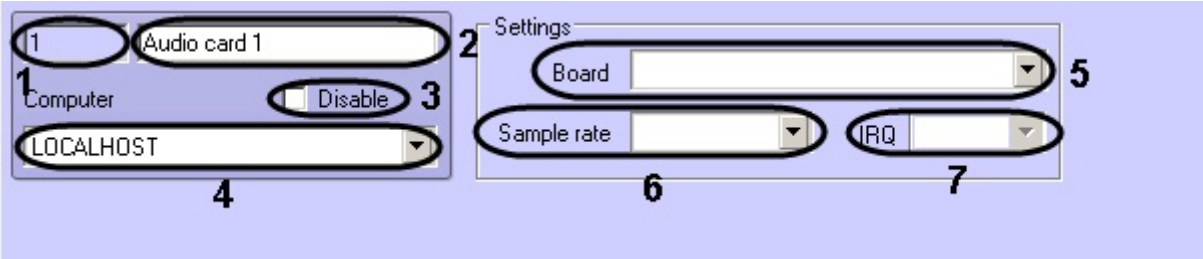


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Audio card** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Audio card** object in the digital distributed video surveillance system.	Sequence of numbers	-	Depends on the number of **Audio card** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name of the **Audio card** object in the digital distributed video surveillance system.	Latin, Cyrillic letters and service characters	Audio card	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Audio card** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	Yes – the **Audio card** object is disabled and is not in use. No – the **Audio card** object is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Audio card** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system.
Settings Group						
5	Board	Is selected from the list	Defines the device for sound digitization. Digitization devices include various sound cards, such as SoundBlaster, AD converters of the video capture cards, USB of the audio signal digitization.	List of audio digitization devices.	Not defined	Depends on the number of audio signal digitization devices installed on the videoserver. For SoundBlaster type audio cards - the name of the card For the AD converters of the video capture cards – the name of the video capture card, including the number of the audio channel. For the USB – the name of the video capture card, including the number of the audio channel. For network devices – the type of network device: AX, LH. IpCamAxis

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
6	Digitization frequency	Is selected from the list	Defines the frequency for audio signal digitization.	Hz	For SoundBlaster type audio cards - 8000. For the AD converters of the video capture cards - 8000.	For SoundBlaster type audio cards - the frequency range of the digitization depends on the type of the audio card 48 000 is the maximum value for any card. For the AD converters of the video capture cards - 8000, 16000, 32000. For USB devices – the frequency range of the digitization depends on the type of device used; 48 000 is the maximum value.
7	IRQ	Is not used	-	-	-	-

*Name of the element is not displayed in the settings panel of the given object.

13.1.2.8.7 The Settings panel of the Microphone object

The settings panel of the **Microphone** object is shown in figure.

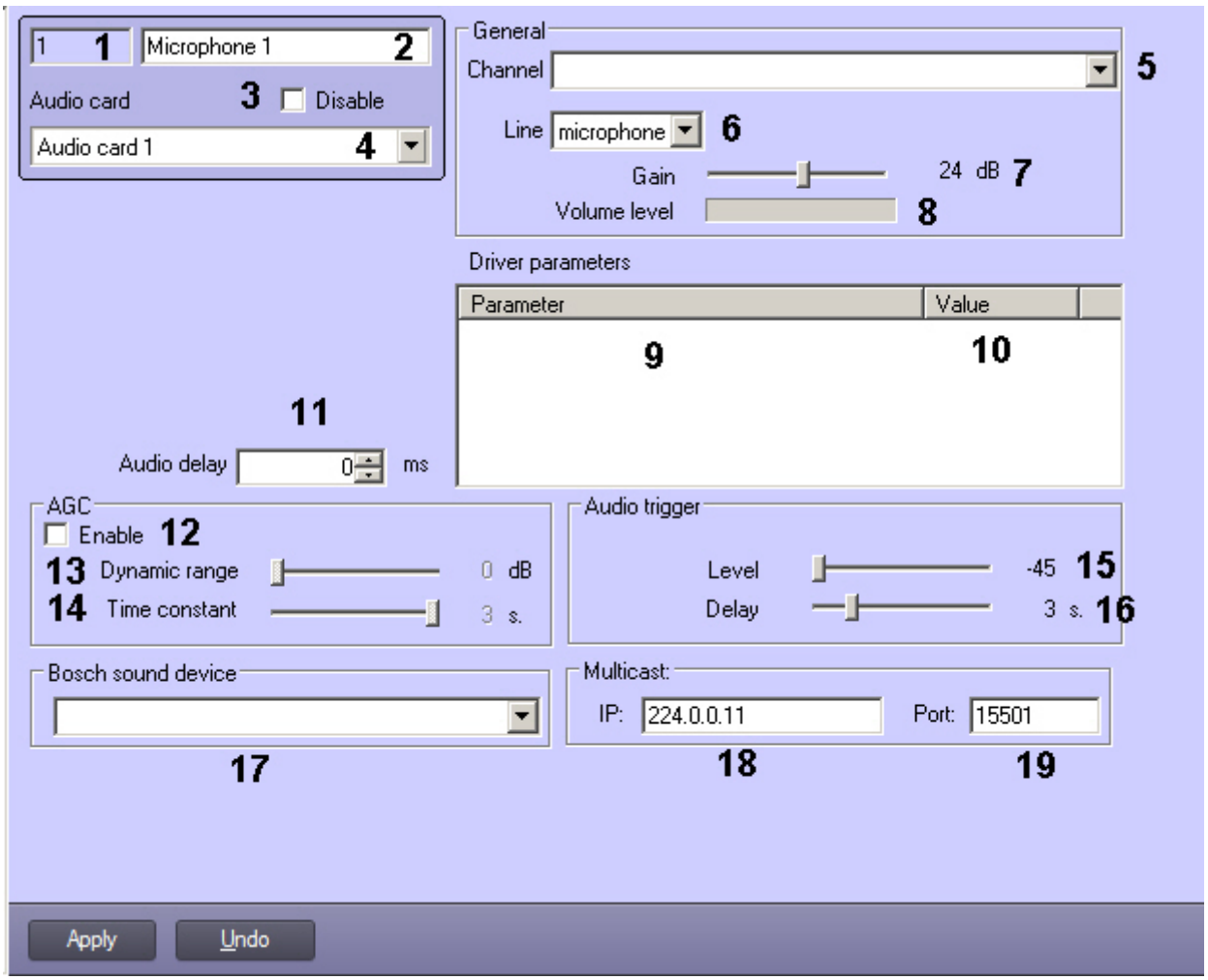


Table describes the settings parameters of the **Microphone** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbol used	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 **Microphone** objects in the system
2	Name	Entering the value in the field	Set the name of the **Microphone** object in the system	Latin, Cyrillic letters and service characters	Microphone	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Is set by a check box	Defines the condition of the **Microphone** object (enabled or disabled) in the system.	Boolean type	No	Yes – the **Microphone** is disabled and is not in use. No – the **Microphone** is enabled and is in use.
4	Audio card	Select from the list	Defines the parent **Audio card** object for the given **Microphone** object	Name of **Audio card** objects registered in the system	Name of **Audio card** parentobject	Depends on the number of Audio cards in the system.
General group						
5	Channel	Select from the list	Defines the number of the channel for the audio signal input in compliance with the RCA-F pin to which the microphone is connected.	Right,left chanel	0	Depends on the type of audio signal digitization card. For AxxonSoft AD converters of the audio signal digitization cards and SoundBlaster type audio cards: 0 – Left channel. 1 – Right channel.
6	Line	Select from the list	Set the source of audio signal	Source type of audio signal	Microphone	Microphone – audio signal comes from the microphone. Phone – the audio signal comes from the telephone line.
7	Volume	Is set in the position	Defines the volume of the audio signal	Volume of the sound in Db	24	From 0 to 45

№	Parameter	Method for setting the parameter value	Parameter description	Symbol used	Default value	Value range
8	Level	Automatically	Displays the volume of the incoming audio signal.	Volume of the sound in Db	-	From 0 to 45
The **Driver parameters** group						
9	Parameter	Automatically	Shows available parameters of IP device driver	-	-	Depends on the connected IP device.
10	Value	Select the value in the list	Sets values of IP device parameters	-	-	Depends on the connected IP device and parameter.
Outside groups						
11	Audio delay	Select the value in the field using **up** and **down** arrows	Sets the delay in milliseconds between the receiving of a audio signal from the audio input device and its output to the speaker / recording to the archive synchronously with the video signal. This parameter is used if the video image comes delayed or advanced, and the sound goes ahead or behind of it.	Sequence of numbers	0	-10000 – 10000
AGC group **(is set with the use of Olkha sound cards:«Olkha-9P», «Olkha-10LP», «Olkha-12U», «Olkha-14»)**						
12	Enable	Is set by a check box	Enables automatic adjustment of audio signal volume	Boolean type	No	Yes – automatic adjustment of audio signal volume is enable No – automatic adjustment of audio signal volume is disabled
13	Dynamic range	Is set in the position	Set the level of audio signal volume after the automatic adjustment	Sound volume in Db	0	From 0 to 45
14	Time constant	Is set in the position	Defines the time period, during which audio signal is leveled to the required volume with automatic adjustment	Time in sec	3	From 0,1 to 6
Audio trigger						

№	Parameter	Method for setting the parameter value	Parameter description	Symbol used	Default value	Value range
15	Level	Is set in the position	Set the volume of the sound, which exeeding leeds to auto recording of audio signal (registration of alarm)	Sound volume in reference units	-45	-45 – audio trigger is on From -44 to 0 –audio trigger is off
16	Delay	Is set in the position	Defines the time period, during which the threshold of audio signal after the end of alarm is being performed	Time in sec	3	From 1 to 16
Bosh sound device group (is set for sound cards IP-cameras Bosch)						
17	Bosh sound device	Select from the list	Set the sound device, audio signals from which shoul be transmitted to loudspeakers of the given IP-camera Bosch	Names of registered sound devices	-	Depends on sound devices, registered in the system
Multicast						
18	**IP** field	Enter the value in 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
19	**Port** field	Enter the value in the field	Sets the port for transmitting the audio data in the **Multicast** mode.	Numbers	Depends on the number of cameras and streams in the system	Any valid non-busy port numbers. The number of ports is determined by the system administrator.

*Name of the element is not displayed in the settings panel of the given object.

13.1.2.8.8 The Settings panel of the Telemetry controller object

The **Telemetry controller** object is designed to register and configure serial ports (COM) used for connecting the PTZ units of the Intellect™ system.

The settings panel of the **Telemetry controller** object is shown in figure.

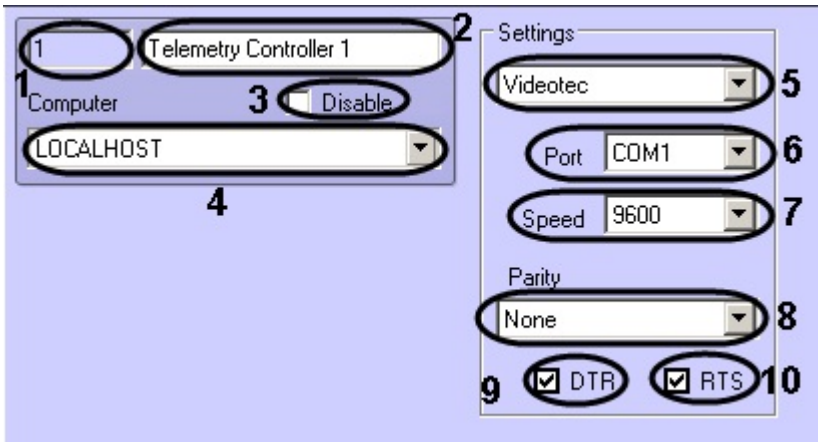


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Telemetry controller** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Telemetry controller** object in the digital distributed video surveillance system.	Sequence of numbers	-	Depends on the number of Telemetry controller objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name of the **Telemetry controller** object in the digital distributed video surveillance system.	Latin, Cyrillic letters and service characters	Telemetry controller No.	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Telemetry controller** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	Yes – the **Telemetry controller** object is disabled and is not in use No – the **Telemetry controller** is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Telemetry controller** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						
5	Controller type*	Is selected from the list	Defines the data communication protocol with the PTZ unit over the serial port (COM). Data communication protocols are supplied by the PTZ vendors.	Name of the PTZ units integrated in the system.	Videotec	Corresponds to the list of the PTZ units integrated in the system.
6	Port	Is selected from the list	Defines the number of the COM port of the computer, to which PTZ will be connected.	List of COM ports available	COM1	Depends on the number of COM ports in the videoserver or Remote administrator workstation. If a non-empty value is selected, then the local COM port priority while handling PTZ device commands is higher than other devices. Otherwise, the COM port priority is set to the default value.

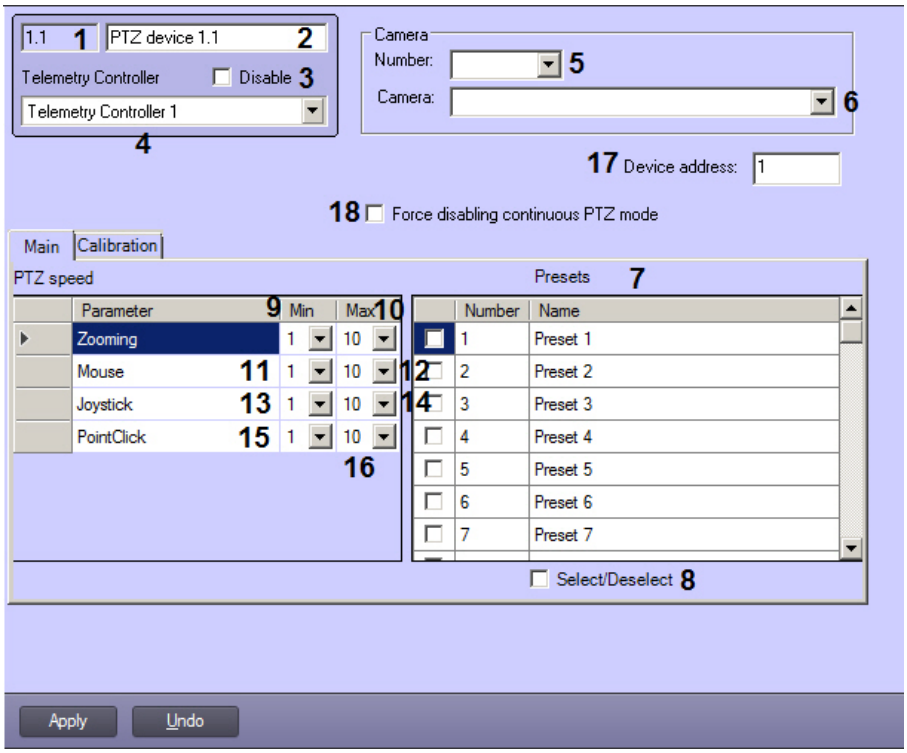
№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
7	Speed	Is selected from the list	Defines the data communication rate for the COM port.	Kb/sec	9600	From 300 to 256000.
8	Parity	Is selected from the list	Defines the parity check mode for the data transmission over the COM port.	List of parity check modes.	None	Even, Odd, None, Mark, Space.
9	DTR	Is identified by the check mark.	Defines the power supply to the PTZ unit via the DTP COM port.	Boolean type	Yes	Yes – the power will be supplied via the DTR port. No – the power will not be supplied via the DTR port.
10	RTS	Is identified by the check mark.	Defines the power supply to the PTZ unit via the RTS COM port.	Boolean type	Yes	Yes – the power will be supplied via the RTS port. No – the power will not be supplied via the RTS port.

*Name of the element is not displayed in the settings panel of the given object.

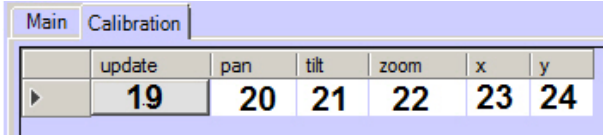
13.1.2.8.9 The Settings panel of the PTZ device object

The **PTZ device** object is designed to register and configure the PTZ device in the Intellect™ system.

The settings panel of the the **PTZ device** object is shown in 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	Symbols used	Default value	Value range
1	Identification number	Automatically	Display the identification number of the **PTZ device** object in the digital distributed video surveillance system	Sequence of numbers	-	Depends on the number of the **PTZ device** objects in the digital distributed video surveillance system
2	Name	Enter the value in the field	Set the name of the **PTZ device** object in the digital distributed video surveillance system	Latin, Cyrillic letters and service characters	PTZ device	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of characters – from 1 to 60.
3	Disable	Is set with the checkbox	Set the status of the **PTZ device** object (enabled or disabled) in the digital distributed video surveillance system	Boolean type	No	Yes – the PTZ device is disabled and is not in use No – the PTZ device is enabled and is in use.
4	Telemetry controller	Is selected from the list	Set the parent **Telemetry controller** object of the digital distributed video surveillance system, to which the given **PTZ device** object refers.	Name of the **PTZ device** objects registered in the system	Name of the parent **Telemetry controller** object.	Depends on the number of **Telemetry controllers** in the digital distributed video surveillance system
The Camera group						
5	Number	Is selected from the list	Set the identification number of the surveillance camera, where the **PTZ device** is installed.	Sequence of numbers	Not defined	Depends on the number of surveillance cameras in the digital distributed video surveillance system
6	Camera	Is selected from the list	Match the **PTZ device** with the surveillance camera, where it is installed. The parameter is used by the Video Monitor and telemetry window for the purposes to control the **PTZ device**.	Name of the **Camera** objects registered in the system	No	Depends on the number of the **Camera** objects in the digital distributed video surveillance system

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
7	Presets	Is set with the checkbox	Select the presets that are to be displayed in the **Telemetry control box**	Boolean type	No	Up to 355 presets can be enabled. Yes – the preset name is displayed in the **Telemetry control box** No – the preset name is not displayed in the **Telemetry control box**
	Name	Enter the value in the field	Set the preset name to display it in the **Telemetry control box**	Latin, Cyrillic letters and service characters	Preset	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive
8	Select/Deselect	Is set with the checkbox	Check/Uncheck all the elements in the **Presets** table	Boolean type	No	Yes – select all the presets No – uncheck all the presets
Zooming speed group						
9	**Min**	Enter the value in the field	Sets the minimal practical speed of optical zoom on the PTZ device	Speed in standard units	0	1 – 10
10	**Max**	Enter the value in the field	Sets the maximal practical speed of optical zoom on the PTZ device	Speed in standard units	0	1 – 10
Mouse group						
11	**Min**	Enter the value in the field	Sets the minimal practical rotation speed of PTZ devices from the Monitor	Speed in standard units	0	1 – 10
12	**Max**	Enter the value in the field	Sets the maximal practical rotation speed of PTZ devices from the Monitor	Speed in standard units	0	1 – 10
Joystick group						
13	**Min**	Enter the value in the field	Sets the minimal practical rotation speed of PTZ devices using joystick	Speed in standard units	0	1 – 10
14	**Max**	Enter the value in the field	Sets the maximal practical rotation speed of PTZ devices using joystick	Speed in standard units	0	1 – 10
Point&Click group						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
15	**Min**	Enter the value in the field	Sets minimal practical rotation speed of PTZ device in direction of mouse click (Point&Click)	Speed in standard units	0	1 – 10
16	**Max**	Enter the value in the field	Sets maximal practical rotation speed of PTZ device in direction of mouse click (Point&Click)	Speed in standard units	0	1 – 10
Outside the groups						
17	**RS-232 address**	Enter the value in the field	Sets address of the PTZ device configured via hardware (with jumpers on the PTZ device board) or software (through a special software for PTZ devices firmware upgrade).	Non-negative integer	1	Integer 1 to 255. Depends on 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 mode is enabled. 1 – the discrete PTZ mode is enabled.
The **Calibration** tab						
19	**update**	Click the button	Get data on the current camera position and display them in the **pan, tilt, zoom** fields	-	-	-
20	**pan**	Automatically on clicking **update**	PTZ device "pan" position	Integer	-	Depends on the model of the connected PTZ device
21	**tilt**	Automatically on clicking **update**	PTZ device "tilt" position	Integer	-	Depends on the model of the connected PTZ device
22	**zoom**	Automatically on clicking **update**	PTZ device zoom value	Non-negative integer	-	Depends on the model of the connected PTZ device
23	**x**	Enter the value in the field	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 in the field	Y coordinate of the point on the map corresponding to the selected position of the camera.		-	Depends on the Map size

13.1.2.8.10 The Settings panel of the Control panel object

The **Control panel** object is designed to register and configure a specialized control panel used for PTZ control in the Intellect™ system.

The settings panel of the **Control panel** object is shown in figure.

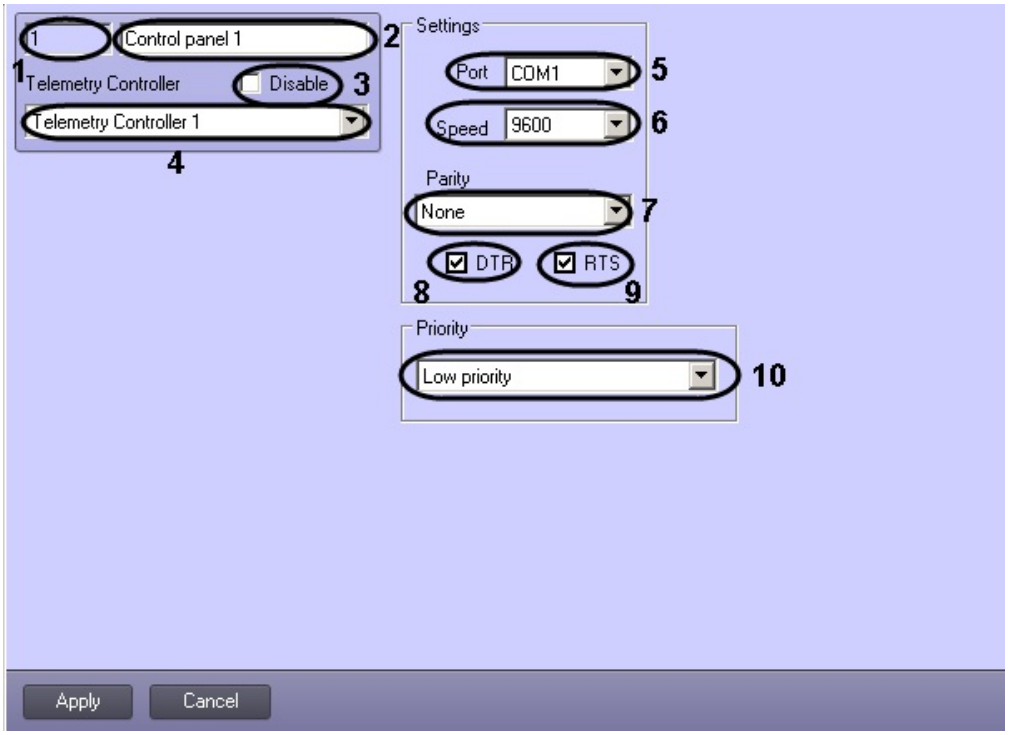


Table describes the parameters of the settings corresponding to the elements of the settings panel of the Control panel object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Control panel** object in the digital distributed video surveillance system.	Sequence of numbers	-	Depends on the number of **Control panel** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the fieldhe	Defines the name of the **Control panel** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Control panel	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Control panel** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	Yes – the Control panel object is disabled and is not in use No – the Control panel is enabled and is in use.
4	Telemetry controller	Is selected from the list	Defines the parent **Telemetry controller** object of the digital distributed video surveillance system, to which the given **Control panel** object refers.	Name of the **Telemetry controller** objects registered in the system	Name of the parent **Telemetry controller** object.	Depends on the number of **Telemetry controller** objects in the digital distributed video surveillance system

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
Settings Group						
5	Port	Is selected from the list	Defines the number of the COM port of the computer, to which the **Control panel** will be connected.	List of COM ports available	COM1	Depends on the number of COM ports in the video server or Remote Administrator Workstation.
6	Speed	Is selected from the list	Defines the data communication rate for the COM port.	Kb/sec	9600	From 300 to 256000.
7	Parity	Is selected from the list	Defines the parity check mode for the data transmission over the COM port.	List of parity check modes.	None	Even, Odd, None, Mark, Space.
8	DTR	Is identified by the check mark.	Defines, whether or not power should be supplied to the control panel via the DTA COM port.	Boolean type	Yes	**Yes** – the power will be supplied via the DTR port. **No** – the power will not be supplied via the DTR port.
9	RTS	Is identified by the check mark.	Defines, whether or not power should be supplied to the control panel via the RTS COM port.	Boolean type	Yes	**Yes** – the power will be supplied via the RTS port. **No** – the power will not be supplied via RTS port.
10	Priority	Is selected from the list	Defines priorities for control of the PTZ units using the **Control panel**.	Names of priorities used to control PTZ units.	Low	**Control prohibited** – the PTZ unit cannot be controlled using the **Control panel**. **Low** – the given PTZ can be controlled no sooner than when the PTZ with standard or high priorities has been controlled. **Standard** – the given PTZ can be controlled no sooner than when the PTZ with high priority has been controlled. **High** – the PTZ with the given priority will be controlled first.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.11 The Settings panel of the Backup archive object

The settings panel of the **Backup archive** object is shown in figure.

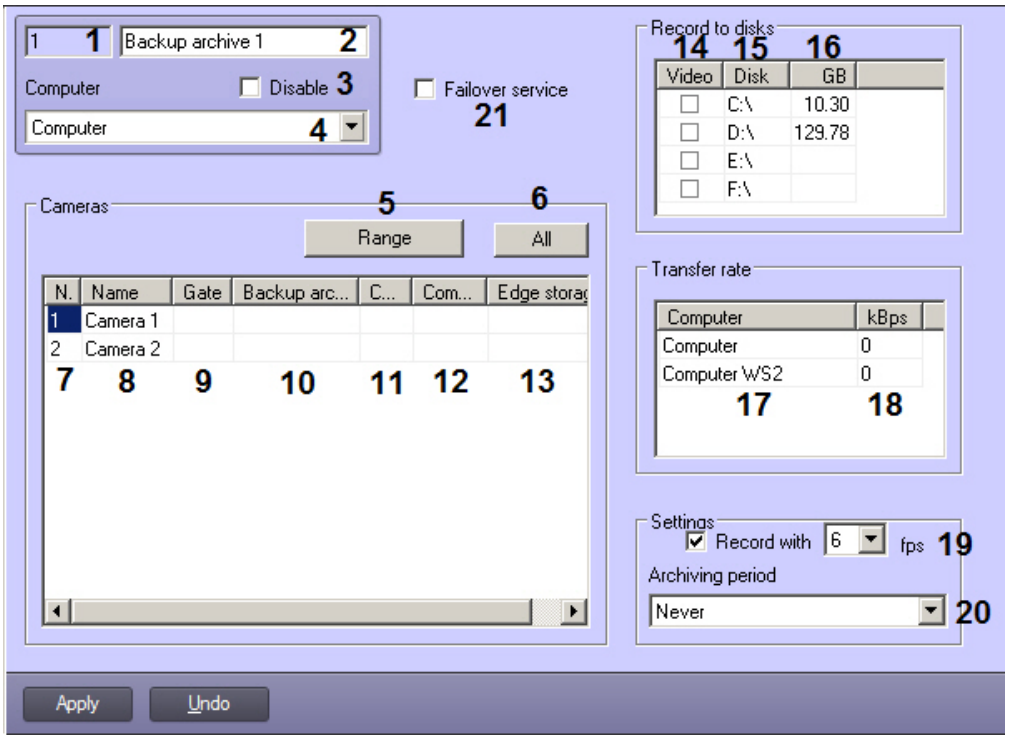


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Backup archive** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	The **Identification number** field	Automatically	Displays the identification number of the Backup archive object in the system.	Sequence of numbers	-	Depends on the number of **Backup archive** objects in the system.
2	The **Name** field	Type-in the value in 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 symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Checkbox is set	Sets the state of the **Backup archive** object (enabled or disabled) in the system.	Boolean type	No	Yes – the **Backup archive** object is disabled and is not in use. No – the **Backup archive** object is enabled and is in use.
4	The **Computer** dropdown list	Selected in the list	Sets the parent **Computer** object of the system for the given **Backup archive** object	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object	Depends on the number of **Computer** objects in the system
The Cameras group						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
5	The **Range** button	The button is pressed	Access to the complex selection of video cameras for copying of video archive to the **Backup archive**	-	-	-
6	The **All** button	The button is pressed	Selection of all cameras registered in the system for copying of video archive to the **Backup archive**	-	-	-
7	The **Number** dropdown list	Selected in the list	Sets the identification number of the surveillance camera for copying of video archive to the **Backup archive**	Sequence of numbers	-	Depends on the number of cameras registered in the system
8	The **Camera** dropdown list	Is selected from the list	Sets the name of the camera for copying of video archive to the **Backup archive**	Names of cameras registered in the system	-	Depends on the number of cameras registered in the system
9	The **Gate** dropdown list	Selected in the list	Sets the Videogate object through which video archive from the selected camera has to be transferred to the **Backup archive**	Name of the Gate objects registered in the system	-	Depends on the number of **Gate** objects registered in the system
10	The **Backup archive** dropdown list	Selected in the list	Sets the **Backup archive** object which will supply the data to the given **Backup archive**	Name of the Backup archive objects registered in the system	-	Depends on the number of **Backup archive** objects registered in the system
11	**Compression** drop-down list	Select value from the list	Specifies the level of video signal compression to record to **Backup archive**	Numbers	-	As increasing the compression level 0, 1, 2, 3, 4, 5 0 – no compression 5 – maximum compression
12	**Compressor** drop-down list	Select value from the list	Specifies the procedure of video stream compression which is in use for video signal recompression at record to the Backup archive. The value is to be selected in the **Compression** list if the compressor is specified.	List of available procedures	-	MJPEG, Motion Wavelet 3.5, Motion Wavelet 7.1

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
13	The **External storage** dropdown list	Select value from the list	Set the **External storage** object used for the archive import from the external storage on IP device	Names of **External storage** objects registered in the system	-	Depends on the number of the **External storage** objects registered in the system
The Record to drives group						
14	The **Video** checkbox	Checkbox is set	Sets the drive to store the **Backup archive**	Boolean type	No	Yes - the Backup archive is stored to the drive No - the Backup archive is not stored to the drive
15	The **Disk** column	Automatically	Displays names of local (network, USB) disks, available for storing the **Backup archive**	Name of available disks (Latin characters)	-	Depends on the total number of available disks
16	The **GB** column	Automatically	Diaplays information about free space on the every available disk	Disk space in GB	-	Depends on free disk space
The **Transfer rate** group						
17	The **Computer** column	Automatically	Sets the list of computers wrom which video is transferred to the **Backup archive**	Names of competers in the hardware tree	-	Depends on the number of **Computer** objects in the system and list of cameras selected for transferring archive
18	The **kBps** column	Type-in the value in the field	Sets the maximum bandwith of transmitting video from the computer to the **Backup archive** via the LAN.	Kbytes/sec	100	Depends on the bandwidth of the local network and resources used by the computer. 0 – bandwidth is not limited
The Settings group						
19	The **Scaling** checkbox	Checkbox is set	Enables scaling of video archive for transmitting it to the **Backup archive**	Boolean type	-	Yes – the scaling function is enabled. No – the scaling function is disabled.
	The **Scaling** dropdown list	Selected in the list	Sets the frame rate of video archive while scaling	Frame/sec	-	1, 2, 3, 4, 6, 8, 12, 25

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
20	The **Archiving period** dropdown list	Selected in the list	Set the timetable of copying video archive to the **Backup archive**	Name of **Time zone** objects registered in the system Never Always	Never	Never – there is no copying of video archive to the **Backup archive**. Always – there is copying of video archive 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 zone – copying of video archive to the Backup archive is performed according to the time zone.
21	The **Failover service** checkbox	Set the checkbox	Enables cooperation of the Backup archive with the Failover service (see also Configuring archive synchronization of main and backup Servers).	Boolean type	No	**Yes** – the *Backup archive* module is in use for synchronization of archive of the main and backup Servers in the Failover mode. **No** – the *Backup archive* module operates as usual.

13.1.2.8.12 The Settings panel of the Keyboard object

The **Keyboard** object is designed to register and configure a special keyboard used for on-line control of major functions of the Intellect™ digital distributed video surveillance system.

The settings panel of the **Keyboard** object is shown in figure.

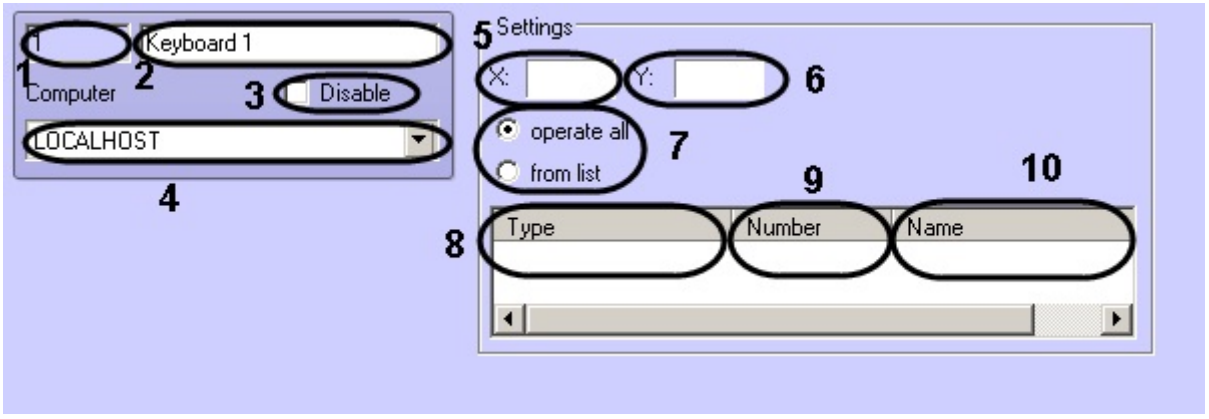


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Keyboard** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Keyboard** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Keyboard** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name of the **Keyboard** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Special keyboard	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Keyboard** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	Yes – the **Keyboard** object is disabled and is not in use No – the **Keyboard** object is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Keyboard** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						
5	X	Entering the value in the field.	Defines the coordinate on the X horizontal axis for 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	Entering the value in the field.	Defines the coordinate on the Y vertical axis for 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 selector in the required position	Defines the interface objects, which will be controlled with the special keyboard.	Types of controllable devices	Operate all	Operate all – the Operator may operate all interface objects according to the settings in the Special keyboard configuration. From list – the Operator may operate only those interface objects, which are defined in the list below.
8	Type	Is selected from the list	Defines the type of interface object, which may also be operated using the **Keyboard**.	Types of objects registered in the system.	Not defined	Depends on the number of interface objects created in the digital distributed video surveillance system.
9	Number	Is selected from the list	Defines the identification number of an interface object, which may also be operated using the **Keyboard**.	Sequence of numbers	Not defined	Depends on the number of created devices, selected in item 8 of the digital distributed video surveillance system.
10	Parameter	Automatically	Defines the device selected in item 9.	Name of the objects of the same type registered in the system	Not defined	Depends on the number of created devices, selected in item 8 of the digital distributed video surveillance system.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.13 The Settings panel of the System restart service object

The settings panel of the **System restart service** object is shown in figure.

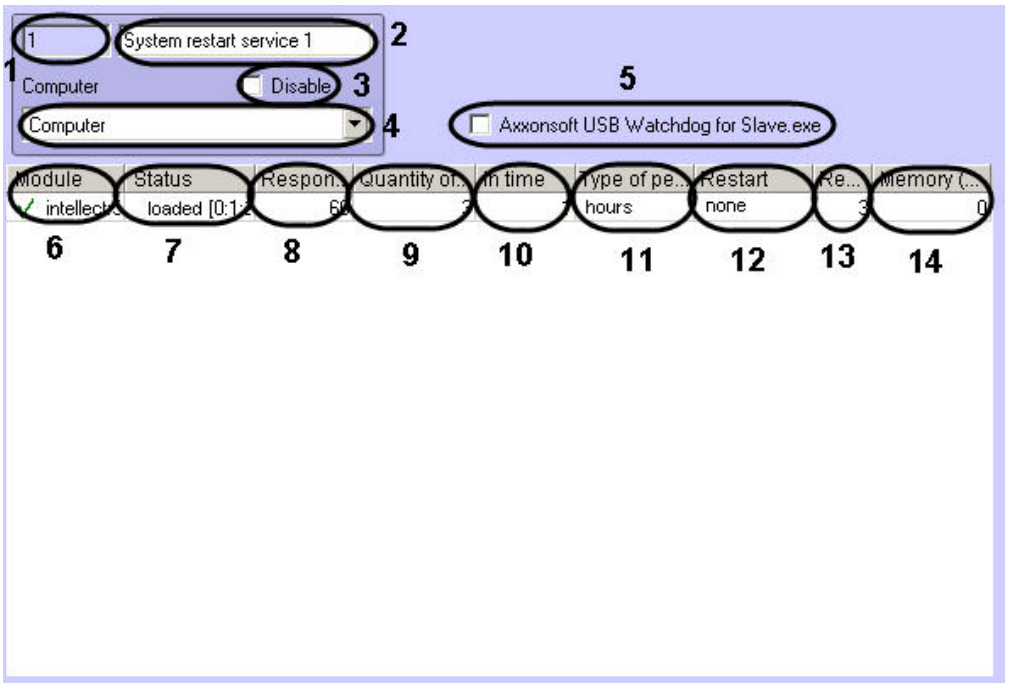


Table describes the parameters of the object settings **System restarting service**.

№	Name of parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Field **Identification number**	Automatically	Displays the object's identification number **System restart service** in the system	Sequence of numbers	-	From 1 and above. Depends on the number of objects **System restart service** in the system
2	Field **Name**	Enter the value in the field	Defines the name of the object **System restart service** in the system	Latin, Cyrillic and service characters	System restarting service	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), case-insensitive Number of symbols – from 1 to 60.
3	Checkbox **Disable**	Is identified by the check mark	Defines the condition (enabled or disabled) of the **System restart service** in the system	Boolean type	No	**Yes** – the **System restart service** is disabled and is not in use **No** – the **System restart service** is enabled and is in use.
4	Dropdown list **Computer**	Is selected from the list	Defines the parent **Computer** object in the system , to which the given object **System restart service** refers	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Name of the parent **Computer** object(object System restarting service must not be edited remotely)

№	Name of parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
5	Checkbox **AxxonSoft USB Watch Dog for Slave.exe**	Is identified by the check mark	Activates computer system of automatic restarting with the albescence of slave.exe. process's activity	Boolean type	No	**Yes** – system of automatic restarting is activated **No** – system of automatic restarting is deactivated
Control table of Intellect modules operation						
6	Column **Module**	Automatically	Displays the list of started modules at the computer	Name f started modules	-	Depends on the number of modules, registered in the system
7	Column **Status**	Automatically	Displays current state of modules	Name of current states and modules	-	**Loaded**–module operates **Unloaded** (red field) – on the expiry of waiting time interval module's response is abscent **Unloaded** – module is unloaded. ***Note**. In the square brackets the time of module working since the last restartin the HH:MM:SS format is displayed*
8	Column **Response time, sec**	Entering of text in the field	Set waiting time interval of module's response in seconds. With the absence of response on the expiry of set time interval the system may be restarted.	Nonnegative integers	60	From 0 and above
9	Column **Quantity of restarts**	Entering of text in the field	Set the maximal quantity of restarts for a period of time, specified in the column **In time** and **Period type**	Nonnegative integers	3	From 0 and above
10	Column **In time**	Entering of text in the field	Set period of time for which maximal quantity restarts of the system may be performed	Nonnegative integers	1	From 0 and above
11	Column **Period type**	Selection of value from the list		Unit s of time measurement	hours	**hours** –time period is measured in hours **days** – time period is measured in days
12	Column **Restart**	Selection of value from the list	Set the type of system's restarting	Name of possible types of restarts	Nothing	**Nothing** – restarting is not being performed **Module** – module's restarting is being performed **Core set** – restarting of the Intellect core set is being performed
13	Column **Remains of restarts**	Automatically	Displays remains or restarts for a time period, set in the columns **In time** and **Type of period**	Nonnegative integers	-	Depends on the maximal quantity of restarts and on the fact how many restarts have been performed for a current time period

№	Name of parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
14	**Memory (Mb)** column	Setting the value in the field	Specifies the threshold of memory consumed by module. When this threshold exceeded the restart is required	Integer non-negative numbers	0	From 0 and above

13.1.2.8.14 The Settings panel of the Voice Notification Service object

The **Voice notification service** object is designed for the registration of the program module, which supports voice notification of the surveillance system operation, upon occurrence of certain events.

The settings panel of the **Voice notification service** object is shown in figure.

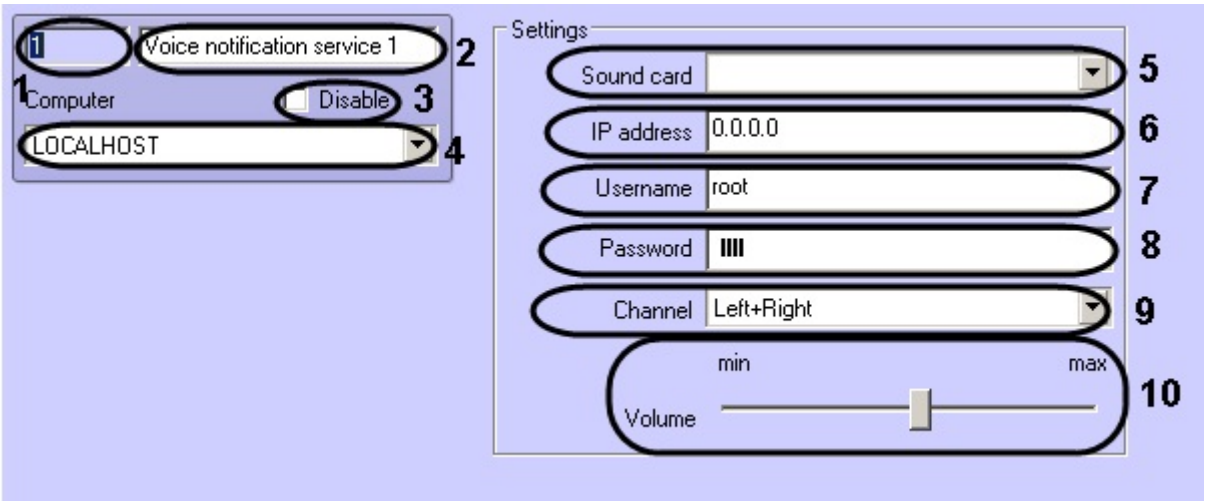


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Voice notification service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Voice notification service** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Voice notification service** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name to the **Voice notification service** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Voice notification service	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Voice notification service** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Voice notification service** is disabled and is not in use **No** – the **Voice notification service** is enabled and is in use.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given Voice notification service object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						
5	Audio card	Is selected from the list	Defines the device, which will receive an audio signal for voice notification.	Types of audio devices registered in the system.	Name of the audio card installed.	Name of the installed audio card – defines the audio card in the video server of Remote Administrator Workstation, which will process the audio signal of the voice notifications. **LinuxHub** – defines the LinuxHub type device, which will reproduce the audio signal of the voice notification. **Axis** – defines the Axis type device, which will reproduce the audio signal of the voice notification.
6	IP-address	Enter the value in the field	Defines the IP-address of LinuxHub and Axis devices. ***NOTE**. This field is active, if LinuxHub and Axis options are selected in the Audio card menu.*	Sequence of numbers	0.0.0.0	Sequence of symbols like: xxx.xxx.xxx.xxx From 0.0.0.0 to 255.255.255.255 depending on the local network settings.
7	User	Enter the value in the field	Defines the user name used for connection to LinuxHub and Axis devices. ***NOTE.** This field is active, if LinuxHub and Axis options are selected in the Audio card menu.*	Latin characters, digits and service characters.	root	A line containing a sequence of any symbols (letters, digits, service characters), case-sensitive. Number of symbols – from 1 to 60.
8	Password	Enter the value in the field	Defines a password used for connection to LinuxHub and Axis devices. ***NOTE**. This field is active, if LinuxHub and Axis options are selected in the Audio card menu.*	Latin characters, digits and service characters.	root	A line containing a sequence of any symbols (letters, digits, service characters), case-sensitive. Number of symbols – from 1 to 60.
9	Channel	Is selected from the list	Defines a channel in the audio card of the video server to reproduce the audio signal.	Name of the audio channel, where the sound is transmitted.	Left+Right	Left+Right – the audio notification signal is transmitted to both channels of the audio card. Left – the audio notification signal is transmitted to the left channel of the audio card. Right – the audio notification signal is transmitted to the right channel of the audio card.
10	Volume	The slide is placed in the required position.	Defines the volume of the audio signal, transmitted to the audio card. ***NOTE.** The option is active, if the Audio board option is selected in the audio card menu.*	Db	24 Db	Min - 0 Max - 45

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.15 The Settings panel of the Voice Message Service object

The **Voice message service** is designed for registration of the program module, which supports transmission of voice messages through telephone lines. This service provides automatic redial of pre-defined telephone numbers and playback of audio files.

The settings panel of the **Voice message service** object is shown in figure.

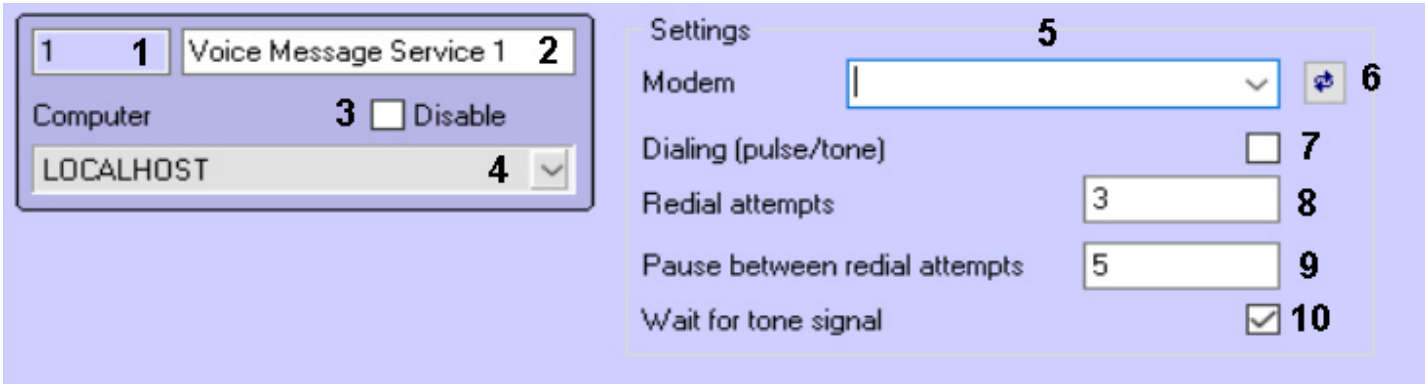


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Voice message service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Voice message service** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Voice message service** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Displays the name of the **Voice message service** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Voice messages service	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Shows the status (enabled or disabled) of the Voice messages service object in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Voice message service** is disabled and is not in use **No** – the **Voice message service** is enabled and is in use.
4	Computer	Is selected from the list	Assigns the parent **Computer** object of the digital distributed system, to which the given **Voice message service** object refers.	Name of the **Computer** objects registered in the system.	Name of the parent **Computer** object	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
5	Modem	Is selected from the list	Defines the voice modem for transmitting the voice messages.	Name of the voice modem registered by the Windows OS.	Not defined	Depends on the number of connected voice modems.
6	-	Press the button.	All connected modems are scanned to identify voice modems and to make up a list of modems.	-	-	-
7	Dialing (pulse/tone)	Is identified by the check mark	Defines number dialling mode: pulse or tone.	Boolean type	Not available	**Yes** – tone dialling. **No** – pulse dialling.
8	Redial attempts	Enter the value in the field	Defines 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 in the field	Defines a time period between redial attempts.	from	3	Recommended number from 30 to 120.
10	Wait for tone signal	Is identified by the check mark	Waits for a dial tone before redialling the number.	Boolean type	Yes	**Yes** - waiting for a dial tone before number redial is required. **No** - waiting for a dial tone before number redial is not required.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.16 The Settings panel of the Voice message object

The **Voice message** object is designed to create a voice message transmitted to the telephone lines. The settings panel of the **Voice message** object is shown in figure.

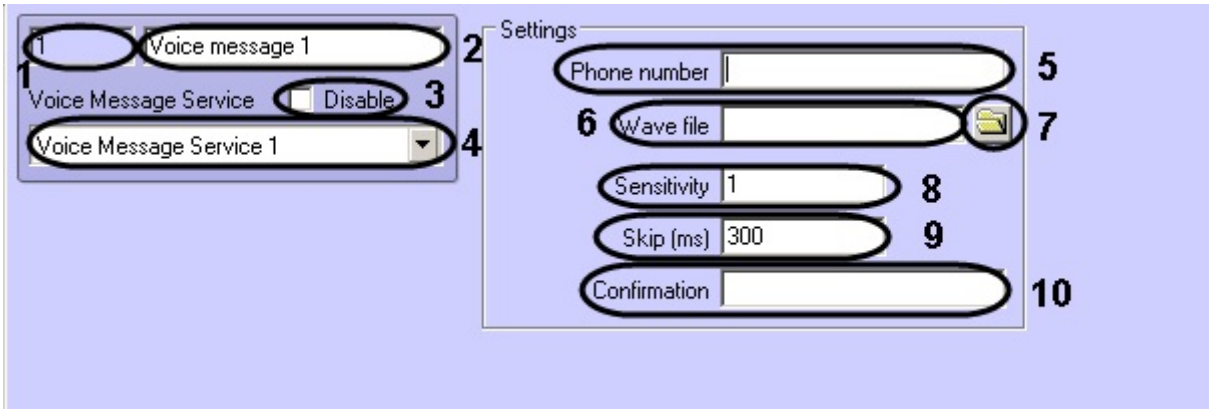


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Voice message** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Voice message** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Voice message** objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Displays the name of the **Voice messages** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Voice message	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Shows the status (enabled or disabled) of the **Voice message** object in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Voice messages** object is disabled and is not in use. **No** – the **Voice message** object is enabled and is in use.
4	Voice messages service	Is selected from the list	Assigns the parent V**oice messages service** object of the digital distributed system, to which the given **Voice message** object refers.	Name of the **Voice messages service** objects registered in the system.	Name of the parent **Voice messages service** object.	Depends on the number of **Voice message service** objects in the digital distributed video surveillance system
Settings Group						
5	Phone number	Enter the value in the field	Defines the phone number of the voice message recipient.	Sequence of numbers	Not defined	A line, containing a sequence of digits. Depends on the voice modem in use.
6	Audio file	Enter the value in the field	Defines the route 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 symbols (letters, digits, service characters), not case-sensitive
7	Wave file	Press the button.	Defines the route 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 select menu.	-	-	-
8	Sensitivity	Enter the value in the field	Defines the maximum noise level in the phone set, 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 in the field	Defines a time period between redial attempts.	ms	300	More than 1
10	Confirmation	Enter the value in the field	Defines a digital code, which the recipient should enter to confirm voice message receipt.	Sequence of numbers	Not defined	A line, containing a sequence of digits. Number of symbols should be equal to 1.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.17 The Settings panel of the Short Message Service object

The **Short message service** object is designed to register and configure the program module, which supports short message (SMS) transmission to a mobile phone via a cellular network.

The settings panel of the **Short message service** object is shown in figure.

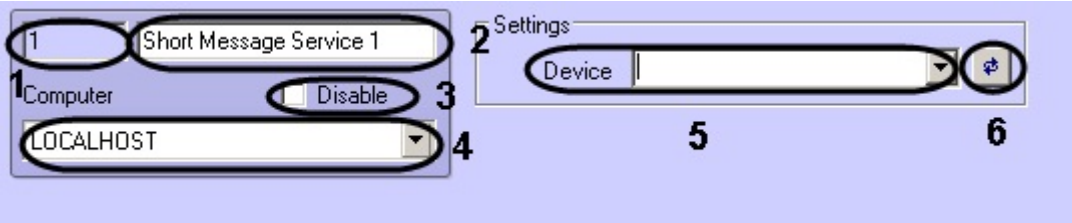


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Short message service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Short message service** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Short message service** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name of the **Short message service** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Short message service	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Short message service** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Short message service** is disabled and is not in use **No** – the **Short message service** is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Short message service** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						
5	Device	Is selected from the list	Defines the GSM device, which will be used to transmit SMS.	Names of the GSM devices registered in the Windows OS.	Not defined	Depends on the number of connected GSM devices.
6	Select device*	The button is pressed.	Scans connected devices to find GSM devices and includes them into the **Devices** list.	-	-	-

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.18 The Settings panel of the Short Message object

The **Short message** object is designed to create short messages (SMS) for transmission to mobiles phones via a mobile network.

The settings panel of the **Short message** object is shown in figure.

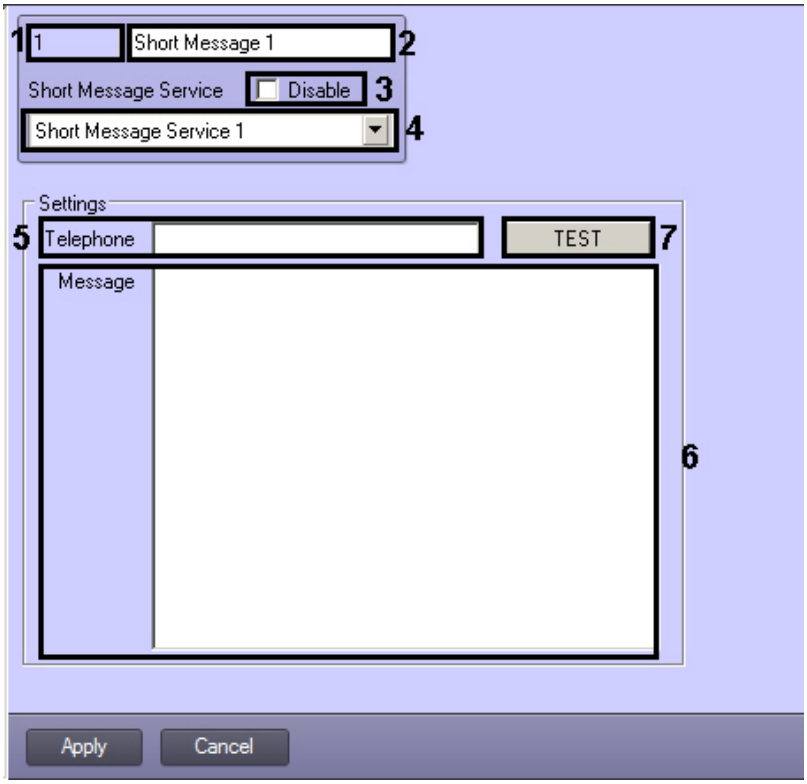


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Short message** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Short message** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of Short message objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the name of the **Short message** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Short message	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Short message** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Short message** object is disabled and is not in use **No** – the S**hort message** object is enabled and is in use.
4	Short message service	Is selected from the list	Defines the parent **Short message service** object of the digital distributed video surveillance system, to which the given **Short message** object refers.	Name of the **Short message service** objects registered in the system	Name of the parent **Short Message Service** object	Depends on the number of **Short message service** objects in the digital distributed video surveillance system
Settings Group						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
5	Phone	Enter the value in the field	Defines a mobile phone number for receiving SMS.	Sequence of numbers	Not defined	Number according to the international dial plan: Example: +79061234567)
6	Message	Enter the value in the field	Defines SMS text, which will be transmitted over the mobile network.	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.
7	TEST	Click the button	Forced sending of a short message to the specified number.	-	-	-

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.19 The Settings panel of the Mail Message Service object

The **Mail message service** object is designed to register the program module, which supports 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 figure.

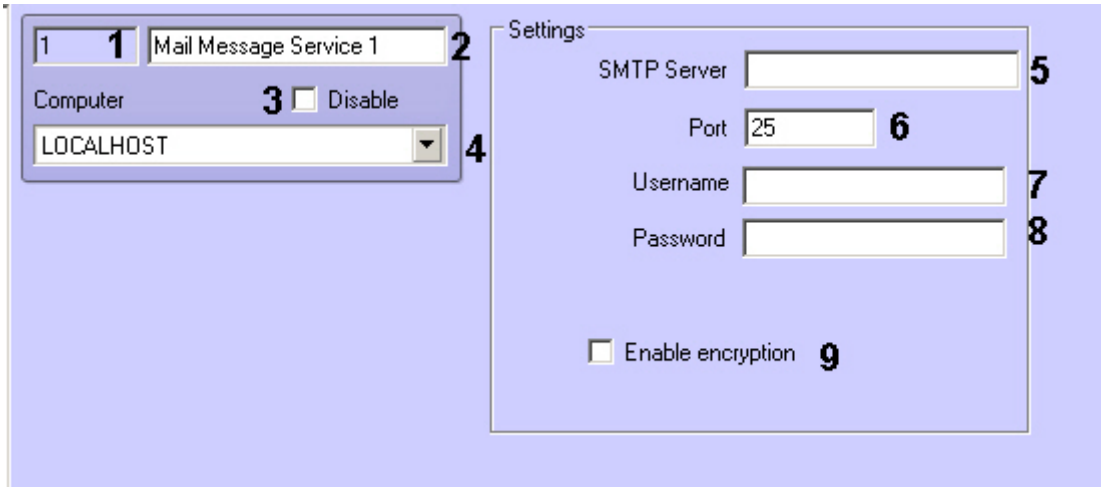


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Mail message service** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Mail message service** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Mail message service** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name of the **Mail message service** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Mail message service	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
3	Disable	Is identified by the check mark	Defines the condition of the **Mail message service** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not availab-le	**Yes** – the **Mail message service** is disabled and is not in use **No** – the **Mail message service** is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Mail message service** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						
5	SMTP server	Enter the value in the field.	Defines the SMTP server address, which will transmit SMS.	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of symbols (letters, digits, service characters), not case-sensitive, number of symbols – from 1 to 60.
6	Port	Enter the value in the field	Defines the number of the SMTP server port, which will transmit SMS.	Sequence of numbers	25	To be defined by the system administrator.
7	User name	Enter the value in the field.	Defines the user name (login) for authorization on the SMTP-server. User name matches a unique mail box name in the mail server.	Latin, service characters and digits.	Not defined	A line containing a sequence of symbols (letters, digits, service characters), case-sensitive, number of symbols – from 1 to 60.
8	Password	Enter the value in the field.	Defines a password for authorization on the SMTP-server.	Latin, service characters and digits.	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), case-sensitive. Number of symbols – from 1 to 60.
9	Enable encryption	Set the checkbox	Enables TLS encryption	Boolean type	No	**Yes** – encryption enabled. **No** – encryption disabled.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.20 The Settings panel of the Mail Message object

The **Mail message** object is designed to create mail messages (e-mail messages) for transmission to the mail boxes of the remote system users. The settings panel of the **Mail message** object is shown in figure.

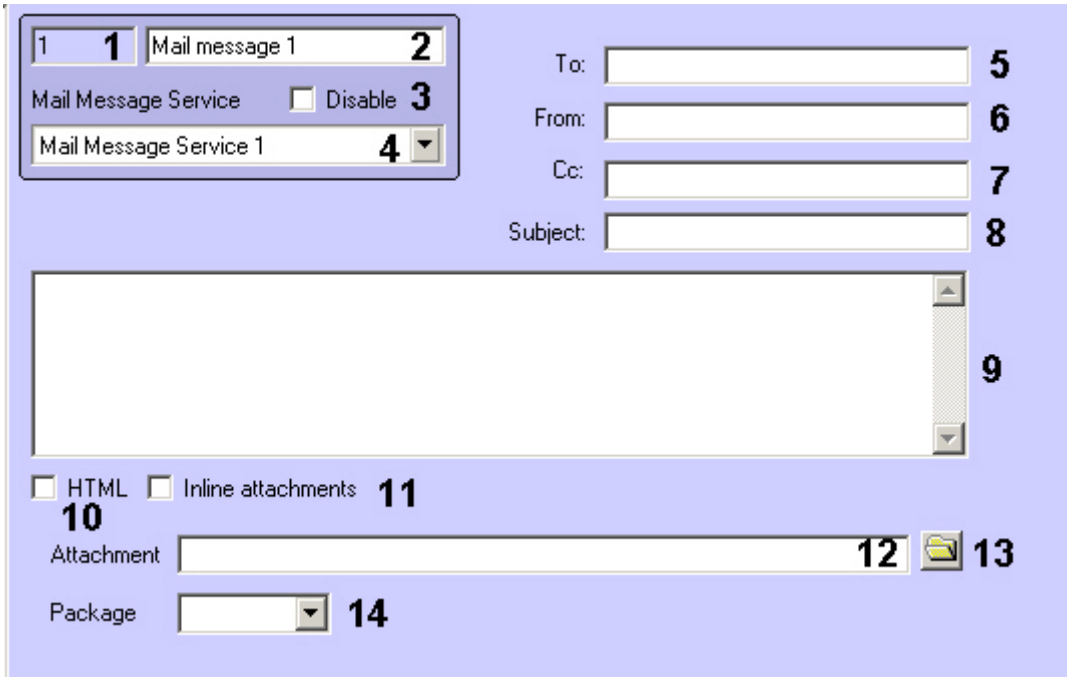


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Mail message** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Mail message** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Mail message** objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the name of the **Mail message** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Mail messa-ge	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Mail message** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not availab-le	Yes – the Mail message object is disabled and is not in use No – the Mail message object is enabled and is in use.
4	Mail message service	Is selected from the list	Defines the parent **Mail message service** object, to which the given **Mail message** object refers.	Name of the **Mail message service** objects registered in the system	Name of the parent **Mail Message Service** object	Depends on the number of **Mail message service** objects in the digital distributed video surveillance system
Settings Group						
5	To	Enter the value in the field.	Defines the mail box address of the mail message recipient.	Latin and service characters	Not defined	A line containing a sequence of symbols (letters, digits, service characters), not case-sensitive, number of symbols – from 1 to 30.

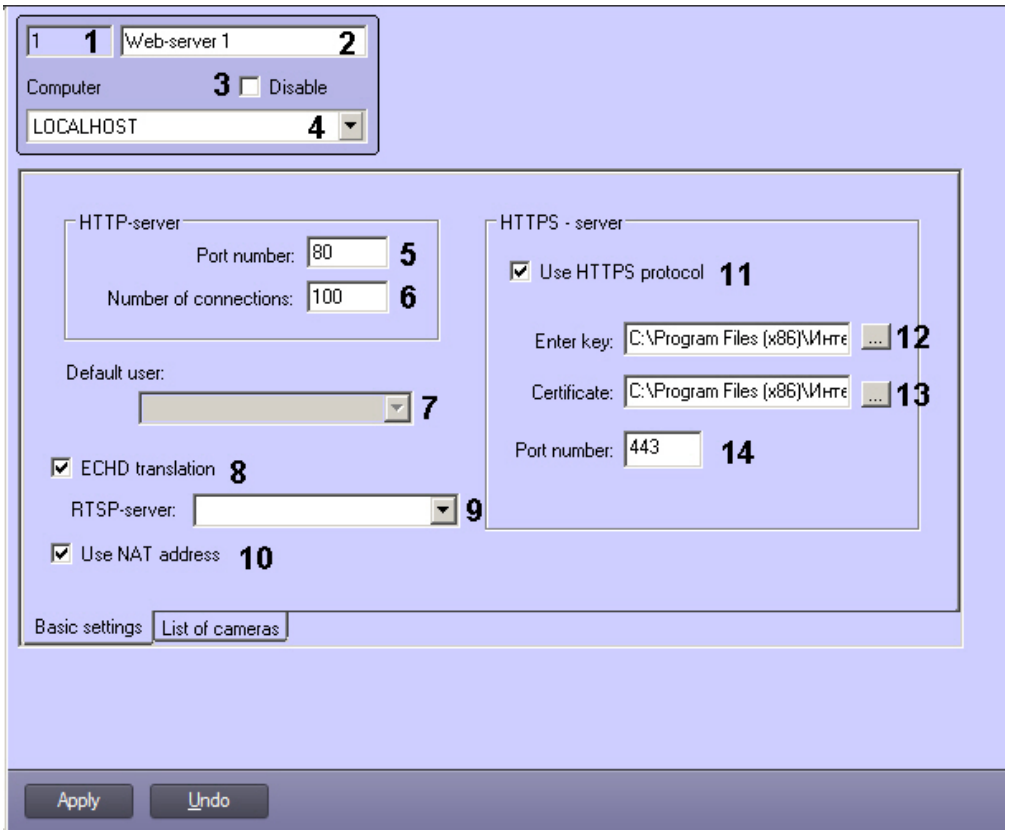
№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
6	From	Enter the value in the field.	Defines the mail box address of the mail message sender.	Latin and service characters	Not defined	A line containing a sequence of symbols (letters, digits, service characters), not case-sensitive, number of symbols – from 1 to 30.
7	CC	Enter the value in the field.	Defines the mail box address of the mail message copy recipient.	Latin and service characters	Not defined	A line containing a sequence of symbols (letters, digits, service characters), not case-sensitive, number of symbols – from 1 to 60. If a mail message needs to be copied to a few mail addresses, the said addresses should be entered separated with a comma.
8	Subject	Enter the value in the field	Defines the subject of the mail message	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.
9	Text message*	Enter the value in the field	Defines the text contents of a mail message.	Latin, Cyrillic and service characters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 250.
10	HTML	Set the checkbox	Enables HTML formatting in the e-mail message text	Boolean type	No	Yes – HTML formatting is applied. No – HTML tags are displayed as plain text if used.
11	Inline attachments	Set the checkbox	Excludes attachments from the e-mail "Attachments" section leaving them in message text only.	Boolean type	No	Yes – the attachments are excluded from the "Attachments" section and displayed in the message text only (if mentioned). No – the attachments are included both in text (if mentioned) and the "Attachments" section of the e-mail.
12	Attachment	Enter the value in the field	Defines 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 any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 250.
13	Select file*	The button is pressed.	Defines a path to the file, which will be attached to the mail message, through selecting the file directly from the standard file select menu.	-	-	-

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
14	Package	Is selected from the list	Defines the compression format for archiving the file, which will be attached to the mail message.	Archiving type	Empty field	Empty field – the file attached to the mail message is transmitted without compression. GZIP – a file attached to the mail message will be compressed in the gzip archive before transmission.

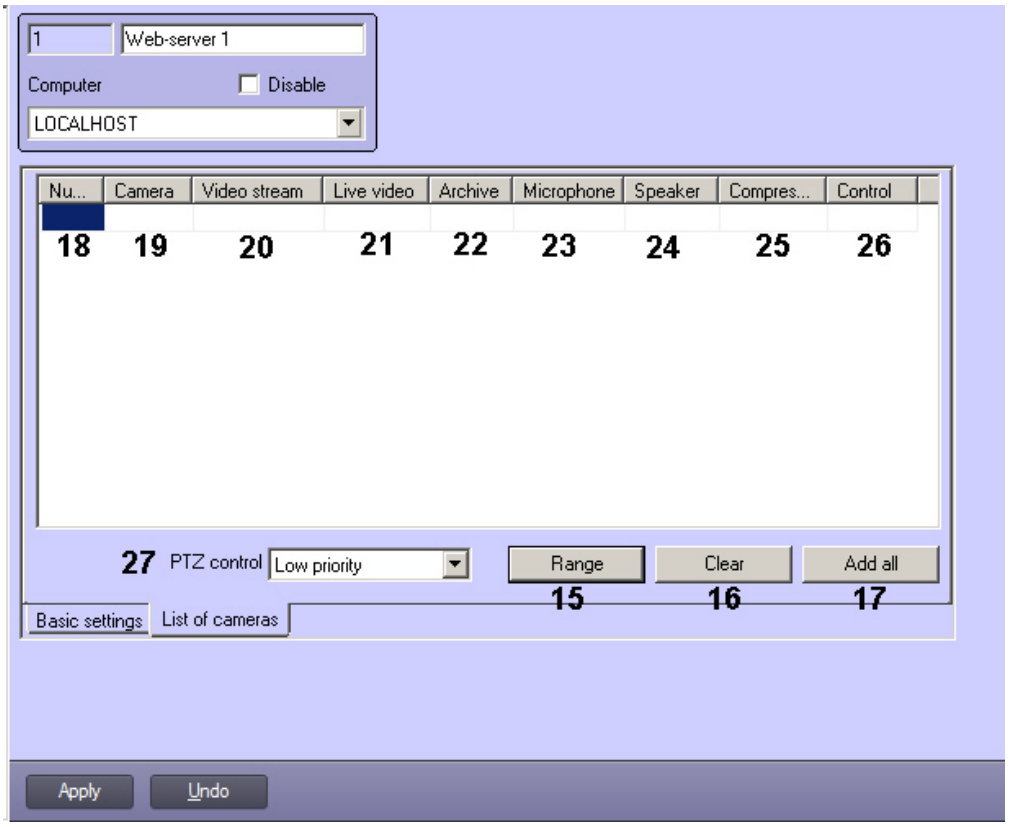
*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.21 The Settings panel of the Web-server object

The **Web-server** object is used for viewing the video surveillance information from an Internet browser and TCP/IP communication environment. The settings panel of the **Web-server** object is shown in figure.



Basic settings tab



List of cameras tab

Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Web-server** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Web-server** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of the **Web-server** objects in the digital distributed video surveillance system.
2	Name*	Type-in the value in the field	Sets the name of the **Web-server** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Web- server	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Checkbox	Sets the state of the **Web-server** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	No	Yes – the **Web-server** object is disabled and is not in use No – the **Web-server** object is enabled and is in use

4	Computer	Selected in the list	Sets the parent **Computer** object of the digital distributed video surveillance system, to which the given Web- server object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object	Depends on the number of the **Computer** objects in the digital distributed video surveillance system
The HTTP-server group						
5	Port's number	Type-in the value in the field	Sets the number of the port used by the HTTP server (for video surveillance with the Web-browser via the Internet).	Sequence of numbers	80	Any allowable port numbers which are not in use. The number of ports is defined by the system administrator.
6	Amount of connections	Type-in the value in the field	Sets the maximum allowable number of connections to the video server via the Web-server module. Each request to view the camera feed and each request to control all PTZ devices is considered as a user connection.	pcs	100	Any integer. In the case where 0 value is specified, video signals will not be displayed on the Web-server monitor.
Without a group						
7	Default user	Selected in the list	Sets the user with rights and authorities to conduct video surveillance from the Remote Workstation via the Web-server	The names of users registered in the system and added to the rights	Not set	Depends on the number of users registered in INTELLECT™
8	ECHD translation	Set the checkbox	Enables http requests used for integration with ECHD.	Boolean type	No	**Yes** – requests used for integration with ECHD are performed for the **Camera** objects under which the **ECHD channel** objects are created. **No** – requests used for integration with ECHD are not performed.
9	RTSP-server	Select value from the list	Sets rtsp server to process ECHD requests	Names of **rtsp Server** objects registered in the system	Not set	Depends on the number of **rtsp Server** objects in distributed digital surveillance system.

10	Use NAT address	Set the checkbox	Enables router address substitution in ECHD requests	Boolean type	No	**Yes** – when requesting the URL of streams through the HTTP API, the IP address of the router specified in the settings panel of the **RTSP Server** object is substituted in response to the request. **No** – when requesting the URL of streams through 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	HTTPS protocol	Set checkbox	Enabling HTTPS protocol when transferring data via Web-server.	Boolean type	No	**Yes** – HTTPS protocol is in use. **No** – HTTPS protocol is not in use.
12	Key	Enter the value in the field	Key for data communication via HTTPS protocol.	Latin, Cyrillic letters and service characters	C:\Program Files (x86)\ Intellect\Modules\SSL\ssl_itv.key	Depends on the location of data encryption key when transferring data via HTTPS protocol.
13	Certificate	Enter the value in the field	Certificate for data communication via HTTPS protocol.	Latin, Cyrillic letters and service characters	C:\Program Files (x86)\Intellect\Modules\SSL\ssl_itv.cert	Depends on the location of certificate file when transferring data via HTTPS protocol.
14	Port number	Enter the value in the field	Sets the number of the port used for HTTPS server (used for video surveillance in the web browser and in the Internet).	Natural number series	443	Any allowable port numbers that are not in use. The number of ports is specified by the system administrator.
The **List of cameras** tab						
15	Range	Click the button	The box for adding cameras as a group is opened.	-	-	-
16	Clear	Click the button	The list of added cameras is cleared.	-	-	-
17	Add all	Click the button	All **Camera** objects created in the system are added to the list.	-	-	-

18	Number	Selected in the list	Sets the number of the camera video from which is transmitted to the remote workstation using the Web-server module.	IDs of the **Camera** objects registered in the system	Not specified	Depends on the number of cameras in the distributed video surveillance system.
19	Camera	Selected in the list	Sets the name of the video camera video from which is transmitted to the Remote Workstation via the Web-server module.	Names of the **Camera** objects registered in the system	Not set	Depends on the number of video surveillance cameras in the digital distributed video surveillance system
20	Video stream	Selected in 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 enabled streams on the camera.
21	Live video	Selected in the list	Sets the source of live video to be 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	Selected in the list	Sets the source of archive footage to be displayed in the Web-server interface	Available means to get archive video	Server	Server – archive footage is received from the Server to which the camera is connected. Videogate – archive footage is received from the Videogate. If a camera is not configured to transmit footage through the Videogate, then this item is unavailable in the list. Backup archive – archive footage is received from the Backup archive
23	Microphone	Select from a list	Specifies the name of microphone associated with the camera from which the sound will be passed through the Web-server	Names of registered **Microphone** objects in the system	Not specified	Depends on the number of microphones in the video surveillance system

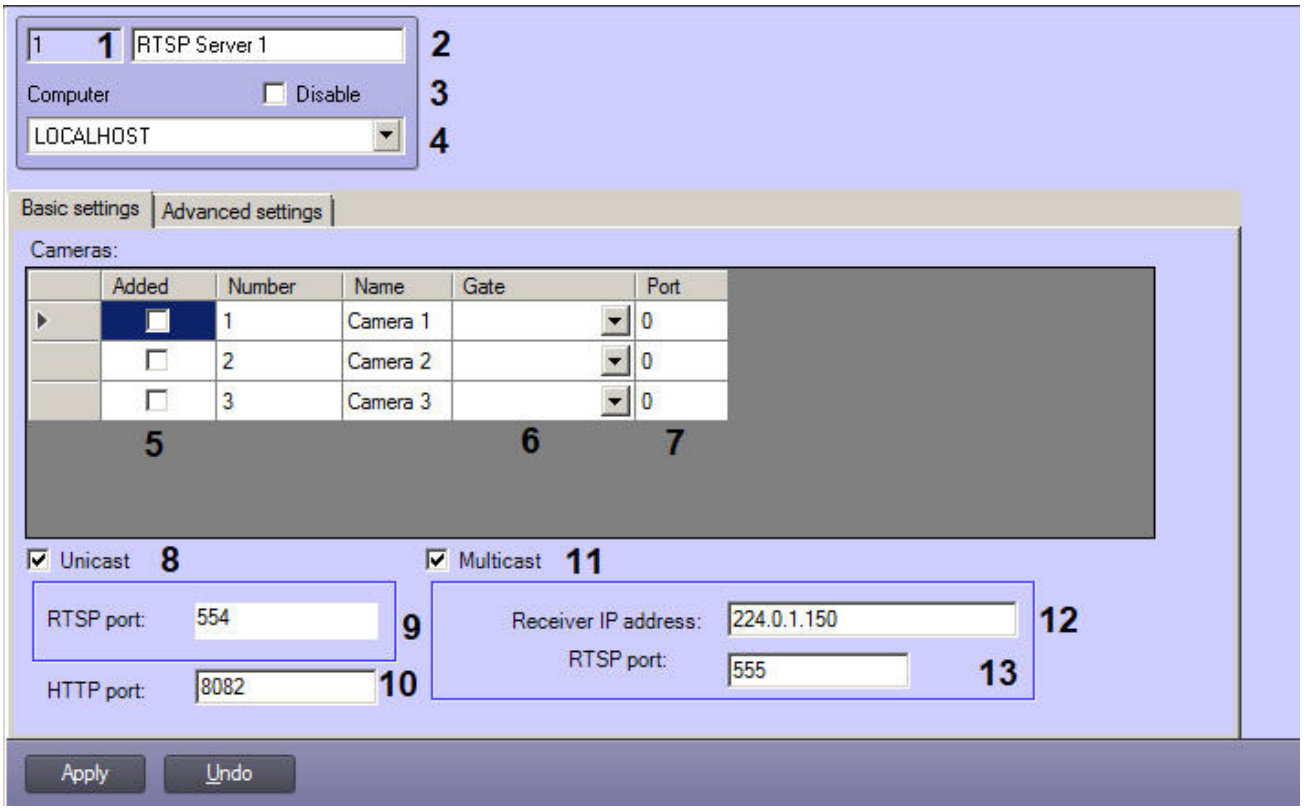
24	Speaker	Select from a list	Specifies the name of speaker associated with the camera which will be in use to playback sound received from the client	Names of registered **Speaker** objects in the system	Not specified	Depends on the number of speakers in the video surveillance system
25	Compressionn	Selected in the list	Sets the compression ratio for video transmitted to Remote Workstations via the Web-server module. The higher the compression ratio the worse the video signal is.	Reference compression ratios	Not specified	Not specified, 1 – 5. Value “1” corresponds to minimum compression ratio, “5” – to maximum. If the compression ratio is not specified, video signal is transmitted with the same compression ratio as set for recording and transmitting video
26	Control	Selected in the list	Sets the camera control (arm/disarm, PTZ, recording to the archive) in accordance with user rights.	Boolean type	Enabled	Enabled – camera control in accordance with user rights is enabled. Disabled – camera control is disabled regardless of the user rights.
27	PTZ control	Selected in the list	Set the prioritiy for the PTZ control 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

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.22 The Settings panel of the RTSP Server object

The settings panel of the **RTSP Server** object is shown in figure.

The **Basic settings** tab



The **Advanced settings** tab

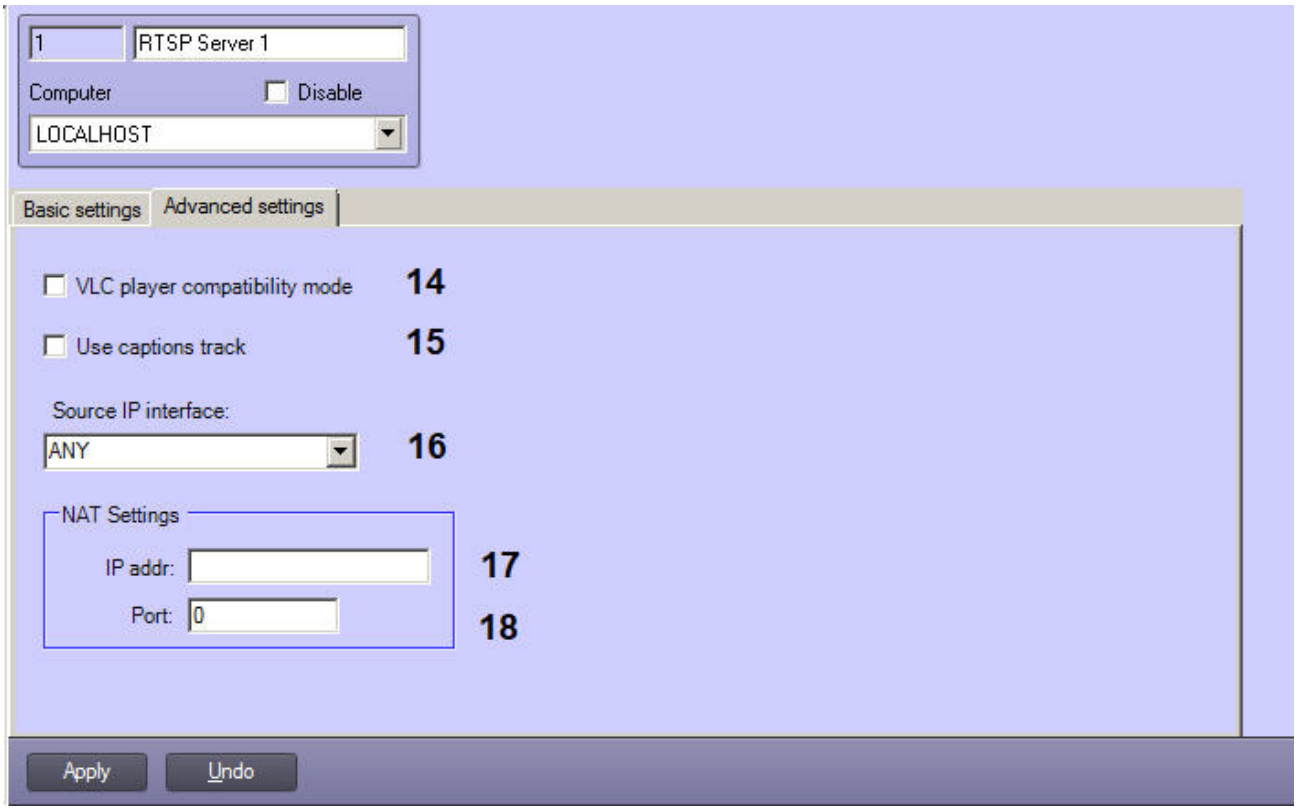


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **RTSP Server** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	ID*	Automatically	Displays the ID of the **RTSP Server** object in the video surveillance system	Sequence of numbers	-	Depends on the number of the **RTSP Server** objects in the video surveillance system
2	Name*	Type-in the value in the field	Sets the name of the **RTSP Server** object in the video surveillance system	Latin, Cyrillic and service characters	RTSP Server	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Checkbox	Sets the state (enabled or disabled) of the **RTSP Server** object in the video surveillance system	Boolean type	No	**Yes** – the **RTSP Server** object is disabled and is not in use. **No** - the **RTSP Server** object is enabled and is in use.
4	Computer	Selected in the list	Sets the parent **Computer** object to which the **RTSP Server** object relates	Names of the **Computer** objects registered in the system	Name of the parent **Computer** object	Depends on the number of Servers in the video surveillance system with distributed architecture
The **Basic settings** tab						
5	Cameras	Checkbox	Specifies cameras video from which is to be transmitted to remote workstations	Boolean type	No	**Yes** – video stream can be viewed at remote workstation. **No** – video stream cannot be viewed at remote workstation
6	Port	Type-in the value in the field	Sets a port via which a video signal from the camera is transmitted. *Note. This column is available only if is the **Multicast** check box is set checked (11).* *Note 2. Specified ports are not addressed directly. Use RTSP port to get video from all cameras in the **Multicast** mode (see item 13).*	Sequence of numbers	-	Any numbers of ports that are not in use. The number of ports is specified by the system administrator.
7	Gate	Select the value in the list	Specifies the **Video gate** through which video is received from the camera	The names of the **Video gate** objects registered in the system	-	Depends on the number of the **Video gate** objects registered in the system

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
8	Unicast	Checkbox	Enables the "unicast" transmitting mode	Boolean type	Yes	**Yes** – the video is transmitted in the "unicast" mode. **No** – the video is not transmitted in the "unicast" mode.
9	RTSP port	Type-in the value in the field	Sets the port via which video is transmitted	Sequence of numbers	554	Any numbers of ports that are not in use. The number of ports is specified by the system administrator.
10	HTTP port	Type-in the value in the field	Sets the port which is to be in use for transmitting video via http-protocol	Sequence of numbers	8081	Any numbers of ports that are not in use. The number of ports is specified by the system administrator.
11	Multicast	Checkbox	Enables video transmission via different RTSP ports. The **Multicast** mode allows reducing Server load due to transmitted data reduction.	Boolean type	No	**Yes** – the video is transmitted in the "multicast" mode. **No** – the video is not transmitted in the "multicast" mode.
12	Receiver IP address	Type-in the value in the field	Set the address from which the broadcast in **Multicast** mode will be performed	IP address	224.0.1.150	From 224.0.0.0 to 239.255.255.255
13	RTSP port	Type-in the value in the field	Sets the port number through which the video signal will be transmitted in the **Multicast** mode. When requesting the 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.	Sequence of numbers	555	Any numbers of ports that are not in use. The number of ports is specified by the system administrator.
The **Advanced settings** tab						
14	VLC player compatibility mode	Checkbox	Enables sending the current time to VLC Media Player instead of the frame time.	Boolean type	No	**Yes** - the current time is sent to VLC Media Player. **No** - the frame time is sent to VLC Media Player.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
15	Use captions track	Checkbox	Enables sending the video captions along with video via RTSP Server displaing them in the receiving app – VLC Media Player.	Boolean type	No	**Yes** - if there are captions on the video they are sent along with video to the the receiving app. **No** - the video captions are not sent via RTSP Server.
16	Source IP interface	Select the value in the list	Sets the name of the network interface that should be used to broadcast the RTSP server.		ANY	The list of available network interfaces of the computer. ANY - the default network interface is used.
The **NAT Settings** group						
17	IP addr	Type-in the value in the field	Sets the IP address of the router that performs the NAT broadcasting.	IP address	-	IP addresses range for local network
18	Port	Type-in the value in the field	Sets the port of the router that performs the NAT broadcasting.	Sequence of numbers	0	0-65535

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.23 The Settings panel of the Operator query panel object

The **Operator query panel** object is the interface frame used to perform user specified functions with a user's set of elements. The elements are configured by the *Intellect* administrator in the *ArpEdit* utility (see the User's Manual for ArpEdit). The settings panel of the **Operator query panel** object is shown in figure.

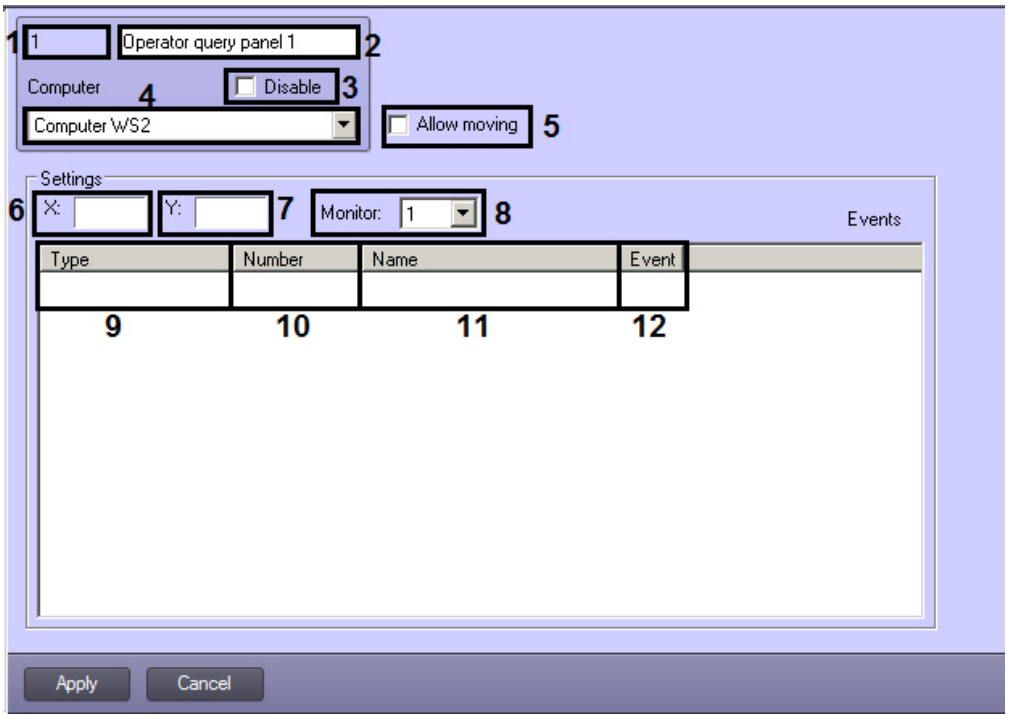


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Operator query panel** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identifier*	Enter the value in the field	File name designed for certain PTZ unit control. The filename is usually the same as the name of the PTZ unit.	Latin, Cyrillic and service characters	-	A line containing a sequence of symbols (Latin and service characters, digits), not case-sensitive Number of symbols – from 1 to 16.
2	Name*	Enter the value in the field	Defines the name of the **Operator query panel** object in the digital distributed video surveillance system. To ensure user friendliness, the object name is usually given the same name as the name of the PTZ unit.	Latin, Cyrillic and service characters	Operator query panel	A line containing a sequence of symbols (Latin and service characters apart from > and < symbols, digits), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the status of the **Operator query panel** object (enabled or disabled).	Boolean type	Not available	**Yes** – the **Operator query panel** object is disabled and is not in use. **No** – the **Operator query panel** object is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Operator query panel** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
5	Allow moving	Is identified by the check mark.	Allows moving the **Operator query panel** over the screen using the mouse.	Boolean type	Not available	**Yes** – movement is allowed. **No** – movement is prohibited.
Settings Group						
6	X	Enter the value in the field.	Defines the coordinate in the X horizontal axis for 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 surveillance monitors installed.
7	Y	Enter the value in the field.	Defines the coordinate in the Y vertical axis for 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 surveillance monitors installed.
8	Monitor	Is selected from the list	Sets the computer monitor number, the to which coordinates are assigned	Sequence of numbers	1	1 to 16
9	Type	Is selected from the list	Defines the object type for displaying the **Operator query panel**.	Types of the objects registered in the system	Not defined	Depends on the number of types of objects created in the digital distributed video surveillance system.
10	Number	Is selected from the list	Defines the number of the object for displaying the **Operator query panel**.	Sequence of numbers	Not defined	Depends on the number of objects created in the digital distributed video surveillance system.
11	Name	Automatically	Defines the name of the object for displaying the **Operator query panel**.	Names of the objects of the selected type registered in the system	Not defined	Depends on the number of objects types created in the digital distributed video surveillance system.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
12	Event	Is selected from the list	Defines the event, after which the **Operator query panel** is displayed	Types of events for the given types of devices.	Empty	Empty – the **Operator query panel** is not displayed. List of available events depends on the selected object.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.24 The Settings panel of the Alarm Message Window object

The **Alarm Message Window** object is designed to display an interface box showing the alarm event, which is initiated by the Intellect digital video surveillance system.

The settings panel of the **Alarm Message Window** object is shown in figure.

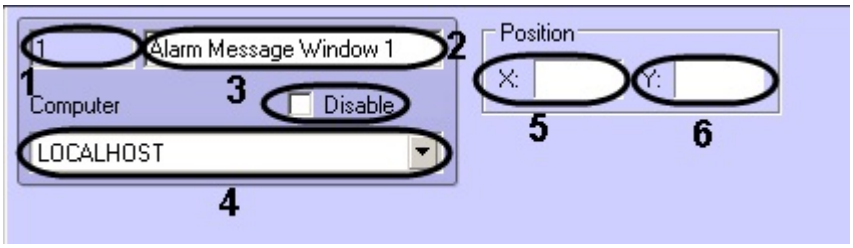


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Alarm Message Window** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number *	Automatically	Displays the identification number of the **Alarm Message Window** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Alarm Message Window** objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the name of the **Alarm Message Window** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Alarm notification window	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Alarm Message Window** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not availab-le	**Yes** – the **Alarm Message Window** object is disabled and is not in use. **No** – the **Alarm Message Window** object is enabled and is in use.
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Alarm Message Window** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
5	X	Enter the value in the field.	Defines the coordinate in the X horizontal axis for 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 surveillance monitors installed.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
6	Y	Enter the value in the field.	Defines the coordinate in the Y vertical axis for 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 surveillance monitors installed.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.25 The Settings panel of the Videogate object

The settings panel of the **Videogate** object is shown in figure.

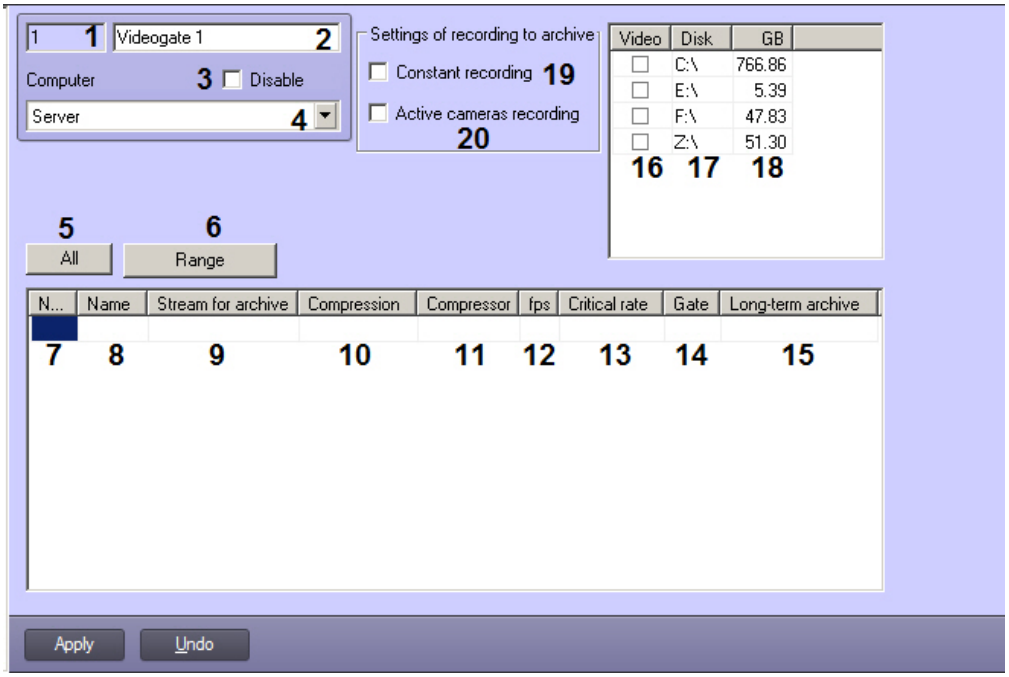


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Videogate** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Videogate** object in the digital distributed video surveillance system.	Sequence of numbers	-	Depends on the number of **Videogate** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Defines the name of the **Videogate** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Archiver.	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Videogate** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Videogate** is disabled and is not in use **No** – the **Videogate** is enabled and is in use.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
4	Computer	Is selected from the list	Defines the parent **Computer** object for the given **Videogate** object	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of **Computer** objects in the digital distributed video surveillance system
5	All	The button is pressed.	Selection of all video cameras registered in the system for transmitting video signals through the video gate	-	-	-
6	Range	The button is pressed.	Access to the complex selection of video cameras for transmitting video signals through the video gate	-	-	-
7	Number	Is selected from the list	Defines the number of the camera for transmitting video signals through the video gate	Sequence of numbers	-	Depends on the number of surveillance cameras in the digital distributed video surveillance system
8	Name	Is selected from the list	Sets the name of the video surveillance camera for transmitting video signals through the video gate	Name of the **Camera** objects registered in the system	-	Depends on the number of surveillance cameras in the digital distributed video surveillance system
9	Stream for archive	Is selected from the list	Set the video stream for record of the archive of the Videogate module	Names of streams transmitted by Server	-	Depends on the number of video streams enabled on Server
10	Compression	Is selected from the list	Sets the level of video signal compression for transmitting video signals through the video gate. With the given value there is additional consumption of Server's resources.	Sequence of numbers	-	In order of rising compression level 0,1,2,3,4,5 (0 – without compression, 5 – maximum compression).
11	Compressor	Select value from the list	Specifies the procedure of video stream compression which is in use for video signal recompression when transmitting video signals through the video gate. The value is to be selected in the **Compression** list if the compressor is specified.	List of available procedures	-	MJPEG, Motion Wavelet 3.5, Motion Wavelet 7.1. If the compression level is specified but **Compressor** is not selected, the MotionWavelet compressor is in use.
12	fps	Enter the value in the field	Sets the video signal rate for transmitting video signals through the video gate.	Sequence of numbers	-	Not more than digitizing of video signal by video capture card. Not less than 0.01.
13	Critical rate	Enter the value in the field	Set the minimum permissible rate of the video signal, when received by the Videogate to control the transmission of video signal through the local net	Sequence of numbers	-	Not more than the frame rate of the video signal, that is transmitted to the Videogate
14	Gate	Is selected from the list	Set the **Videogate** object from which video signal from the selected camera has to be transmitted to the given Videogate ***Important!*** *The selected* ***Videogate*** *object must differ from the configured one, otherwise there will be no video transmission via the Videogate.*	Name of the **Videogate** objects registered in the system	Not defined	Depends on the number of **Videogate** objects, registered in the digital distributed video surveillance system

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
15	Backup archive	Is selected from the list	Set the object **Backup archive**, from which video signal from the selected camera has to be transmitted to the given **Videogate**	Name of the **Backup archive** objects registered in the system.	Not defined	Depends on the number of **Backup archive** objects registered in the digital distributed video surveillance system.
16	Video	Is identified by the check mark	Set the didsk for storing the archive of video signals, going through ther **Videogate**.	Boolean type	-	Yes – the disk is used for storing the **Videogate** module. No – the disk is not used for storing the **Video gate** module
17	Disk	Automatically	Displays the names of local (net, USB) disks, accessible for storing archive of **Videogate** module.	Names of available disks(Latin characters)	List of available hard disks	Depends on the total number (both local and network) of accessible disks.
18	GB	Automatically	Contains information about free space on every available disk	Disk space in GB	-	Depends on the free disk space
19	Constant recording	Setting the checkbox	Enables permanent recording on all video cameras added to the Videogate	Boolean	No	**Yes** – permanent recording is enabled on all video cameras added to the Videogate. **No** – Videogate module archive is recorded only on cameras that are configured for archive recording on Server.
20	Active cameras recording	Setting the checkbox	Enables recording only on cameras requested (displayed) on clients	Boolean	No	**Yes** – Videogate module archive is recorded only on cameras requested (displayed) on clients. **No** – Videogate module archive is recorded on cameras that are configured for archive recording on Server.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.26 The Settings panel of the Event Counter object

The **Event counter** object is designed to register and count events of a certain type, occurring at the pre-defined objects and registered by the INTELLECT™ system.

The settings panel for the **Event counter** object is shown in figure.

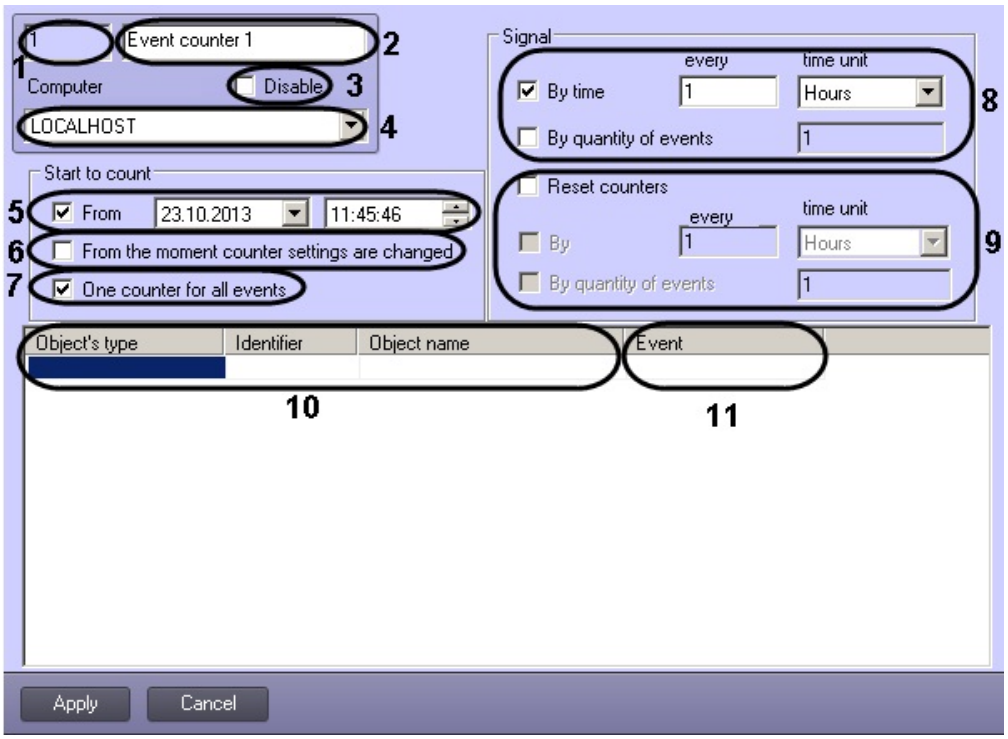


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Event counter** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Event counter** object in the digital distributed video surveillance system.	Sequence of numbers	-	Depends on the number of the **Event counter** objects in the digital distributed video surveillance system.
2	Name*	Specify the value in the field	Sets the name of the **Event counter** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Event counter	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Set the checkbox	Sets the state of the **Event counter** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	No	**Yes** – the **Event counter** object is disabled. **No** – the **Event counter** object is enabled.
4	Computer	Select in the list	Sets the parent **Computer** object of the digital distributed video surveillance system, to which the given **Event counter** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object.	Depends on the number of the **Computer** objects in the digital distributed video surveillance system
The Start to count group						

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
5	From the date of (activation)	Set the checkbox	Allows setting the start to count date and time manually.	Boolean type	Yes	**Yes** – the **Start to count** date and time are set manually. **No** – The **Start to count** date and time are set at the date and time, when the **Event counter** object was last modified.
	From the date of (date)	Specify the value in the field or select it in the dropdown list.	Sets the **Start to count** date.	DATE:MONTH :YEAR	Current system date	09.1752 – 12.9999
	From the date of (time)	Specify the value in the field	Sets the **Start to count** time.	HOURS:MINU TES:SECOND S	Current system time	00:00:0 - 23:59:59
6	From the moment of counters settings changing	Set the checkbox	Sets the **Start to count** date and time at the date and time, when the **Event counter** object was last modified.	Boolean type	No	**Yes** – the **Start to count** date and time are set at the date and time, when the **Event counter** object was last modified. **No** – the **Start to count** date and time are set manually.
7	One counter for all events	Set the checkbox	Sets the counter for all events referred to the **Objects and events** group of the given **Event counter** object.	Boolean type	Yes	Yes – Only one counter will be used for counting all events specified in the **Objects** group. No – the events are counted by different counters (each event is counted by an individual counter).
The Counter notification group						
8	On time (activation)	Set the checkbox	Enables a regular notification in preset periods of time.	Boolean type	Yes	**Yes** – on time notification is enabled. **No** – on time notification is disabled (notification by quantity of events is enabled).
	On time (every)	Specify the value in the field	Sets a notification period as a time period. Notification is performed irrespective of on 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
	On time (time unit)	Select the value in the list	Sets a time unit for the given notification.	Line	Hours	Hours Days
	By quantity of events (activation)	Set the checkbox	Enables a regular notification about events starting from the preset one.	Boolean type	No	**Yes** – notification by quantity of events is enabled. **No** – notification by quantity of events is disabled (on time notification is enabled).

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
	By quantity of events (quantity of events)	Specify the value in the field	Sets a number of event starting from which the notification will be performed. Example: if the parameter has 5 value, 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	On time (activation)	Set the checkbox	Enables a cyclic counter reset in a preset time period.	Boolean type	Yes	**Yes** – a cyclic reset in a preset time period is enabled. **No** – a cyclic reset in a preset time period is disabled (By quantity of events (cyclic reset by quantity of events is enabled).
	On time (every)	Specify the value in the field	Sets a reset period as a time period. Reset is performed irrespective of on 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
	On time (time unit)	Select in the list	Sets a time unit for the given reset.	Line	Hours	Hours Days
	By quantity of events (activation)	Set the checkbox	Enables a counter reset performed upon occurrence of a preset number of events.	Boolean type	No	**Yes** – a cyclic reset upon occurrence of a preset number of events is enabled. **No** – a cyclic reset upon occurrence of a preset number of events is disabled (a cyclic reset on time is enabled).
	By quantity of events (quantity of events)	Specify the value in the field	Sets a reset period for counters as a number of events.	Sequence of numbers	0	0 - 2147483648
The Objects and events group						
10	Object type	Select in the list	Sets the type of object for which the events are to be counted.	Types of objects registered in the system.	Not set	Depends on the number of object types registered in the digital distributed video surveillance system.
	Identifier	Select in the list	Sets the identification number of an object of the preset type for which the events are to be counted.	Sequence of numbers	Not set	Depends on the number of objects of the given type in the digital distributed video surveillance system.
	Object's name	Automatically	Displays the identification number of the selected object.	Latin, Cyrillic and service characters	Not set	Object name aith the preset identifier.

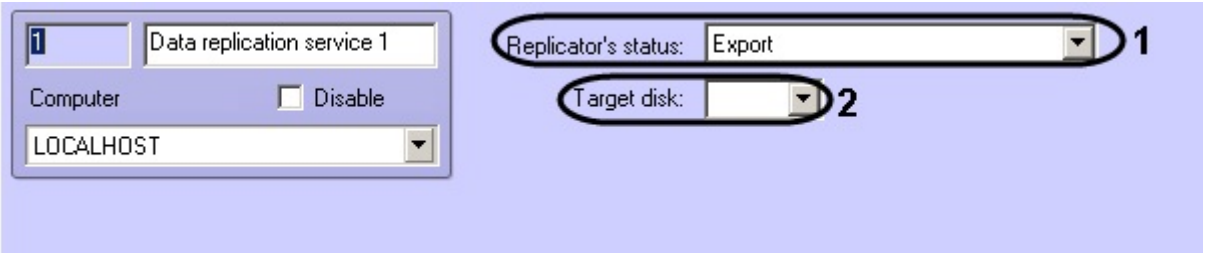
№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
11	Event	Select in the list	Sets an event that is to be counted.	Latin, Cyrillic and service characters	Not set	Depends on the number of types of objects registered in the digital distributed video surveillance system.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.27 The Settings panel of the Data replication service object

The **Data replication service** object is for archive replication from unconnected servers.

The settings panel of the **Data replication service** object is shown in figure.



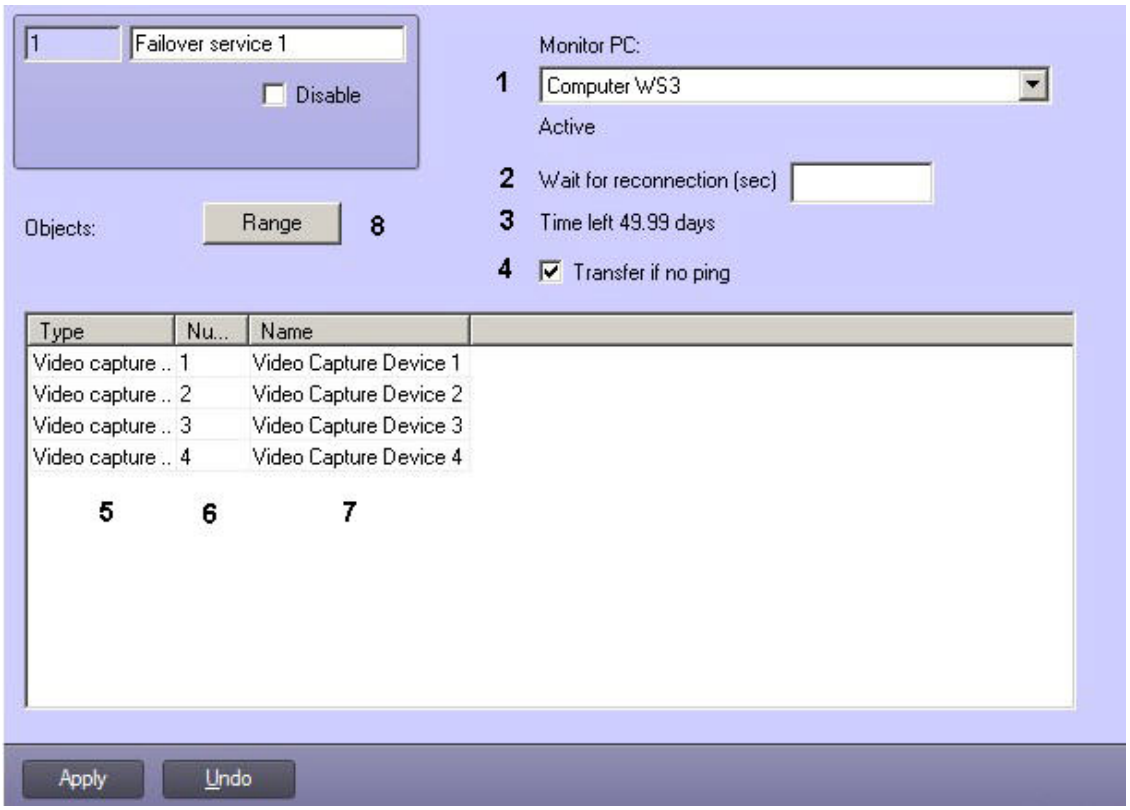
Description of setting parameters relevant to element on the settings panel of the **Data replication service** object is given in table.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Replicator's status	Select in the list	Specifies status of Server – whether it is a data source or a target	Names of present replication roles	Export	**Export** – Server is the source **Target** – Server is the target
2	Target disk	Select in the list	Specifies removable storage used for data transmission	Letter of drive connected to the Server	-	Depends on the number of drives connected to the Server

13.1.2.8.28 The Settings panel of the Failover service object

The **Failover service** object is used to ensure operation of distributed system in the failover mode.

The settings panel of the **Failover service** object is shown in figure.



Description of setting parameters relevant to elements on the settings panel of the **Failover service** object is given in table.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Monitor PC	Select in the list	Sets the name of the Server the state of which is to be under control	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)	Type-in the value in the field	Sets the time period (in seconds) at the end of which configuration will be transferred to backup Server	Sequence of numbers	-	From 0 to 65535
3	Time left __ days	Automatically	Shows the period of time (in days) remaining for restoring the configuration from backup Server and restoring 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	No	Yes - the configuration is transferred if there is no ping. No - it is not taken into account whether the ping is present or absent when transferring the configuration.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
5	Type	Select in the list	Sets the object type in Server configuration that is to be transferred to backup Server in case of connection failure	Types of objects registered on the base of the main Server	-	Depends on the configuration created on the base of the main Server
6	Number	Select in the list	Sets the ID of object of selected type that is to be transferred to backup Server in case of connection failure	ID of objects of selected type that are in Server configuration	-	Depends on the number of objects of selected type in the configuration of main Server
7	Name	Automatically	Sets the object name that is to be transferred to backup Server in case of connection failure	Names of objects of selected type that are in Server configuration	-	Depends on the configuration created on the base of the main Server
8	Range	Click the button	Opens the dialog box for integrated selection of tracking objects	-	-	-

13.1.2.8.29 The Settings panel of the Backup audio archive object

The settings panel of the **Backup audio archive** object is shown in figure.

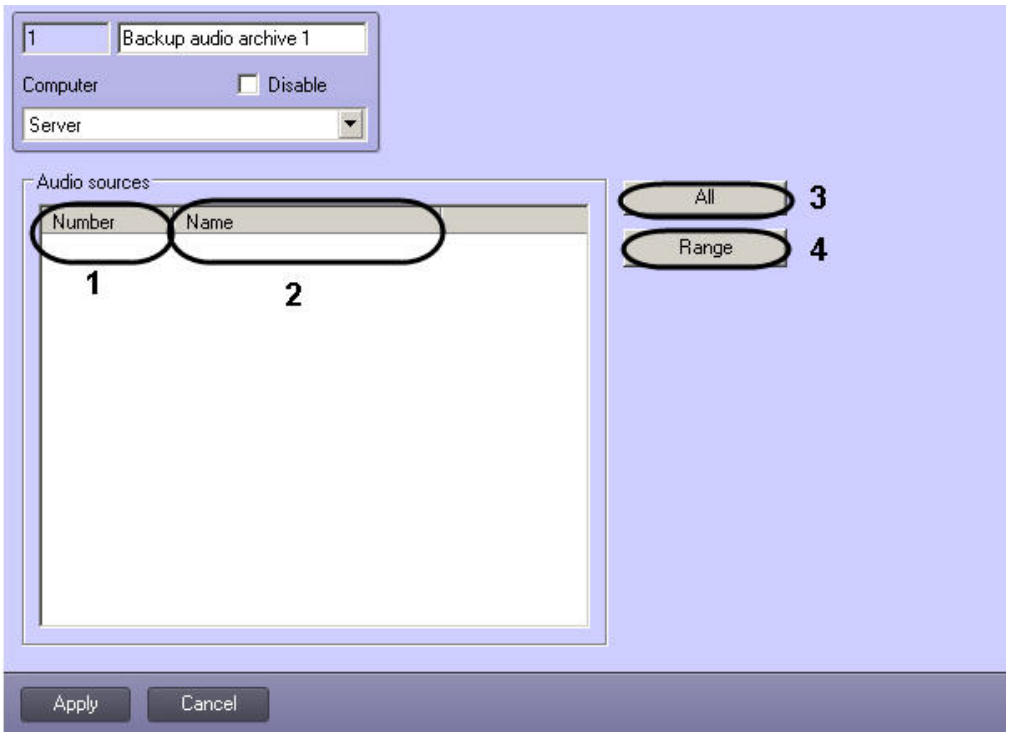
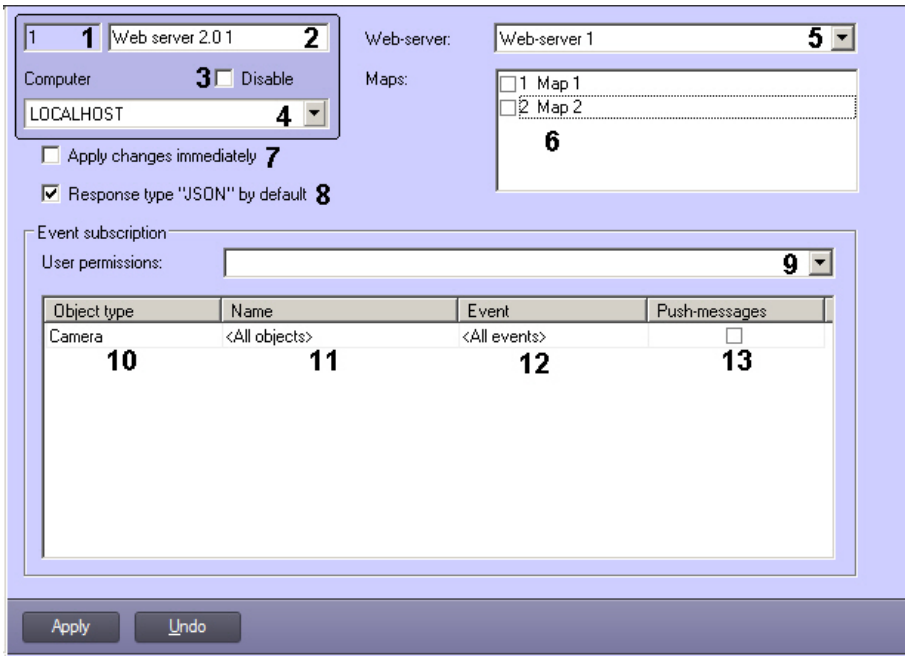


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Backup audio archive** object.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	**Number** drop-down list	Select the value from the list	Sets the ID number of **Microphone** object to copy video archive from	Non-negative integer	-	Depends on the number of **Microphone** objects in the system.
2	**Name** drop-down list	Select the value from the list	Sets the name of the **Microphone** to copy video archive from	Names of the **Microphone** objects registered in the system	-	Depends on the number of **Microphone** objects in the system.
3	**All** button	Click the button	Adds all **Microphone** objects created in the system to the list	-	-	-
4	**Range** button	Click the button	Opens the window for complex adding microphones to the list of **Backup audio archive**	-	-	-

13.1.2.8.30 The Settings panel of the Web Server 2.0 object

The appearance of the configuration panel of the **Web Server 2.0** system object is shown in the figure.



Configuration parameters of the **Web Server 2.0** system object are described in the table.

No.	Parameter name	Parameter configuration method	Description of parameter	Representation	Default value	Possible values
1	**ID number** field	Automatic	Displays the ID number of the **Web Server 2.0** system object in the system	Natural whole numbers	-	Depends on number of **Web Server 2.0** objects in the system

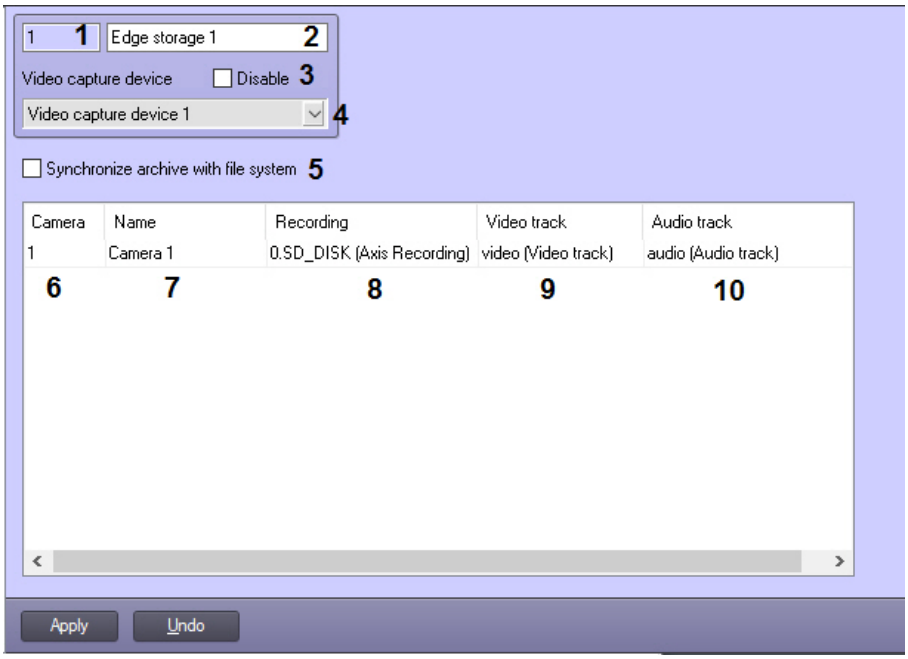
2	**Name** field	Value entered in field	Sets the name of the **Web Server 2.0** object in the system	Latin letters, Cyrillic letters, and miscellaneous characters	Video capture device	Line containing a sequence of any characters (letters, numbers, miscellaneous characters apart from > and < symbols), not case-sensitive From 1 to 60 characters
3	**Disable** check box	Select/clear check box	Sets the state (enabled or disabled) of the **Web Server 2.0** object in the system	Boolean	No	**Yes**: **Web Server 2.0** object is disabled and is not used **No**: **Web Server 2.0** object is enabled and is used
4	**Computer** drop-down list	Value selected from list	Sets **Computer** parent object for the given **Web Server 2.0** object	Name of **Computer** objects registered in the system	Name of parent **Computer** object	Depends on number of **Computer** objects in the system
5	**Web server** drop-down list:	Value selected from list	Sets the **Web server** object whose settings will be used for Web Server 2.0	Names of **Web server** objects registered in the system	-	Depends on number of **Web server** objects registered in the system
6	Map list	Set check boxes	Sets list of Maps to use by Web-server 2.0 to be available on mobile clients	Names of **Map** objects registered in the system	None of maps is selected	Depends on number of **Map** objects registered in the system
7	**Apply changes at once** checkbox	Checkbox	Enabling the **Apply changes at once** feature	Boolean type	No	**Yes** – **Web-server 2.0** object will immediately apply these changes of user rights. **No** – when user rights are changed, access rights are not changed in **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** ckeckbox	Checkbox	Sets default HTTP API response type	Boolean type	No	**Yes** – the response is sent in JSON format if the format is not specified explicitly in the request **No** – the response is sent in XML format if the format is not specified explicitly in the request

9	**User permissions** drop-down list	Value selected from list	Sets the **User permissions** object for which events filter is to be configured	Names of **User permissions** objects registered in the system	-	Depends on number of **User permissions** objects registered in the system
10	**Object type** drop-down list	Value selected from list	Sets type of objects from which events are to be sent to clients	Names of types of objects registered in the system that are included in the selected user permissions	-	Depends on selected user permissions
11	**Name** drop-down list	Value selected from list	Sets name of object from which events are to be sent to clients	Names of objects of the selected type that are registered in the system	-	Depends on number of objects of the selected type that are registered in the system
12	**Event** drop-down list	Value selected from list	Sets event type that is to be sent to clients	Name of events that are available for objects of the selected type	-	Depends on the selected object type.
13	**Push notifications** check box	Select/clear check box	Specifies whether to send push notifications to clients about events of the selected type	Boolean	No	**Yes**: push notifications are sent **No**: push notifications are not sent

13.1.2.8.31 The Settings panel of the Edge storage object

The **Edge storage** object is designed for viewing the video archive in edge storage on IP-devices.

The figure shoes the **Edge storage** object settings panel.

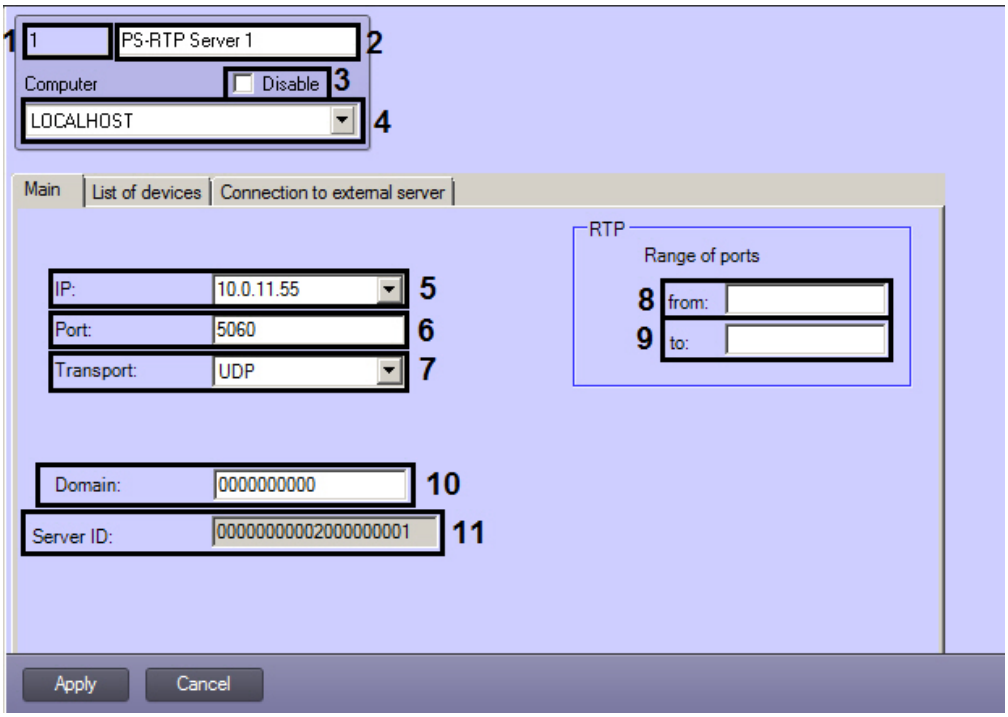


The table describes the settings parameters corresponding to elements of the **Edge storage** settings panel.

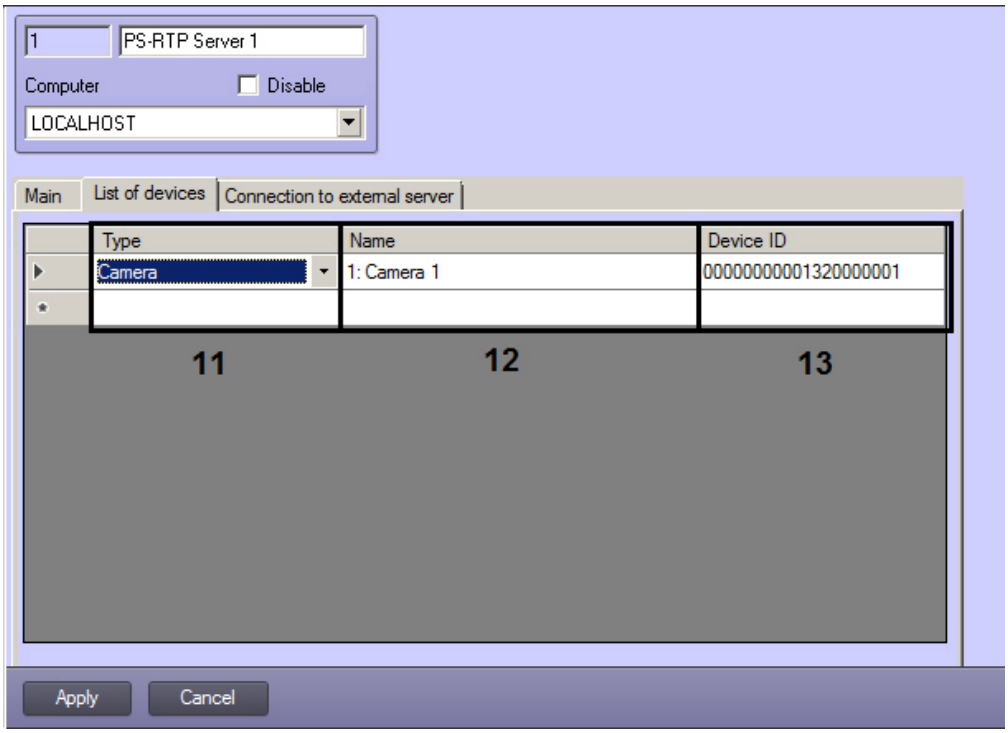
№	Parameter name	Method for setting the parameter value	Description	Presented as	Default value	Value range
1	Identification number	Automatically	Shows the identification number of the **Edge storage** system object in the system.	Sequence of numbers	-	Depends on the number of **Edge storage** objects in the digital distributed video surveillance system.
2	Name	Enter the value in the field	Set 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 symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Disable**	Is set with a checkbox	Set the status (enabled or disabled) of the **Edge storage** object in the system.	Boolean type	No	Yes – the **Edge storage** is disabled and is not in use No – the **Edge storage** object is enabled and is in use.
4	**Video Capture Device**	Is selected from the list	Set the parent **Video Capture Device** object for the given **Edge storage** object.	Name of the **Video Capture Device** objects registered in the system.	Name of the parent **Video Capture Device** object.	Depends on the number of the **Video Capture Device** objects in the system.
5	**Sync archive with file system**	Select/clear checkbox	Enable importing from edge storages to *Intellect* file system	Boolean type	No	**Yes** – archive is imported. **No** – archive is not imported.
6	**Camera**	Select value from the list	Specifies the number of **Camera** object which is used for archive viewing	Set of natural numbers	-	Depends on number of cameras registered in the system
7	**Name**	Automatically	Displays the name of **Camera** object	Name of **Camera** objects registered in the system	-	Depends on number of **Camera** objects registered in the system
8	**Recording**	Select value from the list	Specifies record corresponding to one data source in device	Name of recordings supported by device	-	Depends on number of recordings supported by device
9	**Video track**	Automatically	Specifies the channel of video data within recording	Name of video tracks within recording	-	Depends on number of video tracks within recording
10	**Audio track**	Select value from the list	Specifies the channel of audio data within recording	Name of audio tracks within recording	-	Depends on number of audio tracks within recording

13.1.2.8.32 The Settings panel of the RS-RTP server object

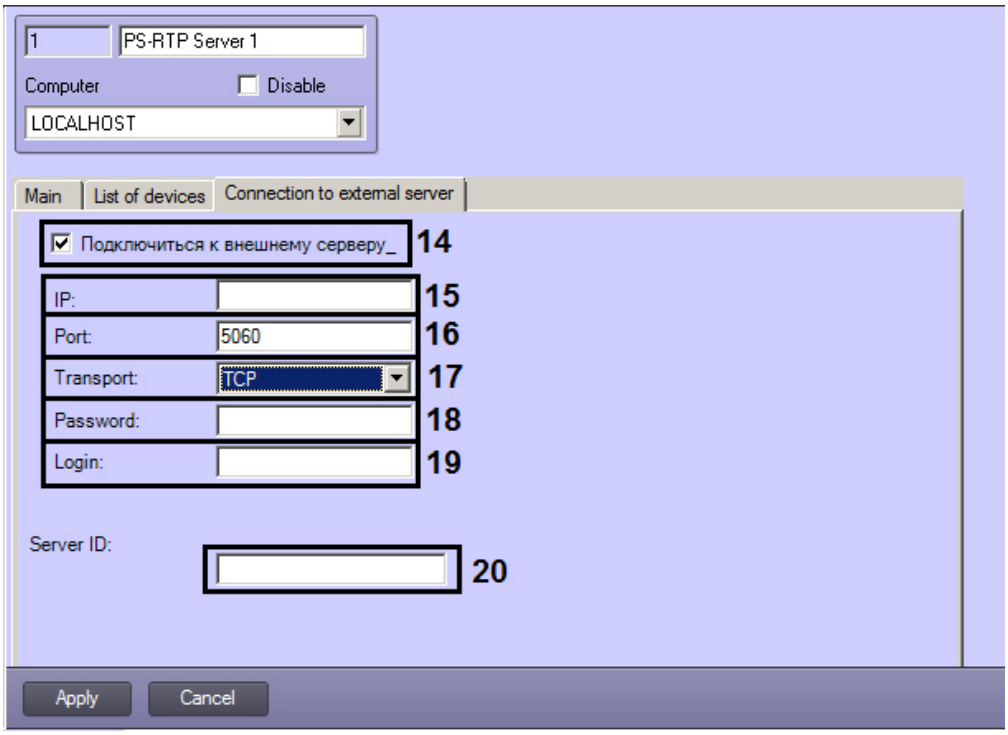
The settings panel of the RS-RTP server object is shown in figures.



The **General** tab



The **Device list** tab



The **Connection to external server** tab

The table describes the parameters of the settings corresponding to the elements of the settings panel of the RS-RTP object.

#	Name	Field type	Description	Format	Default value	Value range
1	**ID**	Automatically	Shows id of **RS-RTP Server object** in the system	Natural number series	-	Depends on the number of **RS-RTP Server objects** in the system
2	**Name**	Enter the value in the field	Sets the name of **RS-RTP Server object**	Latin, Cyrillic and service characters	**RS-RTP server**	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	**Disable**	Checkbox	Sets the state of **RS-RTP Server object** (disabled or enabled)	Boolean type	No	**Yes** – **RS-RTP Server object** is disabled and is not in use. **No** – **RS-RTP Server object** is enabled and is in use.
4	**Computer**	Select in the list	Sets the parent **Computer** object in the digital system with distributed architecture to which the **RS-RTP Server object is assigned.**	Names of the **Computer** objects registered in the system	The name of the parent **Computer** object	Depends on the number of **Computer objects** in the digital surveillance system with distributed architecture.
The **General** tab						
5	**IP:**	Select in the list	Sets IP address of network interface using which the third-party software will control registered in Intellect devices via the GB2818 protocol	IP address	Depends on the parameters of network connection	Depends on the parameters and number of network connections
6	**Port:**	Enter the value in the field	Number of a port through which the third party software will be connected via the GB2818 protocol	Natural number series	5060	0-65535

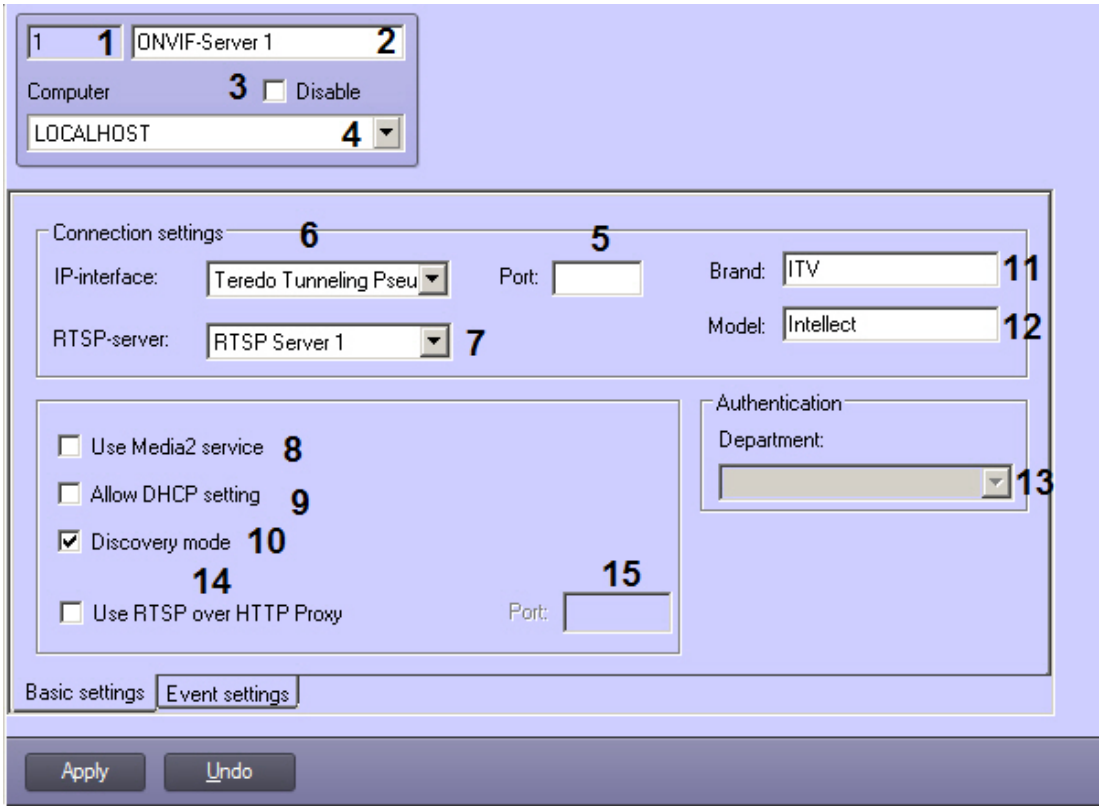
7	**Transport:**	Select value in the list	Data transfer protocol	Supported transport protocols	UDP	UDP, TCP
8	**Server ID**	Automatically	ID of Intellect Server that is in use by the third-party software to connect to RS-RTP Server via the GB2818 protocol	-	-	-
9	**From:**	Enter the value in the field	Lower value of the RTP port range	Natural number series	-	0-65535
10	**To:**	Enter the value in the field	Upper limit of the RTP port range	Natural number series	-	0-65535
The **Device list** tab						
11	**Type**	Select value in the list	Type of object to be controlled via the GB2818 protocol	Names of types of objects in *Intellect* object tree	-	Depends on the number of objects created in *Intellect* object tree
12	**Name**	Select value in the list	Name of object to be controlled via the GB2818 protocol	Names of objects in *Intellect* object tree	-	Depends on the number of objects created in *Intellect* object tree
13	**Device ID**	Automatically	ID of the device that will be in use in the third-party software to control objects via the GB2818 protocol	-	-	-
The **Connection to edge server** tab						
14	**Edge server connection**	Checkbox	Checks if *Intellect* connects to edge supserver using the PS-RTP object via the GB2818 protocol	Boolean type	No	Yes – edge server connection is performed. No – edge server connection is not performed.
15	**IP:**	Enter the value in the field	IP address of supserver	IP address	-	000.000.000.000 – 255.255.255.255
16	**Port:**	Enter the value in the field	Port used to connect to edge server	Natural number series	5060	0-65535
17	**Transport:**	Select value in the list	Transport protocol used to connect to edge server	Supported transport protocols	-	TCP, UPD
18	**Login:**	Enter the value in the field	Username used to connect to edge server	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols
19	**Password:**	Enter the value in the field	Password used to connect to edge server	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols

20	**Server ID:**	Enter the value in the field	ID of supserver via the GB28181 protocol	Natural number series	-	00000000000000000000 - 99999999999999999999

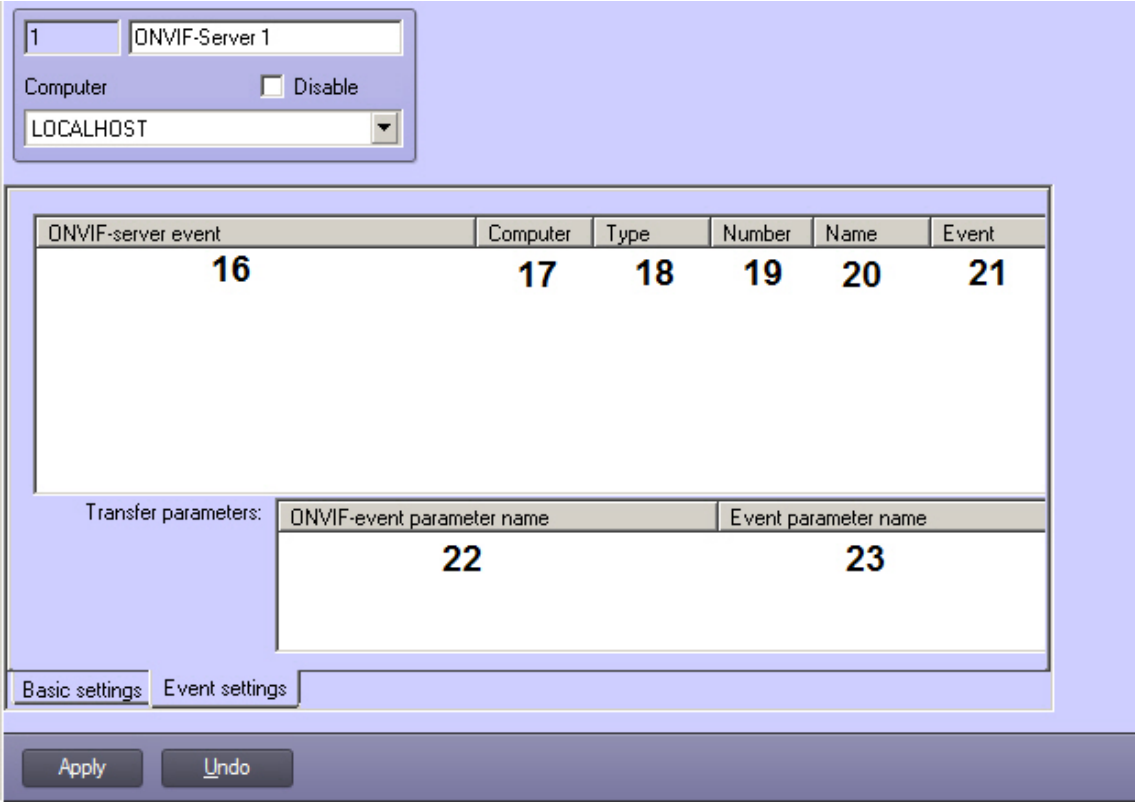
13.1.2.8.33 The Settings panel of the ONVIF-Server object

The **ONVIF-Server** object is designed to transmit *Intellect* video over ONVIF protocol.

The settings panel of the **ONVIF-Server** object is shown in the figure.



The **Basic settings** tab



The **Event settings** tab

Basic elements of the settings panel of the **ONVIF-Server** object are described in the table.

#	Parameter name	Method for setting the parameter value	Parameter description	Representation	Default value	Value range
1	**ID**	Automatically	Displays the identification number of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Sequence of numbers	-	Depends on the number of the **ONVIF-Server** objects in the digital video surveillance system with distributed architecture
2	**Name**	Specify the value in the field	Sets the name of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	PTZ device	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Disable**	Set the checkbox checked	Sets the state (enabled or disabled) of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Boolean type	No	**Yes** – the **ONVIF-Server** object is disabled and not in use. **No** – the **ONVIF-Server** object is enabled and in use.

4	**Computer**	Select in the list	Sets the parent **Camera** object to which the **ONVIF-Server** object corresponds in the digital video surveillance system with distributed architecture	The names of the **Computer** objects registered in the system	The name of the **Computer** parent object	Depends on the number of computers in the digital video surveillance system with distributed architecture
Basic settings tab						
5	**Port number**	Specify the value in the field	Sets the port number used to connect to the Server	Integer greater than 0	-	1– 65 535
6	**IP-interface**	Select in 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 network adapters available in the system
7	**RTSP Server**	Select in the list	Sets the **RTSP Server** object the settings of which are applied by the **ONVIF-Server** object while transmitting video	The names of the **RTSP Server** objects registered in the system	-	Depends on the number of **RTSP Server** objects created in *Intellect*
8	**Use Media2 service**	Set the checkbox checked	Enabling Onvif 2.X standard instead of Onvif 1.X	Boolean type	No	**Yes** – transmitting video in H265 or H264 formats. **No** – transmitting video in MPEG, MJPEG or H264 formats.
9	**Allow DHCP setting**	Set the checkbox checked	Enabling DHCP support	Boolean type	No	**Yes** – DHCP is in use. **No** – DHCP is not in use.
10	**Discovery mode**	Set the checkbox checked	Enabling WS-Discovery mode	Boolean type	Yes	**Yes** – WS-Discovery mode is enabled. **No** – WS-Discovery mode is disabled.
11	**Brand**	Specify the value in the field	Sets the name of brand that will be displayed in third-party clients that support getting the stream over ONVIF	Latin, Cyrillic and service characters	ITV	A line containing a sequence of any symbols (letters, digits and service characters)

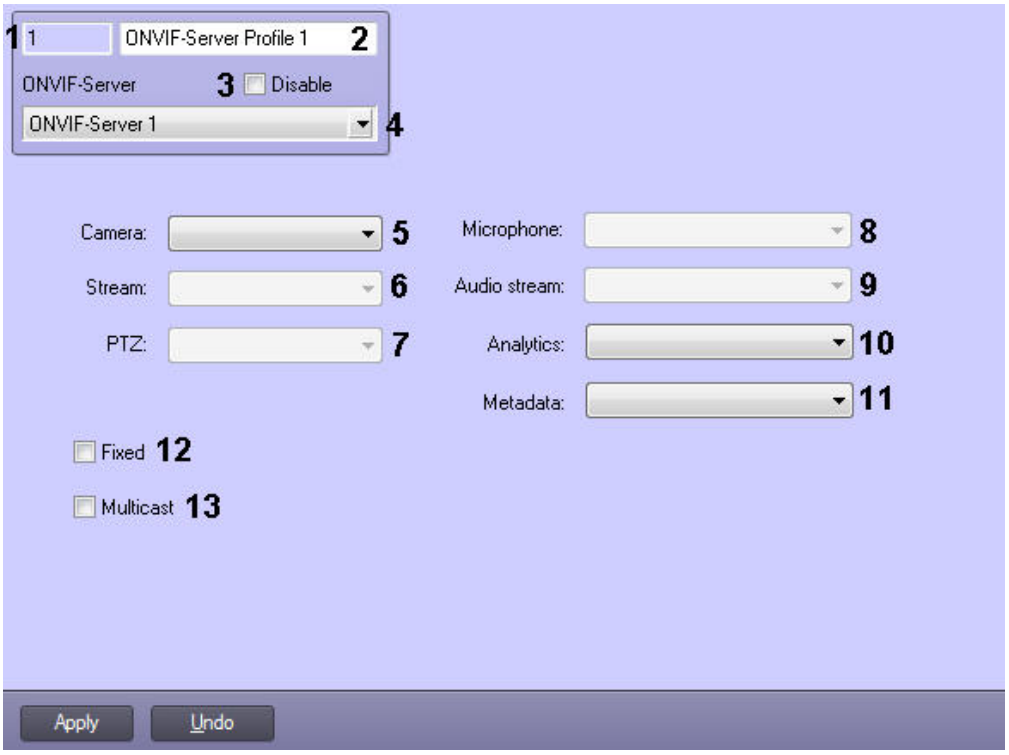
12	**Model**	Specify the value in the field	Sets the name of model that will be displayed in third-party clients that support getting the stream over ONVIF	Latin, Cyrillic and service characters	Intellect	A line containing a sequence of any symbols (letters, digits and service characters)
13	**Departme nt**	Select in the list	Sets the department where the users will be created when they are added via the *ONVIF-Server* interface	The names of the **Department** objects registered in the system	-	Depends on the number of the **department**s registered in *Intellect*
14	**Use RTSP over HTTP Proxy**	Set the checkbox checked	Redirects all RTSP-Server and ONVIF-Server requests to the specified port for the ONVIF-Server operation behind NAT	Boolean type	No	Yes - the RTSP-Server and ONVIF-Server requests are redirected to the specified port No - the RTSP-Server and ONVIF-Server requests are transmitted to the port specified in the **Connection Settings** group (5).
15	**Port**	Specify the value in the field	Sets the port number for the RTSP-Server and ONVIF-Server requests redirection for the ONVIF-Server operation behind NAT	Round number more than 0	-	1– 65 535
Event settings tab						
16	**Onvif-server event**	Select in the list	Sets the ONVIF-event according to the ONVIF specification	The list of available events	-	According to the ONVIF specification
17	**Computer**	Select in the list	Sets the Computer object which is the basis of the object which in turn is an event source in *Intellect*	The names of the **Computer** objects registered in the system	-	Depends on the number of computers in the digital video surveillance system with distributed architecture
18	**Type**	Select in the list	Sets the event type which is an event source in *Intellect*	The names of the object types registered in the system	-	Depends on the number of created objects in the digital video surveillance system with distributed architecture
19	**Number**	Select in the list	Sets the object number which is an event source in *Intellect*	Sequence of numbers	-	Depends on the number of created objects in the digital video surveillance system with distributed architecture

20	**Name**	Automatically	Sets the object name which is an event source in *Intellect*	The names of the object of the selected type registered in the system	-	Depends on the number of created objects in the digital video surveillance system with distributed architecture
21	**Event**	Select in the list	Sets the event name in *Intellect*	The event names received from the objects of the selected type	-	Depends on the object type
22	**Onvif-event parameter name**	Automatically	Sets the ONVIF-event parameter name according to the ONVIF specification	The parameter names of the selected ONVIF-event	-	According to the ONVIF specification
23	**Event parameter name**	Specify the value in the field	Sets the event parameter name in *Intellect*	The event parameter names in *Intellect*	-	Depends on the object type

13.1.2.8.34 The Settings panel of the ONVIF-Server Profile object

The **ONVIF-Server Profile** object is designed to configure the ONVIF device channel.

The settings panel of the **ONVIF-Server Profile** object is shown in the figure.



Basic elements of the settings panel of the **ONVIF-Server Profile** object are described in the table.

#	Parameter name	Method for setting the parameter value	Parameter description	Representation	Default value	Value range

1	**ID***	Automatically	Displays the identification number of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Sequence of numbers	-	Depends on the number of the **ONVIF-Server** objects in the digital video surveillance system with distributed architecture
2	**Name***	Specify the value in the field	Sets the name of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Latin, Cyrillic and service characters	PTZ device	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Disable**	Set the checkbox checked	Sets the state (enabled or disabled) of the **ONVIF-Server** object in the digital video surveillance system with distributed architecture	Boolean type	No	**Yes** – the **ONVIF-Server** object is disabled and not in use. **No** – the **ONVIF-Server** object is enabled and in use.
4	**Onvif-Server**	Select in the list	Sets the parent **ONVIF-Server** object to which the **ONVIF-Server Profile** object corresponds in the digital video surveillance system with distributed architecture	The names of the **ONVIF-Server** objects registered in the system	The 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	The 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 stream that is transmitted via the **ONVIF-Server Profile** object	List of available video streams	-	Depends on the number of activated camera streams
7	**PTZ**	Automatically	Sets the **PTZ** object, used for PTZ control, corresponding to the **ONVIF-Server Profile** object	List of **PTZ** objects corresponding to the selected **Camera** object	-	Depends on the number of **PTZ** objects created and configured in the system
8	**Microphone**	Automatically	Sets the **Microphone** object corresponding to the selected **Camera** object	List of **Microphone** objects corresponding to the selected **Camera** object	-	Depends on the number of **Microphone** objects created and configured in the system
9	**Audio stream**	Automatically	Sets the audio stream to be synchronously transmitted with video	List of available audio streams	-	Depends on the number of 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 checked	Disables deleting the **ONVIF-Server Profile** object using the driver	Boolean type	No	**Yes** – the **ONVIF-Server Profile** object cannot be deleted using the driver **No** – the **ONVIF-Server Profile** object can be deleted using the driver

1 3	**Multicast**	Set the checkbox checked	Enables video transmission via ONVIF-Server in the multicast mode	Boolean type	No	**Yes** – video can be transmitted in the multicast mode. *Note. There are some extra actions besides setting the checkbox checked in order to enable video transmission in the multicast mode – see* Configuring getting video using ONVIF-Server module. **No** – video cannot be transmitted in the multicast mode.

13.1.2.8.35 The Settings panel of the Telegram bot object

The **Telegram bot** object is designed for sending messages to Telegram.

The settings panel of the **Telegram bot** object is shown in figure.

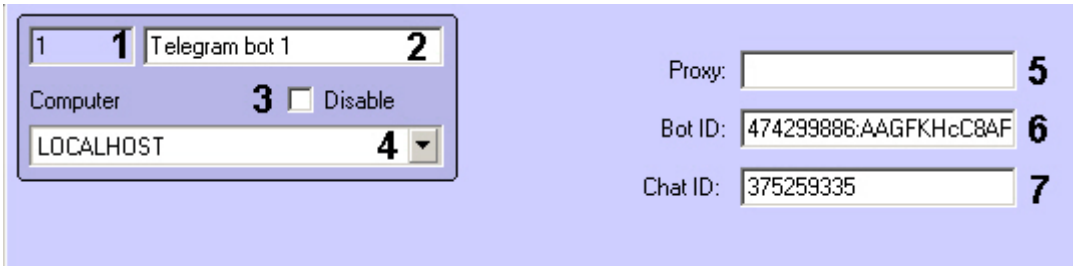


Table describes the parameters of the settings corresponding to the elements of the settings panel of the **Telegram bot** object.

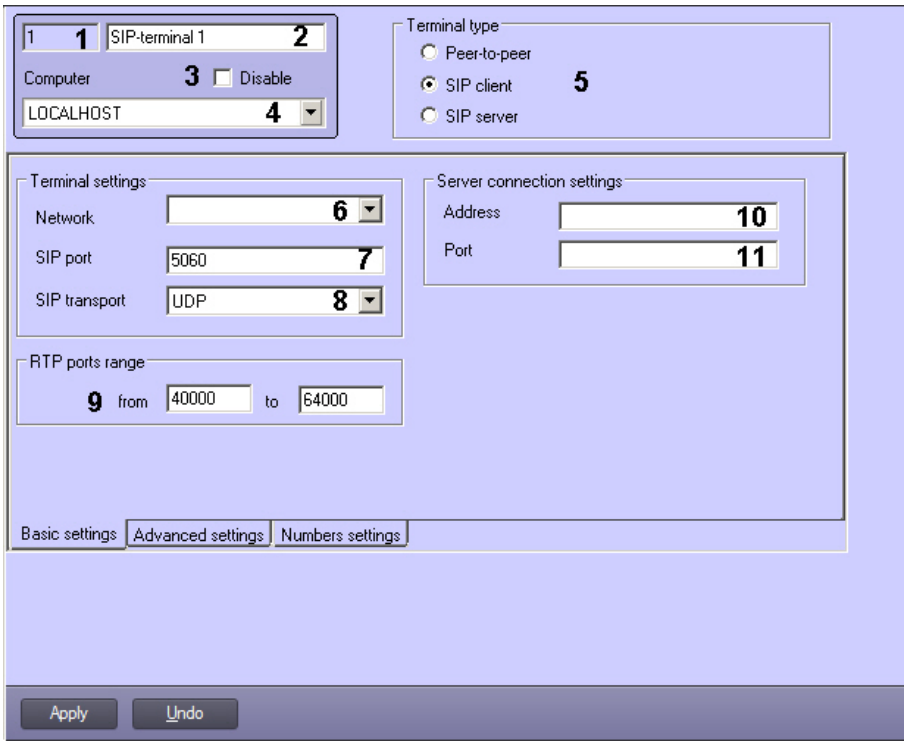
№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Telegram bot** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of Telegram bot objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the name of the **Telegram bot** object in the digital distributed video surveillance system.	Latin and service characters	Telegram bot	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Telegram bot** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	False	**Yes** – the **Telegram bot** object is disabled and is not in use **No** – the Telegram bot object is enabled and is in use.

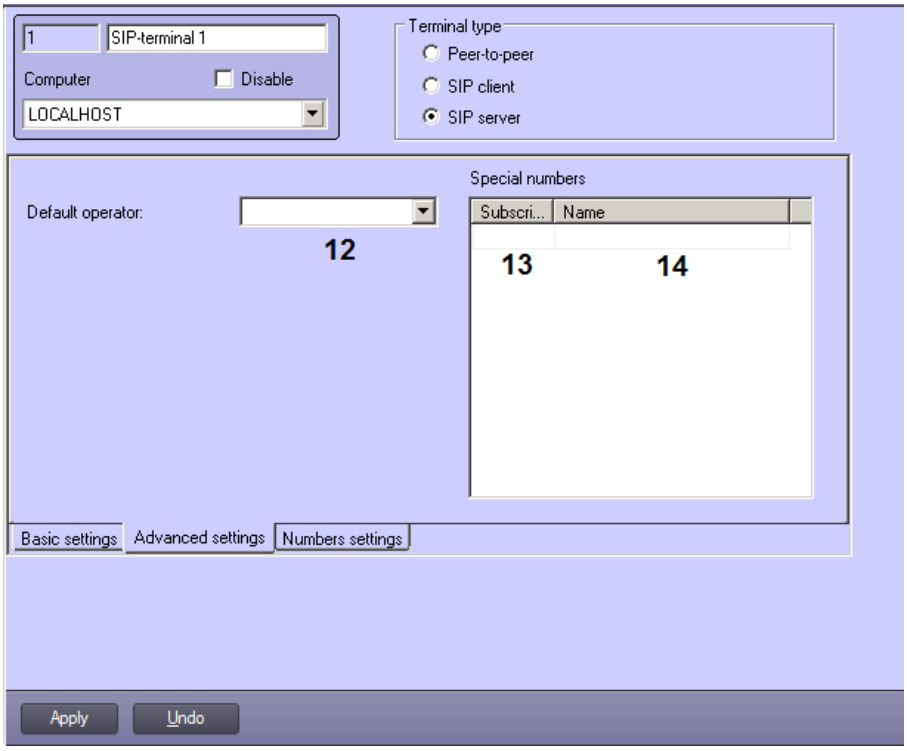
№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
4	Computer	Is selected from the list	Defines the parent **Computer** object of the digital distributed video surveillance system, to which the given **Telegram bot** object refers.	Name of the **Computer** objects registered in the system	Name of the parent **Computer** object	Depends on the number of **Computer** objects in the digital distributed video surveillance system
Settings Group						
5	Proxy	Enter the value in the field	Specifies the proxy server for sending the message.	Latin and service characters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.
6	Bot ID	Enter the value in the field	Specifies the bot identifier in Telegram.	Latin and service characters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.
7	Chat ID	Enter the value in the field	Specifies the chat identifier in Telegram.	Latin and service characters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.8.36 The Settings panel of the SIP-terminal object

The settings panel of the **SIP-terminal** object is shown in the pictures below.


1
SIP-terminal 1
2
Computer
3
Disable
LOCALHOST
4
Terminal type
Peer-to-peer
SIP client
5
SIP server
Terminal settings
Network
6
SIP port
5060
7
SIP transport
UDP
8
RTP ports range
9
from
40000
to
64000
Server connection settings
Address
10
Port
11
Basic settings
Advanced settings
Numbers settings
Apply
Undo


1
SIP-terminal 1
Computer
Disable
LOCALHOST
Terminal type
Peer-to-peer
SIP client
SIP server
Special numbers
Default operator:
12
Subscri...
Name
13
14
Basic settings
Advanced settings
Numbers settings
Apply
Undo

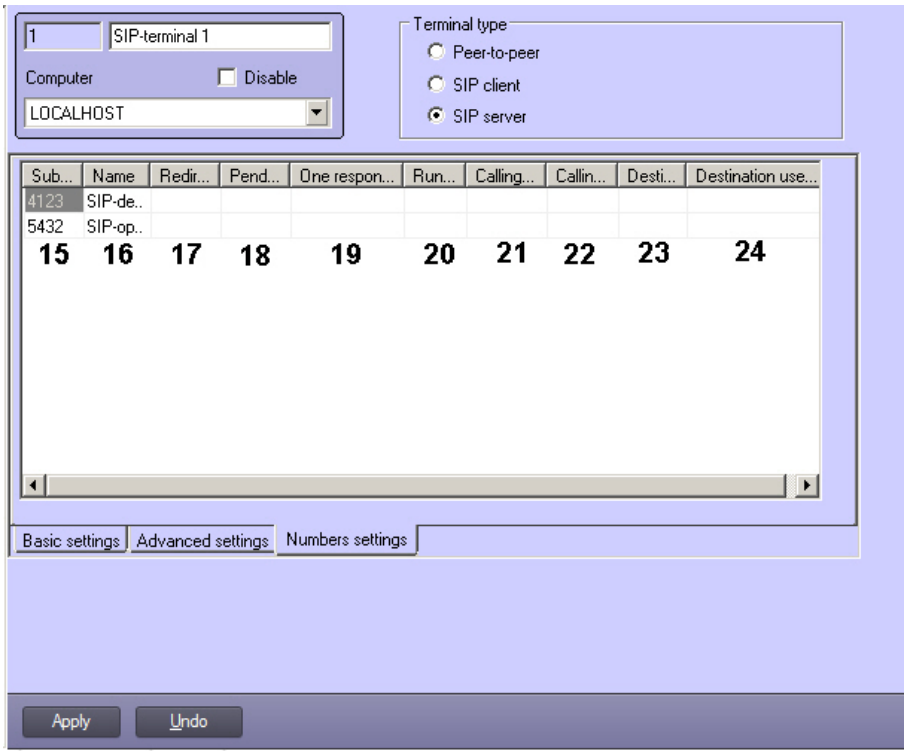


Table describes the parameters of the **SIP-terminal** settings panel.

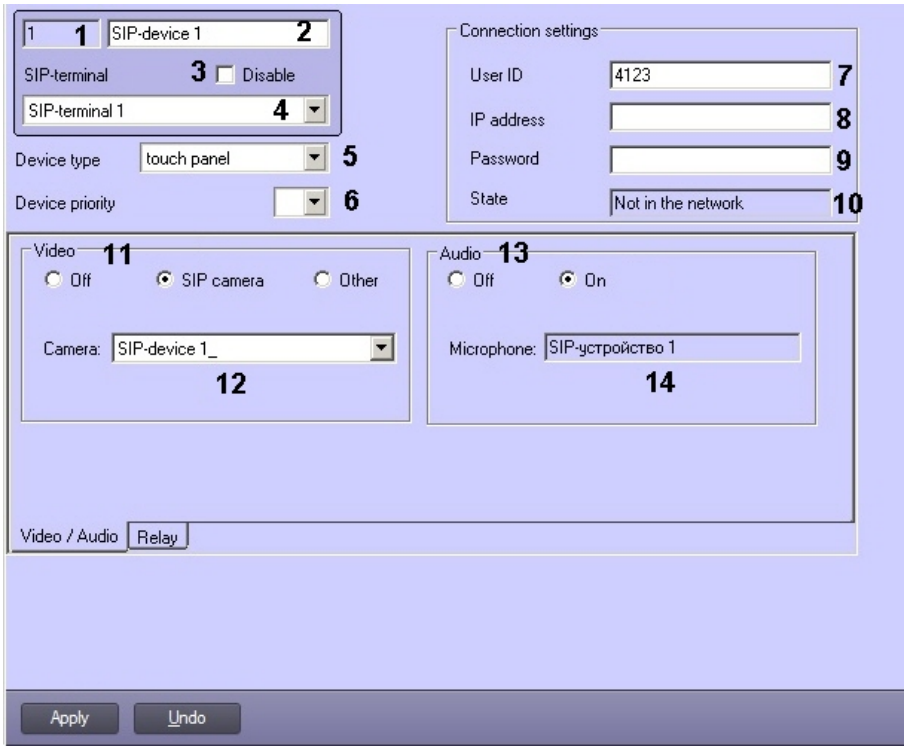
№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
1	The **Identification number** field	Automatically	Shows the identification number of the **SIP-terminal** object in the system.	Sequence of numbers	-	Depends on the number of the **SIP-terminal** objects in the system.
2	The **Name** field	Enter the value in the field	Assigns a name to the **SIP-terminal** object in the system.	Latin, Cyrillic letters and service characters	SIP-terminal	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Is set with a checkbox	Shows the status (enabled or disabled) of the **SIP-terminal** object in the system.	Boolean type	-	Yes – the **SIP-terminal** object is disabled and is not in use. No – the **SIP-terminal object** is enabled and is in use.
4	The **Computer** dropdown list	Is selected in the list	Assigns the parent **Computer** object for the **SIP-terminal** object.	Name of the **Computer** objects registered in the system.	Name of the parent **Compute r** object	Depends on the number of the **Computer** objects in the system.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
5	The **Terminal type** switch	Set switch to the required position	Sets the SIP terminal type	Supported SIP terminal types	Peer-to-peer	**SIP client** — the SIP-terminal acts as a client, it can be connected to any SIP-server **SIP server** — the SIP-terminal acts as a server, any SIP-clients can be connected to it **Peer-to-peer** terminal type is not supported at the present moment.
The **Basic settings** group						
6	The **Network** drop-down list	Is selected in the list	For **SIP-server** terminal type only Sets the IP address of the network adapter that will be used to connect to the network where the SIP-clients are located.	IP-address	Default network adapter	The list of available network adapters
7	The **SIP port** field	Enter the value in the field	For **SIP-server** terminal type only Sets the port number which will receive the data from the SIP-clients	Integer	5060	0-65535
8	The **SIP transport** drop-down list	Is selected in the list	For **SIP-server** terminal type only Sets the transport level protocol to be used.	Supported transport level protocols	UDP	TCP UDP
9	The **RTP ports range, from** and **to** fields	Enter the value in the field	For **SIP-server** terminal type only Sets RTP ports range	Integer	from: 40000 to: 64000	0-65535
10	The **Address** field	Enter the value in the field	For **SIP-client** terminal type only Sets the IP address of the SIP server	IP-address	-	1.0.0.0 - 255.255.255.255
11	The **Port** field	Enter the value in the field	For **SIP-client** terminal type only Sets the port for the SIP server connection	Integer	-	0-65535
The **Advanced settings** tab (for **SIP-server** only)						
12	The **Default operator** drop-down list	Is selected in the list	Sets the default SIP-operator to work with the SIP Panel	Name of the **SIP-operator** objects registered in the system.	-	Depends on the number of the **SIP-operator** objects in the system.
13	The **Subscriber** field	Enter the value in the field	Sets the SIP server special number	Integer	-	>=0

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
14	The **Name** field	Enter the value in the field	Sets the name of the special number	Latin, Cyrillic letters and service characters	-	A line representing a sequence of any symbols
The **Numbers settings** tab (for **SIP-server** only)						
15	The **Subscriber** column	Automatically	Lists the numbers of all devices and operators registered on the SIP-terminal, as well as special numbers.	-	-	-
16	The **Name** field	Automatically	Lists the names of the corresponding devices, operators, and special numbers.	-	-	-
17	The **Redirecting** field	Enter the value in the field	Sets the number to which the corresponding subscriber's calls should be forwarded to.	Integer	-	Numbers of all devices and operators registered on the SIP-terminal, as well as special numbers.
18	The **Pending, sec** field	Enter the value in the field	Sets the time period in seconds, during which it is necessary to wait for a response from the subscriber.	Integer	-	>0
19	The **One responder** checkbox	Set the checkbox	Enables a group call (redirected to several numbers) ending after one of the recipients answers	Boolean type	No	**Yes** – a group call is ended at all recipients after the response of any operator or device. **No** – 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 (conference calling).
20	The **Run macro** drop-down list	Is selected in 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.
21	The **Calling number multicast (video)** field	Enter the value in the field	Sets the IP address for broadcasting the video stream from the calling device in the multicast mode.	IP-address	-	1.0.0.0 - 255.255.255.255
22	The **Calling number multicast (sound)** field	Enter the value in the field	Sets the IP address for broadcasting the audio stream from the calling device in the multicast mode.	IP-address	-	1.0.0.0 - 255.255.255.255
23	The **Destination number multicast (video)** field	Enter the value in the field	Sets the IP address for broadcasting the video stream from the destination device in the multicast mode.	IP-address	-	1.0.0.0 - 255.255.255.255
24	The **Destination number multicast (sound)** field	Enter the value in the field	Sets the IP address for broadcasting the audio stream from the destination device in the multicast mode.	IP-address	-	1.0.0.0 - 255.255.255.255

13.1.2.8.37 The Settings panel of the SIP-device object

The settings panel of the **SIP-device** object is shown in the pictures below.



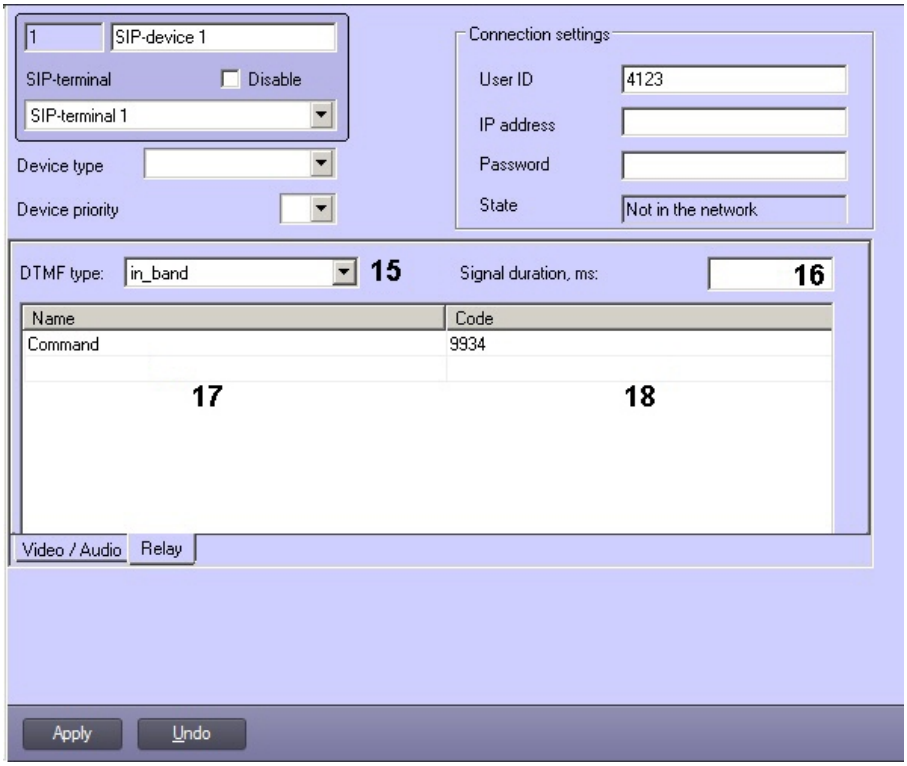


Table describes the parameters of the **SIP-device** settings panel.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
1	The **Identification number** field	Automatically	Shows the identification number of the **SIP-device** object in the system.	Sequence of numbers	-	Depends on the number of the **SIP-device** objects in the system.
2	The **Name** field	Enter the value in the field	Assigns a name to the **SIP-device** object in the system.	Latin, Cyrillic letters and service characters	SIP-device	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Is set with a checkbox	Shows the status (enabled or disabled) of the **SIP-device** object in the system.	Boolean type	-	Yes – the **SIP-device** object is disabled and is not in use. No – the **SIP-device object** is enabled and is in use.
4	The **SIP-terminal** dropdown list	Is selected in the list	Assigns the parent **SIP-terminal** object for the **SIP-device** object.	Name of the **SIP-terminal** objects registered in the system.	Name of the parent **SIP-terminal** object	Depends on the number of the **SIP-terminal** objects in the system.
5	The **Device type** drop-down list	Is selected in the list	Sets the icon type to represent the device on the Map.	Names of the available icon types	-	**SIP client** — the SIP-device acts as a client, it can be connected to any SIP-server **SIP server** — the SIP-device acts as a server, any SIP-clients can be connected to it **Peer-to-peer** terminal type is not supported at the present moment.
6	The **Device priority** drop-down list	Is selected in the list	Sets the device calls priority when displayed on the SIP panel	Integer	-	0 – 10 The higher the number the higher the priority. If the field left empty, the priority is considered minimal.
The **Connection settins** group						
7	The **User ID** field	Enter the value in the field	Sets the SIP-device identification number, i.e. the number to call it.	Integer		>=0
8	The **IP address** field	Enter the value in the field	For **SIP-server** terminal type only Sets the SIP-device IP address.	IP address		1.0.0.0 - 255.255.255.255
9	The **Password** field	Enter the value in the field	For **SIP-server** terminal type only Sets the password specified on the SIP-device.	Latin, Cyrillic letters and service characters		A line representing a sequence of any symbols

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
10	The **State** field	Automatically	For **SIP-server** terminal type only Displays the SIP device state	-	-	-
The **Video/Audio** tab (for **SIP-server** terminal type only)						
11	The **Video** switch	Set the switch to the required position	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.
12	The **Camera** drop-down list	Is selected in 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.
13	The **Audio** switch	Set the switch to the required position	Sets the microphone used for calls	Supported options of audio usage	Off	**Off** — the audio is not used during the call. **On** — the microphone of the SIP-device is used.
14	The **Microphone** field	Automatically	Displays the name of the **Microphone** object corresponding to the SIP device	-	-	-
The **Relay** tab (for **SIP-server** terminal type only)						
15	The **DTMF type** drop-down list	Is selected in the list	Sets the type of the tone DTMF command	Supported signal type	in_bound	in_band – the signal is transmitted as normal sound in an audio stream. rtp_nte – signals are transmitted via RTP separately from the voice stream. sip_info – signals are transmitted in the SIP INFO message. sip_notify – signals are transmitted in the SIP NOTIFY message.
16	The **Signal duration, ms** field	Enter the value in the field	Sets the time period in milliseconds during which the command is to be sent.	Integer		>0
17	The **Name** field	Enter the value in the field	Sets the name of the command displayed on the SIP panel	Latin, Cyrillic letters and service characters		A line representing a sequence of any symbols
18	The **Code** field	Enter the value in the field	Sets the unique command code	Integer		>0

13.1.2.8.38 The Settings panel of the SIP-operator object

The settings panel of the **SIP operator** object is shown in the pictures below.

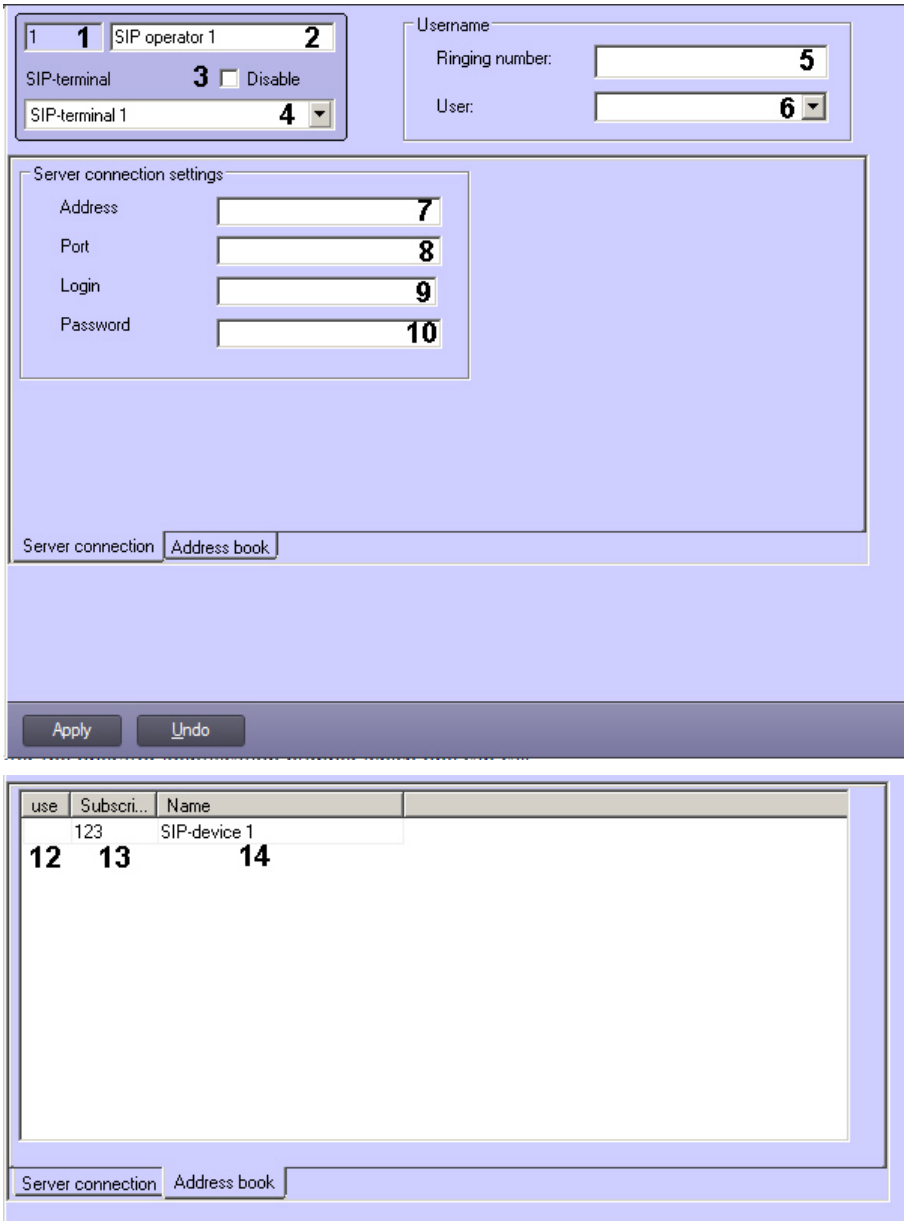


Table describes the parameters of the **SIP operator** settings panel.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
1	The **Identification number** field	Automatically	Shows the identification number of the **SIP operator** object in the system.	Sequence of numbers	-	Depends on the number of the **SIP operator** objects in the system.

№	Parameter	Method for setting the parameter value	Description	Presented as	Default value	Range of values
2	The **Name** field	Enter the value in the field	Assigns a name to the **SIP operator** object in the system.	Latin, Cyrillic letters and service characters	SIP operator	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Is set with a checkbox	Shows the status (enabled or disabled) of the **SIP operator** object in the system.	Boolean type	-	Yes – the **SIP operator** object is disabled and is not in use. No – the **SIP operator object** is enabled and is in use.
4	The **SIP-terminal** dropdown list	Is selected in the list	Assigns the parent **SIP-terminal** object for the **SIP operator** object.	Name of the **SIP-terminal** objects registered in the system.	Name of the parent **SIP-terminal** object	Depends on the number of the **SIP-terminal** objects in the system.
5	The **Ringing number** field	Enter the value in the field	Sets the operator identification number	Integer	-	>=0
6	The **User** drop-down list	Is selected in the list	Sets the corresponding *Intellect* user	Name of the **User** objects registered in the system.		Depends on the number of the **User** objects in the system.
The **Server connection** tab (for **SIP-client** terminal type only)						
7	The **Address** field	Enter the value in the field	Sets the IP address of the SIP-server	IP address	-	1.0.0.0 - 255.255.255.255
8	The **Port** field	Enter the value in the field	Sets the port of the SIP-server	Integer	-	0-65535
9	The **Login** field	Enter the value in the field	Sets the username for connecting to the SIP-server	Latin, Cyrillic letters and service characters	-	A line representing a sequence of any symbols
10	The **Password** field	Enter the value in the field	Sets the password for connecting to the SIP-server	Latin, Cyrillic letters and service characters	-	A line representing a sequence of any symbols
The **Address book** tab						
11	The **use** column	Set the checkbox	Sets the devices, operators and special numbers that should be available in the SIP panel address book of this operator.	Boolean type	No	**Yes** – the number is displayed on the SIP panel **No** – the number is not displayed on the SIP panel
12	The **Subscriber** field	Automatically	Shows the numbers of devices, operators and special numbers	-	-	-
13	The **Name** field	Automatically	Shows the names of devices, operators and special numbers	-	-	-

13.1.2.9 The Interfaces tab

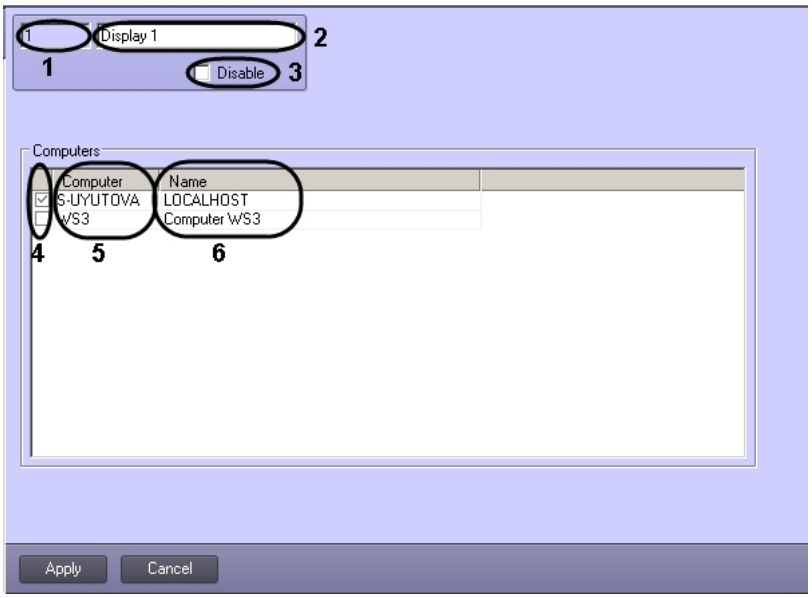
The **Interfaces** tab is designed to create and configure a user interface of the video surveillance and audio monitoring system.

13.1.2.9.1 Interfaces tab components

The **Interface** tab shows a tree of the system objects, corresponding to the user interface components, and a tools panel, which is 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.

13.1.2.9.2 The Settings panel of the Display object

The **Display** object is designed to register virtual screens in the system which are used as a basis for interface components created in the Intellect system. The settings panel of the **Display** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Display** object .

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Display** object in the digital distributed video surveillance system.	Sequence of numbers	-	Depends on the number of **Display** objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the box	Defines the name of the **Display** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Screen	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the condition of the **Display** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean type	Not available	Yes – the **Display** object is disabled and is not in use No – the **Display** object is enabled and is in use.
Computer Group						

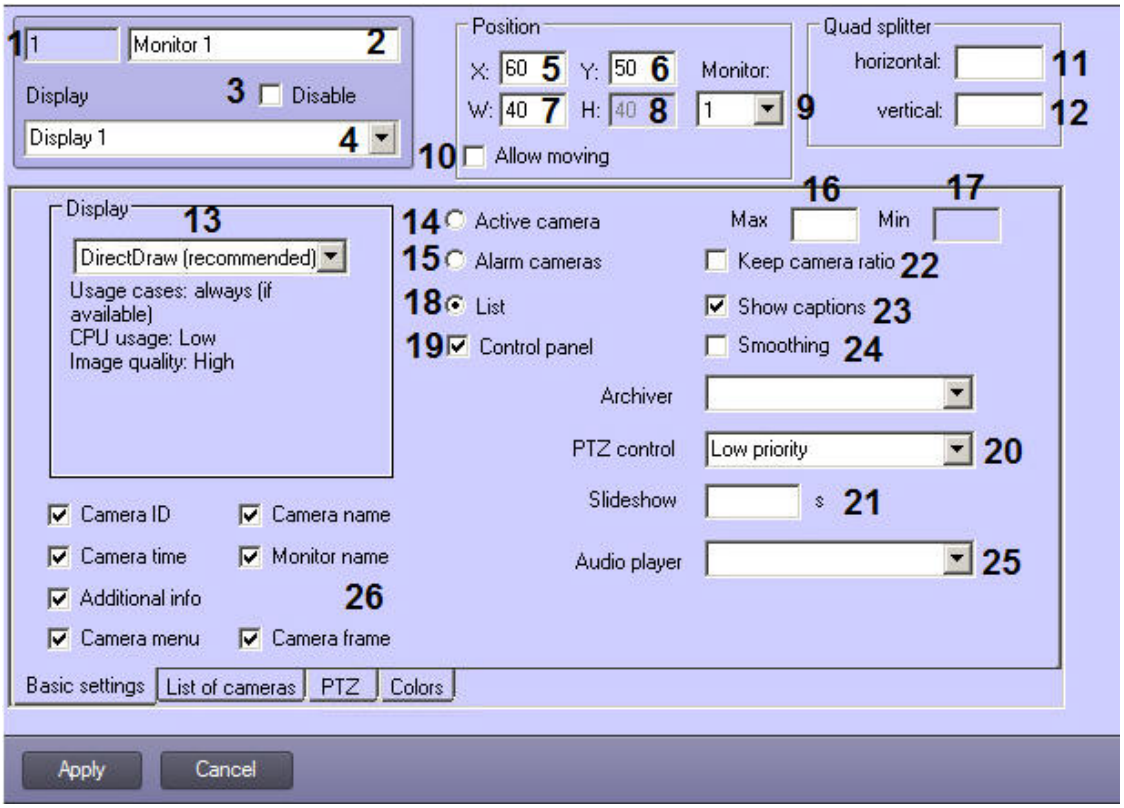
№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
4	Select an element *	Is identified by the check mark	Contains a list of computers (videoserver, Remote Administrator Workstation, Remote Workstation) connected to the given videoserver (Remote Administrator Workstation). The check marks referred to the computers define whether or not the computers should display the **Monitor** objects based on the given **Display** object.	Boolean type	Not available	Yes – the computer will display the **Monitor** object, created on the basis of the given **Display** object. No – the computer will not display the **Monitor** object, created on the basis of the given **Display** object.
5	Computer	Automatically	Defines 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 symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.
6	Name	Automatically	Gives the name to the computer used in the digital distributed video surveillance system	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 distributed video surveillance system. A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Number of symbols – from 1 to 60.

*The name of the element is not displayed in the settings panel of the given object.

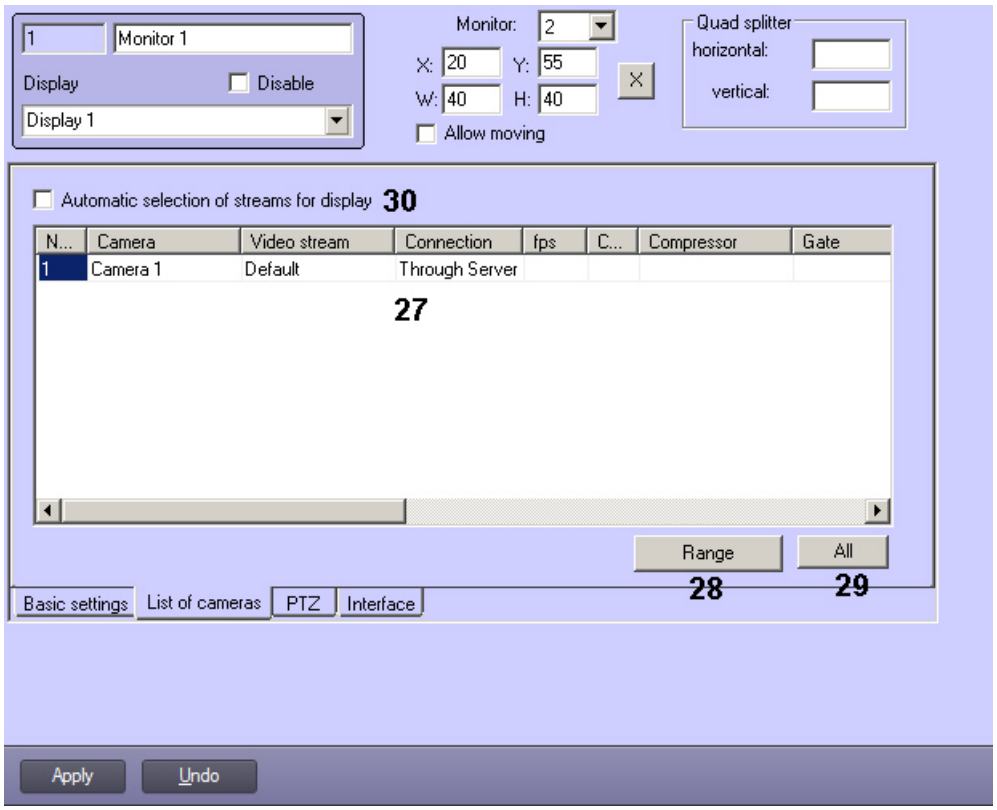
13.1.2.9.3 The Settings panel of the Monitor object

The face of the settings panel for the **Monitor** object is shown in the figures.

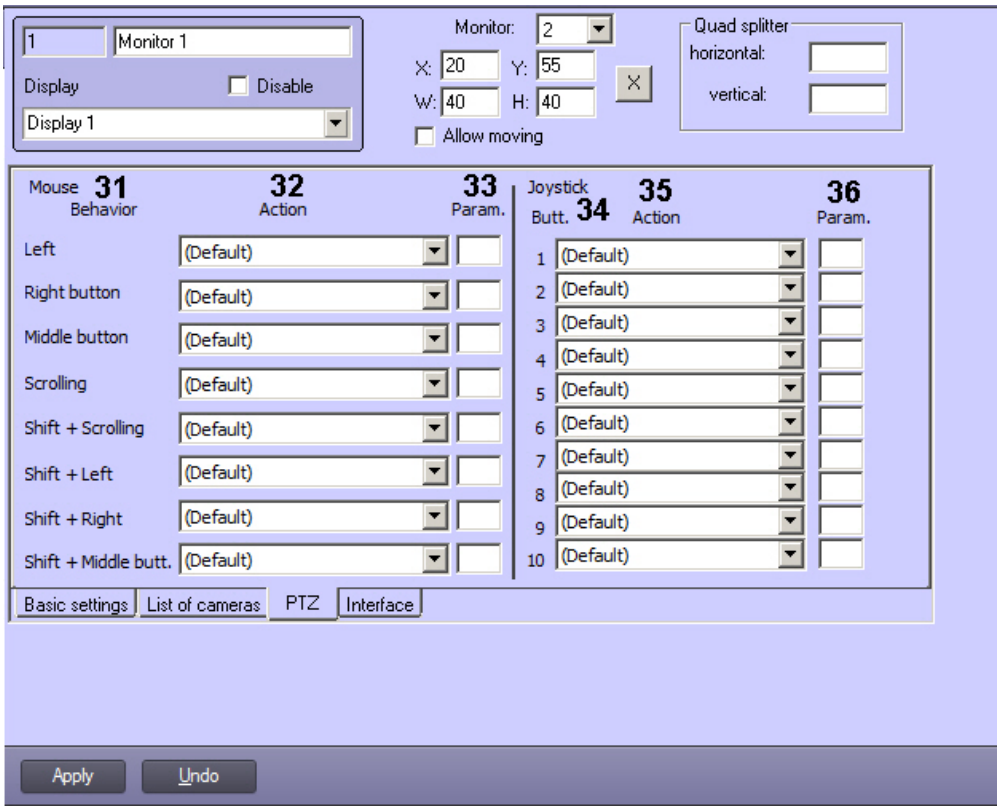
The **Basic settings** tab



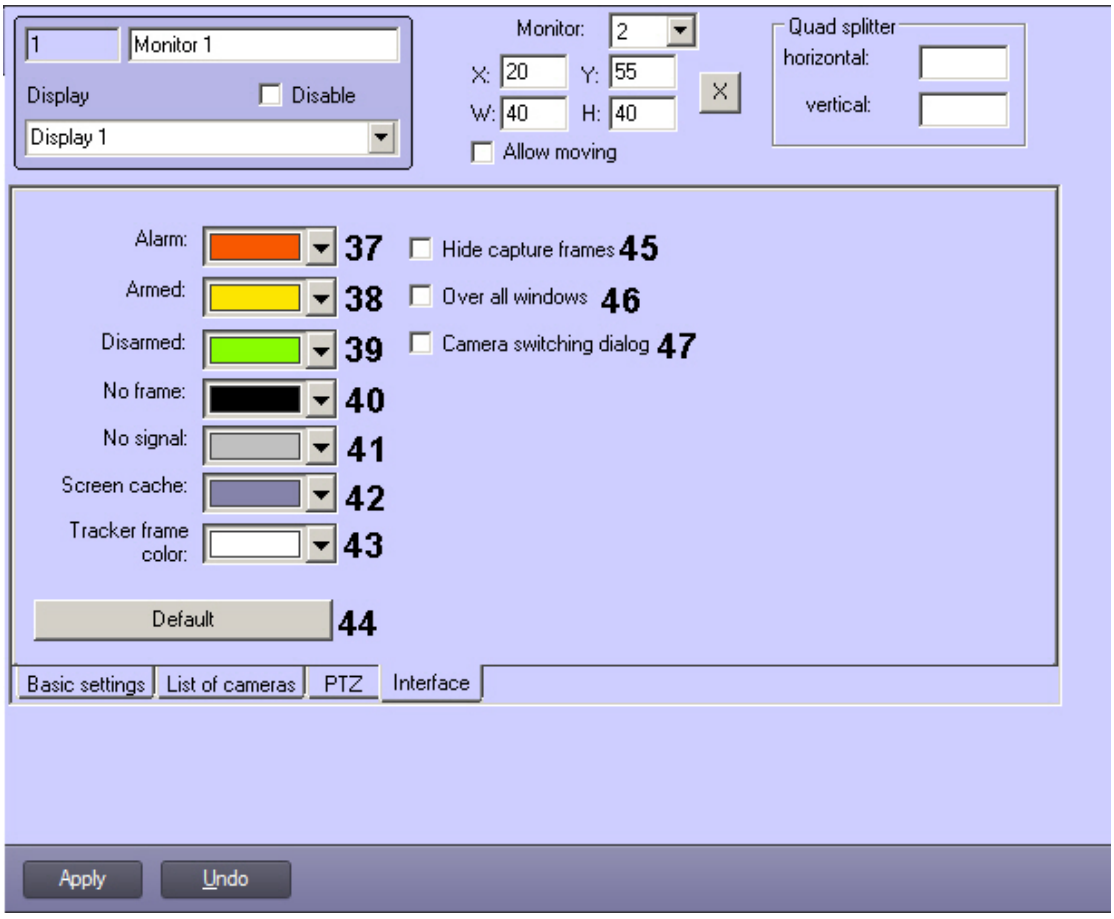
The **List of cameras** tab



The **PTZ** tab

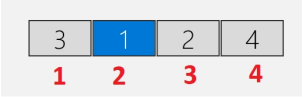


The **Interface** tab



The table describes the setting parameters of the **Monitor** interface object.

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
1	The **Identification number** field	Automatically	Displays the identification number of the **Monitor** interface object in the system.	Sequence of numbers	-	Depends on the number of the Monitor objects in the system.
2	The **Name** field	Enter the value in the field	Defines the name of the **Monitor** object in the system.	Latin, Cyrillic and service digits	Monitor	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Set the checkbox	Defines the mode of the Monitor object (enabled or disabled) in the system.	Boolean type	-	**Yes** – the **Monitor** object is disabled and is not in use **No** – the **Monitor** object is enabled and is in use
4	The **Display** drop-down list	Select in the list	Sets the parent **Display** object for the given **Monitor** object.	Names of the **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** object s in the system.
The **Position** group						
5	The **X** field	Enter the value in the field	Set the X coordinate in the horizontal axis for the upper-left corner of the **Monitor** interface box	% of the screen width	-	From 0 to M*100, where M is the number of the monitors installed
6	The **Y** field	Enter the value in the field	Set the Y coordinate in the vertical axis for the upper left corner of the **Monitor** interface box	% of the screen height	-	From 0 to M*100, where M is the number of the monitors installed
7	The **W** field	Enter the value in the field	Set the width of the **Monitor** interface box	% of the screen width	-	From 20 to 900 if Control panel is enabled. Otherwise, from 0 to 900. This upper bound can be removed using the UnlimitMonitorSize registry key (see Registry keys reference guide).
8	The **H** field	Enter the value in the field	Set the height of the **Monitor** object if the control panel is not active	% of the screen width	-	From 0 to 900 This restriction can be removed using the UnlimitMonitorSize registry key (see Registry keys reference guide).

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
9	The **Monitor** drop-down list	Select in the list	Sets the physical monitor number, the coordinates for which are assigned. 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. On the illustration below, monitor numbers in OS are given in gray while numbers in Intellect are red.  ***Important! 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 a border (for example, upper border).***	Sequence of numbers	1	From 1 to 16
10	The **Allow moving** checkbox	Set the checkbox	Allows hand shifting of the **Monitor** interface box if the control panel is active	Boolean type	-	Yes – hand shifting is allowed. No – hand shifting is prohibited.
Quad splitter group						
11	**horizontal** field	Enter the value in the field	Sets number of video surveillance windows in the horizontal direction to display then on the Monitor. If value is not specified (field is empty) then default grid of video surveillance windows depending on the selected layout is displayed	Natural numbers	-	From 1 to 64
12	**vertical** field	Enter the value in the field	Sets number of video surveillance windows in the vertical direction to display then on the Monitor. If value is not specified (field is empty) then default grid of video surveillance windows depending on the selected layout is displayed	Natural numbers	-	From 1 to 64
The **Basic settings** tab						
13	The **Display** drop-down list	Select in the list	Set the **Display mode** for processing video signals	Names of display modes	DirectDraw (Recommended)	**Direct3D** – is used when it is necessary to display the video from 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 a video card.
14	The **Active camera** switch	Set in the position	Set the display mode for an active camera box	Boolean type	-	**Yes** - The Active camera mode is enabled and is in use **No** - The Active camera mode is disabled and is not in use

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
15	The **Alarms cameras** switch	Set in the position	Set the display mode for alarm cameras' boxes	Boolean type	-	**Yes** - The **Alarms cameras** mode is enabled and is in use **No** - The **Alarms cameras** mode is disabled and is not in use
16	The **Max** field	Enter the value in the field	Specify the maximum number of video cameras, boxes of which are displayed on the Monitor in the **Alarms cameras** and List modes	Sequence of numbers	-	From 1 to 64 Depends on the number of cameras registered in the system
17	The **Min** field	Enter the value in the box	Specify the minimum number of video cameras, boxes of which are displayed on the Monitor in the **Alarms cameras** even on no-alarm	Sequence of numbers	-	From 1 to 64 Depends on the number of cameras registered in the system. 0 – on no-alarm camera boxes are not displayed in the Monitor box.
18	The **List** switch	Set in the position	Set the display mode according to the selected layout.	Boolean type	Yes	**Yes** - The List mode is enabled and is in use **No** - The List mode is disabled and is not in use
19	The **Control panel** checkbox	Set the checkbox	Activates the control panel for the Monitor in the **List** mode	Boolean type	-	**Yes** - The **Control panel** mode is enabled and is in use **No** - The **Control panel** mode is disabled and is not in use
20	The **Telemetry control** drop-down list	Select in the list	Set the prioritiy for the Telemetry control using the **Monitor** object	Names of the Telemetry control priorities	Low priority	**Forbidden** – option of the Telemetry control using the Monitor object is disabled **Low priority** – low priority of control **High priority** – high priority of control
21	The **Slideshow** field	Enter the value in the field	Set the period of automatic slideshow of camera boxes when the control panel is enabled	Period in seconds (s)	-	Whole number from 1 and bigger
22	The **Keep camera ratio** checkbox	Set the checkbox	Specifies the ratio of the width and height of the video in the surveillance windows on the Video surveillance monitor.	Boolean type	-	**Yes** – the ratio of the width and height of the video corresponds to the ratio of the camera. **No** – video fits the entire area of the Surveillance window, while the ratio may be affected.
23	The Show captions checkbox	Set the checkbox	Shows the captions for cameras of the **Monitor** interface box. 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.	Boolean type	Yes	**Yes** – The **Captions** submenu is available in the context menu of the Monitor interface box **No** – The **Captions** submenu is unavailable in the context menu of the Monitor interface box

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
24	**Smoothing** checkbox	Setting checkbox	Is used when it is required to display video with greater resolution on which the ladder effect appears while 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	No	**Yes** – smoothing is applied. **No** – smoothing is not applied
25	The **Audio player** drop-down list	Select in the list	Sets the **Audio player** object used to playback audio signals and export video 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
26	Group of checkboxes used to enable displaying elements of Surveillance windows	Set the checkboxes	Allows enabling and disabling 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 checked	**Yes** – the corresponding element is displayed in Surveillance windows of all cameras added to the Video surveillance monitor. **No** – the corresponding element is not displayed in Surveillance windows on the Video surveillance monitor.
The **List of cameras** tab						
27	The **Number** drop-down list	Select in the list	Set the number of the video camera to display on the Monitor	Sequence of numbers	-	Depends on the number of video cameras registered in the system
	The **Camera** drop-down list	Select in the list	Set the name of the video camera to display on the Monitor	Name of the cameras registered in the system	-	Depends on the number of video cameras registered in the system
	Video stream drop-down list	Select value from the list	Set the number of video stream from camera which is to be displayed when receiving video stream straight from camera	Streams numbers	Default	1, 2, 3, 4 – video streams. Default – default video stream.
	Connection drop-down list	Select value from the list	Set the way of receiving video from camera	Ways of receiving video	Through Server	**Direct** - the video stream is received straight from camera **Through Server** - the video stream is received from the Server, which camera is connected to
	The **Fps** drop-down list	Select in the list	Set the fps for transmitting the video signal to the Monitor of the Client.	Sequence of numbers	-	1, 2, 3, 4, 6, 8, 12, 16, 20, 25, 30

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
	The **Compression** drop-down list	Select in the list	Set the compression for transmitting the video signal to the Monitor of the Client. The given value leads to extra consumption of Server's resources.	Sequence of numbers	-	In the range of rising compression level 0,1,2,3,4,5 0 – the video signal is not compressed 5 – maximum compression of the video signal
	Compressor drop-down list	Select value from the list	Specifies the procedure of video stream compression which is in use for video signal recompression for displaying on the Monitor. The value is to be selected in the **Compression** list if the compressor is specified.	List of available procedures	-	MJPEG, Motion Wavelet 3.5, Motion Wavelet 7.1
	The **Gate** drop-down list	Select in the list	Set the **Gate** object via which the live and archive video from the selected camera is to be transmitted to the Monitor	Names of the **Gateway** objects registered in the system	-	Depends on the number of the **Gate** objects registered in the system
	The Backup archive drop-down list	Select in the list	Set the Backup archive object the video archive from the selected camera of which is to 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
	The External storage	Select in the list	Set the External storage object the video archive from which is to be transmitted to the Monitor via the selected camera	Names of the External storage objects registered in the system	-	Depends on the number of the External storage objects registered in the system
	The **Gateway for Backup archive** drop-down list	Select in the list	Set the **Gate** object via which the video archive of the **Backup archive** object is to be transmitted to the Monitor	Names of the **Gateway** objects registered in the system	-	Depends on the number of the **Gateway** objects registered in the system
	The **VMDA metadata storage** drop-down list	Select in the list	Set the **VMDA metadata storage** to be used for smart search in the archive	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
	The **Display type** dropdown list	Select value in 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.

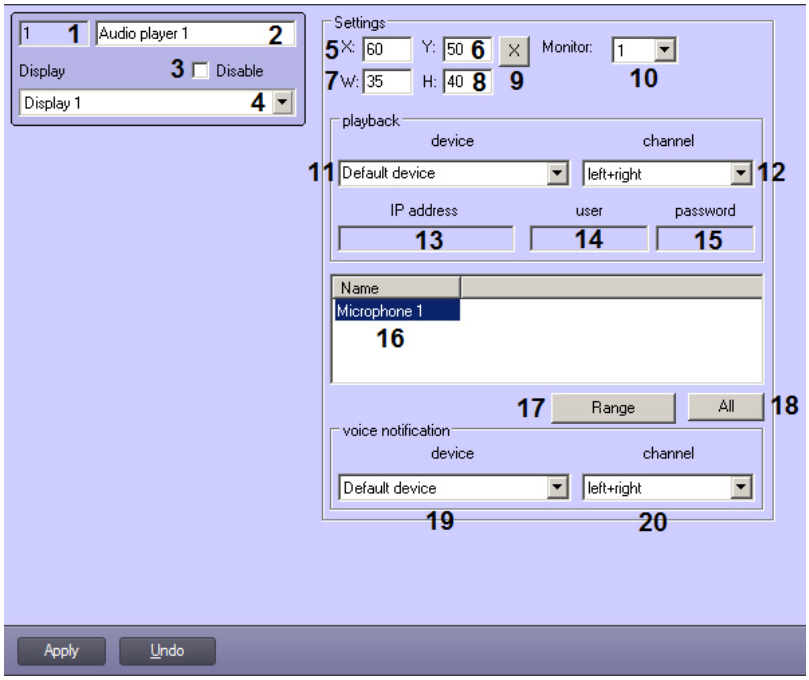
№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
	The **Macro 1** dropdown list	Select value in the list	Sets the first macro to be displayed in the function menu of the camera in the Video Surveillance Window.	Names of the **Macro** objects registered in the system	-	Depends on the number of the **Macro** objects registered in the system
	The **Macro 2** dropdown list	Select value in the list	Sets the second macro to be displayed in the function menu of the camera in the Video Surveillance Window.	Names of the **Macro** objects registered in the system	-	Depends on the number of the **Macro** objects registered in the system
28	The **Range** button	Click the button	Select all cameras registered in the system to display on the Monitor	-	-	-
29	The **All** button	Click the button	Access to complex selection and editing of cameras' parameters to display on the Monitor	-	-	-
30	**Auto select of streams for displaying** checkbox	Setting checkbox	Enables the function of auto select of video stream for displaying in the Monitor. Affects cameras for which the On default video stream is selected - see 25.	Boolean type	No	**Yes** - video stream for displaying is selected depending on the size of video image on the Monitor and required frame frequency **No** -video stream is selected depending on the **Video stream** and **Connection** settings (25-26) and depending on settings of the Server and video camera from which the stream is required.
The **PTZ** tab						
31	**Mouse behavior**	-	The list of available actions with a mouse	-	-	-
32	**Action** drop-down list	Select value from the list	Specify reaction performed while executing the corresponding action using a mouse	Reaction list of the **PTZ device** object	(Default)	Reaction list of the **PTZ device** object
33	**Parameter** field	Enter the value in the field	Specify the value of reaction parameter if it's required	Depends on the selected action	-	Depends on the selected action. It is a preset number for reactions connected with presets, for other reactions it is speed if the selected reaction allows speed specifying as parameter. The speed value from the PTZ device object connected with Camera selected in the Monitor is in use if the parameter is not specified.
34	**Joystick** buttons column	-	List of joystick buttons	-	-	-
35	**Action** drop-down list	Select value from the list	Specify reaction which is to be performed while clicking the joystick button	List of reaction of **PTZ device** object.	(Default)	List of reaction of **PTZ device** object

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
36	**Parameter** field	Enter the value in the field.	Specify the value of reaction parameter if it is required.	Depends on the selected action	-	Depends on the selected action. It is a preset number for reactions connected with presets, for other reactions it is speed if the selected reaction allow speed specifying as parameter. The speed value from the **PTZ device** object connected with Camera selected in the Monitor is in use if the parameter is not specified.
The **Colors** tab						
37	**Alarm** dropdown list	Select value from the list	Set the Viewing tile frame color if there is an alarm on the camera	RGB colors	Red	RGB color palette
38	**Armed** dropdown list	Select value from the list	Set the Viewing tile frame color when the camera is armed	RGB colors	Yellow	RGB color palette
39	**Disarmed** dropdown list	Select value from the list	Set the Viewing tile frame color when the camera is disarmed	RGB colors	Green	RGB color palette
40	**No frame** dropdown list	Select value from the list	Set the Viewing tile frame color when there is no frame from the camera in the Viewing tile	RGB colors	Black	RGB color palette
41	**No signal** dropdown list	Select value from the list	Set the Viewing tile frame color when there is no signal from the camera	RGB colors	Grey	RGB color palette
42	**Screen cache** dropdown list	Select value from the list	Set 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	RGB colors	Purple	RGB color palette
43	**Tracker frame color** dropdown list	Select value from the list	Sets the color of the frame to highlight tracking objects on the video image.	RGB colors	White	RGB color palette
44	**Default** button	Click the button	Set the default settings of the Viewing tile frame color	-	-	-
45	**Hide capture frame** checkbox	Setting checkbox	Hides the frames displayed by the Face detection tool module when a person's face is detected in the video image.	Boolean type	No	**Yes** – the Face detection tool frames are hidden. **No** – the Face detection tool frames are shown.
46	**Over all windows** checkbox	Setting checkbox	Enables the display of the Video Surveillance Monitor on top of all windows.	Boolean type	No	**Yes** – the Video Surveillance Monitor is displayed on top of all windows. **No** – the Video Surveillance Monitor is displayed in the default mode.

№	Parameter	Method of setting the value	Parameter description	Symbols used	Default value	Value range
47	**Camera switching dialog** checkbox	Setting checkbox	Enables a special dialog for selecting a camera in the Video surveillance window.	Boolean type	No	**Yes** – a special dialog is in use for camera selection **No** – the camera is selected in the functional menu of the Video surveillance window.

13.1.2.9.4 The Settings panel of the Audio player object

The settings panel of the **Audio player** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Audio player** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	**Identification number**	Automatically	Displays the identification number of the **Audio player** object in the system.	Sequence of numbers	-	Depends on the number of **Audio player** objects in the system.

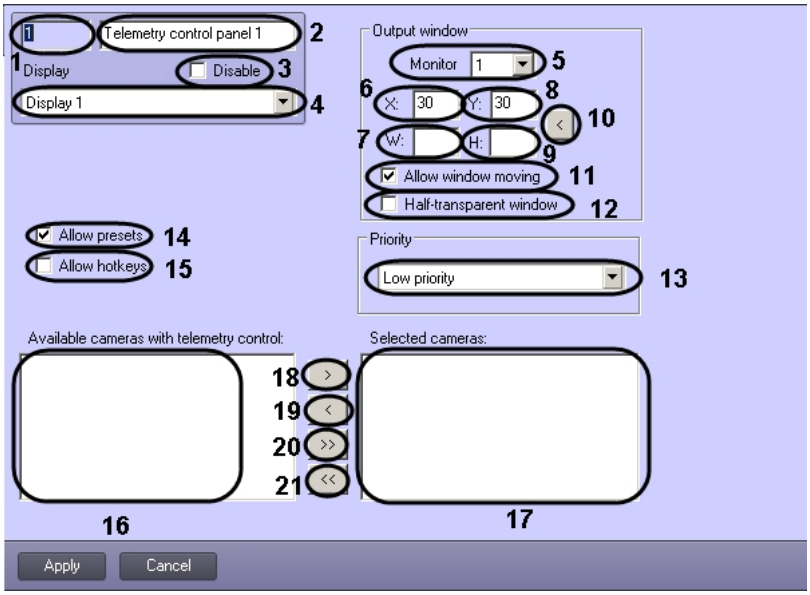
№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
2	**Name**	Enter the value in the box	Defines the name of the **Audio player** object in the system.	Latin, Cyrillic and service characters	Audio player	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Check box **Disable**	Is identified by the check mark	Defines the status (enabled or disabled) of the **Audio player** object in the system.	Boolean type	Not available	**Yes** – the **Audio player** object is disabled and is not in use **No** – the **Audio player** object is enabled and is in use.
4	Dropdown list **Display**	Is selected from the list	Defines the parent **Display** object for the given **Audio player** object.	Names of the **Display** objects registered in the system	Name of the parent **Display** object.	Depends on the number of **Display** objects in the system.
Settings Group						
5	X	Enter the value in the field.	Defines the coordinate in the X horizontal axis for the upper left corner of the Audio player on the screen.	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed.
6	Y	Enter the value in the box.	Defines the coordinate in the Y vertical axis for the upper left corner of the Audio player on the screen.	% of the screen height		From 0 to M*100, where M is the number of monitors installed.
7	W	Enter the value in the box.	Defines the Audio player window width.	% of the screen width	-	From 40 to M*100, where M is the number of monitors installed.
8	H	Enter the value in the box.	Defines the Audio player window height.	% of the screen width	Not defined	From 40 to M*100, where M is the number of monitors installed.
9	The **X** button	Click the button	Opens a test window to set position of the **Audio player** window	-	-	-

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
10	The **Monitor** drop-down list	Is selected from the list	Sets the physical monitor number, the coordinates for which are assigned. 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.	Integer	1	1 to 16
The **Playback** group						
11	Dropdown list **Device**	Is selected from the list	Defines sound device for which audio signals shoul be transmited to playback.	Nemes of audio devices, registered in the system	Device by default	Depends on the number of devices in the system. Standard sound map is the default device.
120	**Channel**	Is selected from the list	Defines the chanal of audio signals' playback	Left+right, left,right	Left+right	Left+right audio signal is transmitted to left and right channels of sound device. Left – audio signal is transmitted to the left channel of the sound device. Right– audio signal is transmitted to the right channel of the sound device
13	**IP address**(is set for audio IP-device)	Enter the value in the field.	Set the IP-adress of the sound device	IP-adress	-	Depends on settings registered in the system of IP-devices
14	**User(is** set for audio IP-device)	Enter the value in the field.	Set the user name to connect to the sound device	-	-	Depends on settings of IP-device
15	**Password(is** set for audio IP-device)	Enter the value in the field.	Set user's password for connection to the sound device	-	-	Depends on settings of IP-device
Name table						
16	Dropdown list **Name**	Select the value from the list	Set the microphone, which audio signals should be recorded and/or played	Names of **Microphone** objects,registered in the system	-	Depends on number of Microphone objects in the system
17	The **Range** button	Click the button	Opens the dialog box for bulk addition of microphones	-	-	-

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
18	The **All** button	Click the button	Adds all the microphones from hardware tree to the list	-	-	-
The **Voice notification** group						
19	Dropdown list **Device**	Select the value from the list	Set the voice notification device when alarms are registered by cameras	Names of voice detection devices, registered in the system	Device by default	Depends on voice notification devices, registered in the system. Standard sound map is the default device.
20	Dropdown list **Channel**	Select the value from the list	Set the channel of voice notification when alarms are registered by cameras	Left+right, left,right	Left+right	Left+right- audio signal is transferred to the left and right channels of the voice notification device.Left- audio signal is transferred to the left channel of the voice notification device.Right- audio signal is transferred to the right channel of the voice notification device

13.1.2.9.5 The Settings panel of the Telemetry control panel object

The settings panel of the **Telemetry control panel** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Telemetry control panel** object.

№	Parameter	Method for setting the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Telemetry control panel** object in the system.	Sequence of numbers	-	1 or more Depends on the **Telemetry control panel** objects in the system.
2	Name*	Type-in the value in the field	Specifies 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 symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Checkbox is set	Sets the status of the **Telemetry control panel** object in the system.	Boolean type	-	**Yes** – the **Telemetry control panel** object is disabled and is not in use **No** – the **Telemetry control panel** object is enabled and is in use.
4	Display	Is selected in the list	Sets the parent Display object for the given **Telemetry control panel** object.	Names of the **Display** objects registered in the system	Name of the parent **Display** object.	Depends on the number of the **Display** objects in the system.
The **Coordinates** group						
5	Monitor	Is selected in the list	The number of monitor in OS for which coordinates are specifying	Numbers of monitors	1	1-16
6	X	Type-in the value in the field.	Sets the coordinate in the X 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 monitors installed.
7	Y	Type-in the value in the field.	Sets the coordinate in the Y 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 monitors installed.
8	W	Type-in the value in the field.	Sets the width of the Telemetry control panel.	% of the screen width.	-	From 18 to M*100, where M is the number of monitors installed.
9	H	Type-in the value in the field.	Sets the height of the **Telemetry control panel**	% of the screen height.	-	From 34 to M*100, where M is the number of monitors installed.
10	Current settings*	Click the button	Sets the current coordinates of the **Telemetry control panel** in X, Y, W and H fields	-	-	-
11	Allow window's moving	Checkbox is set	Allows moving the **Telemetry control** using the mouse panel	Boolean type	Yes	**Yes** – allow moving the **Telemetry control panel** **No** – forbid moving **Telemetry control panel**

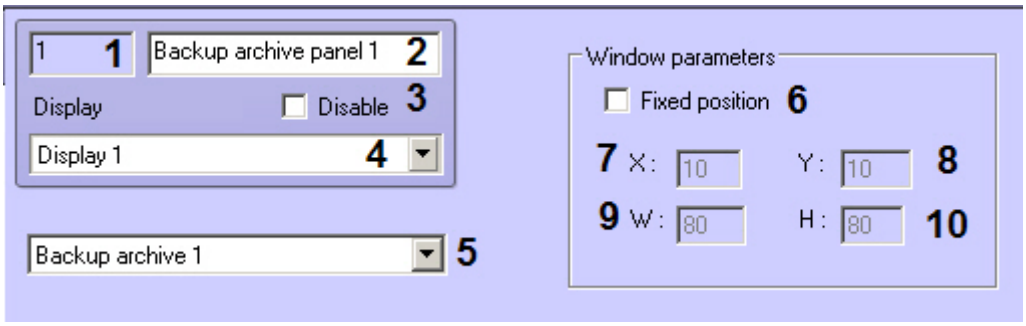
№	Parameter	Method for setting the parameter	Parameter description	Symbols used	Default value	Value range
12	Half-transparent window	Checkbox is set	Displays the half-transparent **Telemetry control panel**	Boolean type	Yes	**Yes-** display the half-transparent **Telemetry control panel**. **No** – do not display the half-transparent **Telemetry control panel**.
13	Priority	Is selected in the list	Sets the priority of Telemetry control	Names of priorities for Telemetry control	Low	**Forbidden** – Telemetry control is forbidden. **Low** – control over PTZ device using the Telemetry control panel is performed after it controls devices with Standard or High ptiority **Standard** - control over PTZ device using the Telemetry control panel is performed after it controls devices with High ptiority. **High** - control over PTZ device using the Telemetry control panel is performed in the first place
14	Allow presets	Checkbox is set	Enables saving presets	Boolean type	Yes	**Yes** – presets saving is enabled. **No** – presets saving is disabled
15	Allow hotkeys	Checkbox is set	Enables Telemetry control using a keyboard	Boolean type	No	**Yes–** keyboard can be used for Telemetry control **No** – keyboard hotkeys are not used for Telemetry control
16	Available cameras with telemetry control	Automatically	Shows cameras with PTZ devices.	Names of the **Camera** objects registered in the system.	The list of all **Camera** objects registered in the system.	Depends on the number of PTZ devices.
17	Selected cameras	Click arrow keys	Shows cameras with PTZ devices that can be controlled using the **Telemetry control panel**	-	-	Depends on the number of PTZ devices.
18	One to the right*	Click the button	Moves specified 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 specified 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 with telemetry control** list.	-	-	-

* The name of the element is not displayed in the settings panel of the given object

13.1.2.9.6 The Settings panel of the Backup archive panel object

The **Backup archive panel** object is designed to register and configure the **Backup archive panel** interface object in the Intellect system, which allows the Operator configuring video data archiving.

The settings panel of the **Backup archive panel** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Backup archive panel** object.

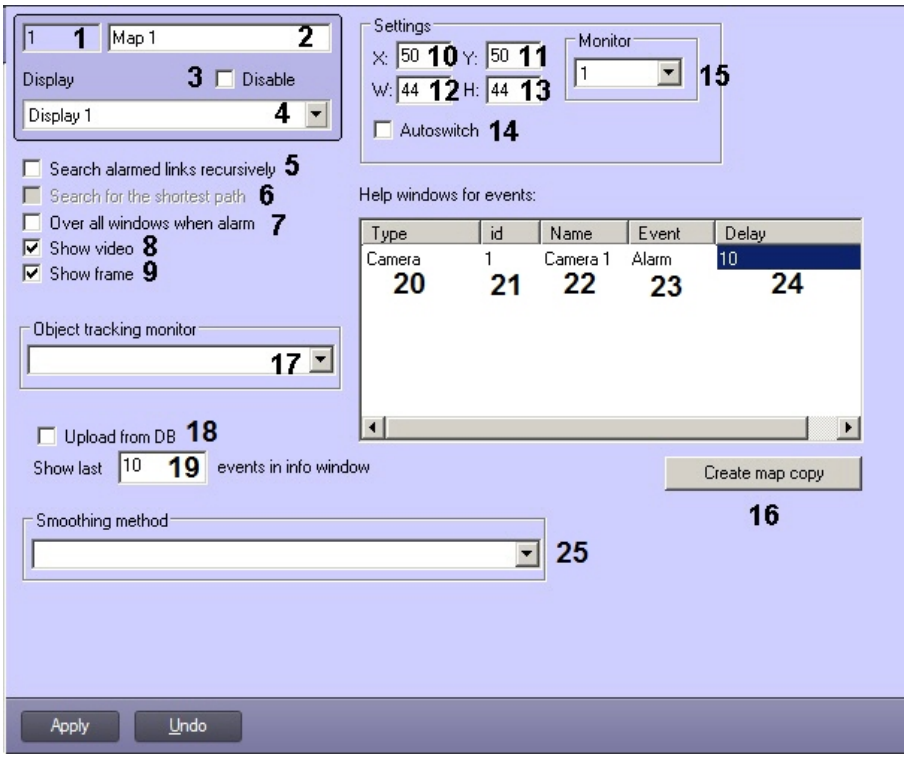
№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Backup archive panel.**	Sequence of numbers	-	From 1 and above. Depends on the number of **Backup archive panel** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the box	Defines the name of the **Backup archive panel** object.	Latin, Cyrillic and service characters	Backup archive panel	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the status of the **Backup archive panel** object.	Boolean type	Not available	Yes – the **Backup archive panel** is disabled and is not in use No – the Backup archive panel is enabled and is in use.
4	Display	Is selected from the list	Defines the parent **Display** object of the digital distributed system, to which the given **Backup archive panel** object refers.	Names of the **Display** objects registered in the system.	Name of the parent **Display**.	Depends on the number of **Display** objects in the digital distributed video surveillance system
5	Backup archive*	Is selected from the list	Defines an Backup archive, which the Operator will control with the **Backup archive panel** interface object.	Name of the **Backup archive** objects registered in the system.	-	Depends on the number of **Backup archive** objects in the digital distributed video surveillance system.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
6	Fixed position	Is set with a check mark	Defines, if the user can drag the **Backup archive panel** over the screen with the mouse.	Boolean type	Not available	Yes – the **Backup archive panel** may not be dragged. No – the **Backup archive panel** may be dragged.
7	X	Enter the value in the box (Automatically, if the **Fixed position** option is checked).	Defines a coordinate in the X 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 video monitors installed.
8	Y	Enter the value in the box (Automatically, if the **Fixed position** option is checked).	Defines a coordinate in the Y 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 video monitors installed.
9	W	Enter the value in the box (Automatically, if the **Fixed position** option is checked).	Defines the width of the **Backup archive panel**.	% of the screen width.	Not defined	From 0 to M*100, where M is the number of video monitors installed.
10	H	Enter the value in the box (Automatically, if the **Fixed position** option is checked).	Defines the height of the **Backup archive panel**.	% of the screen width.	Not defined	From 0 to M*100, where M is the number of video monitors installed.

- The name of the element is not displayed in the settings panel of the given object.

13.1.2.9.7 The Settings panel of the Map object

The **Map** object is designed to register and configure the **Map** interface object in the *Intellect* system, which allows creating and mapping the symbols of the installed devices in the controlled territory and to use the symbols to operate the devices. The settings panel of the **Map** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Map** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	ID*	Automatically	Displays the ID of the **Map** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Map** objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Displays the name of the **Map** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Map	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	**Disable**	Set the checkbox checked	Sets the status of the **Map** object in the digital distributed video surveillance system.	Boolean type	No	**Yes** – the **Map** object is disabled and is not in use **No** – the **Map** object is enabled and is in use.
4	**Display**	Select in the list	Sets the parent **Display** object of the digital distributed system to which the given **Map** object refers.	Names of the **Display** objects registered in the system.	Name of the parent **Display** object.	Depends on the number of **Display** objects in the digital distributed video surveillance system

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
5	**Search alarmed links recursively**	Set the checkbox checked	Defines, if recursive search for the objects in the layers is possible. The recursive search means a search, where the transfer from one layer, containing an object, to another layer, containing a symbol, follows a gradual pattern of moving to the neighboring layers, using consecutive links.	Boolean type	No	**Yes** – a recursive search is enabled. **No** – a recursive search is disabled.
6	**Search for the shortest path**	Set the checkbox checked	Enables the search for the shortest path to the alarmed layer. If there are several paths from the active to the alarm layer, then the shortest path is defined automatically when the **Alarm** signal incomes (only one the **Link to layer** icon with the shortest path will blink in the active layer). Can be enabled only along with the **Search alarmed links recursively** option.	Boolean type	No	**Yes** – search for the shortest path is enabled **No** – search for the shortest path is disabled
7	**Over all windows when alarm**	Set the checkbox checked	Sets, if the window of the **Map** interface object can be displayed over all active applications in case of the **Alarm** signal incomes from any object of the **Map** interface object.	Boolean type	No	**Yes** - the window of the **Map** interface object will be displayed over all active applications in case of the **Alarm** signal incomes from any object of the **Map** interface object. **No** - the window of the **Map** interface object will not be displayed over all active applications in case of the **Alarm** signal incomes from any object of the **Map** interface object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
8	**Show video**	Set the checkbox checked	Enables the function of live and archive video request from map for cameras and objects linked with cameras.	Boolean type	No	**Yes** – the commands to request live and archive video are available in the menu of **Camera** objects and objects linked with cameras. **No** – the commands to request live and archive video are not available in the menu of **Camera** objects and objects linked with cameras.
9	**Show frame**	Set the checkbox checked	Enables the function of frame request from map for cameras and objects linked with cameras.	Boolean type	No	**Yes** – the command to request frame are available in the menu of **Camera** objects and objects linked with cameras. **No** – the command to request frame is not available in the menu of **Camera** objects and objects linked with cameras.
The **Settings** group						
10	**X**	Enter the value in the box	Sets a coordinate in the X horizontal axis for the upper left corner of the window of the **Map** interface object on the screen.	% of the screen width	Not set	From 0 to M*100, where M is the number of video monitors installed.
11	**Y**	Enter the value in the box	Sets a coordinate in the Y vertical axis for the upper left corner of the window of the **Map** interface object on the screen.	% of the screen height	Not set	From 0 to M*100, where M is the number of video monitors installed.
12	**W**	Enter the value in the box	Sets the width of the window of the **Map** interface object.	% of the screen width	Not set	From 0 to M*100, where M is the number of video monitors installed.
13	**H**	Enter the value in the box	Sets the height of the window of the **Map** interface object.	% of the screen width	Not set	From 0 to M*100, where M is the number of video monitors installed.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
14	**Autoswitch**	Set the checkbox checked	Activates autoswitch to the **Alarm** source layer in the **Map** interface object.	Boolean type	No	**Yes** – in case of an alarm from an object, the system will switch to the source layer where the object is located. **No** – in case of an alarm from an object, the system will not switch to the source layer where the object is located.
15	**Monitor**	Select in the list	The number of monitor in OS for which coordinates are specified	Numbers of monitors	1	1-9
16	**Create map copy**	Click the button	Creates another **Map** object with all parameters identical to the given object	-	-	-
17	**Object tracking monitor**	Select in the list	Select the object tracking monitor. Find details in the Using absolute telemetry section of Installing and configuring security system components guide.	Names of available **Monitor** objects	-	Depends on the number of **Monitor** objects created in the system
18	**Upload from DB**	Set the checkbox	Enables uploading events from database to show on the Map	Boolean type	No	**Yes** – the events are uploaded from database on *Intellect* startup, so the events before and after the *Intellect* start can be seen on the Map. **No** – only events emerged after the *Intellect* start are displayed on the Map.
19	**Show last ____ events in info window**	Enter the value in the box	Sets the number of events of the selected object to be shown in the info window on the Map.	Sequence of numbers	10	>=0
Help windows for events table						
20	**Type**	Select in the list	When the event comes in from the object type specified in this parameter, the tooltip with the name of the event is displayed.	Types of objects created in the system	-	Depends on the number of objects created in the system

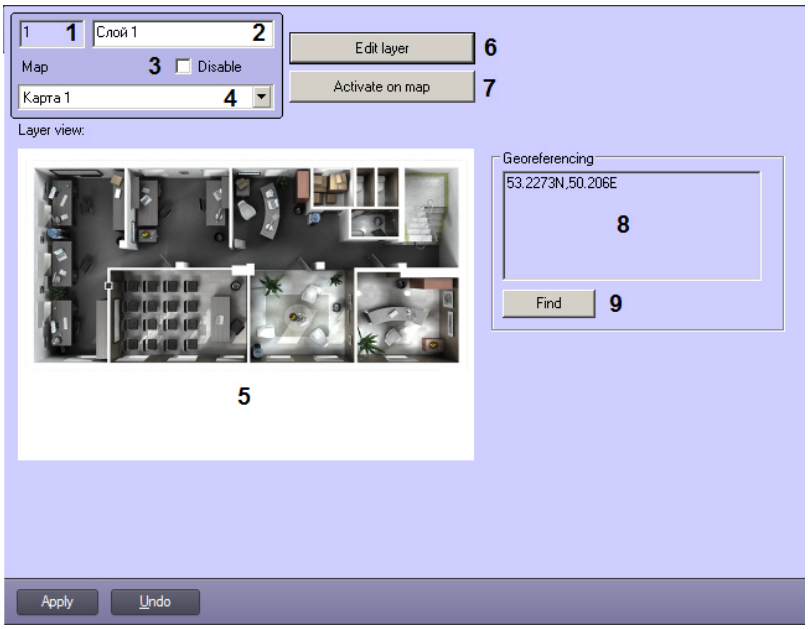
№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
21	**id**	Select in the list	When the event comes in from the object identifier specified in this parameter, the tooltip with the name of the event is displayed.	Identifiers of objects of the selected type created in the system	-	Depends on the number of objects created in the system
22	**Name**	Automatically	When the event comes in from the object name specified in this parameter, the tooltip with the name of the event is displayed.	Names of the objects of the selected type created in the system	-	Depends on the number of objects created in the system
23	**Event**	Select in the list	When the event with the name specified in this parameter comes in, the tooltip is displayed.	Events of the objects of the selected type	-	Depends on the object type
24	**Delay**	Enter the value in the box	Sets the time period in seconds for the tooltip to be displayed.	Integer value	-	>=0
25	**Smoothing method**	Select in the list	Sets the map smoothing method when scaling.	Smoothing method names	-	low quality high quality bilinear interpolation bicubic interpolation nearest neighbor method high quality bilinear interpolation high quality bicubic interpolation

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.9.8 The Settings panel of the Layer object

The **Layer** object is designed to create and configure the Map layers with the controlled objects in the Intellect system.

The settings panel of the **Layer** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Layer** object.

№	Parameter	Method for enter the parameter	Parameter description	Symbols used	Default value	Value range
1	**Identification number***	Automatically	Displays the identification number of the **Layer** object in the digital distributed video surveillance system.	Sequence of numbers	-	From 1 and above. Depends on the number of **Layer** objects in the digital distributed video surveillance system
2	**Name***	Enter the value in the box	Displays the name of the **Layer** object in the digital distributed video surveillance system.	Latin, Cyrillic and service characters	Layer	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60.
3	**Disable**	Is identified by the check mark	Shows the status (enabled or disabled) of the **Layer** object in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Layer** object is disabled and is not in use **No** – the **Layer** object is enabled and is in use.
4	**Map**	Is selected from the list	Defines the parent Map object of the digital distributed system, to which the given **Layer** object refers.	Name of the **Map** objects registered in the system.	Name of the parent **Map** object	Depends on the number of **Map** objects in the digital distributed video surveillance system
5	**Layer view**	-	Shows the layout of the controlled territory.	-	-	-

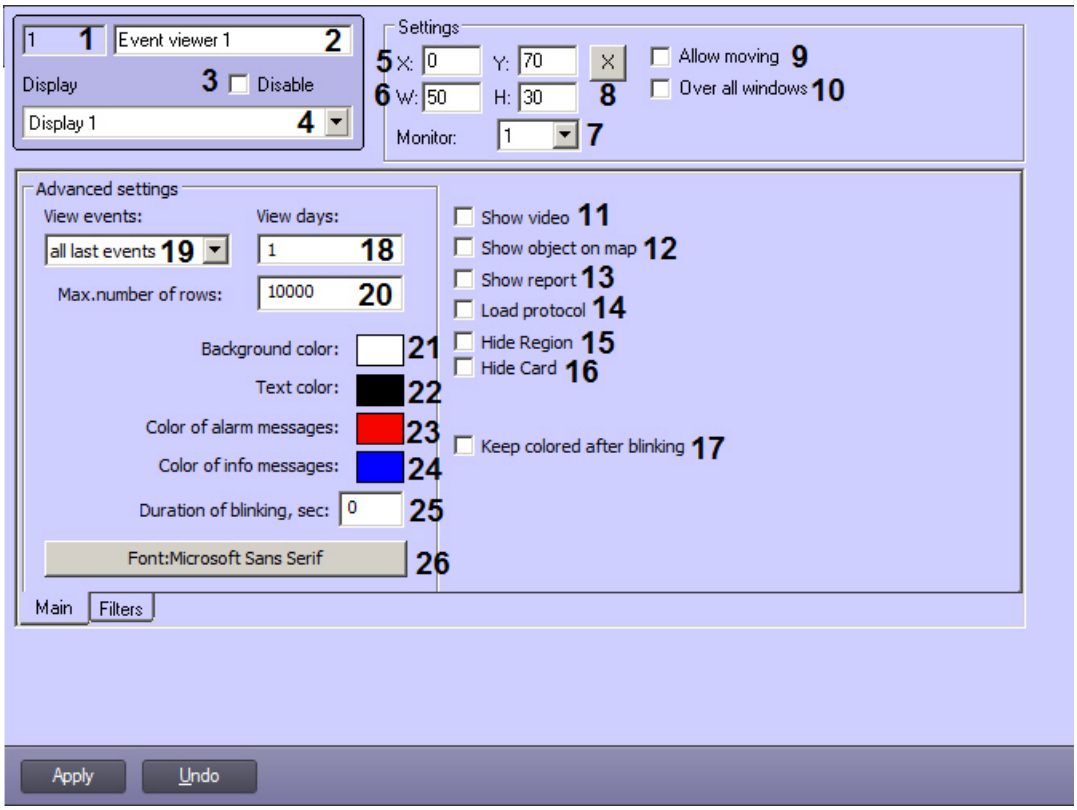
№	Parameter	Method for enter the parameter	Parameter description	Symbols used	Default value	Value range
6	**Edit layer**	Press the button	Displays the panel, which allows to add/remove and configure the symbols of the devices installed in the controlled territory, using the territory layout.	-	-	-
7	**Activate on map**	Press the button	Brings forward to the given layer over all other layers in the **Map** interface object.	-	-	-
8	**Georeferencing**	Via the *Map editor* utility	Shows the coordinates set with 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**	Press the button	Displays a Google map at the coordinates specified in the **Georeferencing** field.	-	-	-

*The name of the element is not displayed in the settings panel of the given object.

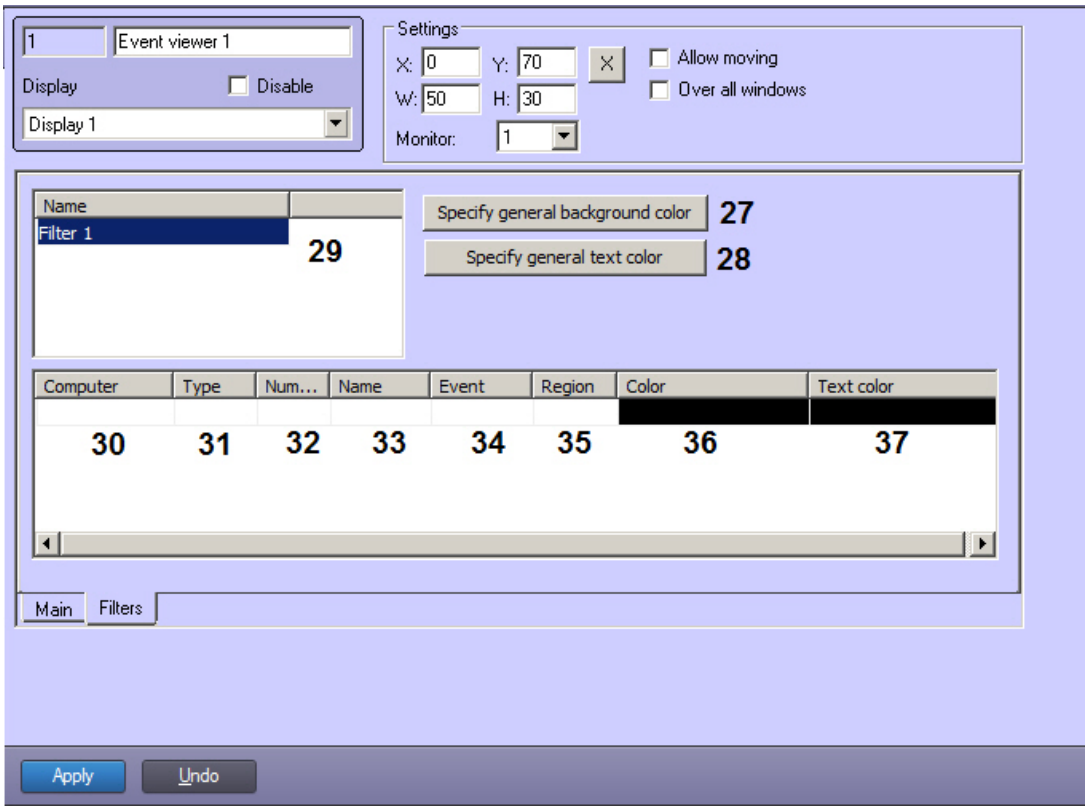
13.1.2.9.9 The Settings panel of the Event viewer object

The **Event viewer** object represents an interface box showing text information about the events initiated by the distributed surveillance system.

The settings panel of the **Event viewer** object is shown in the figures.



The **Main** tab



The **Filters** tab

The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Event viewer** object.

№	Parameter	Method for setting the parameter	Parameter description	Symbol
1	Identification number*	Automatically	Displays the identification number of the **Event viewer** object in the digital distributed video surveillance system.	Sequen
2	Name*	Type-in the value in the field	Sets the name of the **Event viewer** object in the digital distributed video surveillance system.	Latin, C charact
3	**Disable**	Checkbox	Sets the status of the **Event viewer** object (enabled or disabled) in the digital distributed video surveillance system.	Boolean
4	**Screen**	Select in the list	Specifies the parent **Display** object of the digital distributed video surveillance system, to which the given **Event viewer** object refers.	Names register
The **Settings** group				
5	**X**	Type-in the value in the field	Sets the coordinate in the X horizontal axis for the upper left corner of the window of the **Event viewer** interface object on the screen.	% of the
	Y	Type-in the value in the field	Sets the coordinate in the Y vertical axis for the upper left corner of the window of the **Event viewer** interface object on the screen.	% of the
6	**W**	Type-in the value in the field	Sets the window width of the **Event viewer** interface object.	% of the
	H	Type-in the value in the field	Sets the window height of the **Event viewer** interface object.	% of the
7	**Monitor**	Is selected in the list	The number of monitor in OS for which coordinates are specifying	Numbe
8	**X**	Click the button	Open the window to set Event viewer window size and position using mouse	-
9	**Allow moving**	Checkbox	Allows the operator changing the position of the **Event Viewer** by clicking on it.	Boolean
10	**Over all windows**	Checkbox	Allows to display the Event viewer box on top of all windows	Boolean
11	**Show video**	Checkbox	Allows Operator viewing archive footage of the events, initiated by the Event Viewer as Record to disk using the **Event viewer** box.	Boolean
12	**Show object on map**	Checkbox	Allows Operator viewing objects, displayed in the **Event viewer** window, on the map.	Boolean

№	Parameter	Method for setting the parameter	Parameter description	Symbol
13	**Show report**	Checkbox	Allows Operator creating a printed form of the report and printing out the information about all events registered by the **Event viewer** within the pre-set period of time.	Boolean
14	**Load protocol**	Checkbox	Defines, whether or not the latest 1000 events registered by the **Event viewer** with the latest system start, should be downloaded with the launch of Intellect™ software.	Boolean
15	**Hide Region**	Set the checkbox	Hides the **Region** column in the **Event viewer**.	Boolean
16	**Hide Card**	Set the checkbox	Hides the **Card** column in the **Event viewer**. See Card number displaying in the Event viewer window for access events section in Access Manager Module Settings and Operation Guide.	Boolean
17	**Keep colored after blinking**	Checkbox	Allows highlighting the alarm messages by the selected color after the blinking stops.	Boolean
The **Advanced settings** group				
18	**View days**	Type-in the value in the field	Specifies the period over which events are to be displayed in the Event Viewer, if there are more than 10,000 events (or other value set by **Max.number of rows**). If there are less events, then all events are displayed regardless of the value of this parameter.	Days
19	**View events**	Select in the list	Sets the events for displaying in the window of the Event Viewer.	-
20	**Max.number of rows**	Type-in the value in the field	Sets the maximum number of events to display in the Event viewer	Non-ne
21	**Background color**	Select in the list or on the **Select color** panel.	Sets the background color in the Event Viewer box	RGB, CM
22	**Text color**	Select in the list or on the **Select color** panel.	Sets the text color in the Event Viewer box	RGB, CM
23	**Color of alarm messages**	Select in the list or on the **Select color** panel.	Sets the color of the alarm message rows in the **Event viewer** window. **Duration of blinking, sec** is to be other than 0.	RGB, CM
24	**Color of info messages**	Select in the list or on the **Select color** panel.	Sets the color of the information message rows in the **Event viewer** window. **Duration of blinking, sec** is to be other than 0.	RGB, CM
25	**Duration of blinking, sec**	Type-in the value in the field	Sets the duration of alarm message blinking in the **Event viewer** window.	seconds
26	**Font:**<current font>	Click the button	Sets the font of information messages in the **Event viewer** window	Standar box
The **Filters** tab				
27	**Specify general background color**	Click the button	Opens the window to select the message background color in the default filter	-

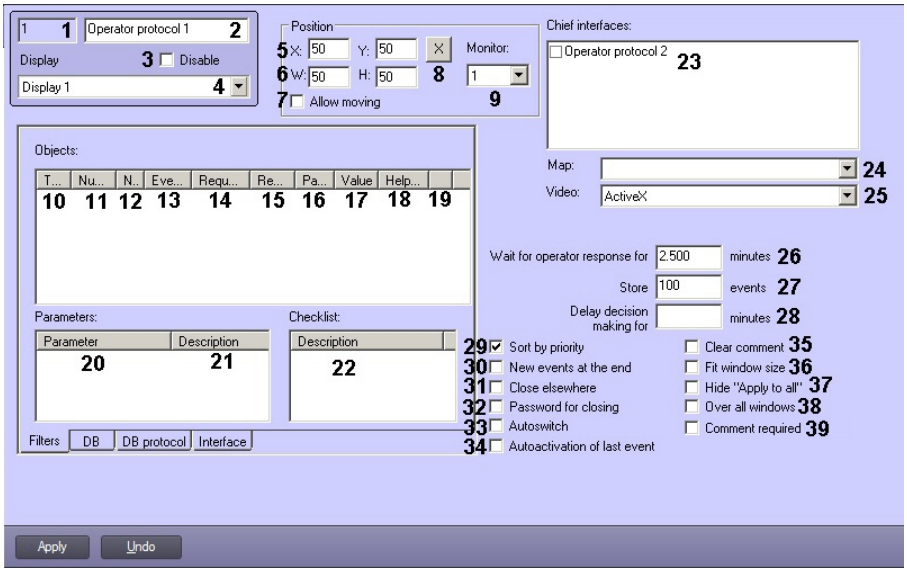
№	Parameter	Method for setting the parameter	Parameter description	Symbol
28	**Specify general text color**	Click the button	Opens the window to select the message text color in the default filter	-
29	**Name**	Specify the value in the field	Sets the filter name in the Event Viewer	Latin ar service
30	**Computer**	Select in the list	Sets the **Computer** object under which objects included in the filter are to be created.	Names register
31	**Type**	Select in the list	Sets the types of objects to be displayed in the **Event viewer**. ***NOTE.*** *If the field is empty, the Event viewer displays all events for all objects in the system.*	Types o the syst
32	**Number**	Select in the list	Sets the identification number of the device. ***NOTE.*** *If the field is empty, the Event viewer displays all events for all objects of the selected type.*	Sequen
33	**Name**	Automatically	Shows the name of the device selected in item 14.	Name o selected system
34	**Event**	Select in the list	Specifies which event coming from selected devices is to be logged. ***NOTE.*** *If the field is empty, the Event viewer displays all events coming from specified devices.*	Names selected
35	**Region**	Select in the list	Sets the region where the objects to log the events from are located.	Name o by the s
36	**Color**	Select in the list	Sets the messages highlight color in the Event Viewer	RGB, CM
37	**Text color**	Select in the list	Sets the messages text highlight color in the Event Viewer	RGB, CM

*The name of the element is not displayed in the settings panel of the given object.

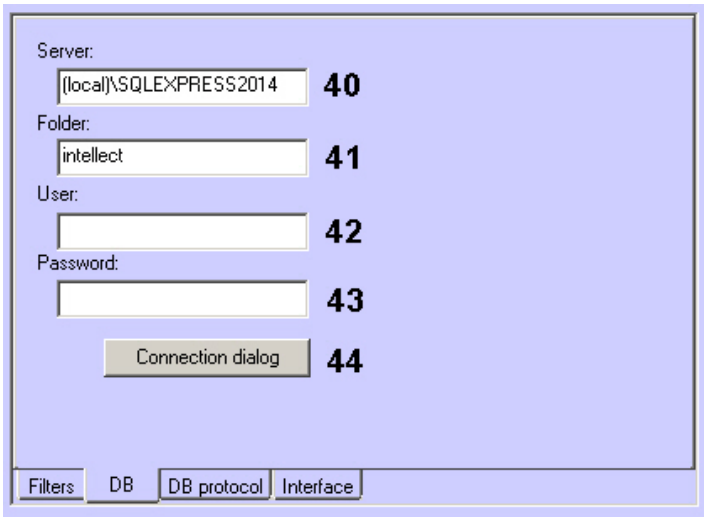
13.1.2.9.10 The Settings panel of the Operator protocol object

The settings panel of the **Operator protocol** object is shown in the figures.

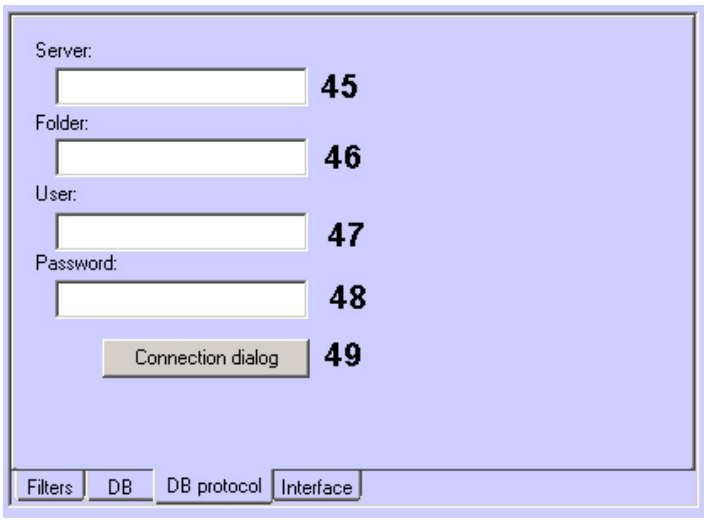
The **Filters** tab



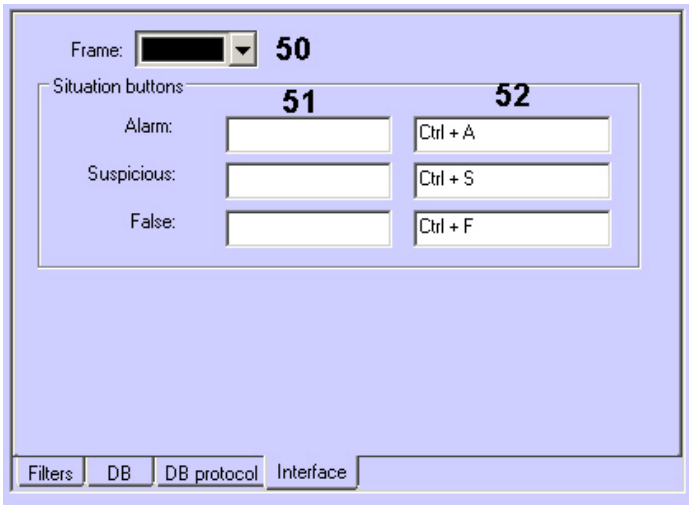
The **DB** tab



The **DB protocol** tab



The **Interface** tab



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Operator protocol**.

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
The **Filters** tab						
1	The **Identification number** field *	Automatically	Shows the identification number of the **Operator protocol** object in the system	Sequence of numbers	-	Depends on the number of **Operator protocol** objects in the system
2	The **Name** field *	Type-in the value in the field	Assigns the name to the **Operator protocol** object.	Latin, Cyrillic and service characters	Operator protocol	A line containing a sequence of any symbols (letters, digits, service, characters apart from > and < symbols), non case-sensitive Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Chechbox is set	Shows the status (enabled or disabled) of the **Operator protocol** object in the system	Boolean type	No	**Yes** – the **Operator protocol** object is disabled and is not in use. **No** – the **Operator protocol** object is enabled and is in use.
4	The **Display** dropdown list	Is selected in the list	Assigns the parent **Display** object , to which the given Operator protocol object refers.	Name of the **Display** objects registered in the system.	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system.
5	The **X** filed	Type-in the value in the field	Sets the coordinate in the X horizontal axis for the upper left corner of the **Operator protocol** interface object on the screen	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed.
	The **Y** field	Type-in the value in the field	Sets the coordinate in the Y vertical axis for the upper left corner of the **Operator protocol** interface object on the screen	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed.
6	The **W** filed	Type-in the value in the field	Sets the window width of the **Operator protocol** interface object	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed.
	The **H** field	Type-in the value in the field	Sets the window height of the **Operator protocol** interface object	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed.
7	The **Allow moving** checkbox	Chechbox is set	Allows hand shifting of the **Operator protocol** interface box	Boolean type	No	**Yes** – hand shifting is allowed. **No** – hand shifting is prohibited.
8	The **X** button	Click the button	Opens a template box to set size and position of the **Operator protocol** interface window	-	-	-
9	The **Monitor** dropdown list	Select in the list	Sets the system ID of the monitor for which the coordinates are set	IDs of the monitors in the OS	1	From 1 to 16

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
10	The **Type** dropdrown list	Select in the list	Sets the type of objects which are to be displayed in the **Operator protocol** interface box	Available object types	-	Depends on the registered objects in the system. Only 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 section).
11	The **Number** dropdrown list	Select in the list	Sets the number of object on which the events are to be displayed in the **Operator protocol** interface box	Sequence of numbers	-	Depends on the number of registered objects of the specified type
12	The **Name** dropdrown list	Automatically	Sets the name of object on which the events are to be displayed in the **Operator protocol** interface box	Names of objects registered in the system	-	Depends on the objects registered in the system
13	The **Event type** dropdrown list	Select in the list	Sets events displayed in the **Operator protocol** interface box	Available events for the selected object	-	Depends on the object type
14	The **Request password** dropdrown list	Select in the list	Defines the necessity of password to process the event	Boolean type	-	**Yes** – confirmation of the password is required to process the event; **No** – confirmation of the password is not required to process the event.
15	The **Region** dropdrown list	Select in the list	Specifies the **Region** object corresponding to the monitored object	List of created **Region** objects	-	Depends on the number of created **Region** objects
16	The **Parameter** field	Type-in the value in the field	Sets the parameter of the monitored object.	Depends on the event type	-	Depends on the event type.
17	The **Value** field	Type-in the value in the field	Sets the parameter value of the monitored object.	Depends on the event type	-	Depends on the event type
18	The **Help file** field	Type-in the value in the field	Sets the full path to the text file in pdf, doc, docx, txt or other format which contains the helping guide about the event processing.	File address in the file system.	-	Depends on the file system limitations.
19	The **Priority** drop-down list	Select in the list	Sets the event priority for sorting by importance	Non-negative integer	-	1 – 10 The higher the value, the higher the priority
The **Parameters** table						
20	The **Parameter** field	Type-in the value in the field	Sets the name of parameter, the value of which is to be displayed in the Operator protocol interface object	Latin, Cyrillic and service characters	-	Depends on parameters sent with event

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
21	The **Description** field	Type-in the value in the field	Type-in the short description of the specified parameter	Latin, Cyrillic and service characters	-	0-255 characters
The **Checklist** table						
22	The **Description** field	Type-in the value in the field	Sets the description of the action that the operator must perform before assigning the status to an event.	Latin, Cyrillic and service characters	-	0-255 characters
Outside the groups						
23	The **Chief interfaces** dropdown list	Checkbox is set	Sets the **Operator protocol** object to which the events are to be sent after the time specified in the **Wait for operator response for** field	List of available Operator protocol objects	-	Depends on the number of created **Operator protocol** objects in the system.
24	The **Map** dropdown list	Select in the list	Sets the **Map** interface object to display the monitored object	List of available **Map** objects in the system	-	Depends on the number of the **Map** objects created in the system
25	The **Video** dro pdown list	Select in the list	Sets the method of the archive and live video displaying from the operator's protocol.	List of available displaying methods	ActiveX	**ActiveX** - archive and live video will open in a separate window. **Monitor** - archive and live video will open on the selected Video Surveillance Monitor.
26	The **Wait for operator response for** field	Type-in the value in the field	Sets the time after which the event type becomes **Not-processed event** or the event is escalated	Min	2.5	0-600 Fractional values can be specified; integer and fractional parts are point-separated. For instance, to set 2 minutes 30 seconds time period specify 2.5.
27	The **Store events** field	Type-in the value in the field	Specifies the maximum events that can be displayed simultaneously in the list of current events	Sequence of numbers	100	Integer that is more than 0
28	The **Delay decision making for** field	Type-in the value in 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. It is possible to specify fractional values, the separator of the integer and fractional part is a point. For example, to set a period of 2 minutes and 30 seconds 2.5 should be specified.

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
29	The **Sort by priority** checkbox	Checkbox is set	Enables sorting by priority. 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).	Boolean type	Yes	**Yes** – sorting by priority is enabled. **No** – sorting by time events are received is enabled.
30	The **New events at the end** checkbox	Checkbox is set	Places new events at the end of the current events list	Boolean type	No	**Yes** – a new event is placed to the end of the list **No** – a new event is added to the beginning of the list
31	The **Close elsewhere** checkbox	Checkbox is set	Decides whether to delete the event from other Operator protocols when it is processed in one of the Operator protocol	Boolean type	No	**Yes** – when the event is processed in one of the Operator protocol, it is deleted from other Operator protocols **No** – when the event is processed in one of the Operator protocol, it stays unprocessed in other Operator protocols
32	The **Password for closing** checkbox	Checkbox is set	Defines the necessity to enter the password to process the event	Boolean type	No	**Yes** – event processing is to be confirmed with a password; **No** – password is not required for event processing.
33	The **Autoswitch** chechbox	Checkbox is set	Enables auto switch to the **Current events** tab in the **Operator protocol** window when a new event occurs.	Boolean type	No	**Yes** – auto switch is enabled **No** – auto switch is disabled
34	The **Autoactivation of last event** checkbox	Checkbox is set	Enables the automatic activation of the last received event tile.	Boolean type	No	**Yes** – the last received event tile is automatically activated; **No** – when the new event is received, the tile selected by the Operator remains active.
35	The **Clear comment** checkbox	Checkbox is set	Enables the comment field clearing after the event is procesed by the Operator	Boolean type	No	**Yes** – the comment field is automatically cleared after the event is procesed by the Operator; **No** – the comment text remains in the comment field after the event is procesed by the Operator.
36	The **Fit window size** checkbox	Checkbox is set	Enables the automatic enlarging the alarm tile to fit the entire Operator protocol window size	Boolean type	No	**Yes** - the alarm tile size is set equal to the size of the Operator Protocol window area which is not occupied by the event control panel; **No** - the tile size is set according to the content size.
37	The **Hide "Apply to all"** checkbox	Checkbox is set	Disables the **Apply to all** button	Boolean type	No	**Yes** - the **Apply to all** button is hidden in the Operator Protocol window, and the Operator is not able to process all alarms at once; **No** - the **Apply to all** button is available in the Operator Protocol window.

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
38	The **Over all windows** checkbox	Checkbox is set	Enables the Operator protocol to be displayed always on top.	Boolean type	No	**Yes** – the Operator protocol window is always displayed above all other windows. **No** – the Operator protocol window is displayed normally.
39	The **Comment required** checkbox	Checkbox is set	Prevents event processing without comment	Boolean type	No	**Yes** – the buttons for classifying events (**Alarm situation**, **Suspicious situation**, **False alarm**) do not appear until the **Comment** field is filled. **No** – the operator can classify (process) the event without entering a comment.
The **DB** tab						
40	The **Server** field	Type-in the value in the field	Sets the name of DB server in which the required database is stored	Latin, Cyrillic and service characters	Name of Server used by system	-
41	The **Folder** field	Type-in the value in the field	Sets the name of the database in which the events are to be stored	Latin, Cyrillic and service characters	Name of main database used by system	-
42	The **User** field	Type-in the value in the field	Sets the user name for authorization in the database server	Latin, Cyrillic and service characters	-	-
43	The **Password** field	Type-in the value in the field	Sets the password for authorization in the database server	Latin, Cyrillic and service characters	-	-
44	The **Connection dialog** button	Click the button	Opens the dialog box of database server connection	-	-	-
The **DB protocol** tab						
45	The **Server** field	Type-in the value in the field	Sets the name of DB server in which the required Event Protocol database is stored (if extracted to a separate DB)	Latin, Cyrillic and service characters	Name of Server used by Event Protocol database (if extracted to a separate DB)	-

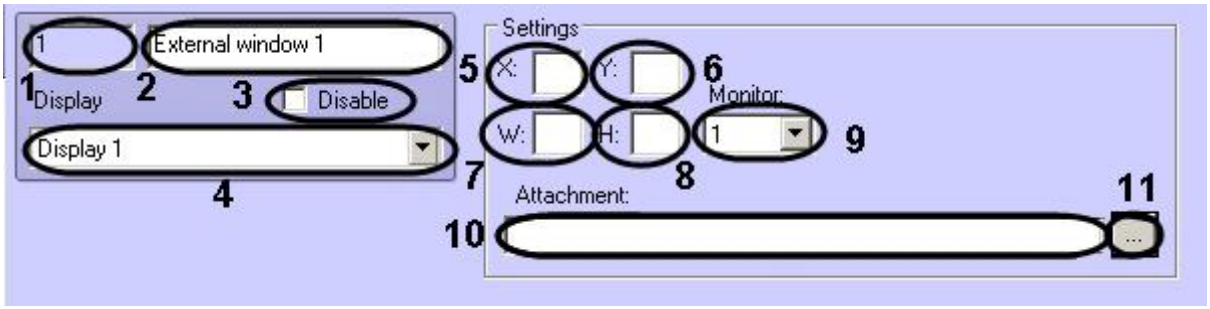
№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
46	The **Folder** field	Type-in the value in the field	Sets the name of the Event Protocol database (if extracted to a separate DB) in which the events are to be stored	Latin, Cyrillic and service characters	Name of Event Protocol database (if extracted to a separate DB) used by system	-
47	The **User** field	Type-in the value in the field	Sets the user name for authorization in the Event Protocol database (if extracted to a separate DB) server	Latin, Cyrillic and service characters	-	-
48	The **Password** field	Type-in the value in the field	Sets the password for authorization in the Event Protocol database (if extracted to a separate DB) server	Latin, Cyrillic and service characters	-	-
49	The **Connection dialog** button	Click the button	Opens the dialog box of Event Protocol database (if extracted to a separate DB) server connection	-	-	-
The **Interface** tab						
50	The **Frame** dropdown list	Select in the list	Sets the frame color of the active event tile	Color palette	Black	RGB color
51	The **Name** text field *	Type-in the value in the field	Sets the custom names for the alarm processing buttons	Latin, Cyrillic and service characters	No	0-255 characters
52	The **Keyboard shortcut** text field *	Press the key combination	Sets the hot keys for the alarm events processing	Keyboard combinations	No	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.

* The field names marked with the asterisk * are not displayed on the settings panel.

13.1.2.9.11 The Settings panel of the External window object

The **External window** object displays in the dialog box showing various applications in the pre-defined screen area. Applications in this context shall mean both applications of AxxonSoft and other manufacturers.

The settings panel of the **External window** object is shown in the figure.



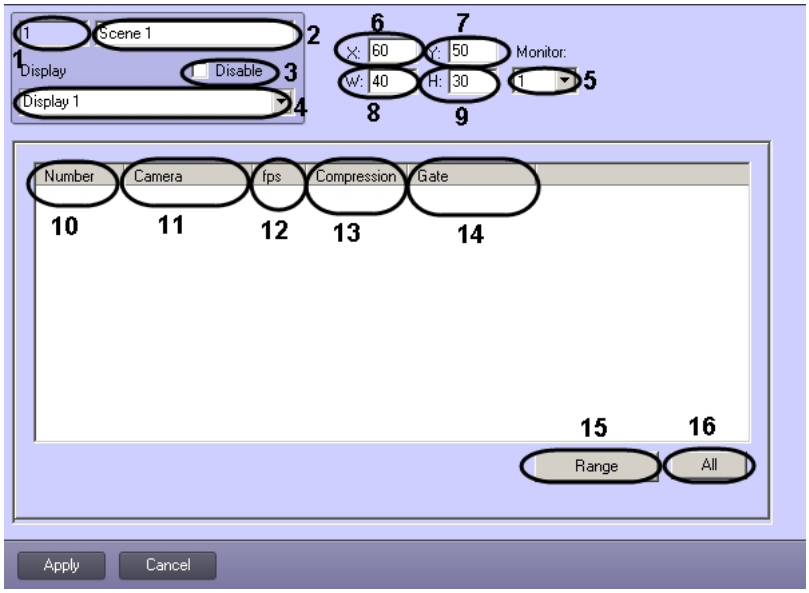
The table describes the parameters of the settings corresponding to the elements of the settings panel of the **External window** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **External window** object.	Sequence of numbers	-	From 1 and above. Depends on the number of **External window** objects.
2	Name*	Enter the value in the field	Defines the name of the **External window** object.	Latin, Cyrillic and service characters	External window	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the status of the **External window** object (enabled or disabled).	Boolean type	Not available	**Yes** – the **External window** object is disabled and is not in use. **No** – the **External window** object is enabled and is in use.
4	Screen	Is selected from the list	Defines the parent **Display** object, to which the given **External window** object refers.	Names of the **Display** objects register-ed in the system	Name of the parent **Display** object.	Depends on the number of **Display** objects available.
Settings Group						
5	X	Enter the value in the field.	Defines the coordinate in the X 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 monitors installed.
6	Y	Enter the value in the field.	Defines the coordinate in the Y 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 monitors installed.
7	W	Enter the value in the field.	Defines the window width of the **External window** interface object.	% of the screen width	Not defined	From 0 to M*100, where M is the number of monitors installed.
8	H	Enter the value in the field.	Defines the window height of the **External window** interface object.	% of the screen width	Not defined	From 0 to M*100, where M is the number of monitors installed.
9	Monitor	Select value from the list	Specifies the number of monitor which is in use for displaying window of external application	Number of Monitors	1	1-9
10	Application	Enter the value in the field	Defines the path to the application, which should be launched. ***Note.*** *All windows of application will be opened simultaneously if the application contains several windows.*	Latin, Cyrillic and service characters	Is not defined	A line containing a sequence of symbols (Latin and service characters, digits) not case-sensitive. Number of symbols – from 1 to 250.
11	Button «…»	Click the button	Displays standard dialog of open the file of Windows OS to specify path to application which is required to run.	-	-	-

*Name of the element is not shown in the given object settings panel.

13.1.2.9.12 The Settings panel of the Scene object

The settings panel of the **Scene** object is shown in the figure.

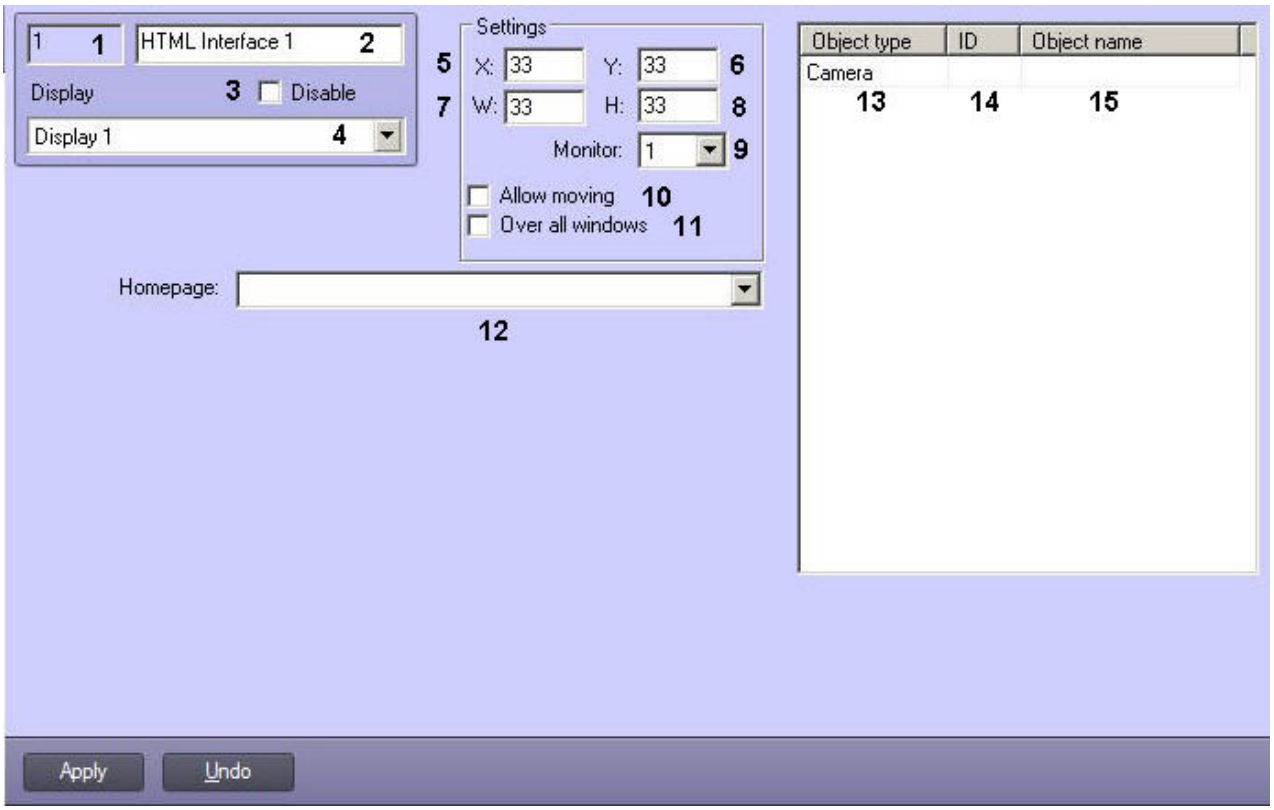


Elements of the settings panel of the **Scene** object are described in the table.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Scene** object.	Sequence of numbers	-	From 1 and above. Depends on the number of **Scene** object.
2	Name*	Enter the value in the field	Defines the name of the **Scene** object.	Latin, Cyrillic and service characters	Scene	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the status of the **Scene** object (enabled or disabled).	Boolean type	Not available	**Yes** – the **Scene** object is disabled and is not in use. **No** – the **Scene** object is enabled and is in use.
4	Screen	Is selected from the list	Defines the parent **Display** object, to which the given **Scene** object refers.	Names of the **Display** objects register-ed in the system	Name of the parent **Display** object.	Depends on the number of **Display** objects available.
5	Monitor	Is selected from the list	Is designed for video surveilance monitor selection on which the panoramic view window has to be displayed	Sequence of numbers	1	1..9
6	X	Enter the value in the field.	Defines the coordinate in the X horizontal axis for the upper left corner of the window of the **Scene** interface object on the screen.	% of the screen width.	Not defined	From 0 to 100
7	Y	Enter the value in the field.	Defines the coordinate in the Y vertical axis for the upper left corner of the window of the **Scene** interface object on the screen.	% of the screen height.	Not defined	From 0 to 100
8	W	Enter the value in the field.	Defines the window width of the **Scene** interface object.	% of the screen width.	Not defined	From 0 to 100
9	H	Enter the value in the field.	Defines the window height of the **Scene** interface object.	% of the screen width.	Not defined	From 0 to 100
10	Number	Is selected from the list	Set camera's number to be displayed	Latin, Cyrillic and service characters.	Is not defined	Depends on number of cameras registered in the system
11	Camera	Is selected from the list	Set camera's name to be displayed	Names of cameras registered in the system	-	Depends on number of cameras registered in the system
12	fps	Is selected from the list	Set fps to be transferred to the **Scene** object	Sequence of numbers	-	1, 2, 3, 4, 6, 8, 12, 16, 20, 25, 30
13	Compression	Is selected from the list	Set the video signal compression level to be transferred to the **Scene** object. With set value there is additional use of Server's resources	Sequence of numbers	-	In order of greater compression 0, 1, 2, 3, 4, 5 0 – no compression 5 – maximum compression
14	Gate	Is selected from the list	Set the **Gate** object from which the video archive and footage from the selected camera is to be received to the **Scene** object	Names of the **Gate** objects registered in the system	-	Depends on the number of **Gate** objects registered in the system

13.1.2.9.13 The settings panel of the HTML Interface object

The **HTML Interface** object is designed for displaying 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.



The table describes parameters of the settings corresponding to the elements of the settings panel of the **HTML Interface** object.

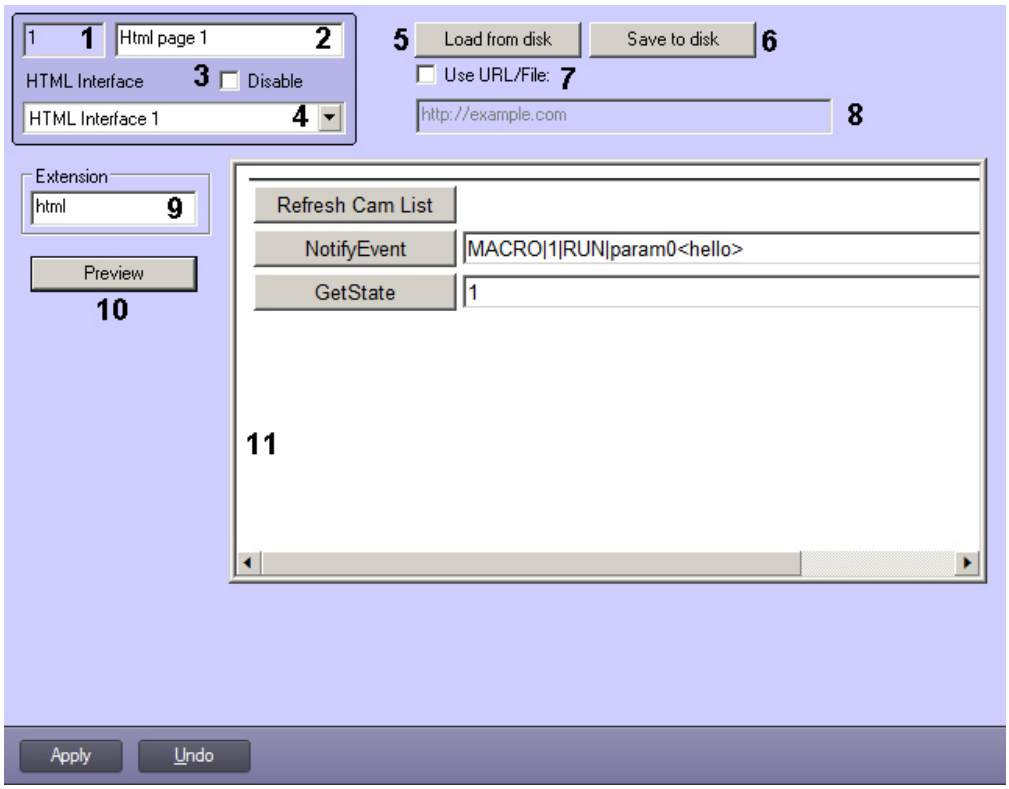
№	Parameter	Method for setting the parameter	Parameter description	Symbols used	Default value	Value range
1	The **Identification number** field	Automatically	Shows the identification number of the **HTML Interface** interface object in the system	Sequence of numbers	-	Depends on the number of **HTML Interface** objects in the system
2	The **Name** field	Enter the value in the field	Sets the name of the **HTML Interface** object in the system	Latin, Cyrillic letters and service characters	HTML interface	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60
3	The **Disable** checkbox	Is set with the checkbox	Sets the status (enabled or disabled) of the **HTML Interface** object in the system	Boolean type	No	**Yes** – the **HTML Interface** object is disabled and is not in use. **No** – the **HTML Interface** object is enabled and is in use

4	The **Display** drop-down list	Select in the list	Sets the parent **Display** object for the given **HTML Interface** object	Names of the **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system
Settings group						
5	The **X** field	Enter the value in the field	Sets the "X" coordinate in the horizontal axis for the upper-left corner of the **HTML Interface** window	% of the screen width	-	From 0 to M*100, where M is the number of the computer monitor installed
6	The **Y** field	Enter the value in the field	Sets the "Y" coordinate in the vertical axis for the upper-left corner of the **HTML Interface** window	% of the screen height	-	From 0 to M*100, where M is the number of the computer monitor installed
7	The **W** field	Enter the value in the field	Sets the width of the **HTML Interface** window	% of the screen width	-	From 0 to M*100, where M is the number of the computer monitor installed
8	The **H** field	Enter the value in the field	Sets the height of the **HTML Interface** window	% of the screen height	-	From 0 to M*100, where M is the number of the computer monitor installed
9	The **Monitor** drop-down list	Select in the list	Sets the monitor number for displaying interface object	Sequence of numbers	1	Depends on the number of installed computer monitor.
10	The **Allow moving** checkbox	Is set with the checkbox	Sets possibility to change position of the **HTML Interface** object using mouse	Boolean type	No	Yes – it is possible to change position of the **HTML Interface** object using mouse. No – it is not possible to change position of the **HTML Interface** object using mouse.
11	The **Over all windows** checkbox	Is set with the checkbox	Allows to display the **HTML Interface** window on top of all windows	Boolean type	No	**Yes** - The **HTML Interface** window is displayed on top of all windows. **No** - The **HTML Interface** window is displayed in standard mode.
12	The **Homepage** drop-down list	Select in the list	Sets start page for displaying in the **HTML Interface** window	Names of the **HTML page** objects registered in the system	-	Depends on the number of the **HTML page** objects in the system
13	**Object type** dropdown list	Select value from the list	Sets the type of object the state of which is to be tracked using HTML interface	Types of objects created in the system	-	Depends on the objects created in the system

14	**ID** dropdown list	Select value from the list	Sets the ID of object the state of which is to be tracked using HTML interface	Natural number series	-	Depends on the objects created in the system
15	**Object name** field	Automatically	Displays the name of the object the state of which is to be tracked using HTML interface	Name of object of selected type with specified ID	-	Depends on the objects created in the system

13.1.2.9.14 The settings panel of the HTML page object

The HTML page object is designed for configuring web-pages displayed in the HTML Interface window. The settings panel of the HTML page object is shown in the figure.



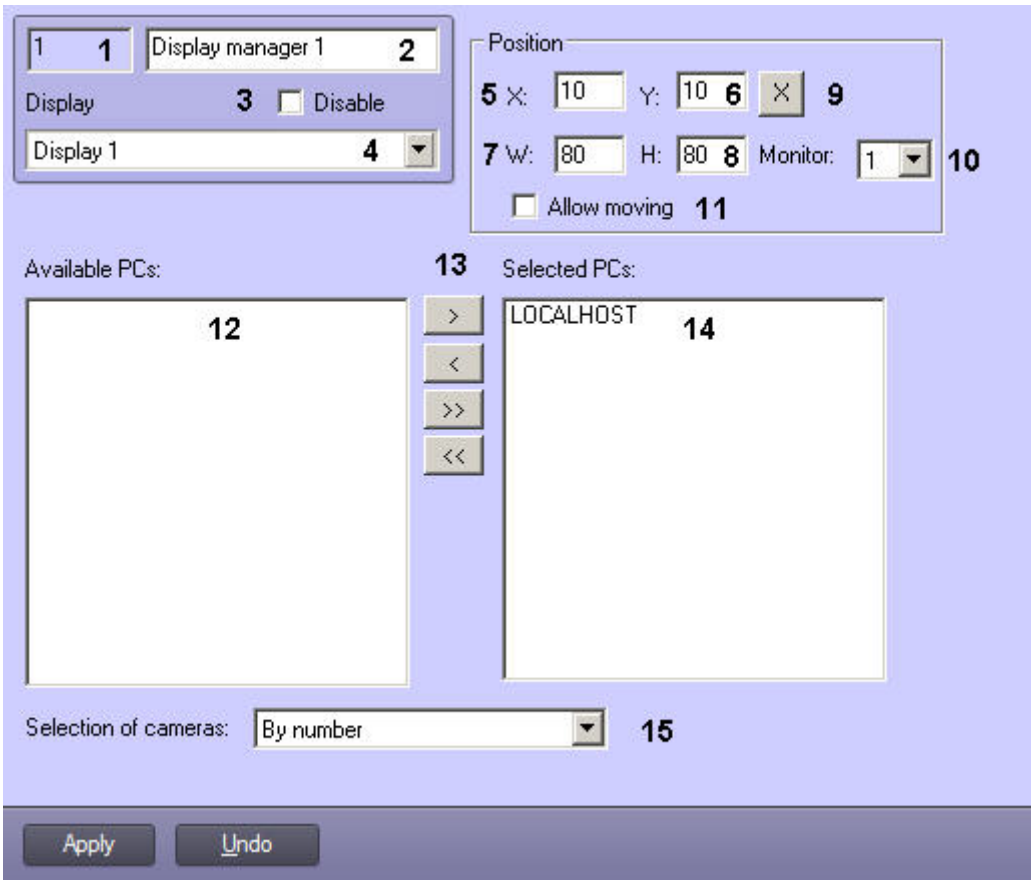
The table describes parameters of the settings corresponding to the elements of the settings panel of the **HTML page** object.

№	Parameter	Method for setting the parameter	Parameter description	Symbols used	Default value	Value range
1	The **Identification number** field	Automatically	Shows the identification number of the **HTML page** interface object in the system	Sequence of numbers	-	Depends on the number of **HTML page** objects in the system
2	The **Name** field	Enter the value in the field	Sets the name of the **HTML page** object in the system	Latin, Cyrillic letters and service characters	HTML page	A line representing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive Number of symbols – from 1 to 60

3	The **Disable** checkbox	Is set with the checkbox	Sets the status (enabled or disabled) of the **HTML page** object in the system	Boolean type	No	**Yes** – the **HTML page** object is disabled and is not in use. **No** – the **HTML page** object is enabled and is in use
4	The **HTML Interface** drop-down list	Select in the list	Sets the parent **HTML Interface** 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	The **Load from disk** button	Click the button	Opens standard dialog of file opening to load file of web-page or some other type from disk.	-	-	-
6	The **Save to disk** button	Click the button	Opens standard dialog of file opening to save file of web-page or some other type to disk.	-	-	-
7	The **Use URL/File** checkbox	Is set with the checkbox	Enables or disables loading of web-page or file of other type by URL	Boolean type	No	Yes – the specified URL is opened while addressing to the HTML page No – the saved file of the HTML page is opened while addressing to the HTML page (see Link to the HTML page object).
8	The **Use URL/File** field	Enter the value in the field	The field is designed for specifying link to web-page or file which will be opened at addressing to the configured HTML page	Link in URL format	-	Number of symbols is not limited
9	The **Extension** field	Is filled in automatically	Display extension of the opened file	Extension of files supported by the Internet Explorer browser	html	From 0 to 16 symbols
10	The **Preview** button	Click the button	Display the selected web page or file in the preview window.	-	-	-
11	Preview window	Is filled in automatically	Preview of web-page or file	-	Not displayed	-

13.1.2.9.15 The Settings panel of the Display manager object

The settings panel of the **Display manager** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Display manager**.

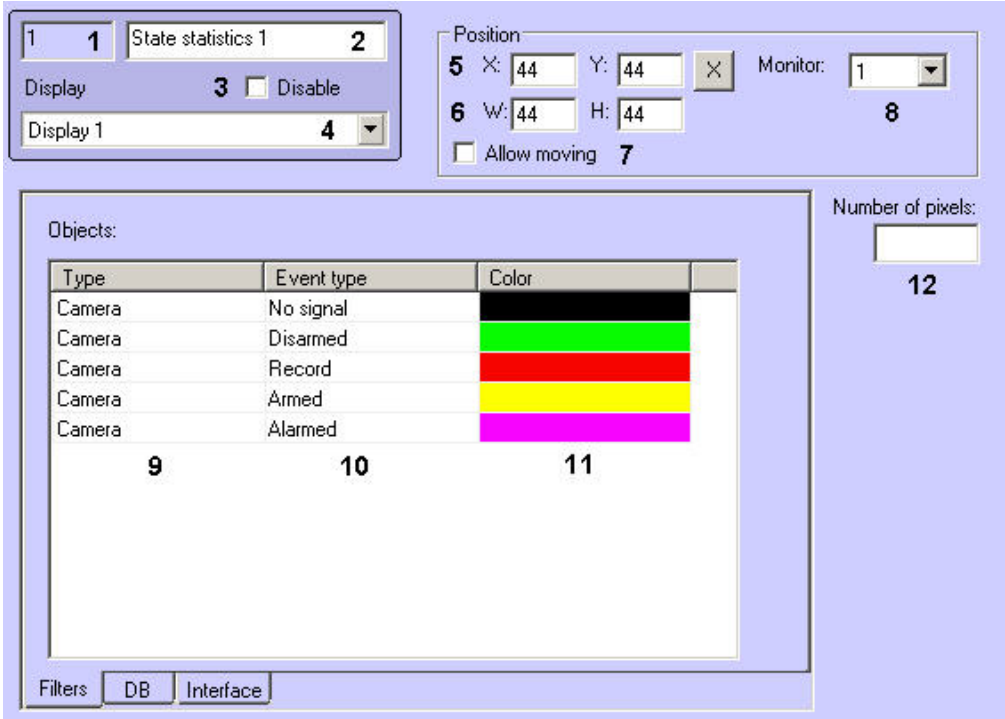
№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
1	The **Identification number** field	Automatically	Shows the identification number of the **Display manager** object in the system	Sequence of numbers	-	Depends on the number of **Display manager** objects in the system
2	The **Name** field	Type-in the value in the field	Assigns the name to the **Display manager** object	Latin, Cyrillic and service characters	Display manager	A line containing a sequence of any symbols (letters, digits, service, characters apart from > and < symbols), non case-sensitive Number of symbols – from 1 to 60
3	The **Disable** checkbox	Set the chechbox	Shows the status (enabled or disabled) of the **Display manager** object in the system	Boolean type	No	**Yes** – the **Display manager** object is disabled and is not in use **No** – the **Display manager** object is enabled and is in use
4	The **Display** dropdown list	Select from the list	Assigns the parent **Display** object , to which the given **Display manager** object refers	Name of the **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
5	The **X** filed	Type-in the value in the field	Sets the coordinate in the X horizontal axis for the upper left corner of the **Display manager** interface object on the screen	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
6	The **Y** field	Type-in the value in the field	Sets the coordinate in the Y vertical axis for the upper left corner of the **Display manager** interface object on the screen	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
7	The **W** filed	Type-in the value in the field	Sets the window width of the **Display manager** interface object	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
8	The **H** field	Type-in the value in the field	Sets the window height of the **Display manager** interface object	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
9	The X button	Click the button	Opens the window for automated setting of the X, Y, W and H parameters	-	-	-
10	The **Monitor** dropdown list	Select in the list	Sets the system ID of the monitor for which the coordinates are set	IDs of the monitors in the OS	1	From 1 to 16
11	The **Allow moving** checkbox	Chechbox is set	Allows hand shifting of the **Display manager** interface box	Boolean type	No	**Yes** – hand shifting is allowed. **No** – hand shifting is prohibited.
12	The **Available PCs** field	The >, <, >>, << buttons	Contains a list of **Computer** objects that have not yet been selected to be managed via the **Display manager**	Names of the **Computer** objects registered in the system	Depends on the number of **Computer** objects in the system	Depends on the number of the **Computer** objects in the system
13	The >, <, >>, << buttons	Click the button	Moving computers from the **Available PCs** list to the **Selected PCs** list and vice versa	-	-	-
14	The **Selected PCs** field	The >, <, >>, << buttons	Contains a list of **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 in the system
15	The **Selection of cameras** dropdown list	Select in the list	Specifies the cameras sorting method in the **Display manager** interface	Available sorting methods	By number	By number By name

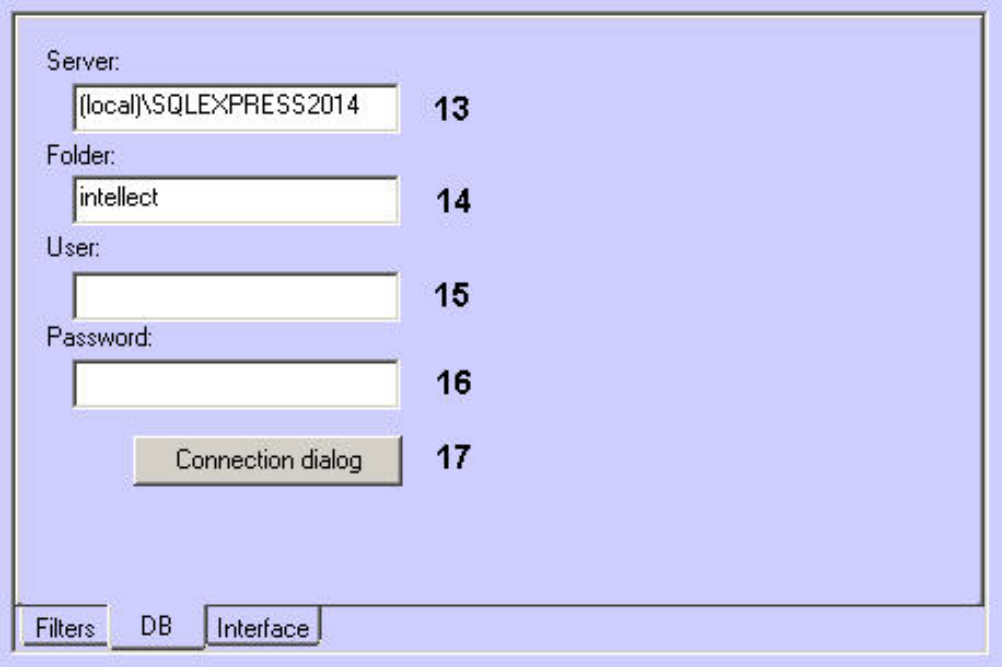
13.1.2.9.16 The Settings panel of the State statistics object

The settings panel of the **State statistics** object is shown in the figures.

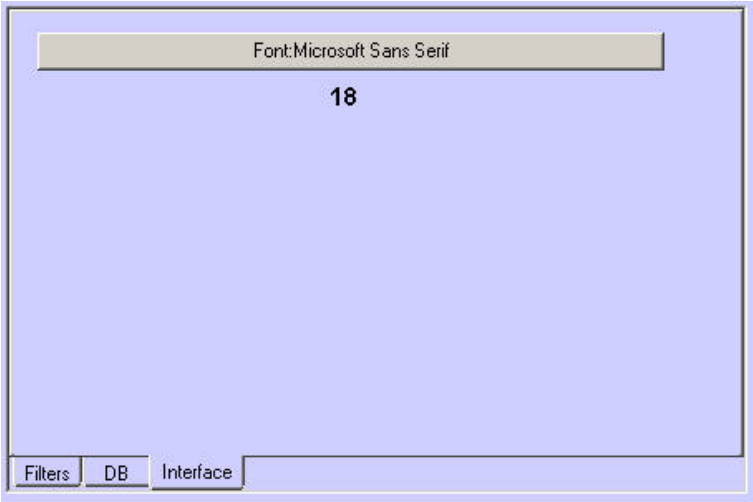
The **Filters** tab



The **DB** tab



The **Interface** tab



The description of the **State statistics** interface object settings is shown in the table.

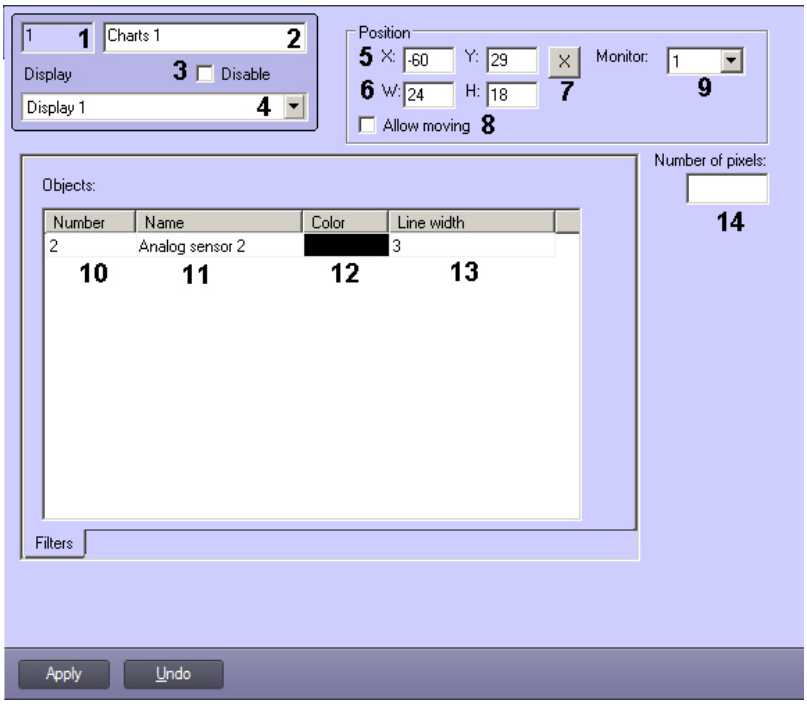
№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
The **Filters** tab						
1	The **Identification number** field	Automatically	Shows the identification number of the **State statistics** object in the system	Sequence of numbers	-	Depends on the number of **State statistics** objects in the system
2	The **Name** field	Type-in the value in the field	Assigns the name to the **State statistics** object	Latin, Cyrillic and service characters	Display manager	A line containing a sequence of any symbols (letters, digits, service, characters apart from > and < symbols), non case-sensitive Number of symbols – from 1 to 60
3	The **Disable** checkbox	Set the chechbox	Shows the status (enabled or disabled) of the **State statistics** object in the system	Boolean type	No	**Yes** – the **State statistics** object is disabled and is not in use **No** – the **State statistics** object is enabled and is in use
4	The **Display** dropdown list	Select from the list	Assigns the parent **Display** object, to which the given **State statistics** object refers	Name of the **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system
5	The **X** filed	Type-in the value in the field	Sets the coordinate in the X horizontal axis for the upper left corner of the **State statistics** interface object on the screen	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
	The **Y** field	Type-in the value in the field	Sets the coordinate in the Y vertical axis for the upper left corner of the **State statistics** interface object on the screen	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
6	The **W** filed	Type-in the value in the field	Sets the window width of the **State statistics** interface object	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
	The **H** field	Type-in the value in the field	Sets the window height of the **State statistics** interface object	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
7	The **Allow moving** checkbox	Chechbox is set	Allows manual moving of the **State statistics** interface box	Boolean type	No	**Yes** – manual moving is allowed. **No** – manual moving is prohibited.
8	The **Monitor** dropdown list	Select in the list	Sets the system ID of the monitor for which the coordinates are set	IDs of the monitors in the OS	1	From 1 to 16
9	The **Type** drop-down list	Select in the list	Sets the object types, which events should be displayed in the State statistics window.	Available object types	-	Depends on the objects 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	The **Event type** drop-down list	Select in 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	The **Color** drop-down list	Select in the list	Sets the color to highlight the selected state in the table and the graph in the **State statistics** window	Color palette	Black	RGB color
12	The **Number of pixels** field	Type-in the value in the field	Sets the number of pixels to be displayed on the graph	Sequence of numbers	0	>=0
The **DB** tab						
13	The **Server** field	Type-in the value in the field	Sets the name of the database server where the required database is stored	Latin, Cyrillic and service characters	-	The name of the server used by the system
14	The **Folder** field	Type-in the value in the field	Sets the name of the database where the events should be stored	Latin, Cyrillic and service characters	-	The name of the main database used by the system
15	The **User** field	Type-in the value in the field	Sets the username for the database server authorization	Latin, Cyrillic and service characters	-	-

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
16	The **Password** field	Type-in the value in the field	Sets the password for the database server authorization	Latin, Cyrillic and service characters	-	-
17	The **Connection Dialog** button	Click the button	Opens the database server connection dialog window	-	-	-
The **Interface** tab						
18	The **Font** button	Click the button	Opens the dialog window for selecting the text font for the table and the graph (except for the legend) in the **State statistics** window	-	-	-

13.1.2.9.17 The Settings panel of the Charts object

The settings panel of the **Charts** object is shown in the figure.



The description of the **Charts** interface object settings is shown in the table.

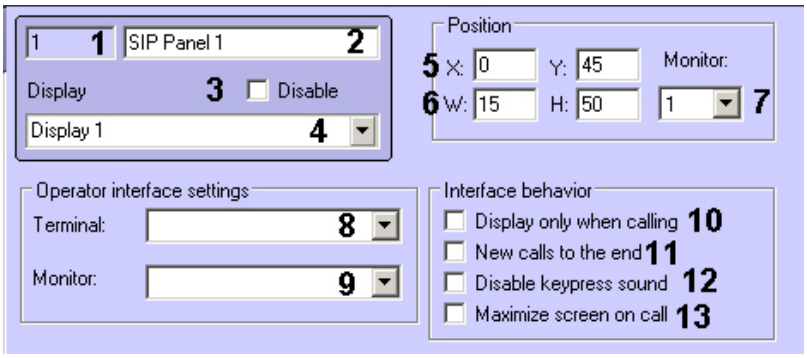
№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
The **Filters** tab						

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
1	The **Identification number** field	Automatically	Shows the identification number of the **Charts** object in the system	Positive integer	-	Depends on the number of **Charts** objects in the system
2	The **Name** field	Type-in the value in the field	Assigns the name to the **Charts** object	Latin, Cyrillic and service characters	Display manager	A line containing a sequence of any symbols (letters, digits, service, characters apart from > and < symbols), non case-sensitive Number of symbols – from 1 to 60
3	The **Disable** checkbox	Set the chechbox	Shows the status (enabled or disabled) of the **Charts** object in the system	Boolean type	No	**Yes** – the **Charts** object is disabled and is not in use **No** – the **Charts** object is enabled and is in use
4	The **Display** dropdown list	Select from the list	Assigns the parent **Display** object, to which the given **Charts** object refers	Name of the **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system
5	The **X** filed	Type-in the value in the field	Sets the coordinate in the X horizontal axis for the upper left corner of the **Charts** interface object on the screen	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
	The **Y** field	Type-in the value in the field	Sets the coordinate in the Y vertical axis for the upper left corner of the **Charts** interface object on the screen	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
6	The **W** filed	Type-in the value in the field	Sets the window width of the **Charts** interface object	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
	The **H** field	Type-in the value in the field	Sets the window height of the **Charts** interface object	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
7	The **X** button	Click the button	Opens a sample box to set the **Charts** window position on the screen.	-	-	-
8	The **Allow moving** checkbox	Chechbox is set	Allows manual moving of the **Charts** interface box	Boolean type	No	**Yes** – manual moving is allowed. **No** – manual moving is prohibited.
9	The **Monitor** dropdown list	Select in the list	Sets the system ID of the monitor for which the coordinates are set	IDs of the monitors in the OS	1	From 1 to 16

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
10	The **Number** drop-down list	Select in the list	Sets the **Analog sensor** object IDs, which readings should be displayed on the chart	Positive integer	-	Depends on the **Analog sensor** objects in the system.
11	The **Name** field	Automatically	Sets the name of the **Analog sensor** object, which readings should be displayed on the chart	Names of the **Analog sensor** objects	-	Depends on the object type
12	The **Color** drop-down list	Select in the list	Sets the color to highlight the corresponding analog sensor on the graph in the **Charts** window	Color palette	Black	RGB color
13	The **Line width** field	Type-in the value in the field	Sets the cart line width	Integer	5	>0
14	The **Number of pixels** field	Type-in the value in the field	Sets the number of pixels to be displayed on the graph	Sequence of numbers	0	>=0

13.1.2.9.18 The Settings panel of the SIP-panel object

The settings panel of the **SIP-panel** object is shown in the figure.



The description of the **SIP-panel** interface object settings is shown in the table.

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
The **Filters** tab						
1	The **Identification number** field	Automatically	Shows the identification number of the **SIP-panel** object in the system	Positive integer	-	Depends on the number of **SIP-panel** objects in the system

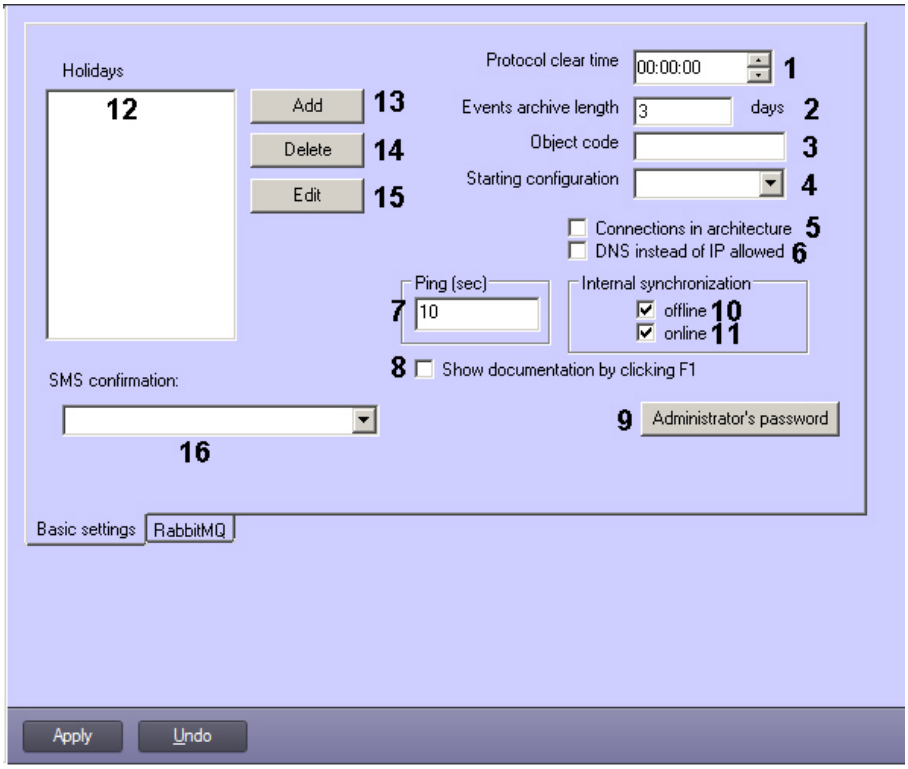
№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
2	The **Name** field	Type-in the value in the field	Assigns the name to the **SIP-panel** object	Latin, Cyrillic and service characters	Display manager	A line containing a sequence of any symbols (letters, digits, service, characters apart from > and < symbols), non case-sensitive Number of symbols – from 1 to 60
3	The **Disable** checkbox	Set the chechbox	Shows the status (enabled or disabled) of the **SIP-panel** object in the system	Boolean type	No	**Yes** – the **SIP-panel** object is disabled and is not in use **No** – the **SIP-panel** object is enabled and is in use
4	The **Display** dropdown list	Select from the list	Assigns the parent **Display** object, to which the given **SIP-panel** object refers	Name of the **Display** objects registered in the system	Name of the parent **Display** object	Depends on the number of the **Display** objects in the system
5	The **X** filed	Type-in the value in the field	Sets the coordinate in the X horizontal axis for the upper left corner of the **SIP-panel** interface object on the screen	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
	The **Y** field	Type-in the value in the field	Sets the coordinate in the Y vertical axis for the upper left corner of the **SIP-panel** interface object on the screen	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
6	The **W** filed	Type-in the value in the field	Sets the window width of the **SIP-panel** interface object	% of the screen width	-	From 0 to M*100, where M is the number of monitors installed
	The **H** field	Type-in the value in the field	Sets the window height of the **SIP-panel** interface object	% of the screen height	-	From 0 to M*100, where M is the number of monitors installed
7	The **Monitor** dropdown list	Select in the list	Sets the system ID of the monitor for which the coordinates are set	IDs of the monitors in the OS	1	From 1 to 16
8	The **Terminal** drop-down list	Select in 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 Panel** objects in the system
9	The **Monitor** drop-down	Select in 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
10	The **Display only when calling** checkbox	Set the checkbox	Enables displaying of the **SIP-panel** interface box only at call	Boolean type	No	**Yes** – the SIP panel is only displayed during call. **No** – the SIP panel is always displayed.

№	Parameter	Method for specifying the parameter	Parameter description	Symbol	Default value	Range of values
11	The **New calls to end** check box	Set the checkbox	Enables adding new calls to the end of the list.	Boolean type	No	**Yes** – new calls are added to the end of the list. **No** – new calls are added to the top of the list.
12	The **Mute keypress sound** check box	Set the checkbox	Mutes the sound of keys clicked on the SIP panel	Boolean type	No	**Yes** – keypress sound disabled. **No** – keypress sound is turned on.
13	The **Maximize screen on call** check box	Set the checkbox	Enables automatic display switching on call	Boolean type	No	**Yes** – when a call is made to the SIP terminal corresponding to the SIP panel, the Display to which the SIP panel is added is automatically shown. **No** – the displays are not switched automatically on any call to the SIP terminal corresponding to the SIP panel.

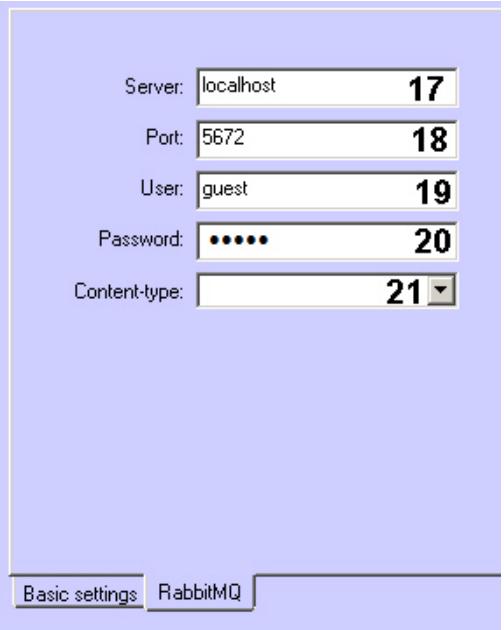
13.1.2.10 The Programming tab

13.1.2.10.1 The Settings panel of the Security zone object

The **Security zone** panel is designed to define the common settings of the Intellect™ system. The settings panel of the **Security zone** object is shown in the figure.



The **Basic settings** tab



The **RabbitMQ** tab

The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Security zone** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
The **Settings** group						
1	Event viewer clearing time	Enter a value in the field using the **up** and **down** buttons	Indicates the time of day at which to start cleaning up the Event Viewer database in accordance with the **Events archive length** parameter.	HH:MM:SS	Current system time at the moment of object setting panel opening	00:00:00 to 23:59:59
2	Events archive length	Type-in the value in the field	Sets the number of days for keeping the information about the events registered by the Intellect™ system and recorded in the Event log. This parameter influences on all computers in the distributed system.	Days	3	Not less than 0
3	Object code	Type-in the value in the field	Defines the number of the access control card, which is automatically displayed in the User settings panel, when the object is being created in the Facility code field.	Sequence of numbers	Not specified	More than 1

4	Run macro at start	Is selected from the list	Defines the macro command, which will be automatically launched with the Intellect™ system startup.	Names of the **Macro** objects registered in the system	Not specified	Depends on the number of **Macro** objects created in the digital distributed video surveillance system.
5	Connections in the architecture	Is identified by the check mark	Specifies computers with which the created **Computer** object is to exchange system configuration parameters data: with all computers in the video surveillance system with distributed architecture or only with the **Computer** object under which the object was created.	Boolean type	Not specified	**Yes** – when creating a new computer the **Connection** checkboxes in the **Architecture** tab are set checked for all computers in the architecture. **No** – when creating a new computer the **Connection** checkbox in the **Architecture** tab is set checked only for the computer on which this new object is created.
6	DNS instead of IP allowed	Checkbox	Enables setting address of Server/ Remote Administrator's workplace/Remote Client in the **Architecture** tab as DNS name - not only IP address.	Boolean type	No	**Yes** – DNS name (instead of IP address) of Server/ Remote Administrator's workplace/Remote Client can be specified in the **Architecture** tab when configuring computer interoperability in distributed system. Validation of the specified address is disabled. **No** – IP address of Server/Remote Administrator's workplace/Remote Client is to be specified in the **Architecture** tab when configuring computer interoperability in distributed system.
7	Ping (sec.)	Type-in the value in the field	Sets Server-computer ping period.	Non-negative integer number	10	>=0
8	Show documentation by clicking F1	Set the checkbox	Enables opening documentation in the pdf format by clicking F1, when *Intellect* is started. Administrator's Guide is opened on the Server and Remote Administrator's workplace; Operator's Guide is opened on the Remote Client.	Boolean type	No	**Yes** – documentation is shown by clicking F1. **No** – feature of showing documentation by clicking F1 is disabled.

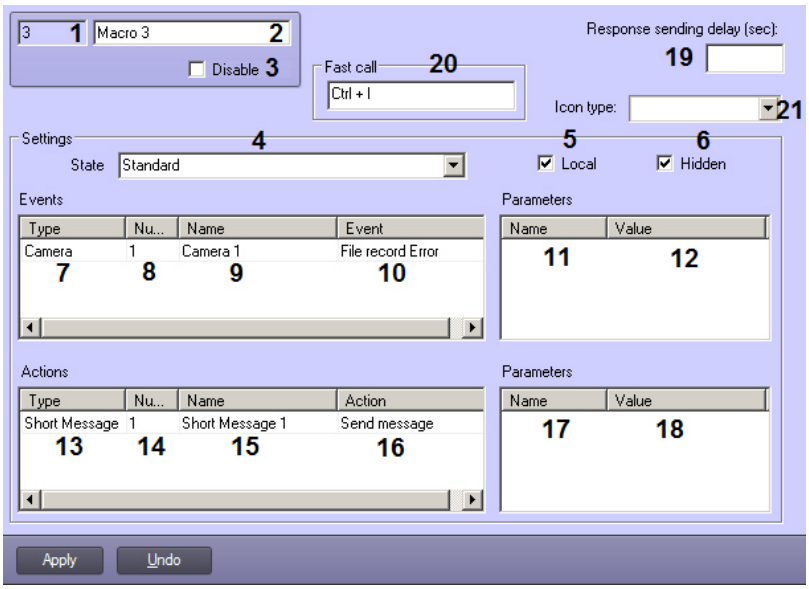
9	Administrator's password	Click the button	Gives a command to open a dialog box for assigning the Administrator's password.	-	-	-
The **Internal synchronization** group						
10	offline	Checkbox	Enables offline synchronization of events	Boolean type	Yes	**Yes** – offline synchronization is enabled. When the computer is reconnected, it gets all the events for the period there was no connection. **No** – offline synchronization is disabled. When the computer is reconnected, it does not get the events for the period there was no connection.
11	online	Checkbox	Enables online synchronization of events	Boolean type	Yes	**Yes** – online synchronization is enabled. Events are sent right after they happen according to computer interaction configuration parameters. **No** – online synchronization is disabled. Events are not sent.
Holidays group						
12	Date*	-	List of calendar days which will be defined as holidays in the *Intellect* software	Date	Not specified	Date format:: DD-MM-YY
13	Add	Click the button	Opens the **Calendar** dialog box to set the date of new holiday	-	-	-
14	Delete	Click the button	Deletes the selected holiday date from the **Date** list	-	-	-
15	Change	Click the button	Opens the **Calendar** dialog box to change the selected holiday date in the list	-	-	-
SMS confirmation						
16	SMS confirmation	Type-in the value in the field	Defines the **Short message** object for two-factor authentication – see Configuring two-factor authentication	Names of the **Short message** objects registered in the system	Not specified	Depends on the number of **Short message** objects created in the system.

RabbitMQ tab						
16	Server	Type-in the value in the field	Sets the RabbitMQ host address	Latin characters, digits and service characters	localhost	Host IP address or name
17	Port	Type-in the value in the field	Sets the RabbitMQ host port	Latin characters, digits and service characters	5672	0 – 65535
18	User	Type-in the value in the field	Sets the RabbitMQ host user name	Latin characters, digits and service characters	guest	Depends on registered RabbitMQ users
19	Password	Type-in the value in the field	Sets the RabbitMQ host user password	Latin characters, digits and service characters	guest	Depends on registered RabbitMQ users
20	Content-type	Select from the list	Sets the type of content sent/ received	Supported content type	plain/text	**application/json** – a message in JSON format is sent/ received **plain/text** – Intellect event is sent/received in the following format: "TYPE|ID| EVENT"

*The name of the element is not displayed in the settings panel of the given object.

13.1.2.10.2 The Settings panel of the Macro object

The **Macro** object is designed to support automatic execution of a pre-defined sequence of commands upon occurrence of certain events, registered by the Intellect™ system. The settings panel of the **Macro** object is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Macro** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range

1	Identification number*	Automatically	Displays the identification number of the **Macro** command object in the video surveillance system.	Sequence of numbers	-	Depends on the number of **Macro** command objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the **Macro** command object name.	Latin, Cyrillic and service characters	Macro	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), case-insensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the **Macro** command object status (enabled or disabled).	Boolean type	Not available	**Yes** – the **Macro** command object is disabled and is not in use **No** – the **macro** command object is enabled and is in use.
Settings Group						
4	State	Enter the value in the field	Defines the message displayed in the information board of the main menu of the Intellect system, when the given macro command is running.	Latin, Cyrillic and service characters	Not defined	1. **Standard** – no message will be displayed in the information board of the main menu of the Intellect system. 2. A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 60.
5	Local	Is identified by the check mark	Defines the computers, which will execute the given macro command (all computers of the digital distributed video surveillance system or only the given computer). *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.*	Boolean type	Not available	**Yes** – the given macro command will be executed by all computers of the digital distributed video surveillance system. **No** – the macro command will be executed only by the given computer.

6	Hidden	Is identified by the check mark	Defines, whether or not this macro command will be displayed in the main control panel of the Intellect system to be launched manually.	Boolean type	Not available	**Yes** – no macro command will be displayed in the main control panel of the Intellect system. **No** – the macro command will be displayed in the main control panel of the Intellect system.
Events Subgroup						
7	Type	Is selected from the list	Defines the type of objects in the digital distributed video surveillance system, in which registration of events initiates macro command execution.	Types of objects registered in the system.	Empty field	Depends on the total number of types of objects created in the digital distributed video surveillance system.
8	Number	Is selected from the list	Defines the identification number of the object in the digital distributed video surveillance system, in which registration of events initiates macro command execution.	Sequence of numbers	Empty field	Depends on the total number of the given types of objects created in the digital distributed video surveillance system.
9	Name	Automatically	Displays the name of the selected object in the digital distributed video surveillance system.	Name of the objects of the same type registered in the system	Empty field	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 60.
10	Event	Is selected from the list	Defines the event, which, when registered for the pre-defined object, initiated macro command execution.	Events registered for the given type of objects.	Empty field	List of events is created separately for each type of object.
Parameters Subgroup ***NOTE.*** *The given subgroup is not active for some types of objects.*						
11	Name	Automatically	Defines an additional parameter for the selected type of object in the **Events** subgroup.	Latin, service characters and digits.	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 60.

12	Value	Enter the value in the field	Defines the value for the parameter of the **Name** column.	Latin, service characters and digits.	Empty field	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 250.
Action Subgroup						
13	Type	Is selected from the list	Defines the type of objects in the digital distributed video surveillance system, to which the command is forwarded, when the conditions defined in the **Events** subgroup for macro command initiation are met.	Types of objects registered in the system.	Empty field	Depends on the total number of types of objects created in the digital distributed video surveillance system.
14	Number	Is selected from the list	Defines the identification number of the object in the digital distributed video surveillance system, to which the command is forwarded, when the conditions defined in the **Events** subgroup for macro command initiation are met.	Sequence of numbers	Empty field	Depends on the total number of the given types of objects created in the digital distributed video surveillance system. 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.
15	Name	Automatically	Displays the name of the selected object in the digital distributed video surveillance system.	Name of the objects of the same type registered in the system	Empty field	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 60.

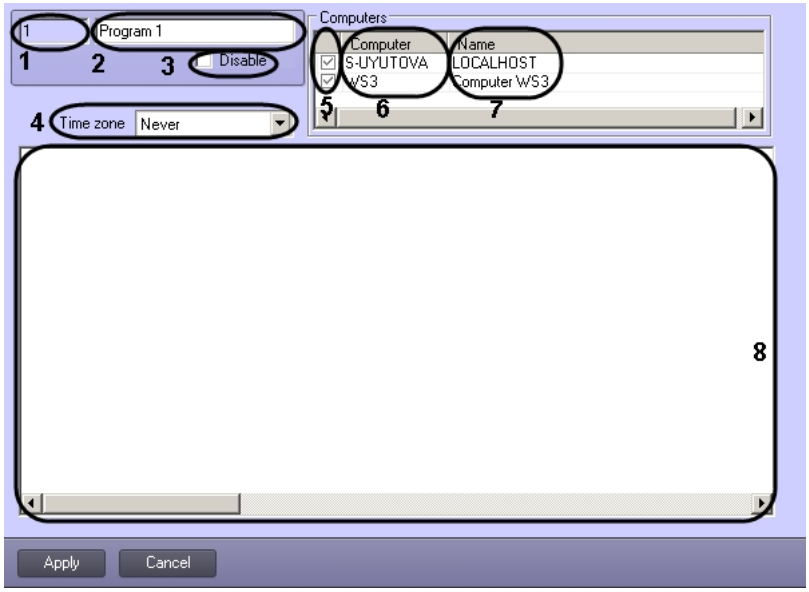
16	Action	Is selected from the list	Defines the action, which the given device performs, when the conditions for the given macro command initiation are met.	Actions, registered by the system for the given type of objects.	Empty field	List of events is created separately for each type of object.
Parameters Subgroup ***NOTE.*** *The given subgroup is not active for all types of objects.*						
17	Name	Automatically	Defines an additional parameter for the selected type of object in the **Actions** subgroup.	Latin, service characters and digits.	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 60.
18	Value	Enter the value in the field	Defines the value for the parameter of the Name column.	Latin, service characters and digits.	Empty field	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols – from 1 to 250.
Outside the groups						
19	Response sending delay (sec.)	Enter the value in 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 events do not reoccur over the specified period.*	Integer number	-	>0
20	Fast call	Left-click in the field and click the required key combination	Sets a shortcut for a macro. ***Note****. If the same combination of hot keys is set for several macros, when clicking a key combination, all of these macros run.*	Key combinations	No	Some keys of the main or numeric keyboard, as well as these keys in combination with Shift, Ctrl and Alt.

21	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.

*The name of the element is not displayed in the **User's rights** settings panel object.

13.1.2.10.3 The Settings panel of the Program object

The **Program** object creates specialized programs in the embedded environment of the INTELLECT™ software. The settings panel of the **Program** object is shown in the figure.



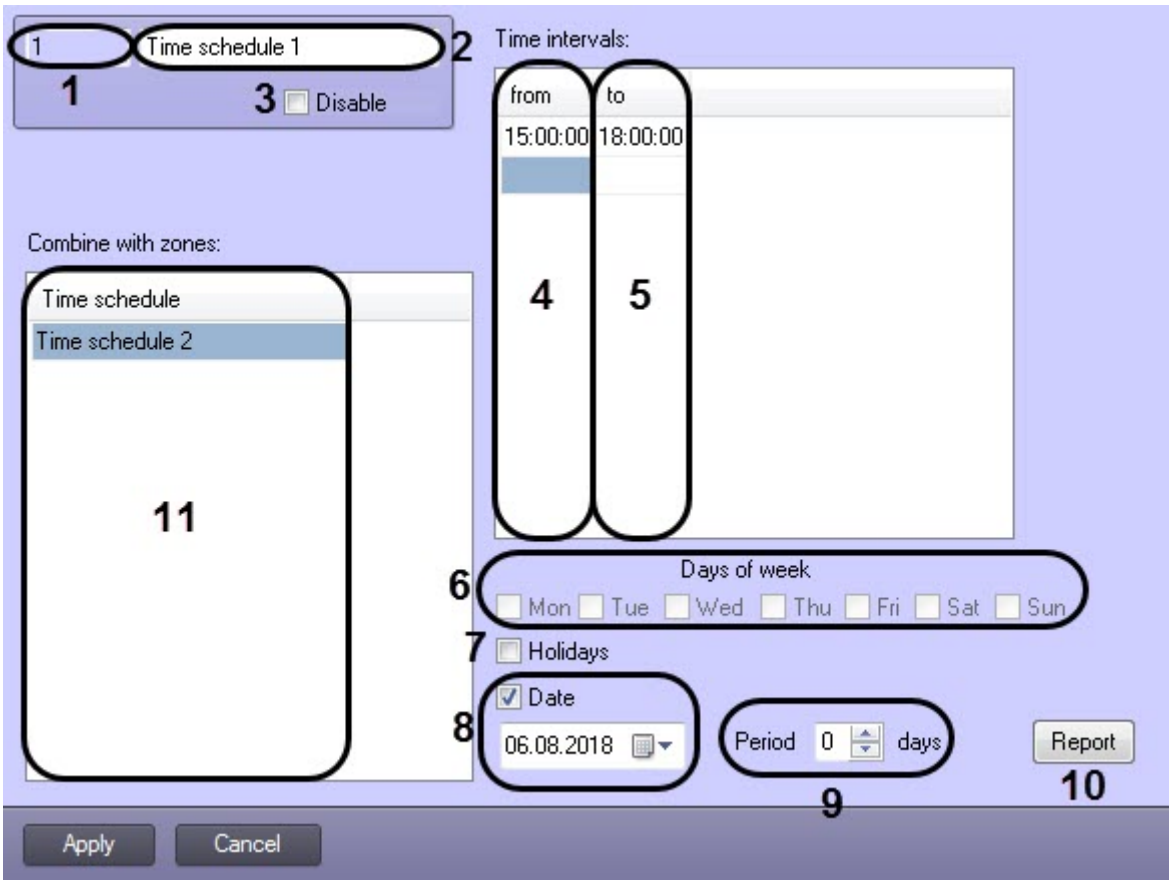
The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Program** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Program** object in the video surveillance system.	Sequence of numbers	-	Depends on the number of **Program** objects in the digital distributed video surveillance system.
2	Name*	Enter the value in the field	Defines the **Program** object name.	Latin, Cyrillic and service characters	Program	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), case-insensitive. Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Defines the status of the Program object (enabled or disabled).	Boolean type	Not available	**Yes** – the **Program** object is disabled and is not in use **No** – the **Program** object is enabled and is in use.
4	Time zone	Is selected from the list	Defines the time period during which the given program will operate.	Time zone registered by the system	Never	**Never** – this program will never be executed. **Always** – this program is always in the state of execution. List of created time zones – the program will be executed within a pre-defined time period.
Computers Group						
5	Select an element*	Is identified by the check mark	Defines the computer for the execution of the given program.	Boolean type	Not available	**Yes** – the program will be executed by the pre-defined computer. **No** – the program will not be executed by the computer.
6	Computer	Automatically	Defines the computer name in the local network.	Computer name in the local network.	Computer name in the local network.	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols - 60.
7	Name	Automatically	Defines the computer name	Name of the Computer object registered in the system	Name of the Computer object registered in the system	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Number of symbols - 60.
Out of the groups						
8	Text editor*	Enter the value in the field	Is used to enter the text of the executed program.	Latin, Cyrillic, service characters and digits.	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive. Unlimited number of symbols.

*The name of the element is not displayed in the User's rights settings panel object.

13.1.2.10.4 The Settings panel of the Time schedule object

The **Time schedule** object defines the time parameters in the Intellect™ system for any actions, which are to be initiated within certain periods of time. The settings panel of the **Time schedule** object is shown in the figure.



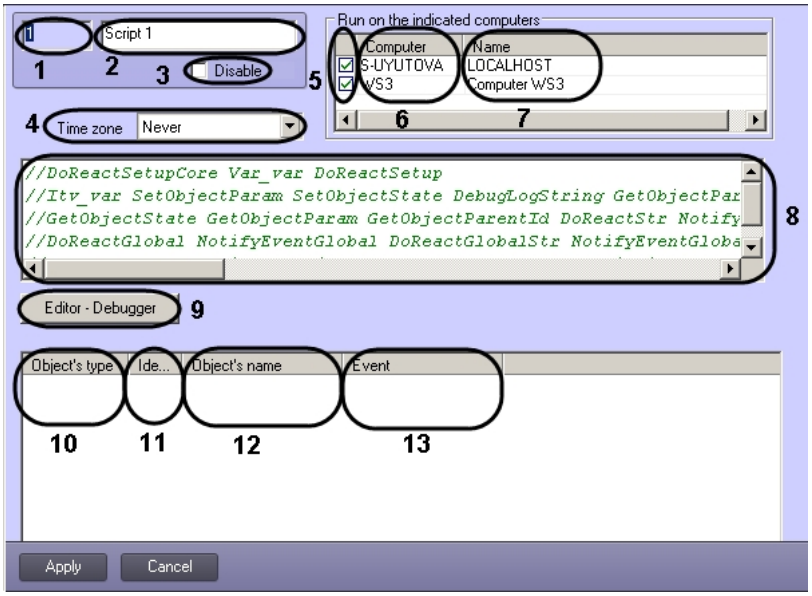
The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Time schedule** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Displays the identification number of the **Time schedule** object.	Sequence of numbers	-	Depends on the number of the **Time schedule** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Sets the **Time schedule** object name.	Latin, Cyrillic and service characters	Time schedule	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), case-insensitive. Number of symbols – from 1 to 60.
3	Disable	Checkbox	Sets the state (enabled or disabled) of the **Time schedule** object in the digital distributed video surveillance system.	Boolean type	No	**Yes** – the **Time schedule** object is disabled and is not in use. **No** – the **Time schedule** object is enabled and is in use.
The **Settings** group						
The **Time intervals** subgroup						
4	From	Enter the value in the field	Sets the initial point of the time interval.	Sequence of numbers	Not set	Time interval entry format: HH:MM
5	To	Enter the value in the field	Sets the end point of the time interval.	Sequence of numbers	Not set	Time interval entry format: HH:MM
Out of the subgroup						
6	Days of week	Checkbox ***NOTE.*** *Is not active, if the Days field is checked (item 8).*	Sets the days of the week, when the given time schedule is active.	Boolean type	No	**Yes** – the time schedule is active on the selected day. **No** – the time schedule is not active on the selected day.
7	Holidays	Checkbox ***NOTE.*** *Is not active, if the Days field is checked (item 8).*	Gives a command to use the given time schedule on holidays.	Boolean type	No	**Yes** – the given time schedule is to be used on holidays. **No** – the given time schedule is not to be used on holidays.
8	Days*	Checkbox	Defines, whether the given time schedule should be used permanently or only within a pre-defined period of time.	Boolean type	No	**Yes** – the given time schedule should be used within a pre-defined period of time. **No** – the given time schedule should always be used.
	Date	Enter the value in the field	Sets the initial point, from which the use of the given time schedule is to start.	Sequence of numbers	Not active	Data entry format: DD:MM:YY
9	Period	Select in the list	Specifies periodicity in days of N triggering of time schedule starting from the specified date (i.e. time schedule triggers each N day).	Sequence of numbers	Empty field	From 0 to 999999999999999
10	Report	Button	Displays the box with time-schedules activity table	-	-	-
11	Time schedule	Select in the list	Sets the time schedule that is to be combined with the given time schedule	The names of the **Time schedule** objects registered in the system	-	Depends on the number of the **Time schedule** objects registered in the system

* The name of the element is not displayed in the settings panel of the object.

13.1.2.10.5 The Settings panel of the Script object

The **Script** object is designed to create specialized programs in JScript language. The settings panel of the **Script** is shown in the figure.



The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Script** object.

Table 11.2—47

№	Parameter	Method for entering the parameter	Parameter description	Symbols used	Default value	Value range
1	Identification number*	Automatically	Shows the identification number of the **Script** object in the digital video surveillance system.	Sequence of numbers	-	Depends on the number of **Script** objects in the digital distributed video surveillance system
2	Name*	Specify the value in the field	Assigns the name to the **Script** object.	Latin, Cyrillic and service characters	Script	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), case-insensitive Number of symbols – from 1 to 60.
3	Disable	Checkbox is set	Sets the state (enabled or disabled) of the **Script** object in the digital distributed video surveillance system.	Boolean type	Not available	**Yes** – the **Script** object is disabled and is not in use **No** – the **Script** object is enabled and is in use.
4	Time zone	Select in the list	Specifies the time period for the operation of the given program.	Time zone name registered in the system.	Never	**Never** – the program will never be executed. **Always** – the program is always executed. List of created time zones – the programs are executed during the time period as defined by the time zone.
The **Computers** group						
5	Select element*	Checkbox is set	Assigns the computer for the execution of the given script.	Boolean type	No	**Yes** – the script is executed on the computer. **No** – the script is not executed on the computer.
6	Computer	Automatically	Specifies the computer name in the local network	Computer name in the local network.	Computer name in the local network.	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive Number of symbols - 60.
7	Name	Automatically	Specifies the name of the computer in the digital distributed video surveillance system.	Name of the **Computer** object registered in the system.	Name of the **Computer** object registered in the system.	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive Number of symbols - 60.
No group						
8	Text editor*	Specify the value in the field	Specifies the text of the executed script.	Latin, Cyrillic and service characters	Not set	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive Unlimited number of symbols.
9	Editor - Debugger	Press the button	Gives a command to open a debugging window of the script.	-	-	-
10	Object's type	Select in the list	Sets the type of the object on receiving event from which the script is executed	Types of objects registered in the system	-	Depends on the number of the objects registered in the system
11	Identifier	Select in the list	Sets the identifier of the object on receiving event from which the script is executed	Identifiers of the objects of the selected type registered in the system	-	Depends on the number of the objects of the selected type registered in the system

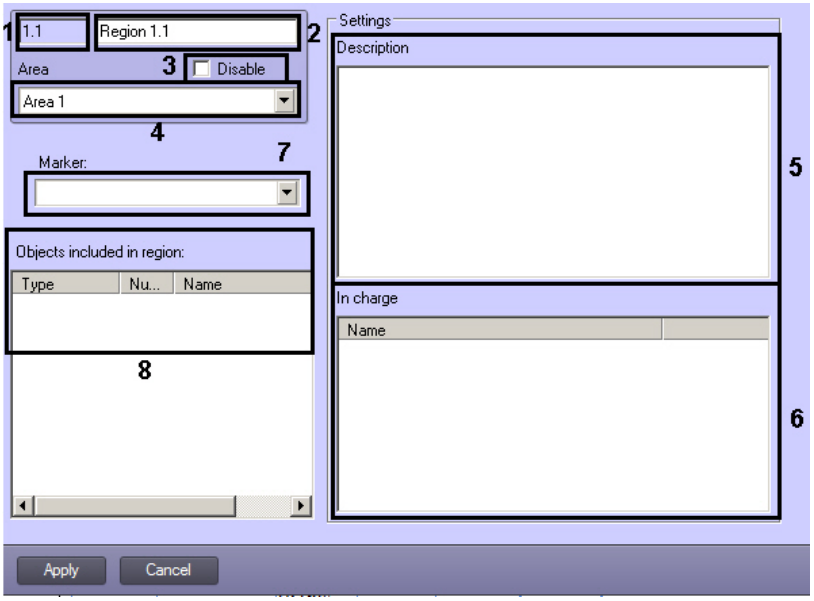
*The name of the element is not displayed in the settings panel of this object.

13.1.2.10.6 The Settings panel of the Region object

The **Region** object is designed to create zones, which break down secured areas into structural elements. The **Region** objects allow:

1. group hardware based on the attributes of a certain region;
2. execute certain operations concurrently with all objects of the same type belonging to the same region.

The settings panel of the **Region** object is shown in the figure.



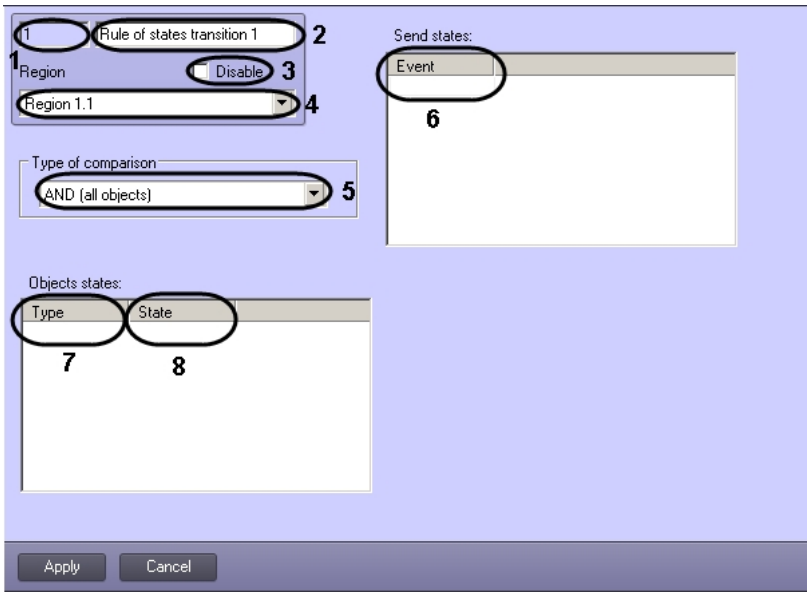
The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Region** object.

№	Parameter	Method for entering the parameter	Parameter description	Sym-bols used	Default value	Value range
1	Identification number*	Automatically	Shows the identification number of the **Region** object in the digital video surveillance system.	Sequ-ence of numb-ers	-	Depends on the number of **Region** objects in the digital distributed video surveillance system
2	Name*	Enter the value in the field	Assigns the name to the **Region** object.	Latin, Cyrill-ic and servi-ce chara-cters	Region	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), case-insensitive Number of symbols – from 1 to 60.
3	Disable	Is identified by the check mark	Shows the status (enabled or disabled) of the **Region** object in the digital distributed video surveillance system.	Bool-ean type	Not available	**Yes** – the **Region** object is disabled and is not in use. **No** – the **Region** object is enabled and is in use.
4	Area	Is selected from the list	Assigns the parent **Area** object, to which the given **Region** object refers.	Name of the Area object-s regist-ered in the system.	Name of the parent **Area** object	Depends on the number of **Area** objects in the digital system.
Settings Group						
5	Description	Enter the value in the field	Defines the description of the given region.	Latin, Cyrill-ic and servi-ce chara-cters	Not defined	A line containing a sequence of any symbols (letters, digits, service characters), case-insensitive Number of symbols – from 1 to 60.
6	Description	Is selected from the list	Defines the users registered by the system, responsible for the given region.	Latin, Cyrill-ic and servi-ce chara-cters	Not defined	Depends on the number of users registered by the system.
7	Marker	Select from the list	Specifies the set of signs which will be in use while displaying region on the interactive map	Available set of signs specified by means of the ddi.exe utility	Not specified	Depends on the number of available sets of signs
8	Objects included into region	Automatically	Displays the list of objects related to this region	Type, number and name of objects included into region	Not specified	Depends on the number of the objects related to this region

*The name of the element is not displayed in the settings panel of the given object

13.1.2.10.7 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.

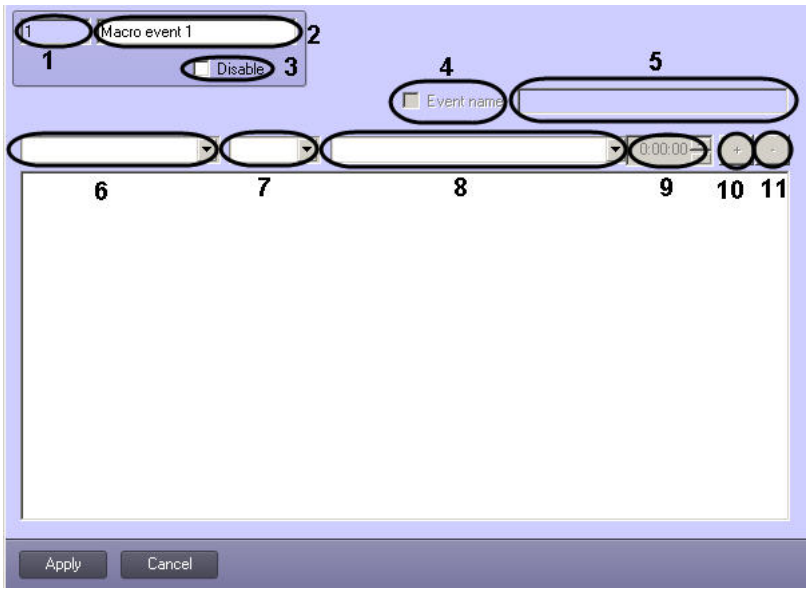


The table describes the parameters of the settings corresponding to the elements of the settings panel of the **Rule of states transition** object.

№	Parameter	Method for entering the parameter	Parameter description	Symbol used	Default value	Value range
1	The **Identification number** field	Automatically	Shows the identification number of the **Rule of states transition** object in the digital video surveillance system	Sequence of numbers	-	Depends on the number of **Rule of states transition** objects in the digital video surveillance system
2	The **Name** field	Type-in the value in the field	Assigns the name to the **Rule of states transition** object.	Latin, Cyrillic and service characters	Rule of states transition	A line containing a sequence of any symbols (letters, digits, service, characters apart from > and < symbols), case-insensitive Number of symbols – from 1 to 60.
3	The **Disable** checkbox	Checkbox	Shows the status (enabled or disabled) of the **Rule of states transition** object in the digital video surveillance system	Boolean type	No	**Yes** – the **Rule of states transition** object is disabled and is not in use. **No** – the **Rule of states transition** object is enabled and is in use.
4	The **Region** drop-down list	Is selected in the list	Assigns the Region parent object to which the **Rule of states transition** object relates	Name of the **Region** objects registered in the system	Name of the **Region** parent object	Depends on the number of **Region** objects registered in the digital system
The **Type of comparison** group						
5	The **Type of comparison** drop-down list	Is selected in the list	Sets the limitation of **Rule of states transition**	List of limitations	AND (all objects)	**AND** (all objects) - rule activates if all objects of selected types pass into the specified states **OR** (at least one object) - rule activates if at least one object passes into the one specified state
The **Send states**: group						
6	The **Event** drop-down list	Is selected in the list	Assigns the event generated by the **Region** object when the rule condition is met	List of events which the **Region** object can generate	-	Alarm end, Armed, Alarm accepted, Alarm in zone, Disarmed
The **Objects' state**: group						
7	The **Type** drop-down list	Is selected in the list	Assigns the type of objects needed for forming the rule of states transition	List of available types	-	Relay, sensor, camera
8	The **State** drop-down list	Is selected in the list	Assigns the state of objects of specified type when it is needed to change the **Region** state	List of states which objects of specified type can take	-	Depends on the selected object type

13.1.2.10.8 The Settings panel of the Macro event object

The **Macro event** object is designed for creating events in case of occurrence the chain of events in the specified time period. Settings panel of the **Macro event** object is presented in the figure.



Description of settings parameters corresponding to the elements of **Macro event** object's settings panel is presented in the table.

№	Parameter	How to enter the parameter	Parameter description	Symbols used	Default value	Value range
1	**Identification number*** field	Automatically	Displays the identification number of the **Macro event** object	Sequence of numbers	-	Depends on the number of **Macro event** objects in the digital distributed video surveillance system
2	**Name*** field	Enter the value in the field	Defines the name of the **Macro event** object	Latin, Cyrillic and service characters	Macro event	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	**Disable** checkbox	Is set with a checkbox	Defines the condition of the **Macro event** object (enabled or disabled) in the digital distributed video surveillance system	Boolean type	No	Yes – the **Macro event** object is disabled and is not in use. No – the **Macro event** object is enabled and is in use.
4	**Event name** checkbox	Is set with a checkbox	The checkbox defines whether the macro event is generated while the occurrence of the chained events or by expiration the time-out of waiting the event.	Boolean type	No	Yes – event is generated. No – event is not generated.
5	**Event name** field	Enter the value in the field	Defines the name of macro event which is transmitted in the param0 parameter.	Latin, Cyrillic and service characters		A line containing a sequence of any symbols (letters, digits, service characters), not case-sensitive Not more than 120 symbols.
6	**Object type*** drop-down list	Enter the value in the field	Defines the objects type, events from which are to be controlled.	Object types created in the system	-	Depends on objects created in the system

7	**Number*** drop-down list	Select from the list	Sets the number of objects of selected type, event from which are to be controlled.	Identifiers of objects of selected type registered in the system	-	Depends on number of objects of selected type
8	**Event type*** drop-down list	Select from the list	Sets the event type of selected object which is to be controlled	List of events available for the object of selected type	-	Depends on the selected object type
9	**Time-out*** field	Enter the value in the field	Sets the time-out of waiting for occurrence the event of selected type.	HH:MM:SS	-	Time in HH:MM:SS format
10	**+** button	Click the button	Adds event to the chain	-	-	-
11	**-** button	Click the button	Removes event from the chain with all underneath events in the chain.	-	-	-

*Name of the element is not displayed on the object's settings panel.

13.1.2.11 The Users tab

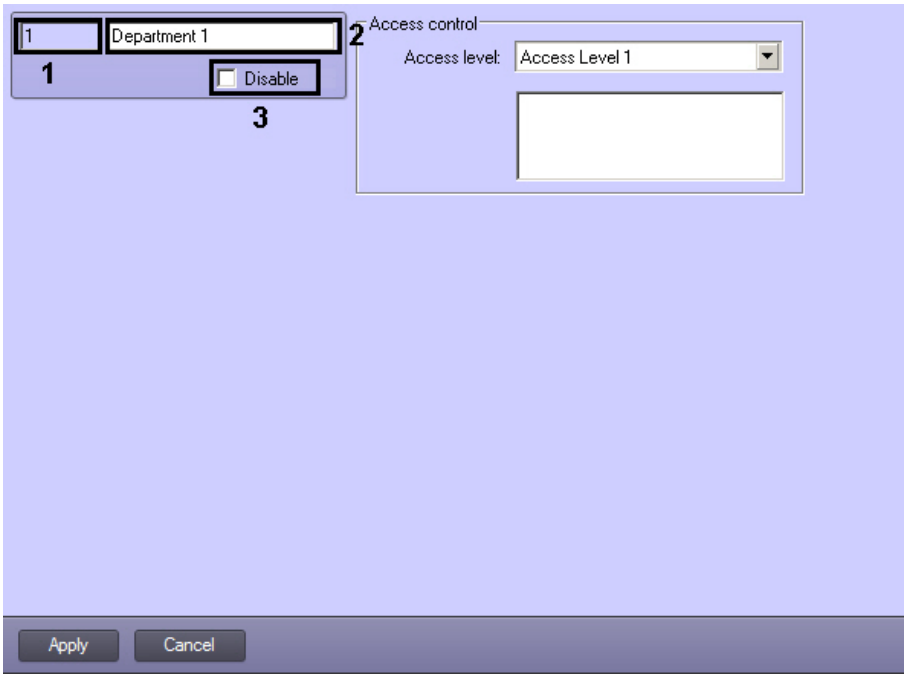
13.1.2.11.1 The Users tab components

There are the following elements on the **Users** tab:

1. The tree of departments and users in them. The settings panels of the **User** and **Department** objects contain parameters used when configuring *ACFA Intellect* – that is why only the main settings are described in this document.
2. The list of user rights.

13.1.2.11.2 The Settings panel of the Department object

The settings panel of the **Department** object is shown in the figure.

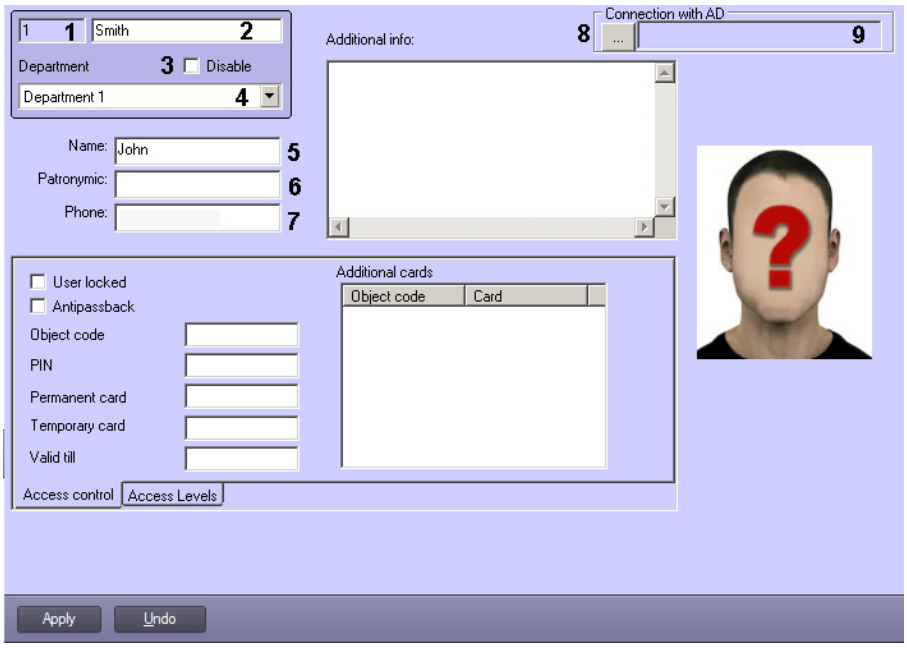


Basic elements of the settings panel of the **Department** object are described in the table.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	The **ID** field	Automatically	Displays the identification number of the **Department** object	Sequence of numbers	-	Depends on the number of the **Department** objects in the system
2	The **Name** field	Enter the value in the field	Sets the name of the **Department** object	Latin, Cyrillic and service characters	Department	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60.
3	The **Disable** chackbox	Set the checkbox	Defines the status of the **Department** object (enabled or disabled)	Boolean type	No	Yes – the **Department** object is disabled and is not in use. No – the **Department** object is enabled and is in use.

13.1.2.11.3 The Settings panel of the User object

The settings panel of the **User** object is shown in the figure.



Basic elements of the settings panel of the **User** object are described in the table.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
1	The **ID** field	Automatically	Displays the identification number of the **User** object in the system	Sequence of numbers	-	Depends on the number of the **User** objects in the system

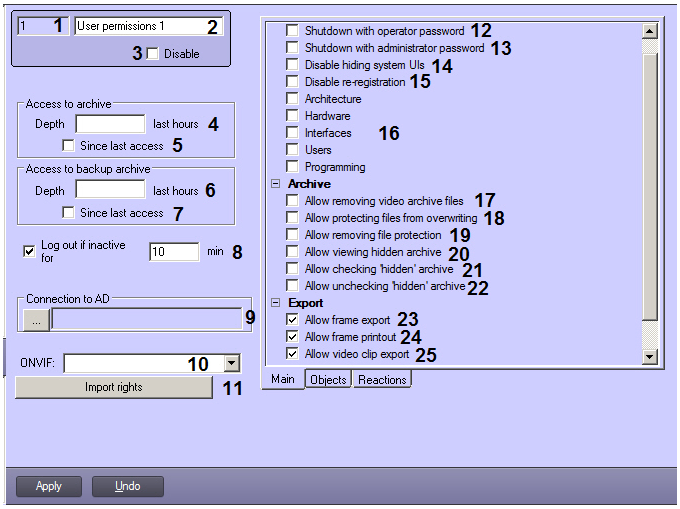
№	Parameter	Method for setting the parameter value	Parameter description	Symbols used	Default value	Value range
2	The **Username** field	Enter the value in the field	Sets the name of the **User** object in the system (usually the user's last name)	Latin, Cyrillic and service characters	**User**	A line containing a sequence of any symbols (letters, digits, service characters apart from > and < symbols), not case-sensitive. Number of symbols – from 1 to 60. Do not use **rs** as username when registering Operator accounts as this name is used by default in *Intellect Web Report System*.
3	The **Disable** checkbox	Set the checkbox	Defines the status of the **User** object (enabled or disabled) in the system	Boolean type	No	Yes – the **User** object is disabled and is not in use. No – the **User** object is enabled and is in use.
4	The **Department** drop-down list	Select the value in the list	Defines the **Department** parent object for **User** object	The names of the **Department** objects registered in the system	The name of the **Department** parent object	Depends on the number of the **Department** objects in the system
5	The **Name** field	Enter the value in the field	The user's first name	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols
6	The **Patronymic** field	Enter the value in the field	The user's patronymic	Latin, Cyrillic and service characters	-	A line containing a sequence of any symbols
7	The **Phone** field	Enter the value in the field	The user's phone number for two-factor authentication – see Configuring two-factor authentication	Phone number	-	+ [country code] [city code] [subscriber number] For example, +11234567890
8	The **Connection with AD** button	Click the button	Opens a dialog box to configure the connection between the *Intellect* and the Windows Active Directory users	-	-	-
9	The **Connection with AD** field	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 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.

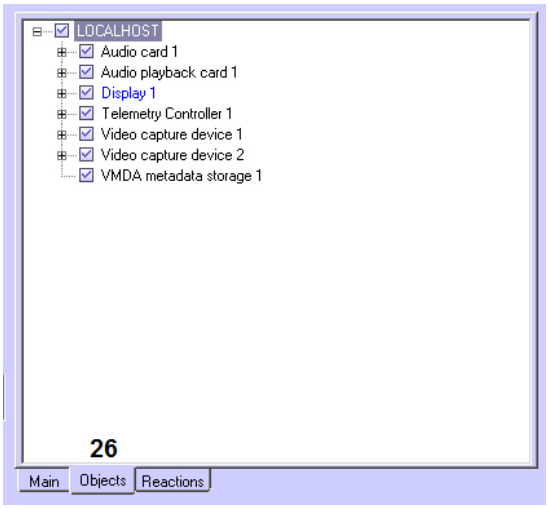
Face recognition and search interface being part of *Face-Intellect* software also allows adding and editing user's photo (see *Face-Intellect* documentation in AxxonSoft documentation repository for details on its setting up and configuration).

13.1.2.11.4 The Settings panel of the User permissions object

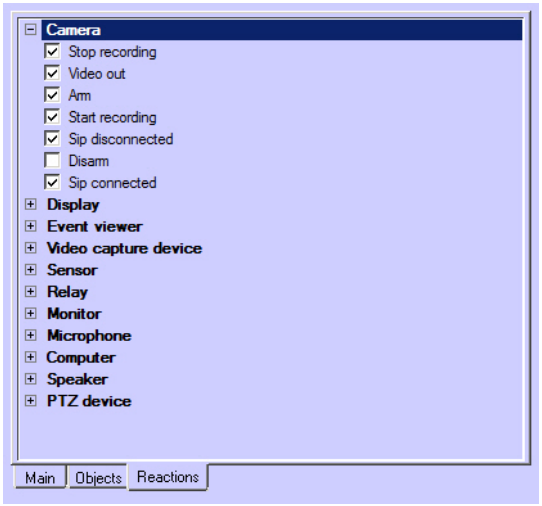
The settings panel of the **User permissions** object is shown in the figure.



The **Main** tab



The **Objects** tab



The **Reactions** tab

Elements of the settings panel of the **User permissions** object are described in the table.

№	Parameter	Method for setting the parameter value	Parameter description	Symbols us
1	The **ID** field*	Automatically	Displays the identification number of the **User permissions** object in the system	Sequence of
2	The **Name** field*	Enter the value in the field	Sets the name of the **User permissions** object in the system	Latin, Cyrilli characters
3	The **Disable** checkbox	Set the checkbox	Defines the status of the **User permissions** object (enabled or disabled) in the system	Boolean typ
The **Access to archive** group				
4	The **Depth __ last hours** field	Enter the value in the field	Sets the number of last hours of video archive that can be viewed	Nonnegative
5	The **Since last access** checkbox	Set the checkbox	Sets the time to define the archive depth	Boolean typ
The **Access to backup archive** group				
6	The **Depth __ last hours** field	Enter the value in the field	Sets the number of last hours of backup archive that can be viewed	Nonnegative
7	The **Since last access** checkbox	Set the checkbox	Sets the time to define the backup archive depth	Boolean typ
No group				
8	The **Log out if inactive for __ minutes** checkbox and field	Set the checkbox, enter the value in the field	Sets the time period (in minutes) when the operator is inactive - at the end of this period the session is to be terminated	Boolean typ
9	The **Connection to AD** button	Click the button	Opens a dialog box to configure the connection between the *Intellect* user permissions and Windows Active Directory security groups	-
10	The **ONVIF** dropdown list	Select the value in the list	Sets user rights to use the ONVIF Server	Supported t permissions
11	The **Import rights** button	Click the button	Configure import of user permissions settings from several other **User permissions** objects.	-
The **Configuring** group				

12	The **Shutdown with operator password** checkbox	Set the checkbox	Allows shutting down Intellect using the password of the authorized User	Boolean typ
13	The **Shutdown with administrator password** checkbox	Set the checkbox	Allows shutting down Intellect using the password of the Administartor	Boolean typ
14	The **Disable hiding system UIs** checkbox	Set the checkbox	Allows hiding interfaces in Intellect	Boolean typ
15	The **Disable re-registration** checkbox	Set the checkbox	Allows changing the user in Intellect	Boolean typ
16	The group of **Tabs*** checkboxes	Set the checkbox	Specifies the tabs of the System settings dialog box that can be accessed when the User gets the corresponding rights	Boolean typ
The **Archive** group				
17	The **Allow removing video archive files** checkbox	Set the checkbox	Defines whether video archive files can be removed from the Monitor interface	Boolean typ
18	The **Allow protecting files from overwriting** checkbox	Set the checkbox	Sets possibility of rewrite protecting of files	Boolean typ
19	The **Allow removing file protection** checkbox	Set the checkbox	Sets possibility to disable rewrite protection of files	Boolean typ
20	The **Allow viewing hidden archive** checkbox	Set the checkbox		Boolean typ
21	The **Allow checking "hidden" archive** checkbox	Set the checkbox		Boolean typ
22	The **Allow unchecking "hidden" archive** checkbox	Set the checkbox		Boolean typ
The **Export** group				
23	The **Allow frame export** checkbox	Set the checkbox	Sets possibility to export archive frames	Boolean typ
24	The **Allow frame printout** checkbox	Set the checkbox	Sets possibility to print archive frames	Boolean typ
25	The **Allow video clip export** checkbox	Set the checkbox	Sets possibility to export video archive records	Boolean typ
The **Objects** tab				

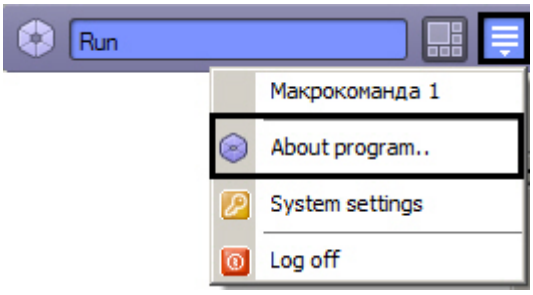
26	The **list of system objects***	Set the checkboxes	Displays the objects created in the system and allows setting the administration and monitoring rights	-
The **Reactions** tab				
27	The **list of system object reactions***	Set the checkboxes	Sets the list of system object reactions that Operator can run	Boolean typ

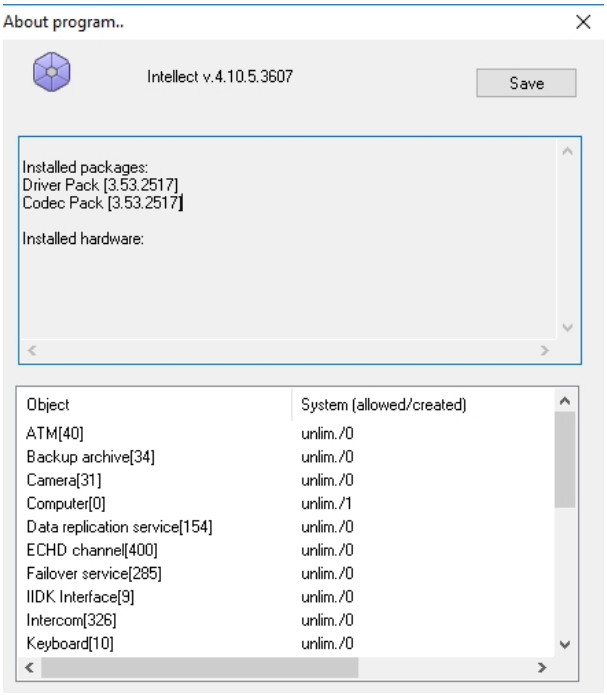
* The name of the object is not displayed on the settings panel

13.1.3 Information about program

The information about 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 **Execute** 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).

13.2 Appendix 2. Relevant information on using Windows operating system

13.2.1 Working with Windows OS registry

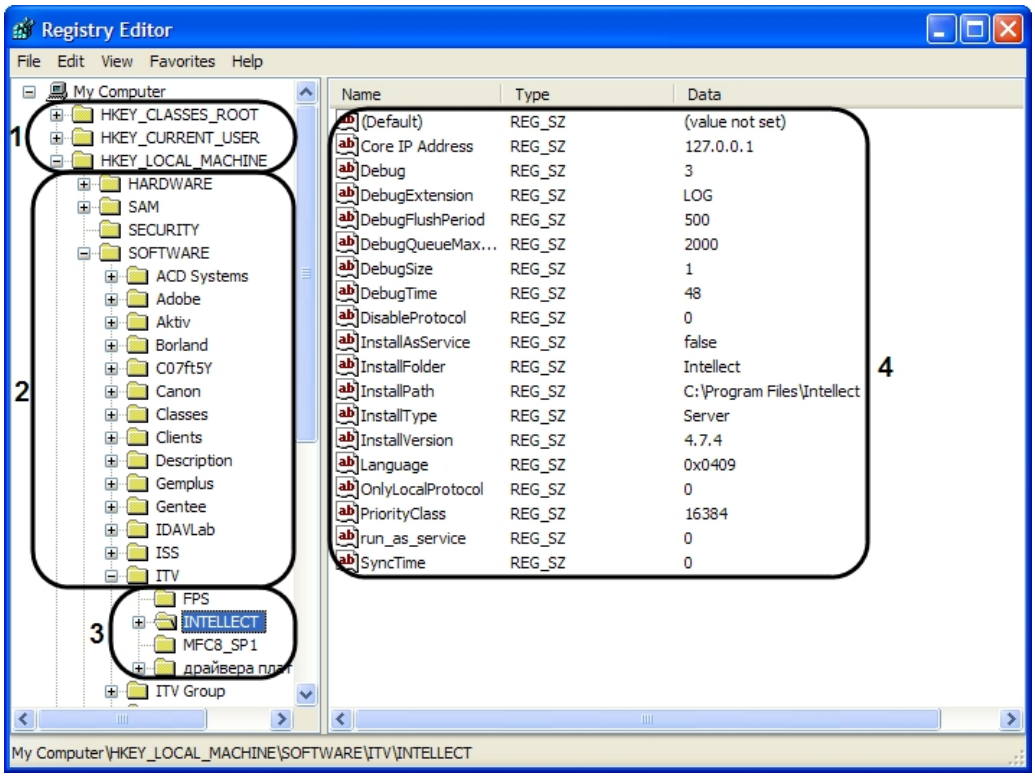
13.2.1.1 General information about Windows OS registry

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.

The registry can be edited by the regedit.exe program included in the standard set of service programs in Windows. The information is stored in two hidden files in a Windows folder: system.dat and user.dat . The registry is a hierarchical tree structure, the branches of which constitute the keys that contain values or subkeys. The registry has six main branches described in the table.

Branch name	Description
HKEY_CLASSES_ROOT	Contains the information of software configuration, including the links from file extensions to programs, drag-and-drop parameters, printer settings and COM port settings.
HKEY_CURRENT_USER	Contains user settings of the system. This section is created and populated from the HKEY_USERS section upon user logon.
HKEY_LOCAL_MACHINE	Contains the parameters of the computer, its drivers and other hardware. The data in this section is shared by all users of the computer.
HKEY_USERS	Contains the information about all users registered on the computer. There are two types of parameters – shared by all users, and specific to each user.
HKEY_CURRENT_CONFIG	Contains the information about current hardware configuration.
HKEY_DYN_DATA	Points to a subsection in the HKEY_LOCAL_MACHINE section related to Plug and Play devices. This section changes upon adding or removing devices to or from the computer.

The branch structure is visually similar to the structure of the user folders, allowing nested branches. Figure shows the main elements of the registry.



1. Branches;
2. Keys;
3. Subkeys;
4. Parameters;

Each parameter has three components: name, type and value. A key can have only one parameter with no name, which serves as a default value of the key. It is recommended to assign meaningful names to parameters, indicating its purpose.

The values in the registry can be of particular types. The most commonly used types are described in the table.

Data type	**Description**	**Purpose**
REG_DWORD	4 bytes in hexadecimal or decimal format.	Many service or driver parameters are of this type. Example: 0x00000240(576) — decimal value is given in parenthesis.
REG_BINARY	Binary data of an arbitrary form. Maximum length – 16 bytes.	Most data on hardware components is stored as binary. In the regedit.exe window it is displayed in hexadecimal format, for example 01 00 00 00.
REG_SZ	A string ending with a null symbol.	Example: C:\Windows
REG_MULTI_SZ	Multi-line text. An array of strings ending with a null each. An array itself ends with two nulls.	Lists and other records in readable format are of this type. The records are separated by commas and other symbols in the editor.
REG_EXPAND_SZ	Data string of variable length ending with a null.	Undisclosed links to environment variables are of this type.
REG_FULL_RESOURCE_DESCRIPTOR	A sequence of nested arrays.	This type is designed for storing the list of device resources and drivers.

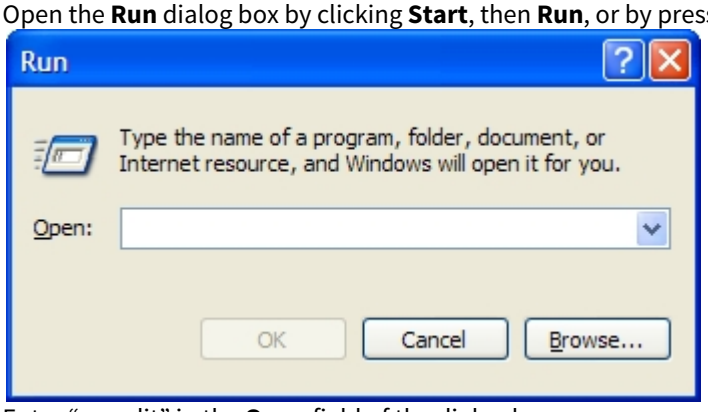
13.2.1.2 Using the registry editor

13.2.1.2.1 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.

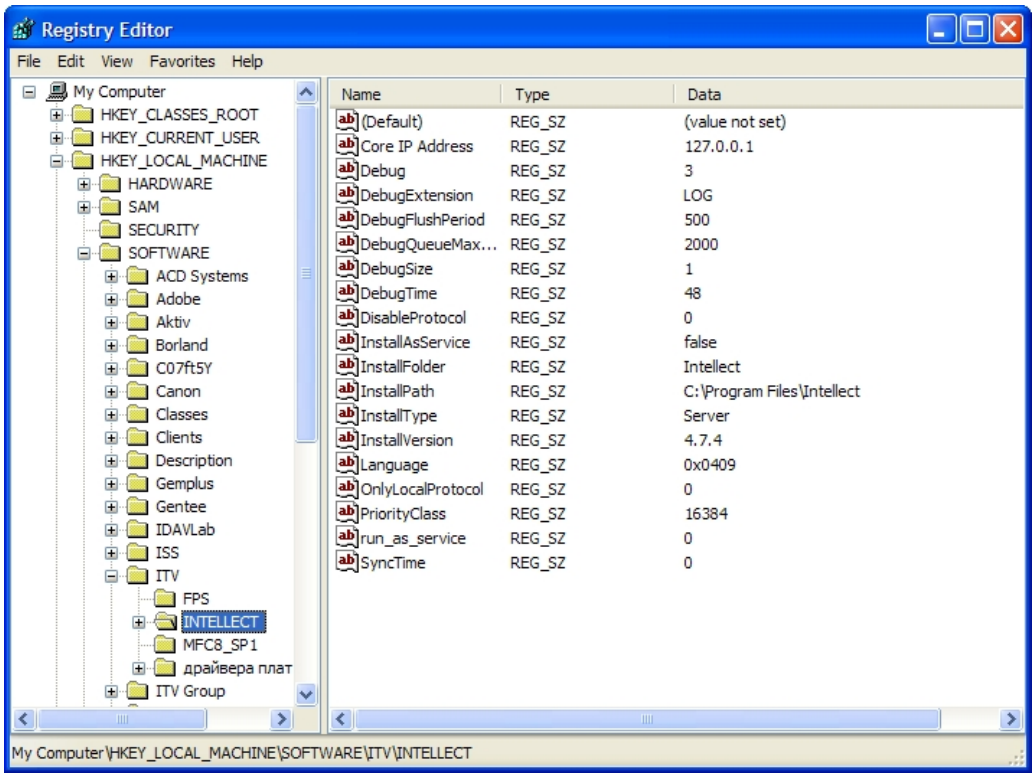
To start the editor, do the following:

1. Open the **Run** dialog box by clicking **Start**, then **Run**, or by pressing WIN+R keys on the keyboard.

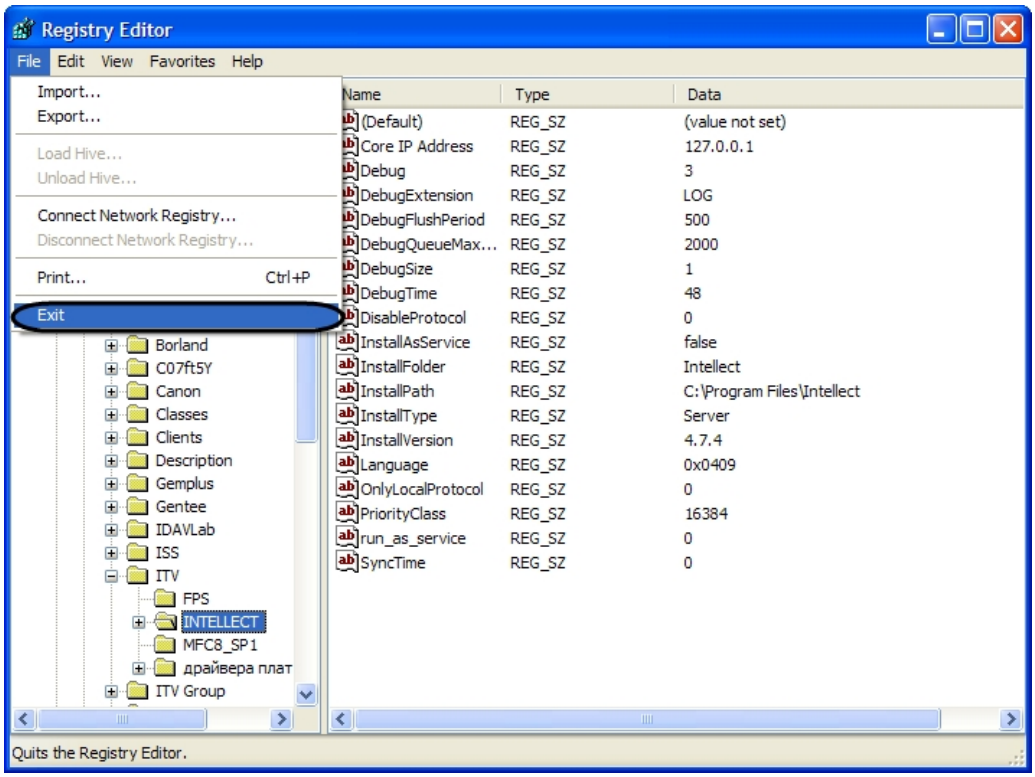


2. Enter “regedit” in the **Open** field of the dialog box.
3. **Click OK.**

The registry editor window will open.

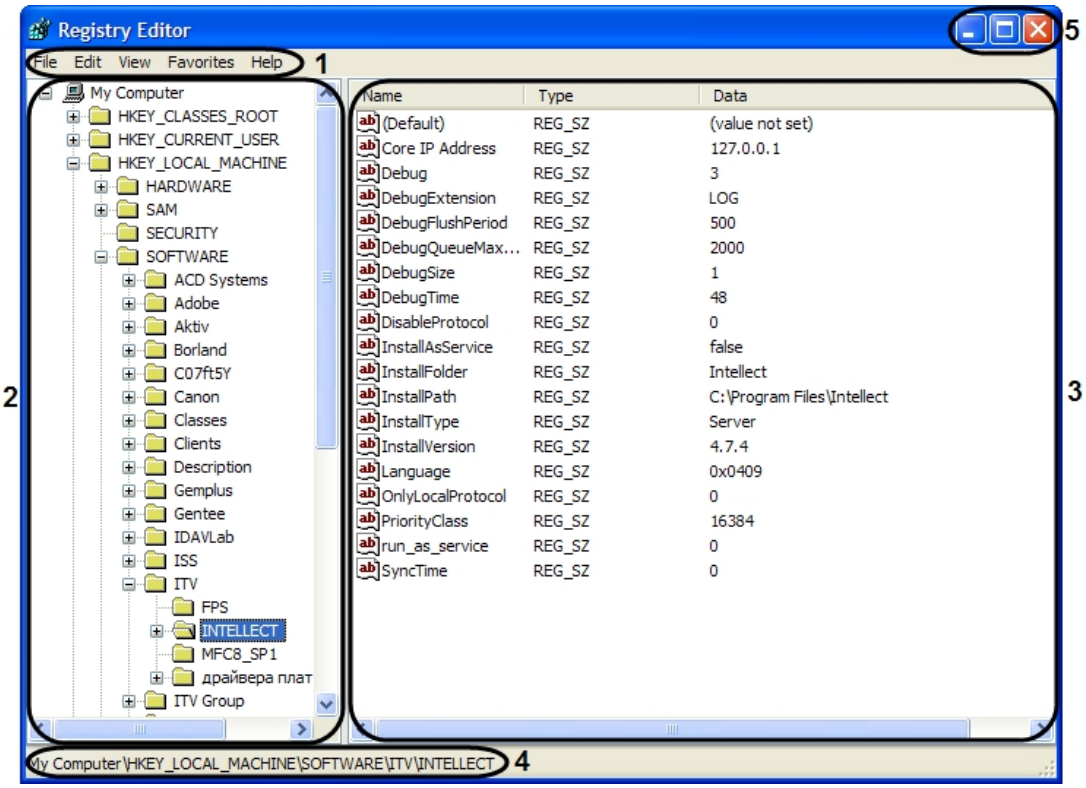


To close the registry editor, click the button, or select **Exit** from File menu.



13.2.1.1.2.2 Interface elements of the registry editor

Figure shows the elements of the registry editor window.



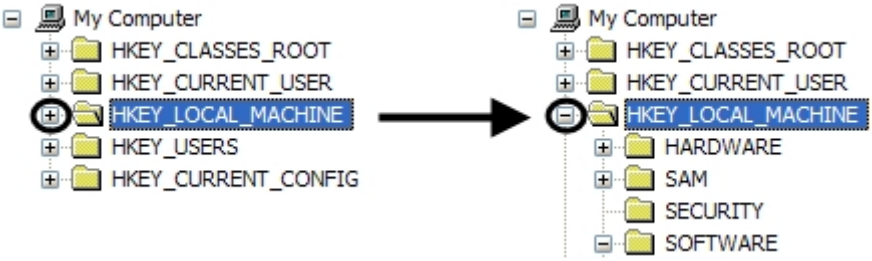
1. Main menu. Contains the commands and settings.
2. Registry tree. Displays the structure of the registry.
3. Parameters table. Displays the parameters of the selected key.
4. Information line. Displays the pathname of the selected object.

5. Control buttons (left to right): Minimize, Restore, Close.

13.2.1.2.3 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.

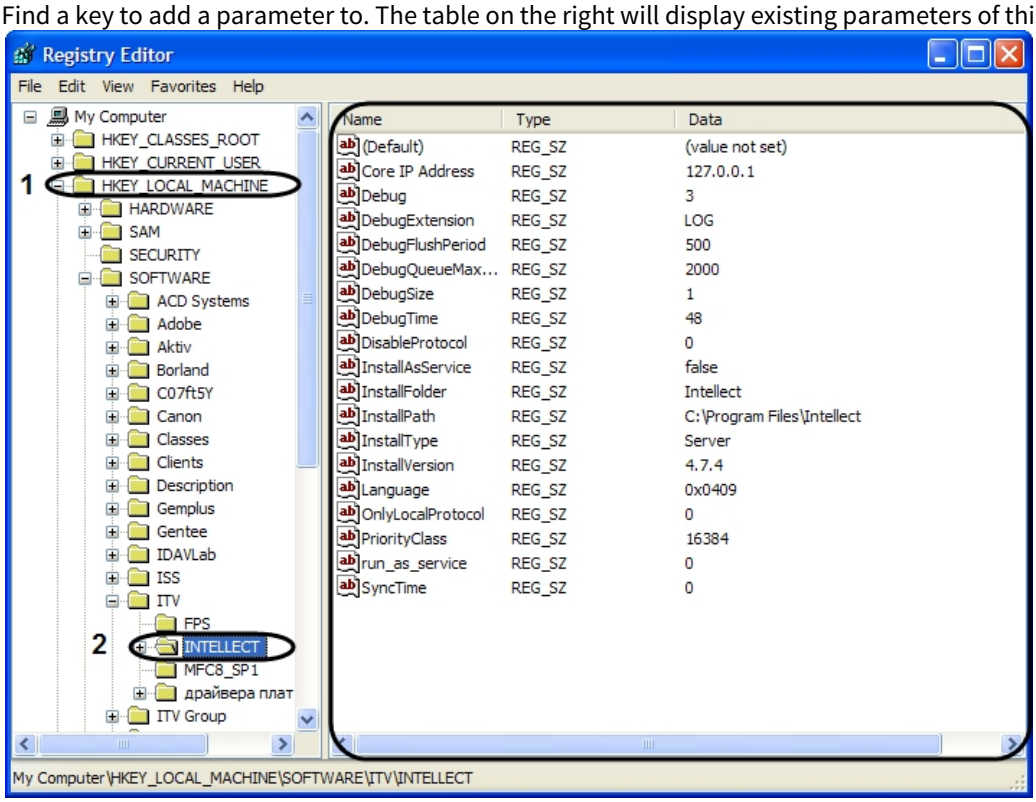


To contract the branch, click the minus icon next to it.

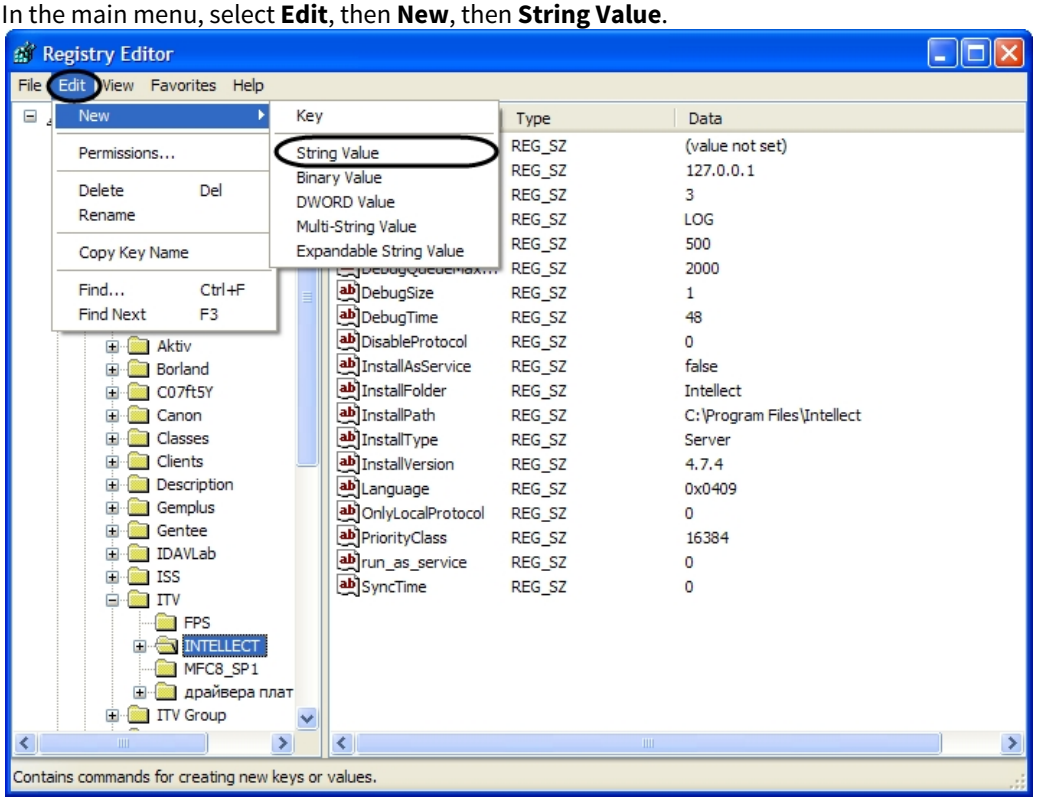
13.2.1.3 Adding string parameters to the registry

To add a string parameter to a key, do the following:

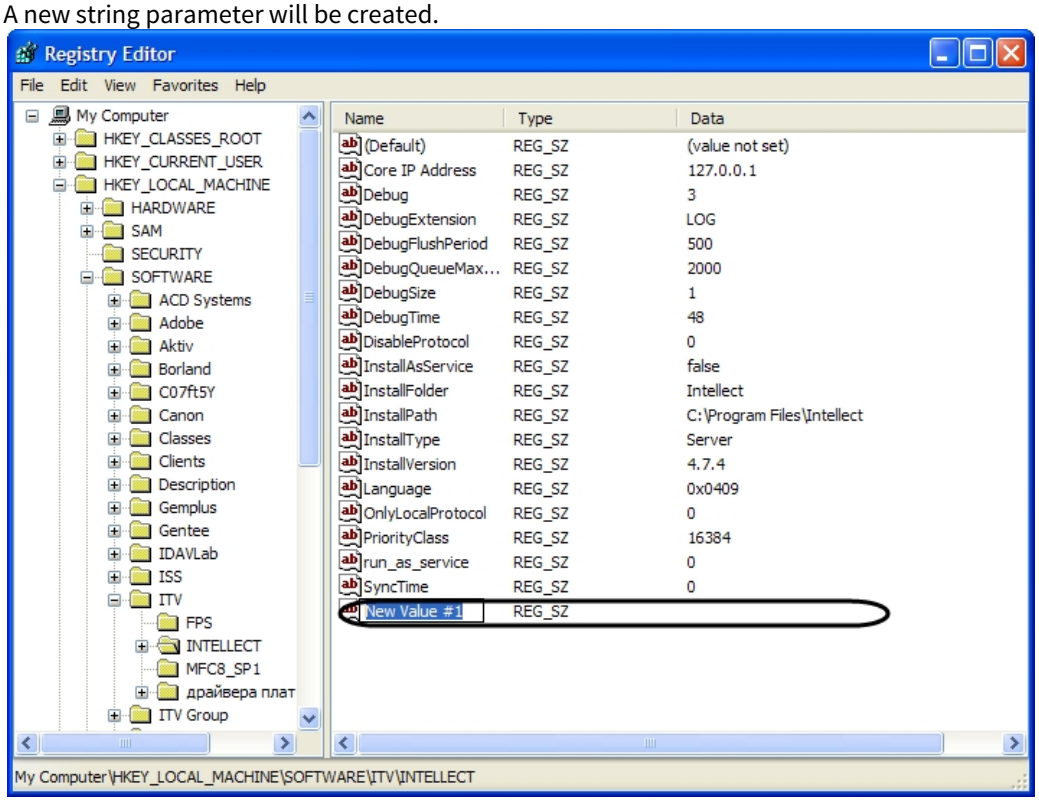
1. Select the required branch and click the plus icon. All folders (keys) inside this branch will be displayed.
2. Find a key to add a parameter to. The table on the right will display existing parameters of this key.



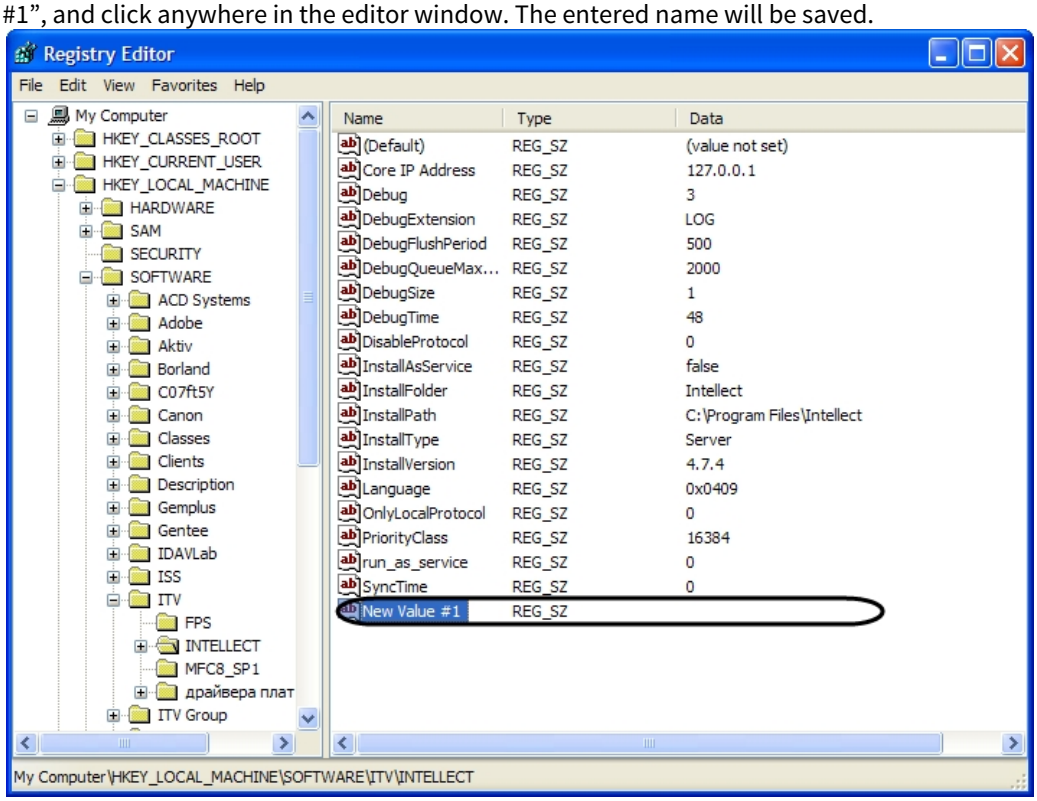
3. In the main menu, select **Edit**, then **New**, then **String Value**.



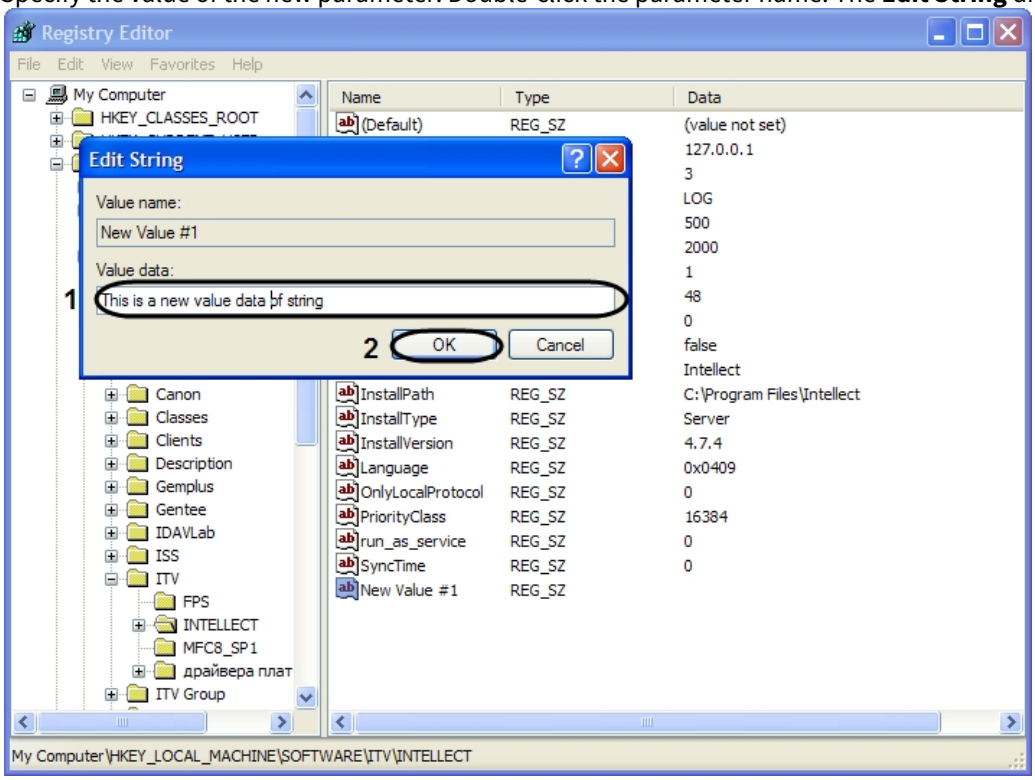
4. A new string parameter will be created.



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.

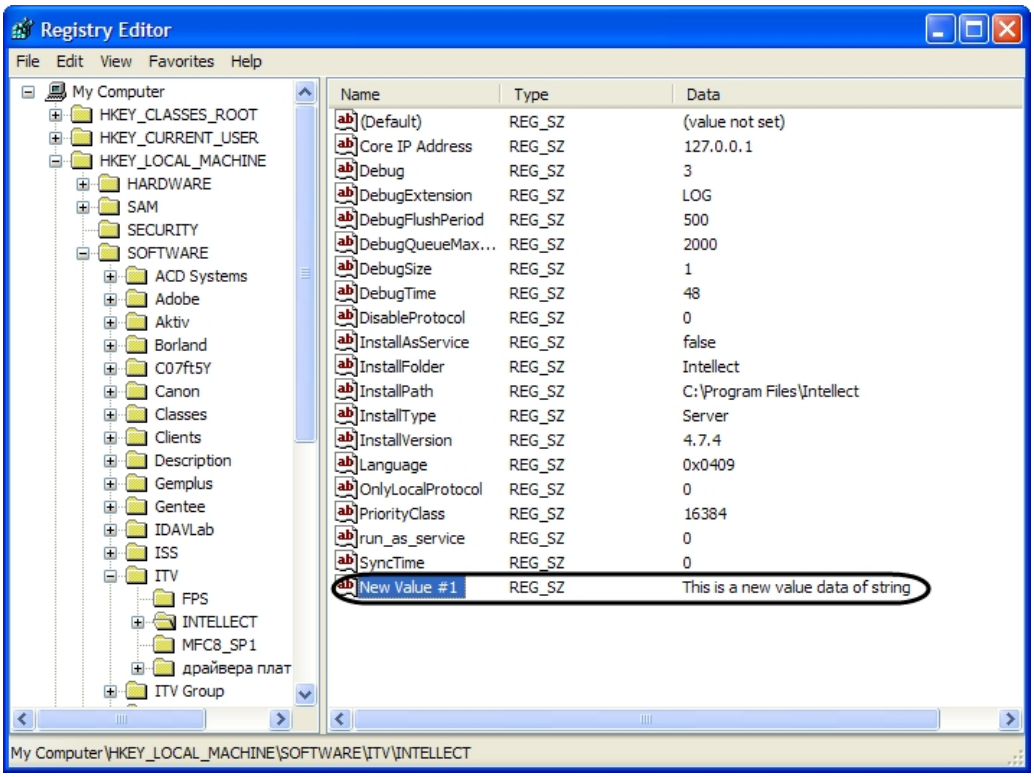


6. Specify the value of the new parameter. Double-click the parameter name. The **Edit String** dialog box will open.



Enter the value into the **Value Data** field (1) and click **OK** (2).

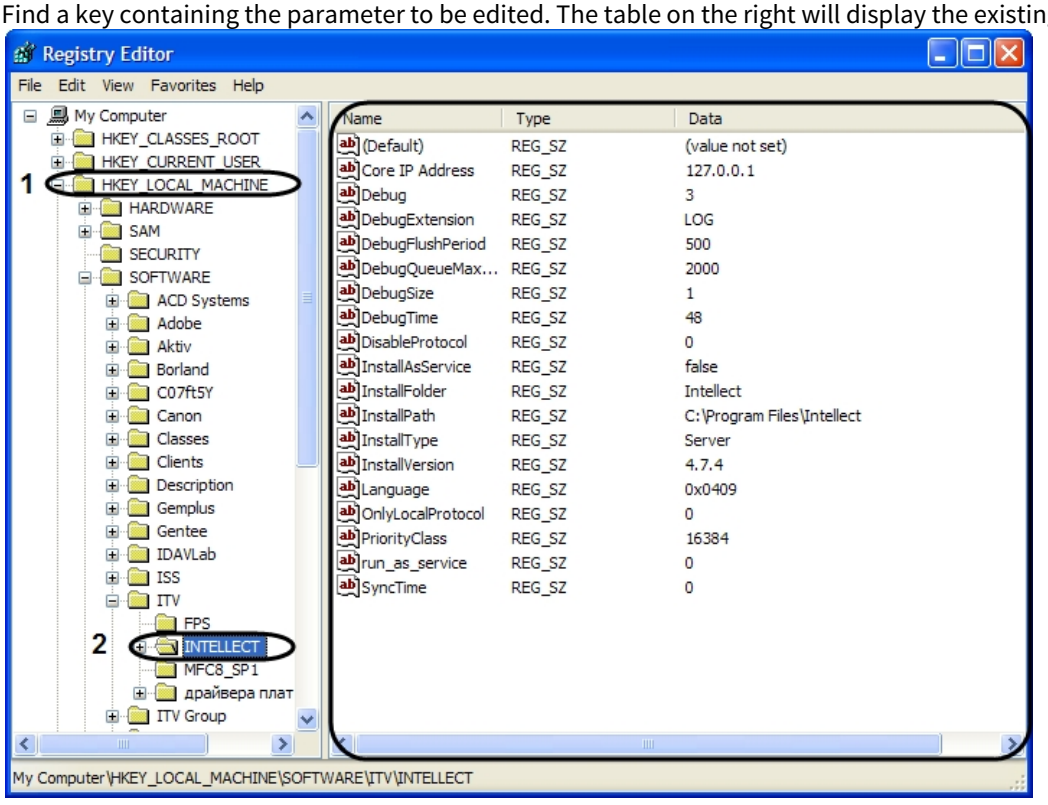
A string parameter with a specified value will be created. To edit the value, repeat step 5.



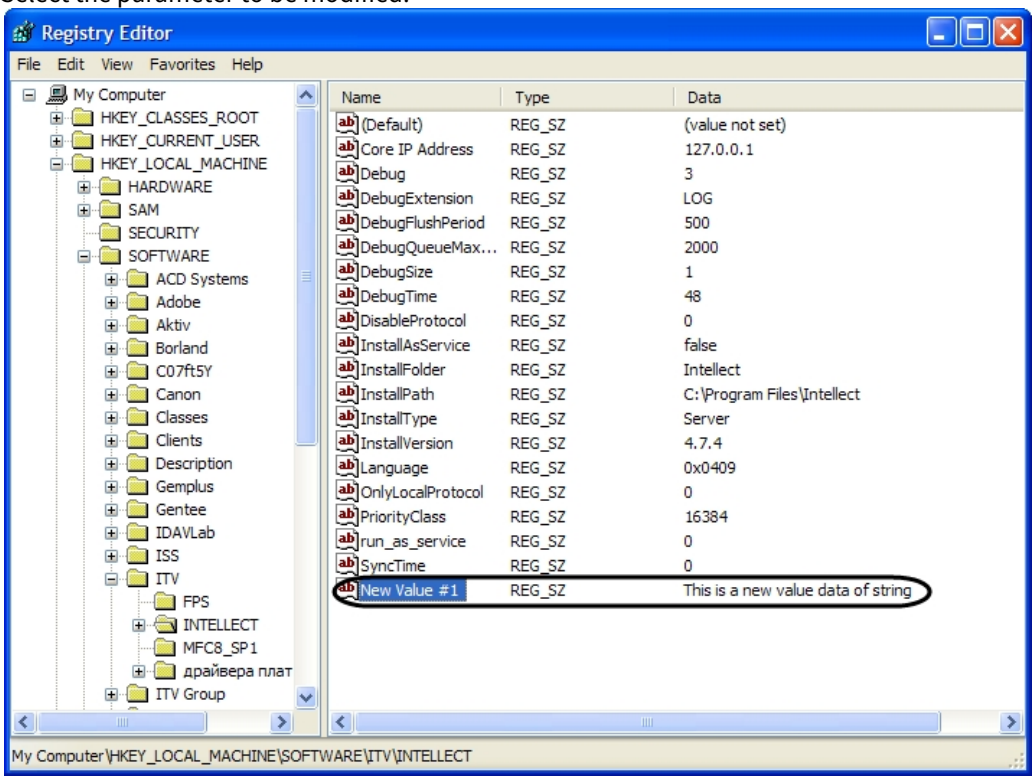
13.2.1.4 Modifying the value of string parameters in Windows OS registry

To modify the value of a string parameter, do the following:

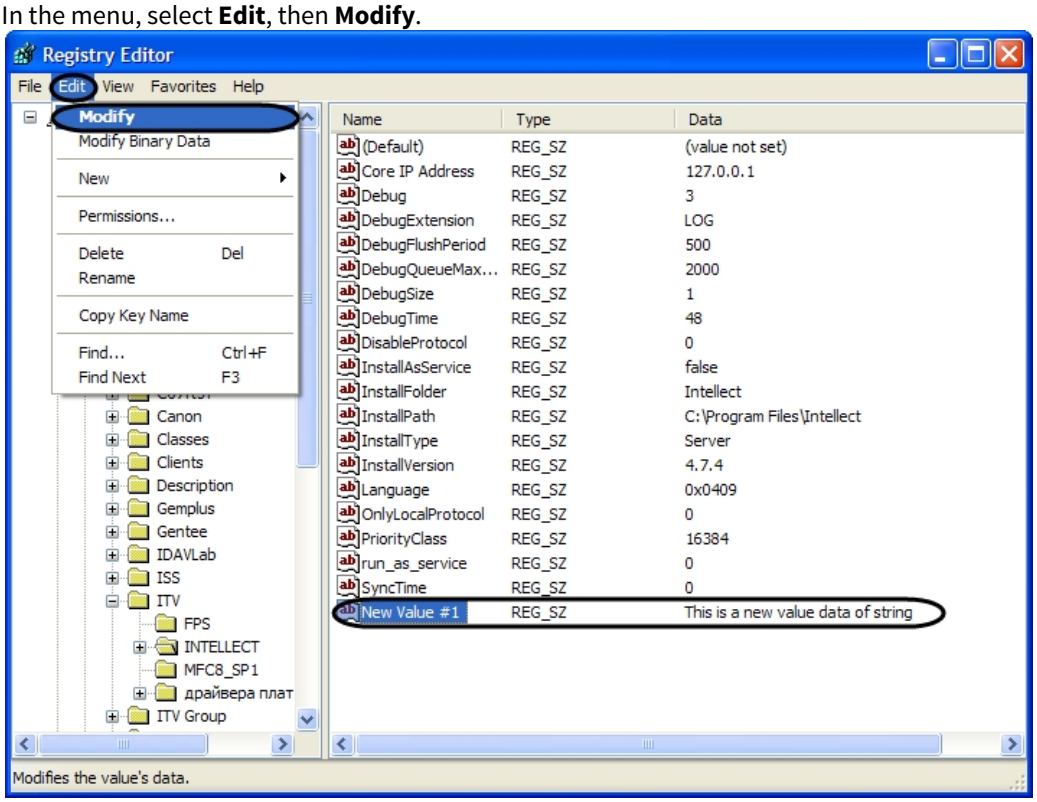
1. Select the required branch and click the plus icon. All folders (keys) inside this branch will be displayed.
2. Find a key containing the parameter to be edited. The table on the right will display the existing parameters of this key.



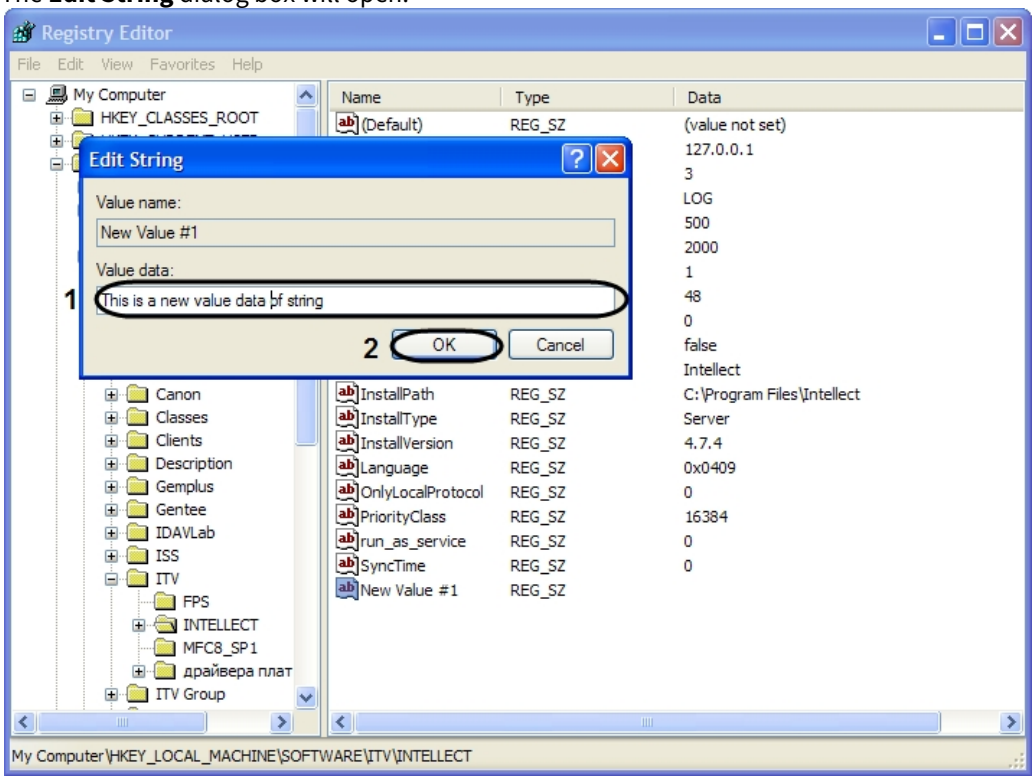
3. Select the parameter to be modified.



4. In the menu, select **Edit**, then **Modify**.

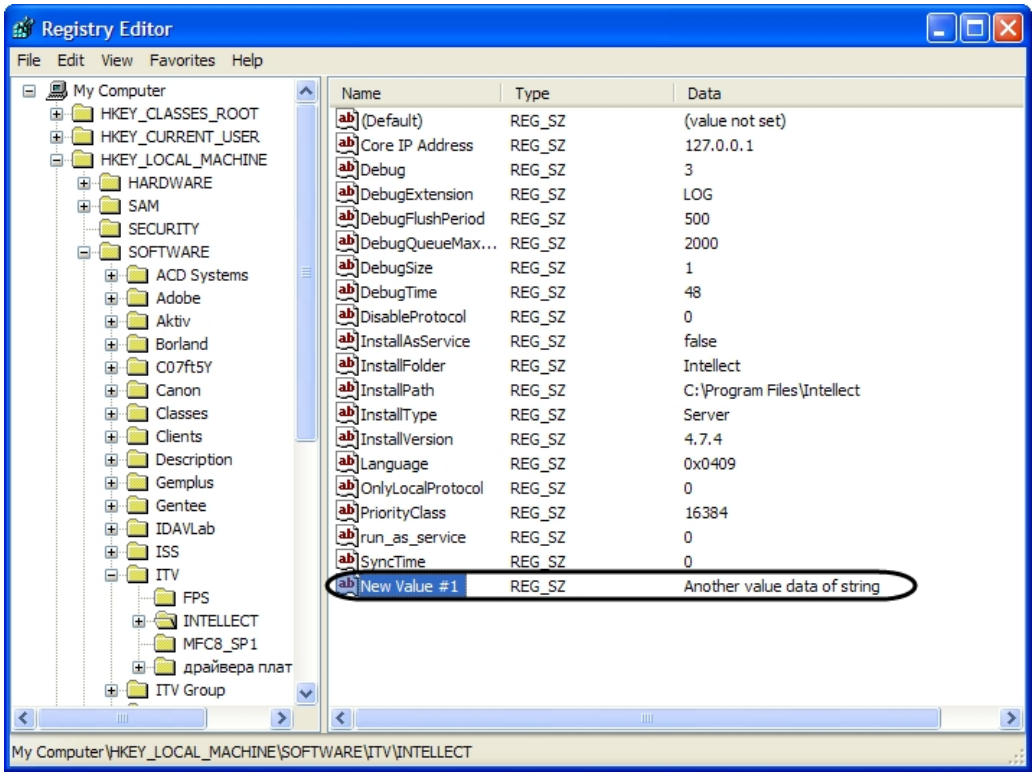


The **Edit String** dialog box will open.



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.

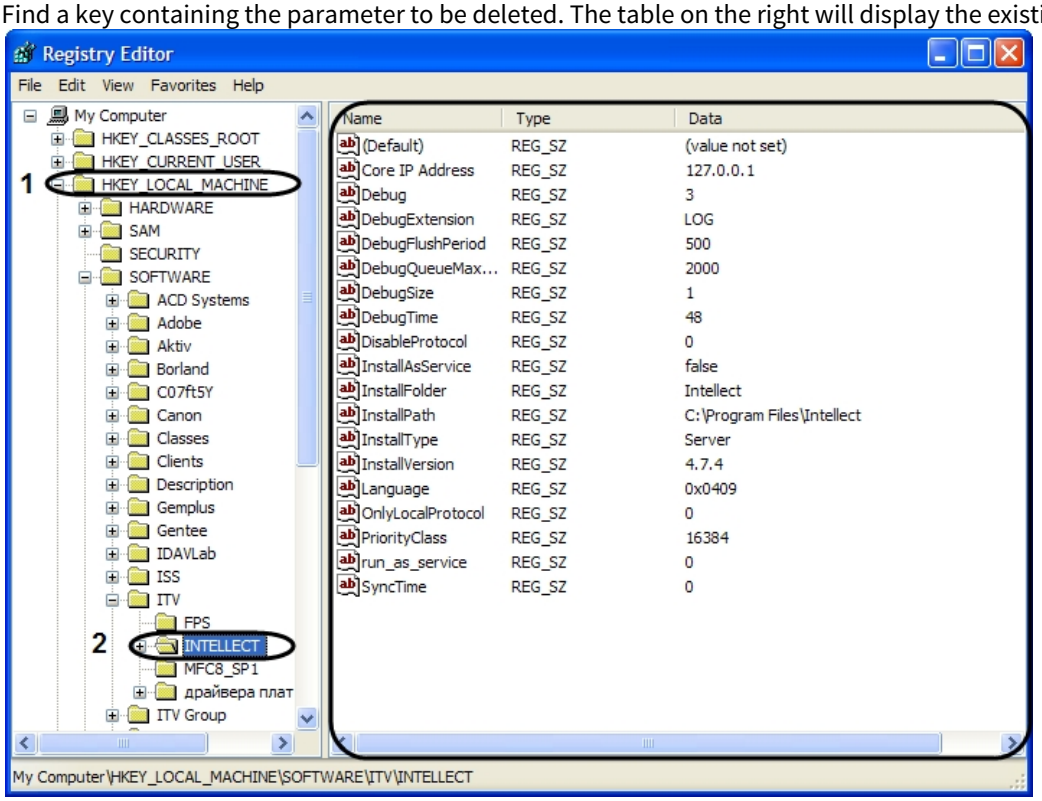


13.2.1.5 Deleting parameters from the Windows OS registry

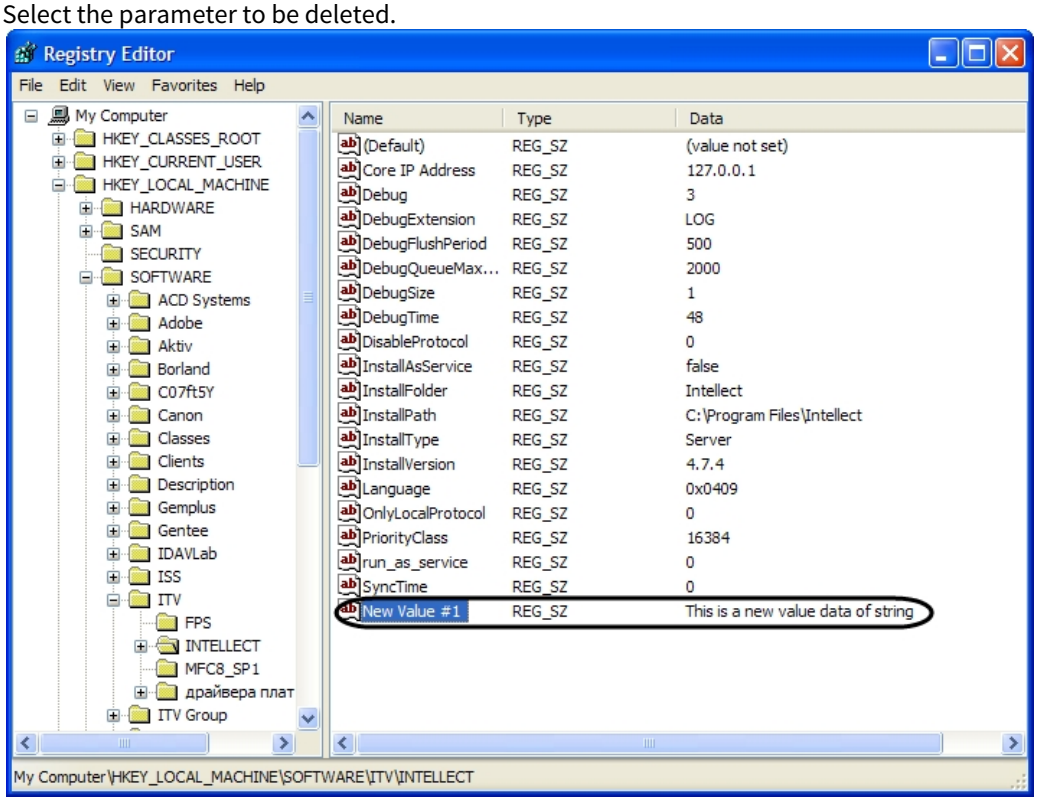
To delete a string parameter from the registry, do the following:

1. Select the required branch and click the plus icon. All folders (keys) inside this branch will be displayed.

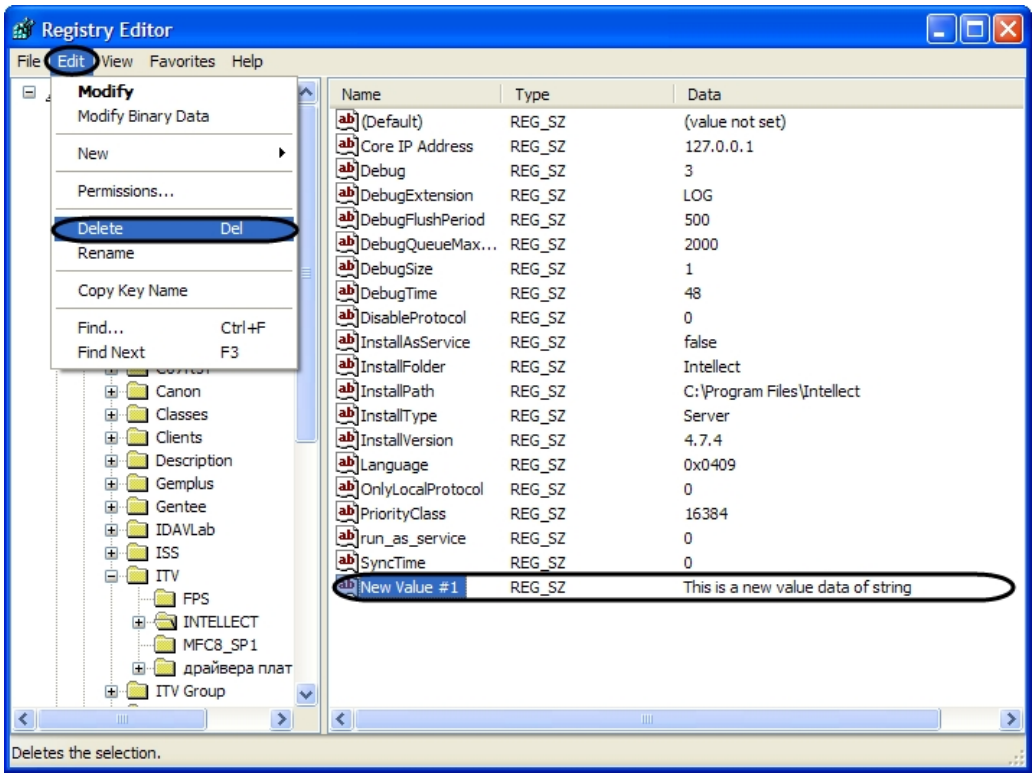
2. Find a key containing the parameter to be deleted. The table on the right will display the existing parameters of this key.



3. Select the parameter to be deleted.



4. In the menu, select **Edit**, then **Delete**.



The string parameter will be deleted from the registry.

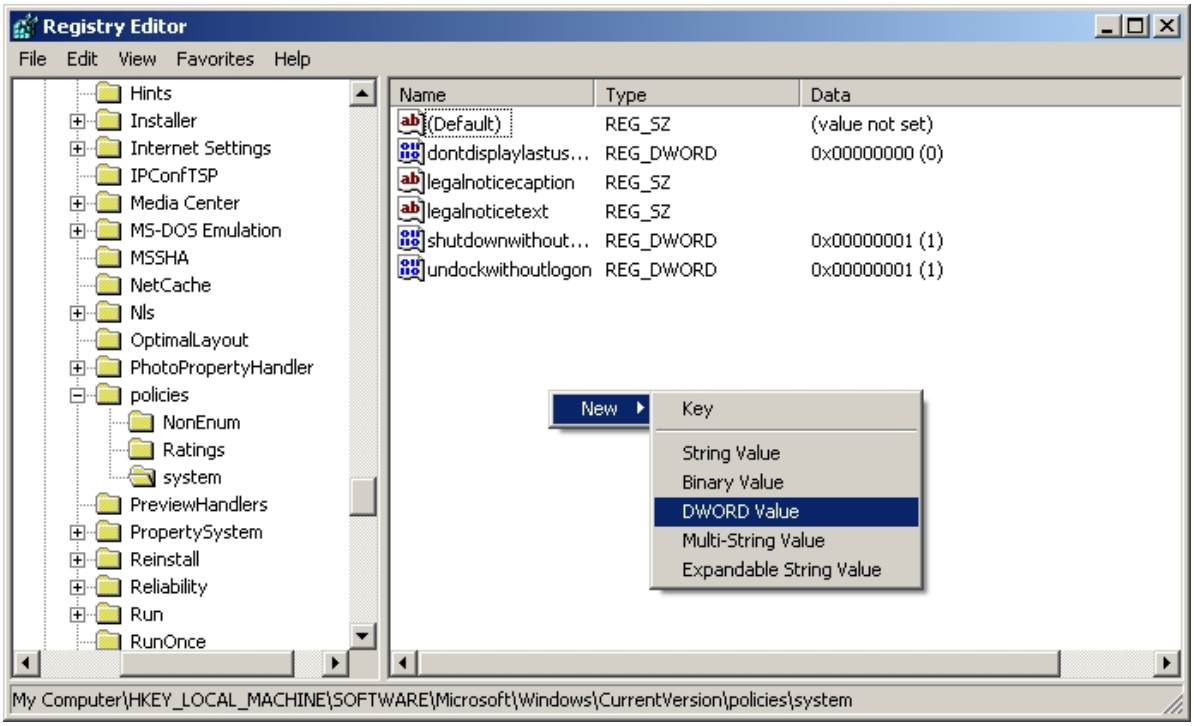
> **Note.**
>
> The **Edit** menu can also be opened as a context menu by right-clicking the required parameter.

13.2.1.6 Configuring network drives visibility when UAC is enabled in Windows OS

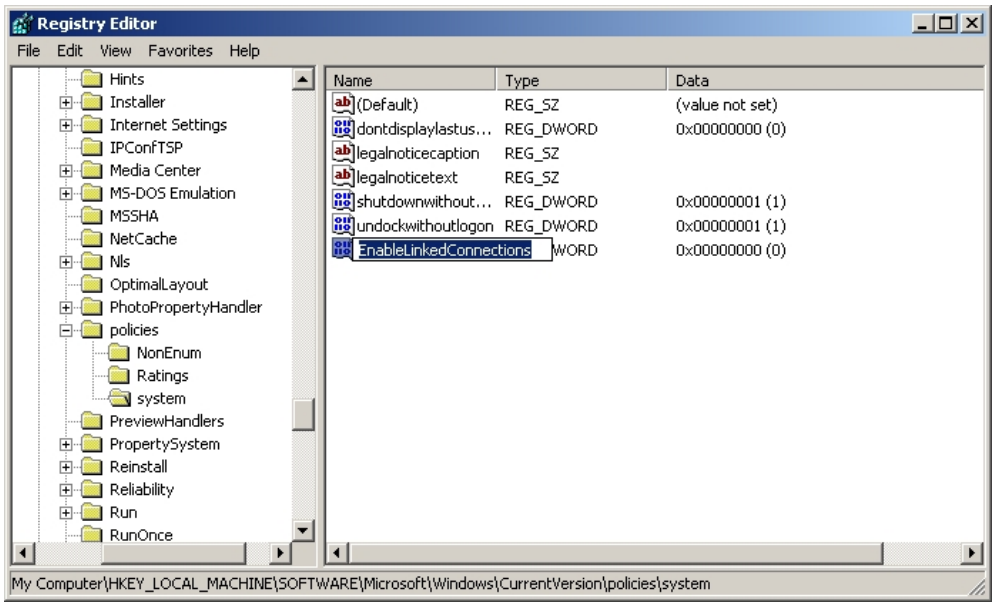
To configure archive storing to network drives when UAC is enabled in *Intellect,* create the EnableLinkedConnections key in the registry. For this do the following::

1. Open subsection of HKEY_LOCAL_MACHINE \ SOFTWARE \Microsoft \Windows \CurrentVersion \Policies \System registry.

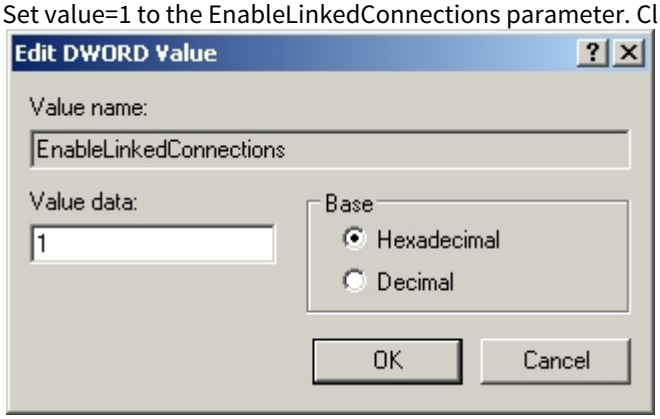
2. Create a new DWORD value.



3. Set EnableLinkedConnections name to the new value and click Enter.



4. Set value=1 to the EnableLinkedConnections parameter. Click the **OK** button.



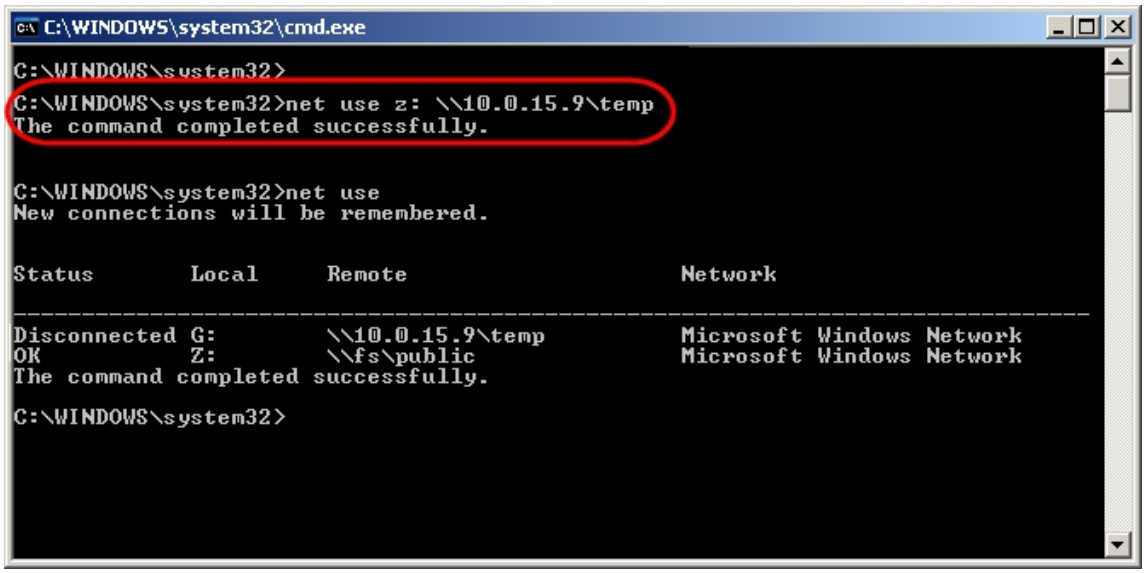
5. Exit the registry editor and restart your computer.

The EnableLinkedConnections registry key is created.

13.2.2 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:

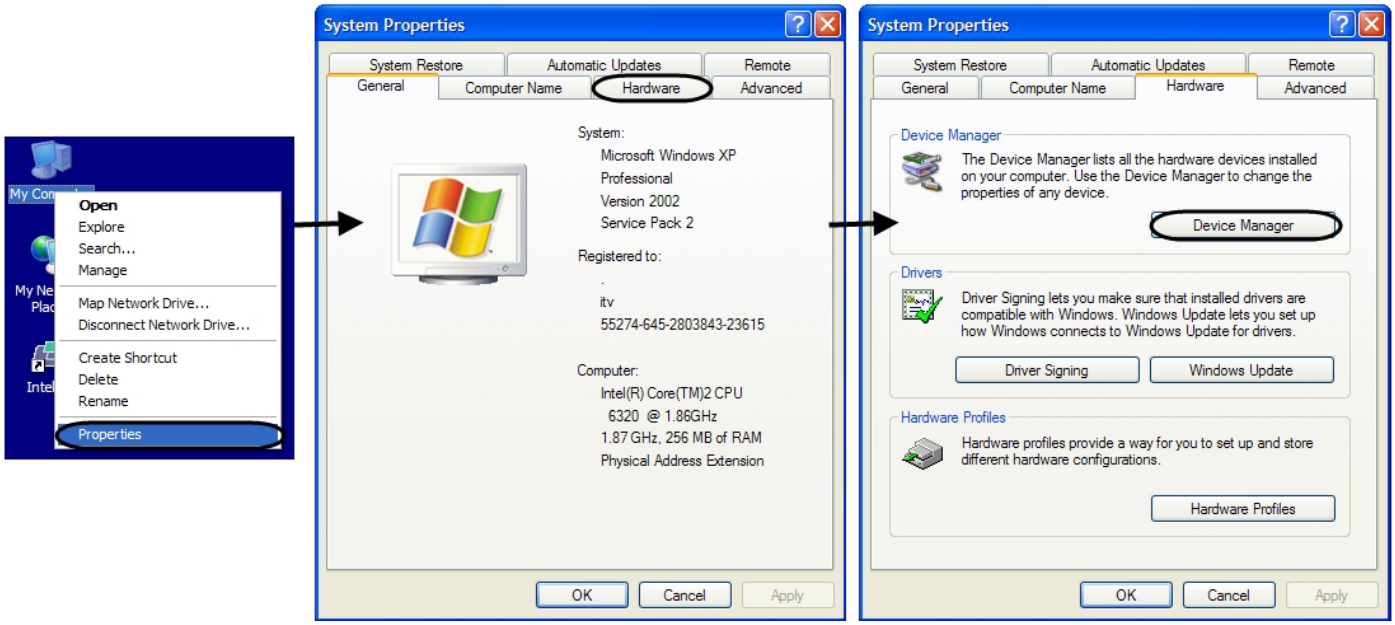
1. Call a command prompt. Select **Run** in **Start** menu and enter «cmd» in entry field and click **OK**.
2. Enter «net use Z: \\Address\Folder» in the command prompt; **Z** is letter of Roman alphabet that will represent net disk in the system, **Address** is IP-address of net disk, **Folder** is a name of folder.



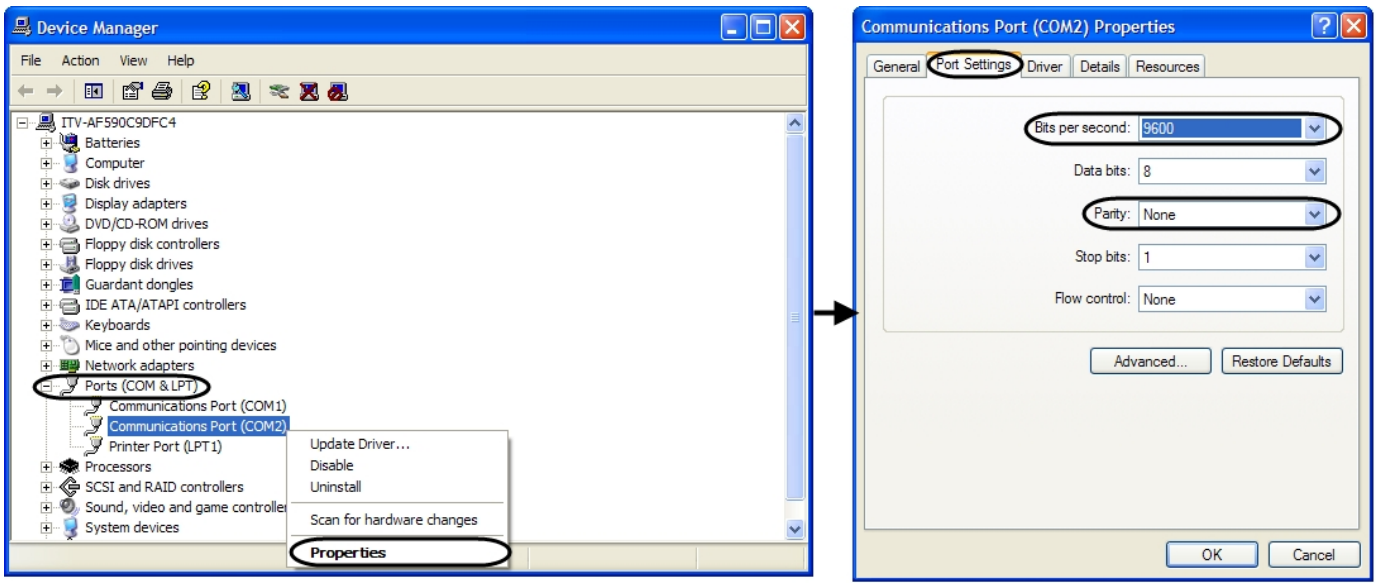
Net disk appears in *Intellect* settings after beeing connected.

13.2.3 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.



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

13.2.4.1 General information on Intellect™ operation as a 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 up such applications as Windows OS and various other applications installed on the Server).

> **Note.**
>
> In INTELLECT™ installed as a Server user can log off INTELLECT™ and service remains started and INTELLECT™ restart is possible.

64-bit modules are not available when installing *Intellect* as a Service. 32-bit modules will be started after *Intellect* is installed as a Service. See also Configuring of using 64-bits modules.

While installing the *Intellect* software as a service 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 the Windows OS means. Users in the IntellectUsers group have the rights to configure the *Intellect* as a Service and access its interfaces. When it is necessary to arrange the access to the *Intellect* as a Sevice interfaces for a large number of users, it may be convenient to use the Active Directory (AD) - see Configuring INTELLECT™ as a Service to work with Active Directory (AD).

> **Note.**
>
> To start *Intellect* as another user admin rights must be assigned to this user or rights are to be advanced as described in the OS settings for correct operation of Remote Admin Workstation or Server section.

> **Note.**
>
> Detailed information about user groups and about working with them see in the http://windows.microsoft.com web-site.

When the user from the IntellectUsers group enters a system, the Intellect software restarts under this user. If the Intellect software launch under the user name is not needed, i.e. the Intellect software is to be launched under the SYSTEM user name, restart is to be disabled using the Tweaki.exe utility – see The Settings panel of the Windows section part.

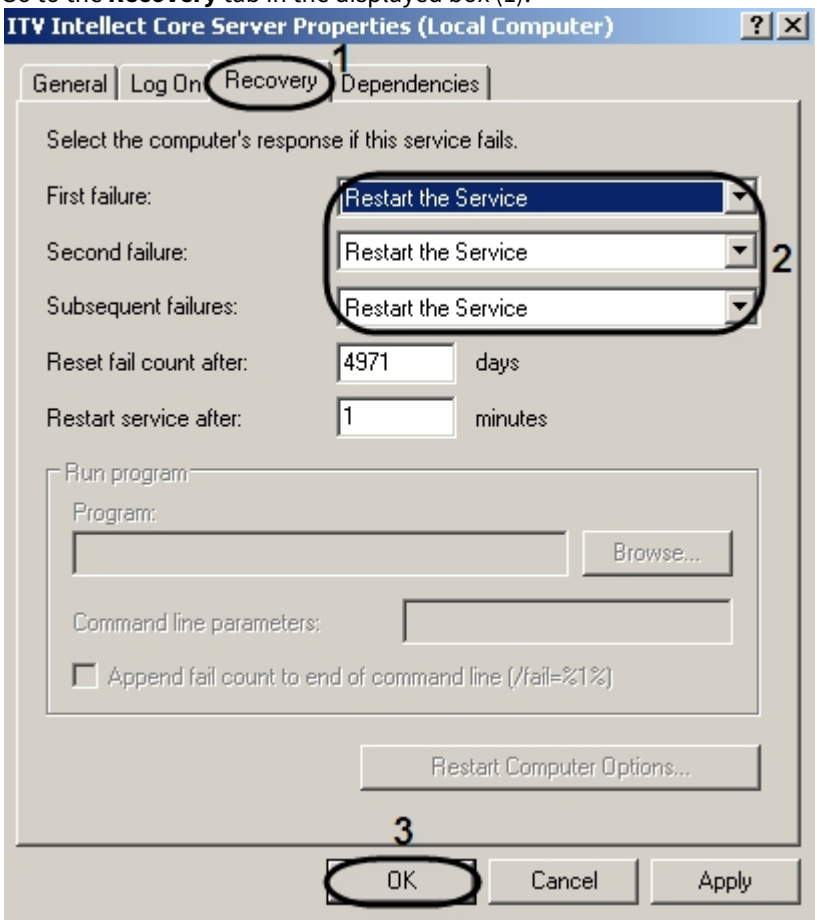
> **Note.**
>
> When INTELLECT™ is started under some user (not under SYSTEM), then if user is changed and the first user has not logged off, INTELLECT™ will not restart – it will be started under the first user.

If INTELLECT™ is installed as a Service and database connection is performed via Windows account information, then for operation under the user different from the user who installed INTELLECT™ this user is to have SQL server permissions.

13.2.4.2 Configuring the restart of the ITV Intellect Core Server service

If the ITV 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).



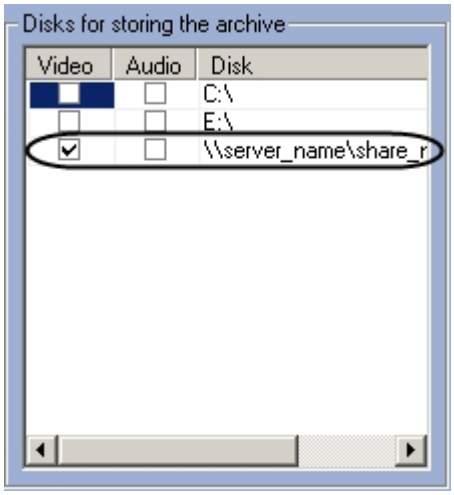
6. In the corresponding drop-down lists select the actions to be performed in case of the first, second and subsequent system failures (2).
7. To save the changes, click the **OK** button (3).

The restart of the ITV Intellect Core Server service is now configured.

13.2.4.3 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.

13.2.4.4 Enabling INTELLECT™ as a Service startup

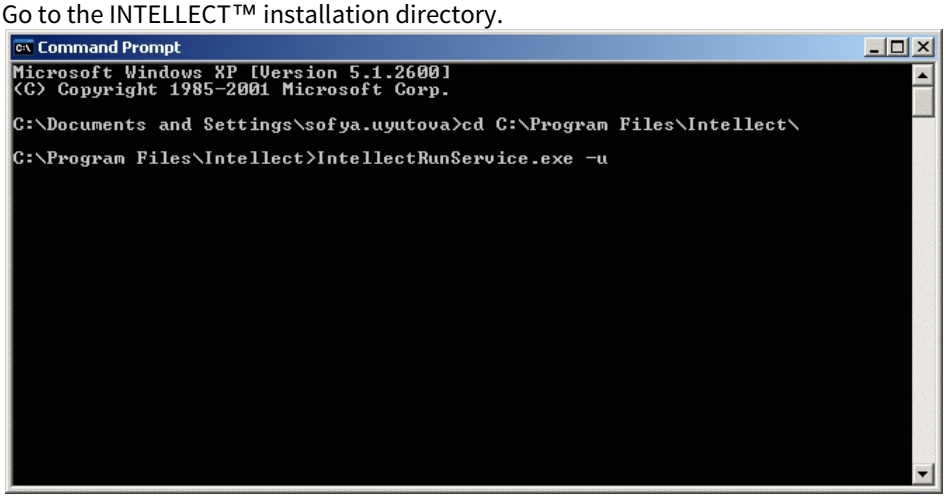
If INTELLECT™ was not installed as a Service and you want to make it such, do one of the following:

1. Reinstall INTELLECT™ and set the **Install Intellect as a service** checkbox (see Installing and removing INTELLECT™ software section).
2. Use the command prompt. In this case do the following:
   a. Run the Windows cmd.exe command prompt:
      i. Under the administartor account with disabled UAC.
      ii. As administrator under the administartor account or user account with enabled UAC.
   b. Go to the INTELLECT™ installation directory.
   c. Run "IntellectRunService.exe -i" command in the Windows command prompt. As a result the **ITV Intellect Core Server** service is registered in the system.

13.2.4.5 Disabling INTELLECT™ as a Service startup

To disable the startup of INTELLECT™ as a Server, do the following:

1. Restart INTELLECT™. In this case do the following:
    a. Remove INTELLECT™ (see Removing INTELLECT™ software section).
    b. Install INTELLECT™ without setting the Server checkbox (see Installing INTELLECT™ software section).
2. Use the command prompt. In this case do the following:
    a. Run the Windows cmd.exe command prompt:
        i. Under the administartor account with disabled UAC.
        ii. As administrator under the administartor 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.

13.2.4.6 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.

13.2.5 The list of TCP ports used in INTELLECT™

On the page:

- Intellect base
- ATM-Intellect and Monitoring
- Auto-Intellect
- Detector Pack
- Face-Intellect
- 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
1	ARCHIVER.RUN	Archive	21007	-
2	ARCHPANEL.RUN	Backup archive panel	22118	-
3	ATM	ATM	21090	-
4	AUDIO.RUN	Microphone	21008	-
5	AUDIO.RUN	Microphone	20903	VIDEO.RUN

6	AUDIO.RUN	Microphone	20904	VIDEO.RUN
7	AUDIO.RUN	Backup audio archive	20911	-
8	AUDIO.RUN	Audio playback card	20910 and 24008	-
9	CAM_TITLE.RUN	Captioner	21077	-
10	CAM_TITLE.RUN	Captioner	20900	VIDEO.RUN
11	CONFCHEKUTIL.RUN	Configuration check	22220	-
12	DIALOG.RUN	Operator query panel	21058	-
13	DRS.RUN	Data replication service	22175	-
14	EVENT_COUNTER.RUN	Event counter	22153	-
15	EVENT_VIEWER.RUN	Event viewer	21055	-
16	IIDK_TEST.EXE	IIDK interface	21030	-
17	JAVA.EXE	Web-server 2.0	22212	-
18	KEYB.RUN	Keyboard	21005	-
19	LDAPIMPORT.RUN	LDAP service	22252	-
20	LIVEPLAYER.RUN	Live sound switch	22199	-
21	MAP.RUN	Map	21051	-
22	MC_CLIENT.RUN	Intercom Control Monitor	22179	-
23	MESSAGE.RUN	Alarm Message Window	21056	-
24	MMS.RUN	Mail Message Service	21031	-
25	OPERATORPROTOCOL.RUN	Operator protocol	22215	-
26	PLAYER.RUN	Audio player	20910	AUDIO.RUN
27	PLAYER.RUN	Audio player	21060	-
28	SLAVE.EXE	Computer	21111	-
29	SMS.RUN	Short Message Service	21035	-

30	STREAMINGSERVER.RUN	rtsp Server	22228	-
31	TELEMETRY.RUN	Telemetry Controller	21010	-
32	TELEMETRY_PANEL.RUN	Telemetry control panel	22101	-
33	TITLEVIEWER.RUN	Search by captions	20978	CAM_TITLE.run
34	TITLEVIEWER.RUN	Search by captions	22112	-
35	VIDEO.RUN	-	20900	-
36	VIDEO.RUN	Video Capture Device	21050	-
37	VIDEO.RUN	Video stream archiever	20901	-
38	VIDEO.RUN	Video stream gate	20902	-
39	VMDADB.RUN	VMDA metadata storage	22219	-
40	VMS.RUN	Voice Message Service	21032	-
41	VNS.RUN	Voice notification service	21004	-
42	WEBSERVER.RUN	Web-server	21034	-
43	WINDOW.RUN	External window	21053	-
44	OPCIE.RUN	HTML Interface	22141	-
45	Manitou.run	Manitou software	22302	-
46	QueuesManager.run	Queues Manager	22322	-
47	display_manager.run	Display Manager	22323	-
48	SipPanel.run	SIP panel	22331	-
49	StreamTerminal.run	SIP terminal	22332, 22537	-
50	BacNetInt.run	BacNet	22350	-

ATM-Intellect and Monitoring

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	VIDEOSRV.EXE	IIDK interface	21030	-

2	VIDEOSRV.EXE	VideoServer	20900	VIDEO.RUN
3	VIDEOSRV.EXE	ATM machine	22174	-
4	VIDEOSRV_C.RUN	ATM-Intellect Pro	22001	-
5	VIDEOSRV_E.RUN	Search in archive	22003	-
6	VIDEOSRV_M.RUN	Monitoring	22222	-
7	VIDEOSRV_R.RUN	Monitoring reports	22223	-
8	VIDEOSRV_S.RUN	ATM-Intellect Workstation	22002	-
9	VIDEOSRV.EXE	ATM-Intellect Pro	7777	VIDEOSRV.EXE
10	EVENTATM.EXE (Integration with ATM through XFS)	-	8888	VIDEOSRV.EXE
11	TELLMEDLL.DLL (Integration with ATM through the SKS software)	-	8888	VIDEOSRV.EXE
12	VMON_ITV.DLL (Integration with ATM through the “Gold Crown” software)	-	8888	VIDEOSRV.EXE
13	STATEUPS.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
14	BATDISCH.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
15	POWEROFF.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
16	POWERON.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
17	VPIPECLIENT.EXE (Internet FPSU operation)	-	7777	VIDEOSRV.EXE
18	VPIPECLIENT.EXE (Internet FPSU operation)	-	8555	VPIPESERVER.EXE
19	VIDEOSRV.EXE	ATM-Intellect Pro	7777	VPIPESERVER.EXE
20	VIDEOSRV.EXE	ATM-Intellect Workstation	7777	VIDEOSRV.EXE

21	VIDEOSRV.EXE	ATM-Intellect Workstation	7777	CPDVAlarmServer.exe
22	CPDVNETSERVER.EXE	CPDV	24345	VIDEOSRV.EXE
23	CPDVNETSERVEREX1.EXE	CPDV	7755	VIDEOSRV.EXE
24	VIDEOSRV.EXE	Agent of Control	7777	VIDEOSRV.EXE
25	STATEUPS.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
26	BATDISCH.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
27	POWEROFF.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
28	POWERON.EXE (UPS operation)	-	8888	VIDEOSRV.EXE
29	forward.run	Data gateway	22327	-

Note.

If CPDV is in use, then between CPDV communication server and *ATM-Intellect Workstation* 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
1	DT_SERVER.RUN	Traffic Detector	22151	-
2	DT_SERVER.RUN	Traffic Detector	20900	VIDEO.RUN
3	DT_SERVER.RUN	Traffic Detector	22152	-
4	DT_SERVER.RUN	Traffic Detector	20988	-
5	DT_VIEWER.RUN	Traffic Monitor	22152	-
6	ITV_VEHICLE_DETECTOR.RUN	Vehicle Detector	22182	-
7	LPRDB.RUN	External Plates DB	22100	-
8	RADAR.RUN	Speed traps server	22157	-

9	ROSSI_FLOW.RUN	Potok recognition server	22119	-
10	TRAFFIC_PROCESSOR.RUN	Vehicle Processor	22181	-
11	URMLPR.RUN	LPR channel	22137	-
12	URMLPR.RUN	LPR channel	20900	VIDEO.RUN
13	VEHICLE_TRACER.RUN	Vehicle Tracer	22187	-
14	VEHICLE_TRACER.RUN	Vehicle Tracer	20986	-
15	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
1	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
1	FACE_MONITOR.RUN	Face Monitor	21919	-
2	FACE_RECOGNITION_PROXY.RUN	Face Search Server	22207	-
3	FACE_RECOGNITION_WEB_PROXY.RUN	Web access to face search	22214	-
4	FIR_MONITOR.RUN	Recognized Faces Monitor	22135	-
5	FIR_MONITOR.RUN	Recognized Faces Monitor	20985	FIRSERVER.RUN
6	FIR_MONITOR.RUN	Recognized Faces Monitor	20900	VIDEO.RUN
7	FIRSERVER.RUN	Face Recognition Server	22136, 10000	-
8	WEBVIEWER.RUN	Web-interface viewing module	22216	-
9	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
1	ALERTNURSES.RUN	Alert nurse	22196	-
2	POS.RUN	POS terminal	21012	-
3	POSAGGREGATOR.RUN	POS Replicator	22245	-
4	POSVIEWER.RUN	Receipt viewer	22111	-
5	POSVIEWER.RUN	Receipt viewer	20977	POS.RUN
6	McMixer.run	McMixer	22321	-

13.2.5.1 ACFA subsystem

№	Module name	Name of the corresponding object in INTELLECT™	Connection port	Corresponding module to which connection is made
1	abc.run	ABC	22031	-
2	abc_cr.run	ABC control reader *	22235	-
3	agency_person.run	Visitor Management System	21057	-
4	aiu.run	"777 ROVALANT" system *	22145	-
5	aiu3.run	Rovalant 777 ISS *	22217	-
6	anson.run	Anson ACS *	22267	-
7	APDA.run	Tempo Reale ACS *	22188	-
8	apollosdk.run	ApolloSdk	22204	-
9	Bagulnik2.run	Bagulnik2 *	22195	-
10	biosmart.run	BioSmart *	22236	-
11	bolid.run	"Bolid" (COM server)	21025	-

12	castle.run	Castle server	22183	-
13	castle_cr.run	CASTLE control reader *	22231	-
14	chrysantemum.run	PRHK *	22198	-
15	DB_Import.run	Data import	21022	-
16	Dunai2.run	Dunai 2 *	22255	-
17	dunai3.run	Dunai 3 *	22255	-
18	Elsys.run	Elsys *	22206	-
19	forsec.run	ForSec *	22166	-
20	forteza.run	Forteza *	22237	-
21	Galaxy.run	Galaxy Dimension	22189	-
22	galaxy2.run	Honeywell ACS/SGPS	22239	-
23	gate_cr_z2.run	Z2 control reader *	21222	-
24	Hid.run	VertX / Edge ACS	22220	-
25	hunter.run	HUNTER PRO SFA	22256	-
26	intrepid.run	Intrepid Interface Module	22172	-
27	Intrepid2.run	Intrepid Grunt	22229	-
28	Intrepid3.run	Intrepid II System	22240	-
29	keyking.run	KeyKing ACS	22244	-
30	keywatcher.run	KeyWatcher ACS	22258	-
31	keywatcher_interface.run	KeyWatcher ACS Interface	22259	-
32	kodos.run	Kodos server *	22130	-
33	kodos_cr.run	KODOS control reader *	22155	-
34	kronverk.run	Kronverk *	22139	-
35	ksu_cr.run	KSU control reader *	22338	-

36	legos2.run	"Octagram" ACS/SFA *	22190	-
37	Magistrator.run	Magistrator *	22161	-
38	nac.run	"NAC" ACS *	21020	-
39	nc.run	HoneyWell N1000	21052	-
40	ncg9.run	Controller NCG-9	22266	-
41	net.run	"Net" system *	22185	-
42	nskat.run	SKAT ACS *	22248	-
43	opc_wrapper.run	OPC Wrapper	22263	-
44	Optex.run	Optex System	22232	-
45	orion.run	Bolid (SDK Orion) *	22173	-
46	paradox.run	Paradox SFA/ACS	22192	-
47	parsec_pr_x08.run	PR-x08 control reader *	22226	-
48	Paxton_NET2.run	ACS Paxton NET2	22233	-
49	pelco.run	PELCO	22234	-
50	perco.run	"Perco" ACS *	21019	-
51	PercoS20.run	Perco S20 controller *	22246	-
52	PhotoIdentification.run	Photo Identification	22163	-
53	pl.run	Polon Alfa System	22242	-
54	pnet3.run	ParsecNET 3 ACS/SFA *	22264	-
55	ravelin.run	Gate Parking ACS	22227	-
56	RifString.run	RifString system *	22197	-
57	Rosslare.run	Rosslare ACS *	22203	-
58	rovalant_a6_a16.run	"ROVALANT (A6, A16)" system *	22165	-

59	rubeg8_isb.run	Rubeg 8 ISS *	22256	-
60	rubezh.run	Rubeg SFA *	22261	-
61	rubicon.run	Rubicon SFA *	22209	-
62	rusguard.run	"RusGuard" ACS *	22250	-
63	salto.run	SALTO Server	22208	-
64	satel.run	"Satel"	21998	-
65	securiton.run	"Securiton" ACS *	22247	-
66	sintegral.run	Strelec-Integral SFA *	22257	-
67	sphinx.run	Sphinx server	22177	-
68	strelec.run	"Strelec" SFA *	22162	-
69	topol.run	Topol PSS *	22241	-
70	trombon.run	Trombone SFA	22224	-
71	tss2.run	"TSS" ACS/SFA *	22218	-
72	unipos.run	"UniPos" 7002	22184	-
73	nipos5xxx.run	UniPos ACFA 5100-5200	22211	-
74	vers_rs.run	VERS ACS*	22126	-
75	WorkTime.run	Work Time Accounting	22133	-
76	xabc.run	Fortecia ACS *	22260	-
77	zline.run	"ZLine" FSA *	22243	-
78	account_manager.run	Access Manager	22291	-
79	event_manager.run	Event Manager	22287	-
80	dsc.run	"DSC" FSA	22292	-
81	IntellectToNextBridge.run	ACFA Intellect - Axxon Next Bridge	22293	-
82	rubezh_global.run	"Rubezh Global" FSA *	22294	-
83	satel2.run	"Satel INTEGRA"	22296	-

84	Unicard.run	"Unicard" ACS	22298	-
85	zk.run	"ZK Teco" ACS	22299	-
86	glx2.run	"Galaxy Dimension v.2" FSA	22300	-
87	sintegral_web.run	"Strelec Integral Web Api" ACS *	22301	-
88	XTralis2WayProtocol.run	"ADPRO" PID	22303	-
89	Chomtech.run	"Chomtech" ACS	22304	-
90	Rbg08.run	"Rubezh-08" ACS *	22305	-
91	topol3.run	"Topol-3" PID	22306	-
92	nedap_retail.run	"Nedap retail" FSA	22307	-
93	WinPak.run	"HoneyWell WinPak" ACFA	22308	-
94	fs80cr.run	BioSmart FS80 control reader	22309	-
95	evs_sk.run	"EVS" ACS *	22310	-
96	acfa_emulator.run	Virtual Access Server	22311	-
97	pvscr.run	PVS control reader	22312	-
98	bsveins.run	"Biosmart UniPass" ACS *	22313	-
99	RubezhGlobal.run	Third-party integration for R3 protocol of the Rubezh company. Not included to ACFA-Intellect.	22314	-
100	an.run	OPC Wrapper	22315	-
101	nedap_aeos.run	"Nedap AEOS" ACS	22317	-
102	parsec_pr_p08.run	Parsec PR-P08 control reader	22318	-
103	suprema_cr.run	Suprema BioMini control reader	22319	-
104	UfdVolna.run	"Volna Alpha" PID	22320	-
105	SCardDriver.run	PCSC Wrapper control reader	22324	-
106	NoderEe12.run	"Aritech FP2000" FSA	22325	-
107	LockerBox.run	"LockerBox" ACS *	22326	-
108	suprema_2.run	"Suprema 2" ACS	22328	-
109	NoderEw1.run	"Noder EE12" ACS	22329	-

110	hikvision.run	"HikVision" ACS	22330	-
113	suprema_realscan.run	Suprema Realscan control reader	22333	-
114	stalt.run	"Stalt-SV" ACS *	22334	-
116	percoS20v2.run	"PERCo-S-20" ACS *	22340	-
117	dingo.run	Dingo *	22346	-
118	snmpwrapper.run	SNMP Wrapper Parent object	22277	-
119	MorphoLite.run	MorphoAccess SIGMA Lite	22345	-
120	ratek.run	Ratek *	22352	-
221	gateipbase.run	Gate-IP-Base *	22351	-
222	elfar.run	EL-Far	22349	-
223	fp_sync.run	Face synchronization module *	22357	-
224	vanderbilt_spc.run	Vanderbilt SPC	22355	-
231	alcoframe.run	Alcoframe	22365	-
232	virdi.run	Virdi Server	22371	-
233	modbuswrapper.run	Modbus Wrapper	22373	-
234	zk.run	"ZK Teco" ACS	22299	-
235	Stx1000.run	STX	22383	-
236	rakinda.run	Rakinda	22384	-
237	schindler.run	Schindler PORT	22386	-
240	texecom.run	Texecom panel	22369	-
241	textreader.run	Text reader *	22372	-
242	pcscwrapper.run	Smart-card wrapper *	22324	-

* These integrations are not included into the English version of ACFA subsystem and are given here for information only.

13.2.6 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/

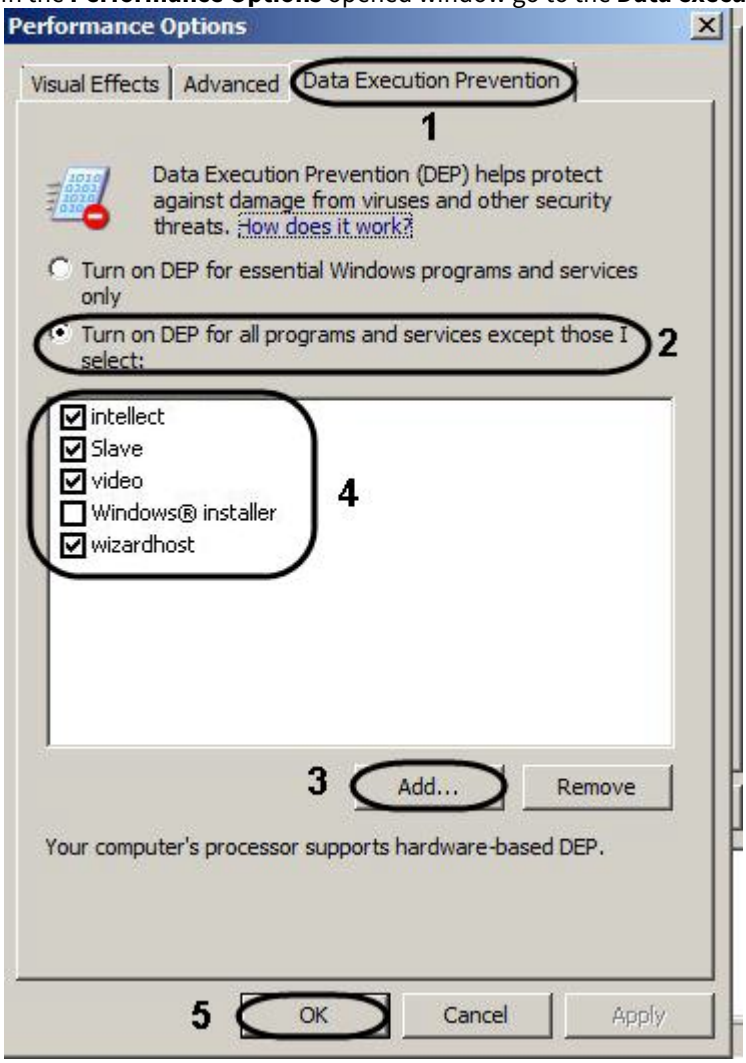
13.2.7 Disable the Data execution prevention (DEP) function for Intellect software package

> **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.

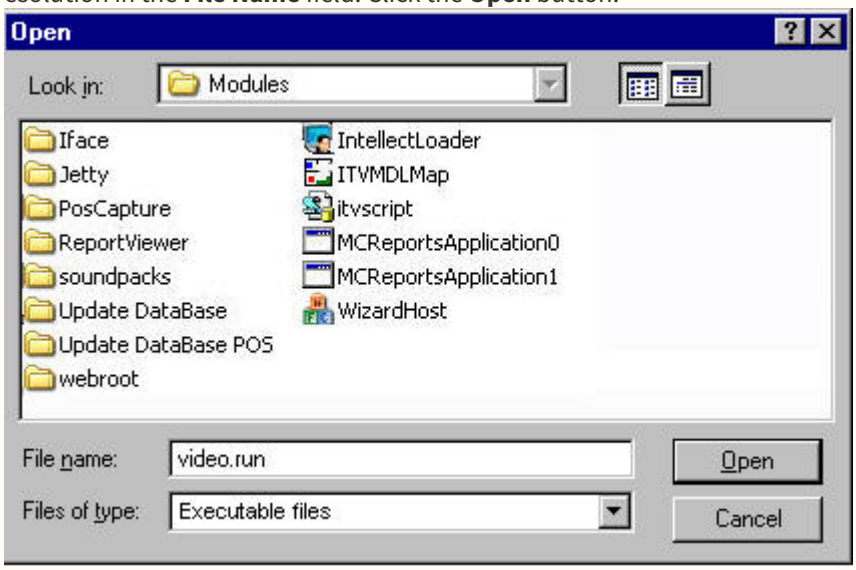
3. In the **Performance Options** opened window go to the **Data executing prevention** tab (1).



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.

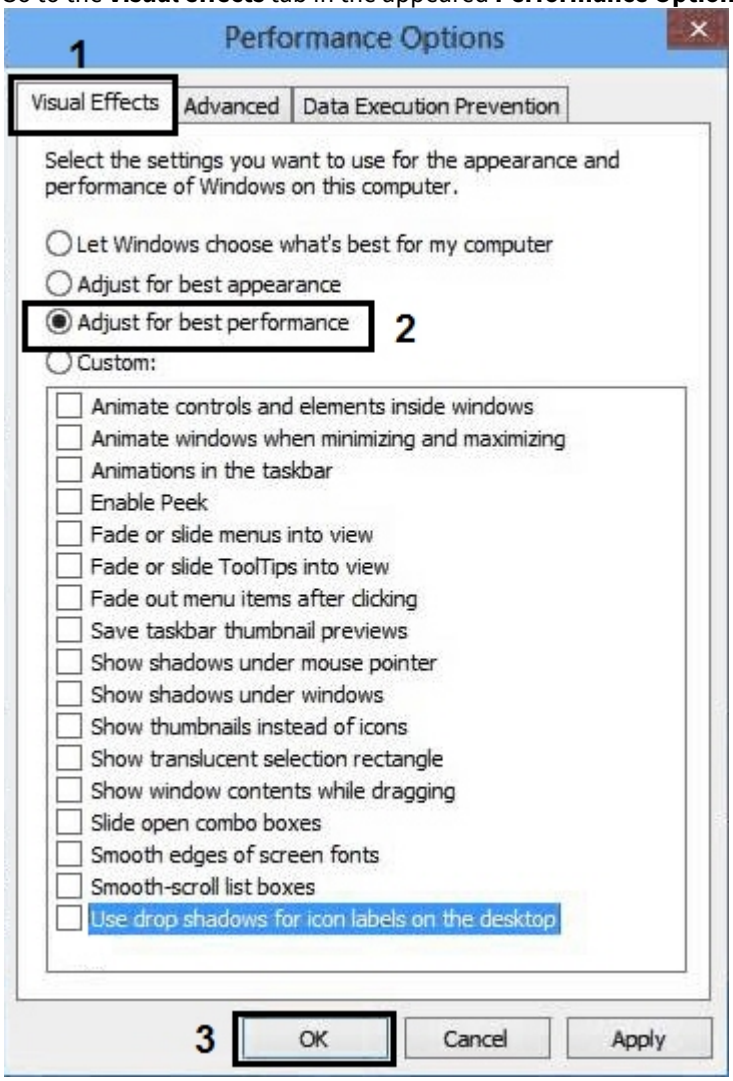
It is also possible the full DEP disabling on the computer. For full DEP disabling perform the **bcdedit.exe /set {current} nx AlwaysOff** command using the Windows command line from the <Windows>\system32 directory.

13.2.8 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.

13.2.9 Features of ElasticSearch service operation

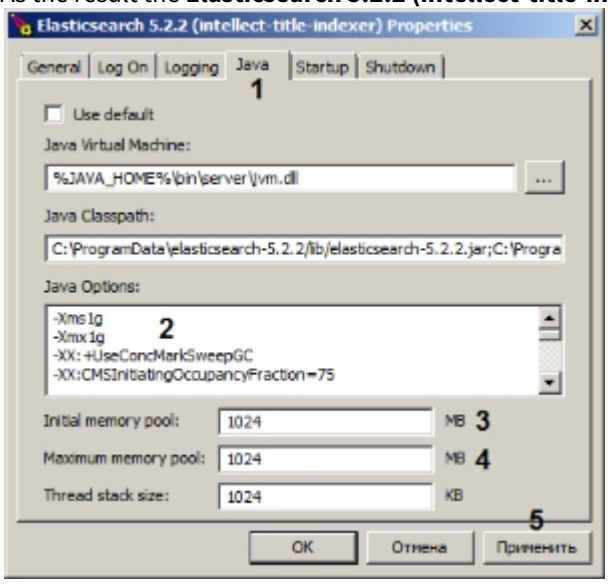
The ElasticSearch service is required for search by captions. It is included into the *Intellect* installation kit. If there is no need in search by captions, the service can be disabled at **Control panel - Administrative Tools - Services**. There is also SearchIndex parameter in the cam_title.run.config file to disable the use of the Elastic Search – see XML-file parameters reference guide.

13.2.9.1 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.

13.2.9.2 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.

13.3 Appendix 3. INTELLECT™ software database management

13.3.1 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.

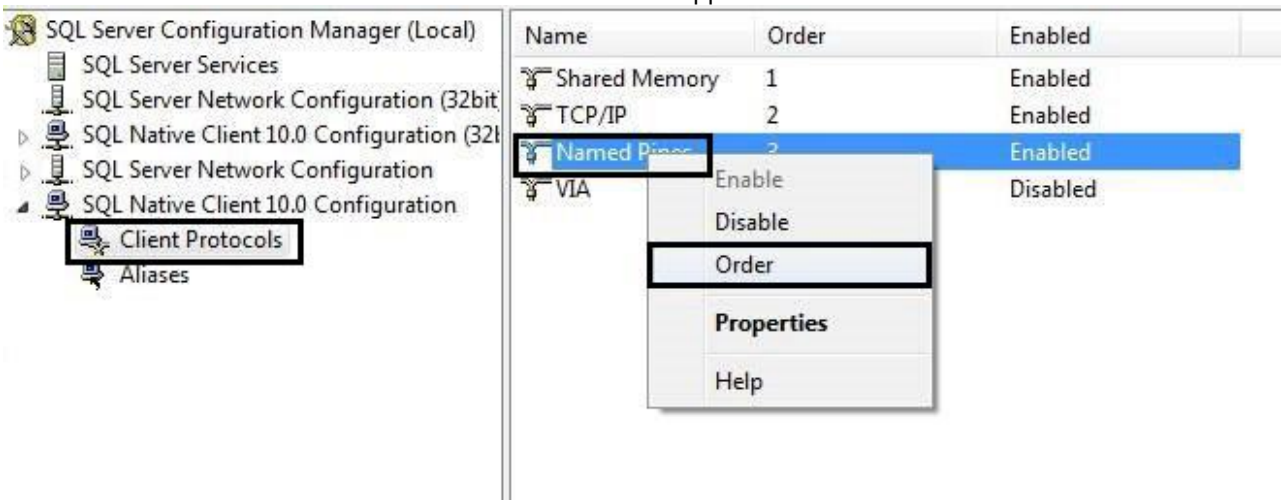
13.3.2 Guidelines on INTELLECT ™ system database use

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.

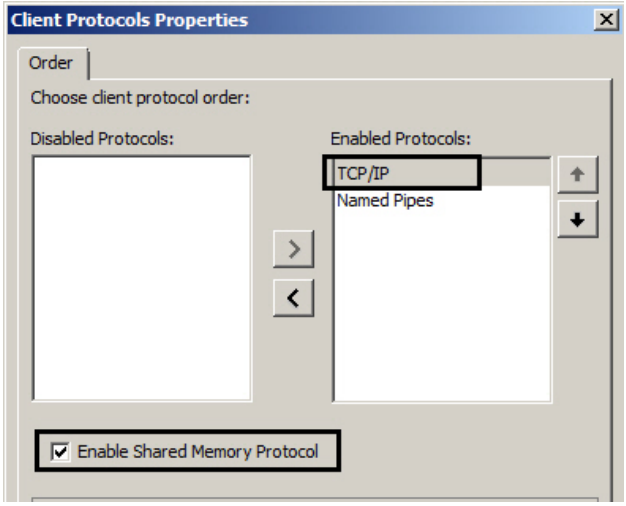
   > **Note**
   >
   > It is recommended to configure the automatic backup of Intellect database in MS SQL Server, for example, once a week (by default, the automatic backup is not configured).

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.
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** -> **All Programs** -> **Microsoft SQL Server Express 2014** -> **Configuration Tools**).
   b. In the right 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 left part of the window, right-click any protocol in the list and select the **Order** item in the context menu that appears.

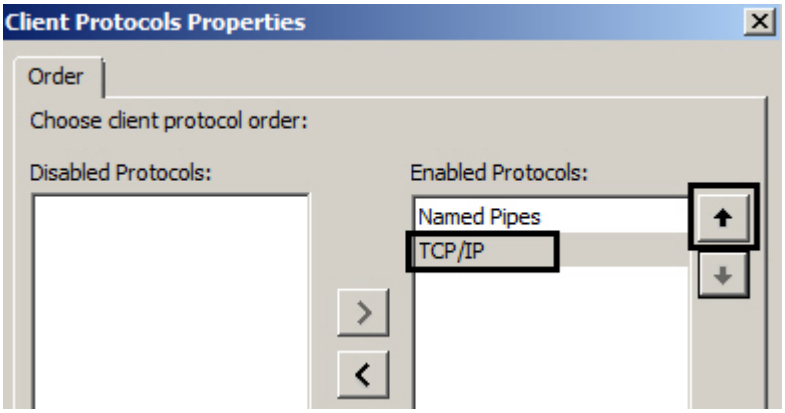


   c. In the **Client Protocols Properties** dialog box that appears, the list of client protocols for the local SQL databases in descending priority order is displayed in the **Enabled Protocols** field. Make sure that the **TCP/IP** item is located at the very top of the **Enabled Protocols** list. Also 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 to the top of the list.



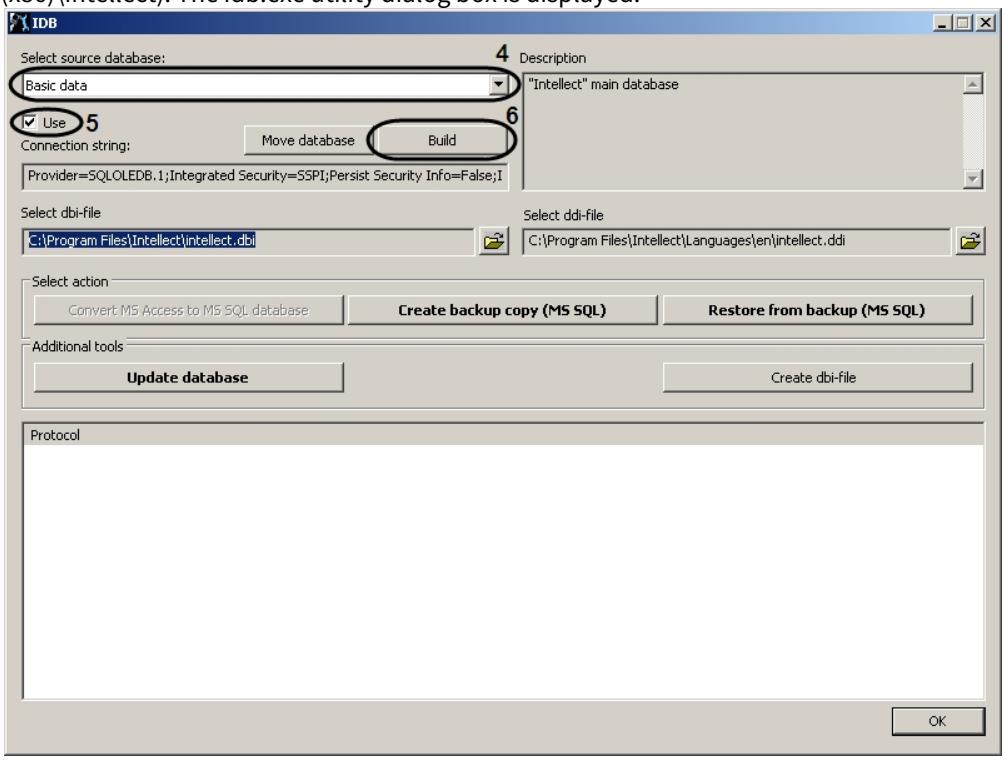
13.3.3 Converting the database from MS Access to MS SQL format

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.

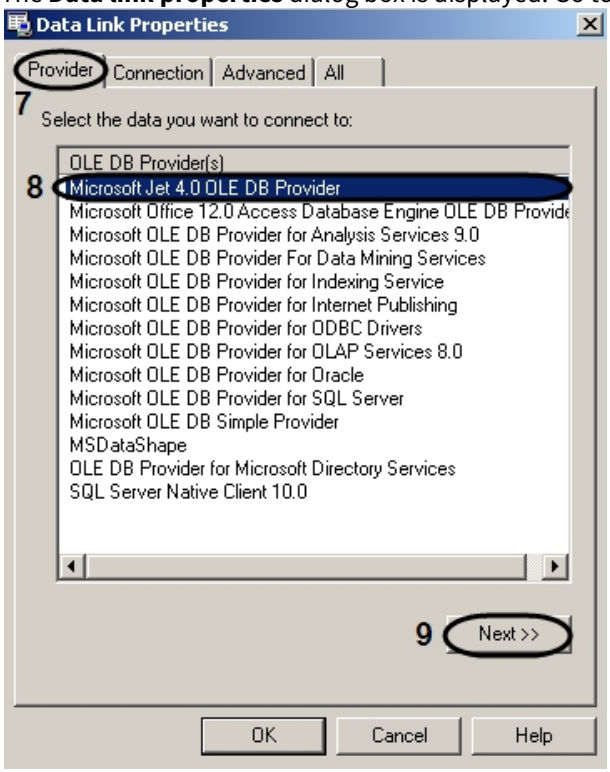
To convert the database from MS Access to MS SQL server format, follow the steps:

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.

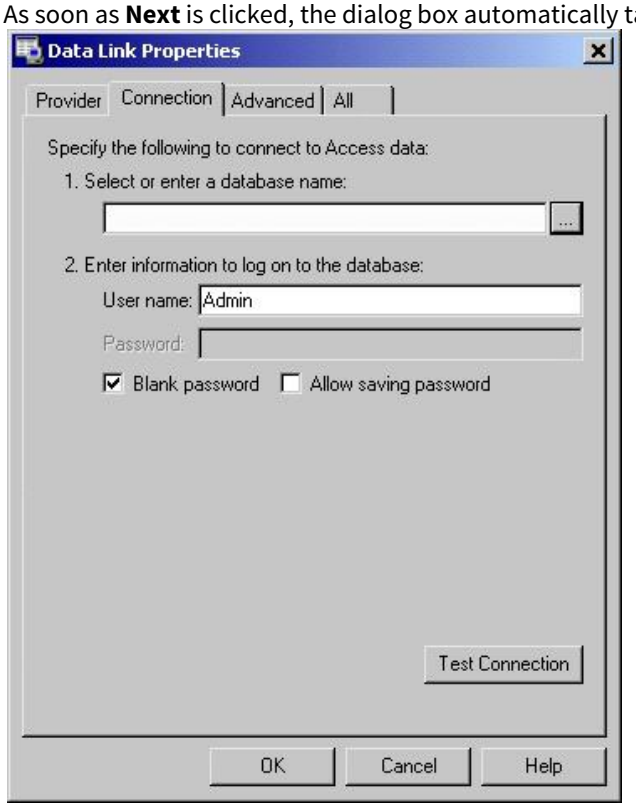


4. Choose the **Basic data** item from the **Select data source** list.
5. Check the **Use** checkbox, if not checked before.
6. Click **Build**.
7. The **Data link properties** dialog box is displayed. Go to the **Provider** tab in the **Data link** properties dialog box.

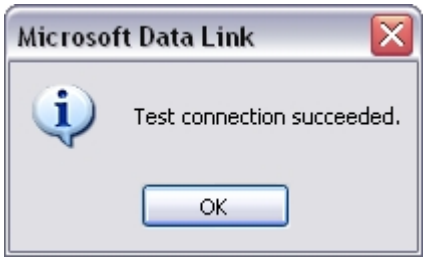


8. Select **Microsoft Jet 4.0 OLE DB** Provider from the **OLE DB Providers** list.
9. Click **Next**.

10. As soon as **Next** is clicked, the dialog box automatically takes you to **Connection** tab.

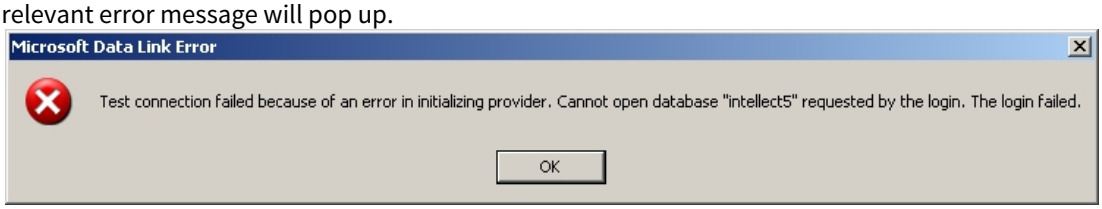


11. Type the complete path to the database file in the **1. Select or enter a database name** or select the necessary file from the file opening dialog box, which is displayed by the **...** button.
12. Enter the user name (login) for database access in the **User** field. If database access is not protected, 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.

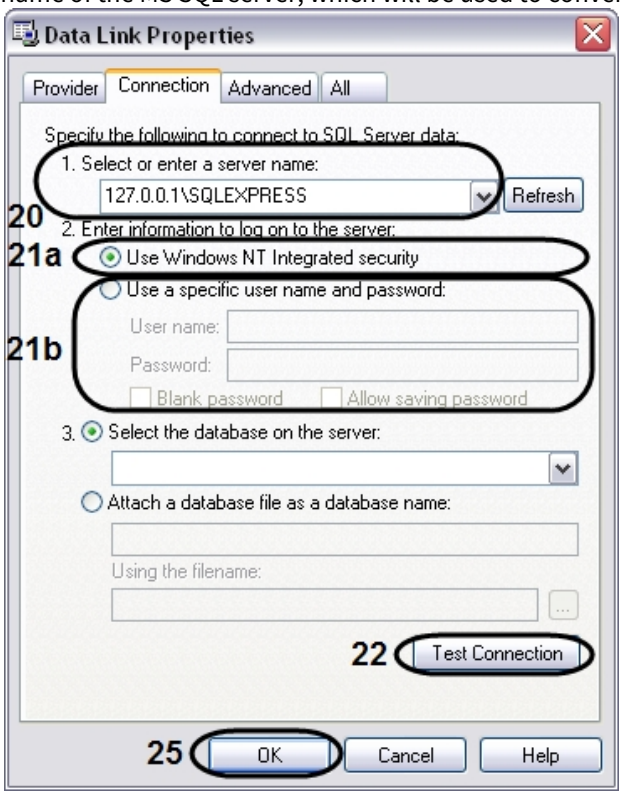
17. Click **OK** in the **Data link properties** dialog box. The window closes.
18. Update the database structure. To do that click the **Convert MS Access to MS SQL** button in the idb.exe utility dialog box.

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.



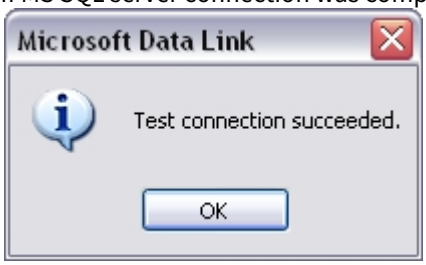
21. The **Enter information to log on to the server** box is checked to enter the type and authentication parameters of MS SQL server connection. MS SQL server authentication is performed through the user account, authorized in Windows OS, or the user name (login) and password, that protect the MS SQL 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.

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.

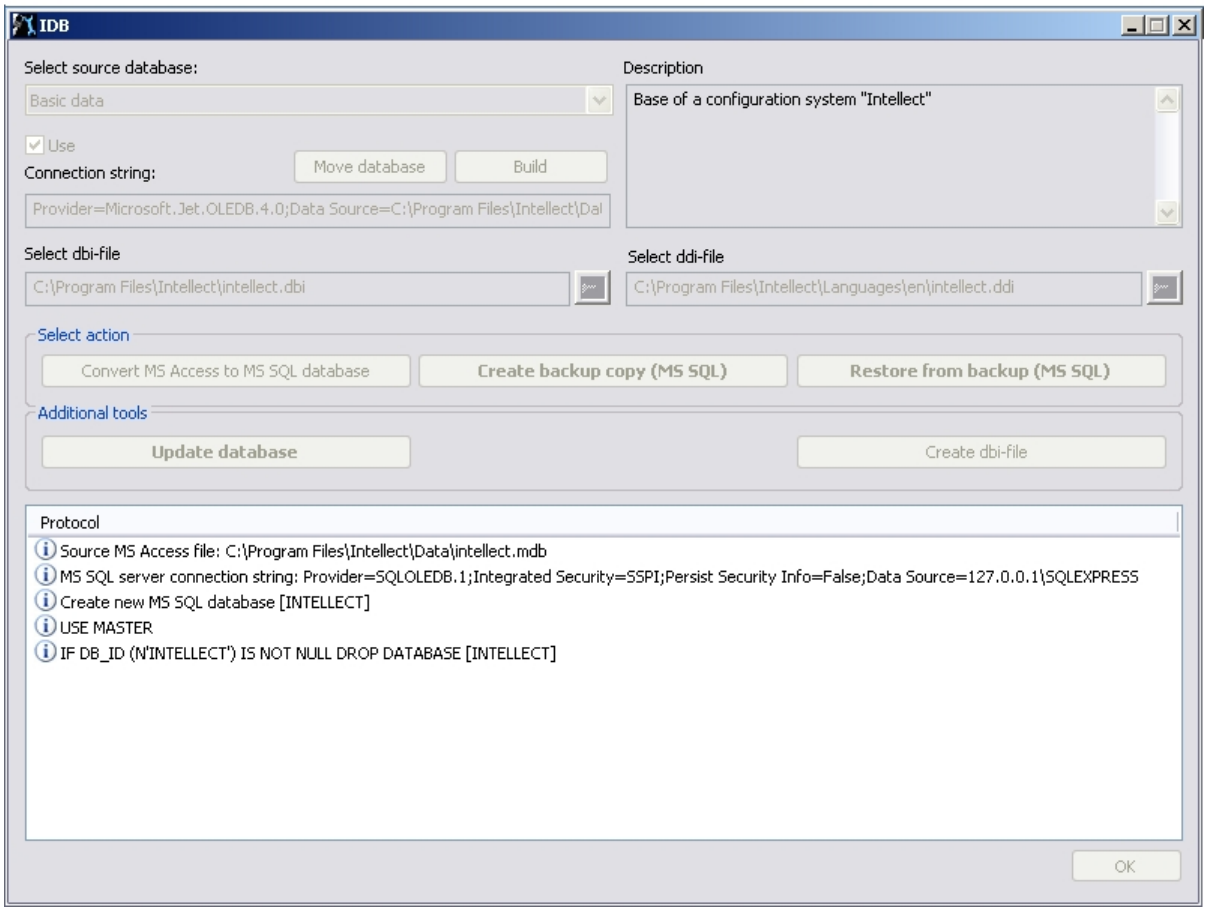


Enter the name to be used for database storage on the MS SQL server in the top field. It is default recommended to use INTELLECT as the database name.

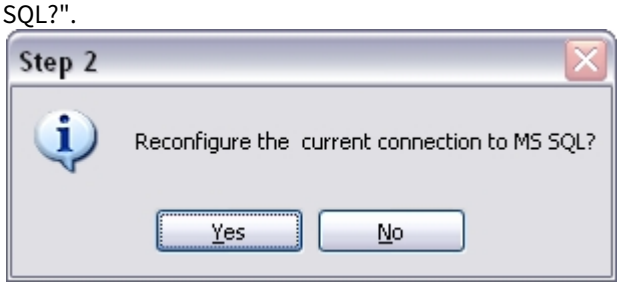
> **Note.**
>
> If the MS SQL server has a database with the same name, as has been entered in the **Enter the database name** field, it will be overwritten.

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.

13.3.4 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.

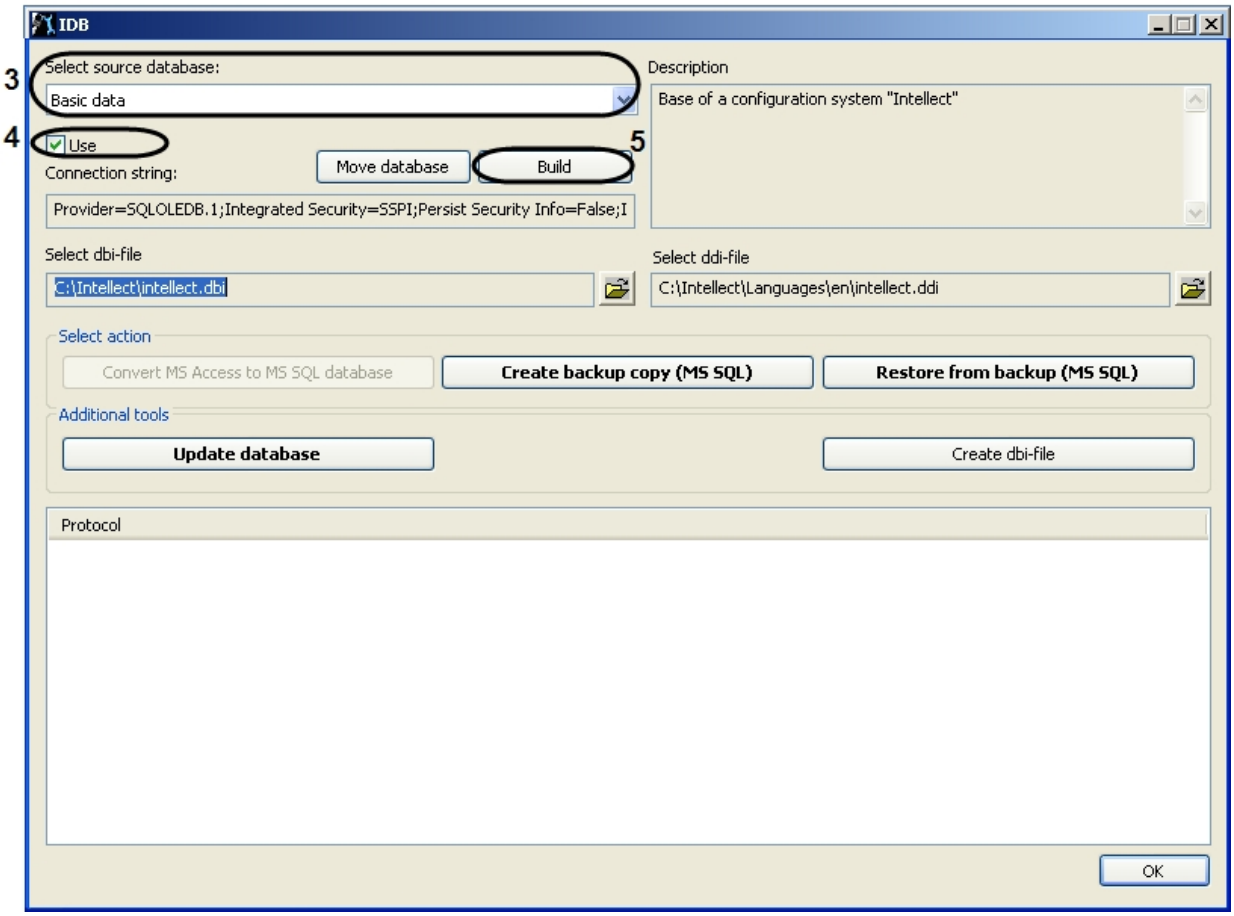
Note.

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.

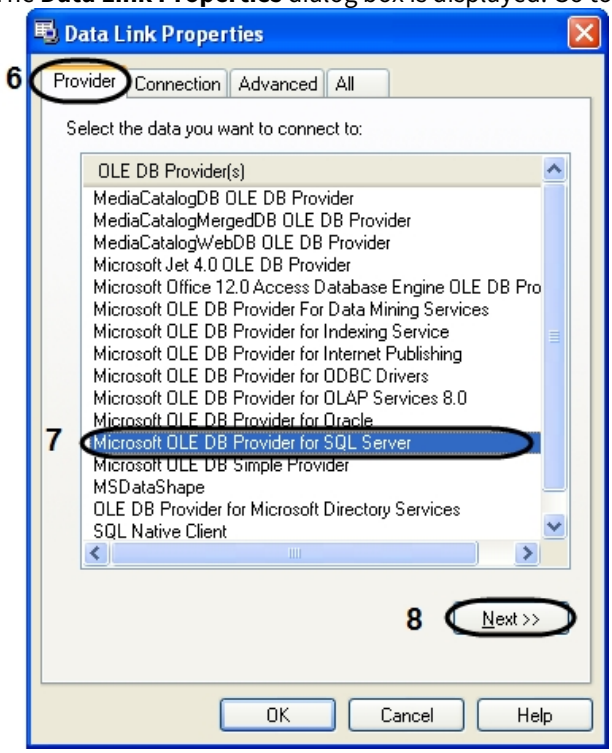
To connect the INTELLECT™ software Configuration database, do the following:

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.

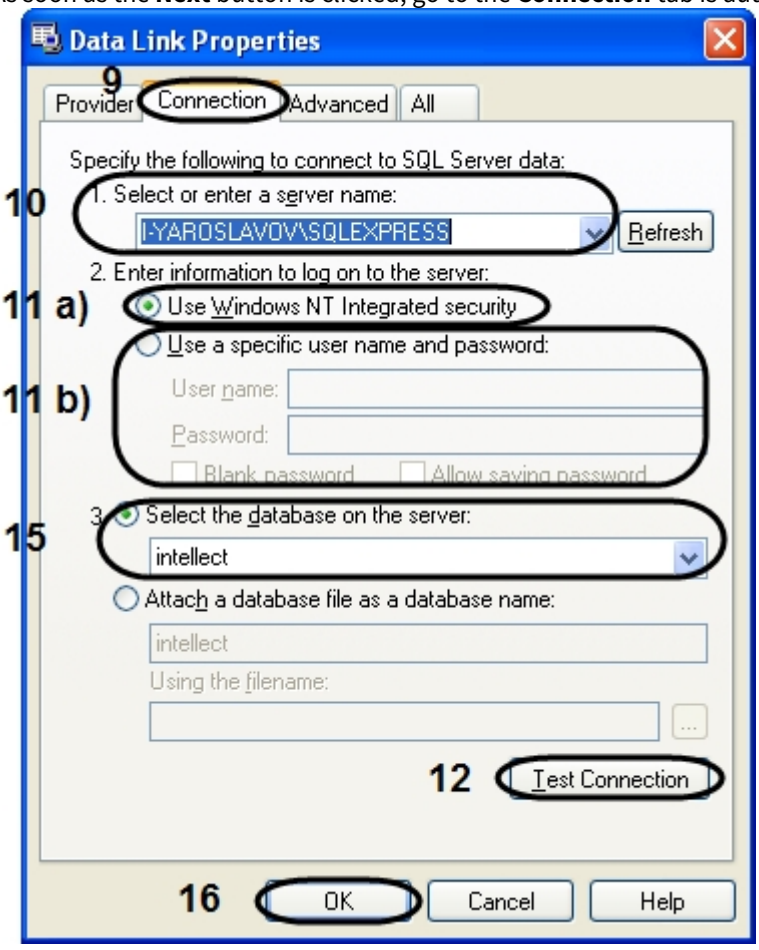


3. Choose the **Basic data** item in the **Select source database** list.
4. Set the **Use** checkbox, if not set before.
5. Click the **Build** button.

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

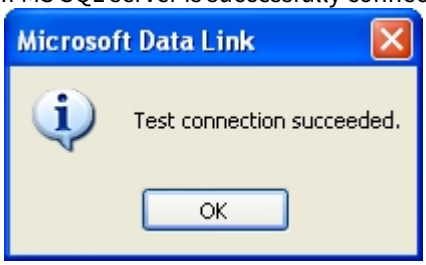
> **Note.**
>
> In case of dynamic host configuration protocol (DHCP) use for the local database, set «127.0.0.1» IP address (without using computer names and "local" value) in the **1.Select or enter a server name**. Set «127.0.0.1» value when the static IP address is use. Otherwise there is disconnection 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.

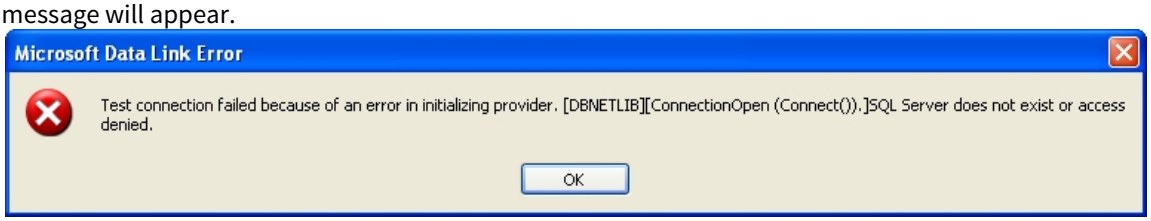
    b. If MS SQL server authentication is performed through the user login and password, do the following:
        i. Switch to the **Use a specific user name and password**;
        ii. Specify the user name (login) to connect to the MS SQL server in the **User name** field.
        iii. If access to the MS SQL server is protected with a password, set the **Blank password** checkbox unchecked and specify the database access password in the **Password** field.

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.

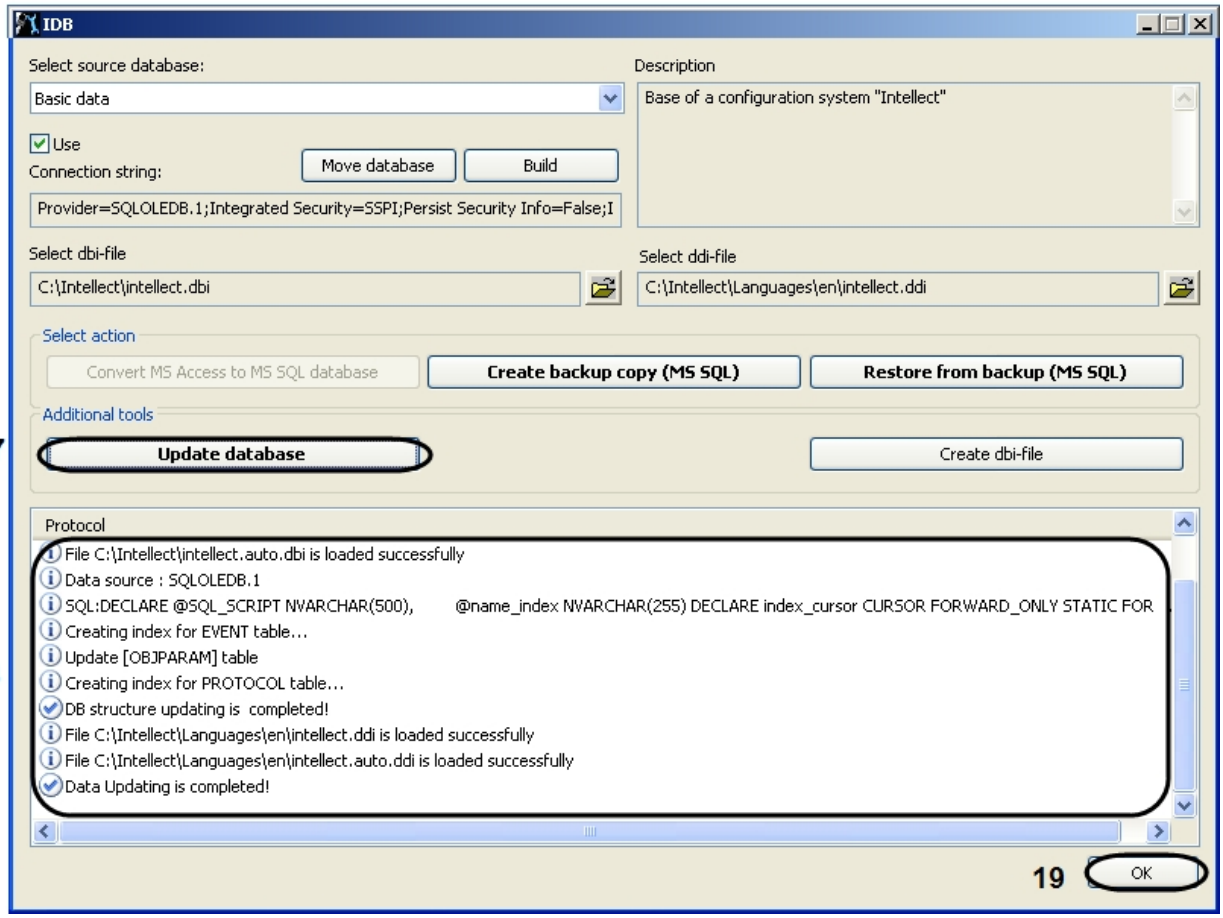


Click the **OK** button to close the box. Then specify the correct password and try the MS SQL server connection again.

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.

13.3.5 Viewing INTELLECT™ software database

To view the database stored on MS SQL server, do the following:

1. Download (x86, x64) 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** box.

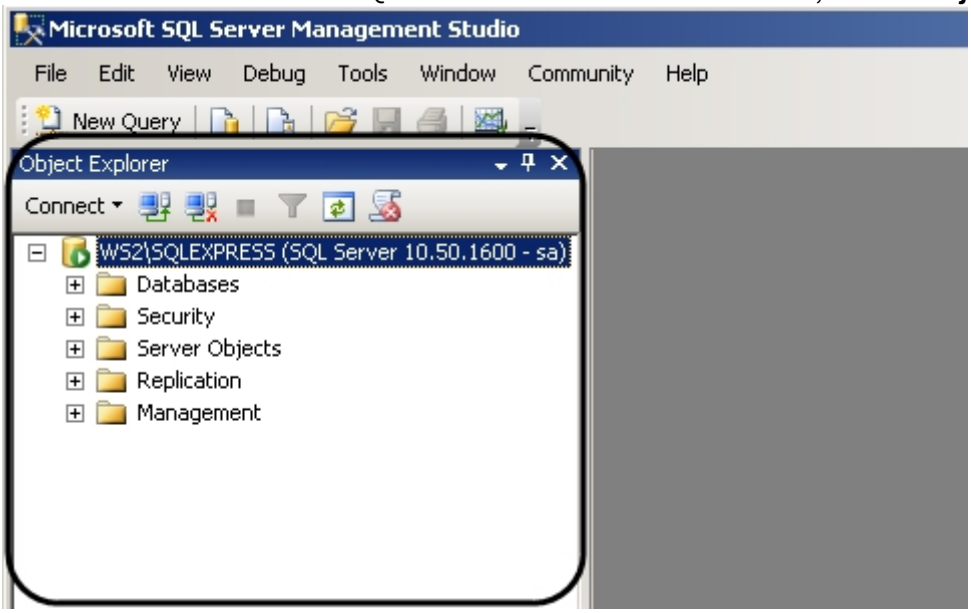


   a. Select the **Database Engine** type in the **Server type** list (1).
   b. Select the name of MS SQL server to wich it is necessary to connect in the **Server name** list (2).
   c. Select authentication type used for connecton to MS SQL server in the **Authentication** list (3).

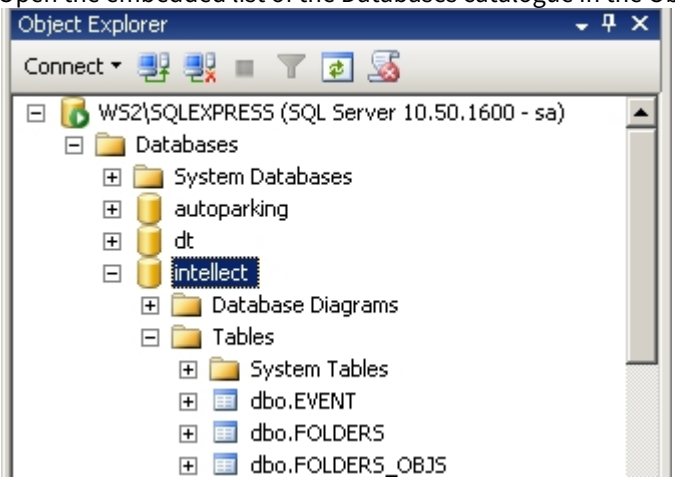
> **Note.**
>
> The type of authentication that was selected while creating MS SQL server is specified.

> **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).

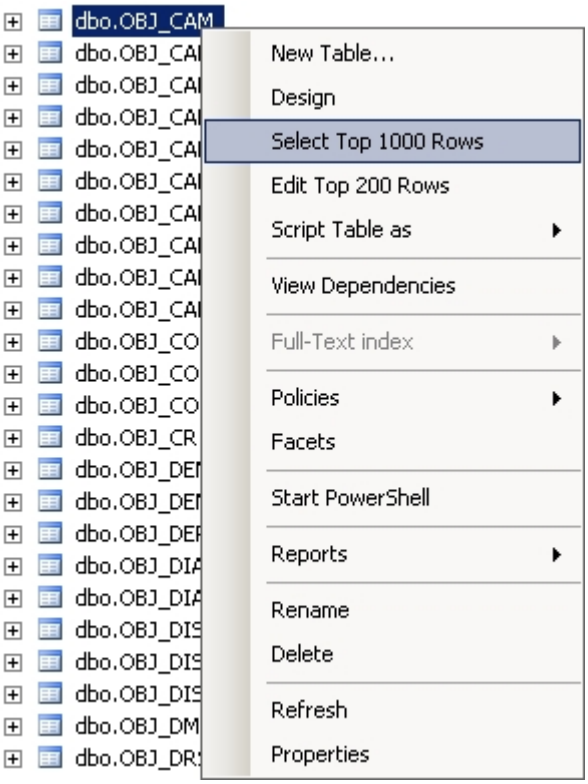
4. Click **Connect** to connect to MS SQL server. If the connection is successful, then the **Object Explorer** box is displayed.



5. Open the embedded list of the Databases catalogue in the Object Explorer box and go to the required database.

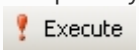


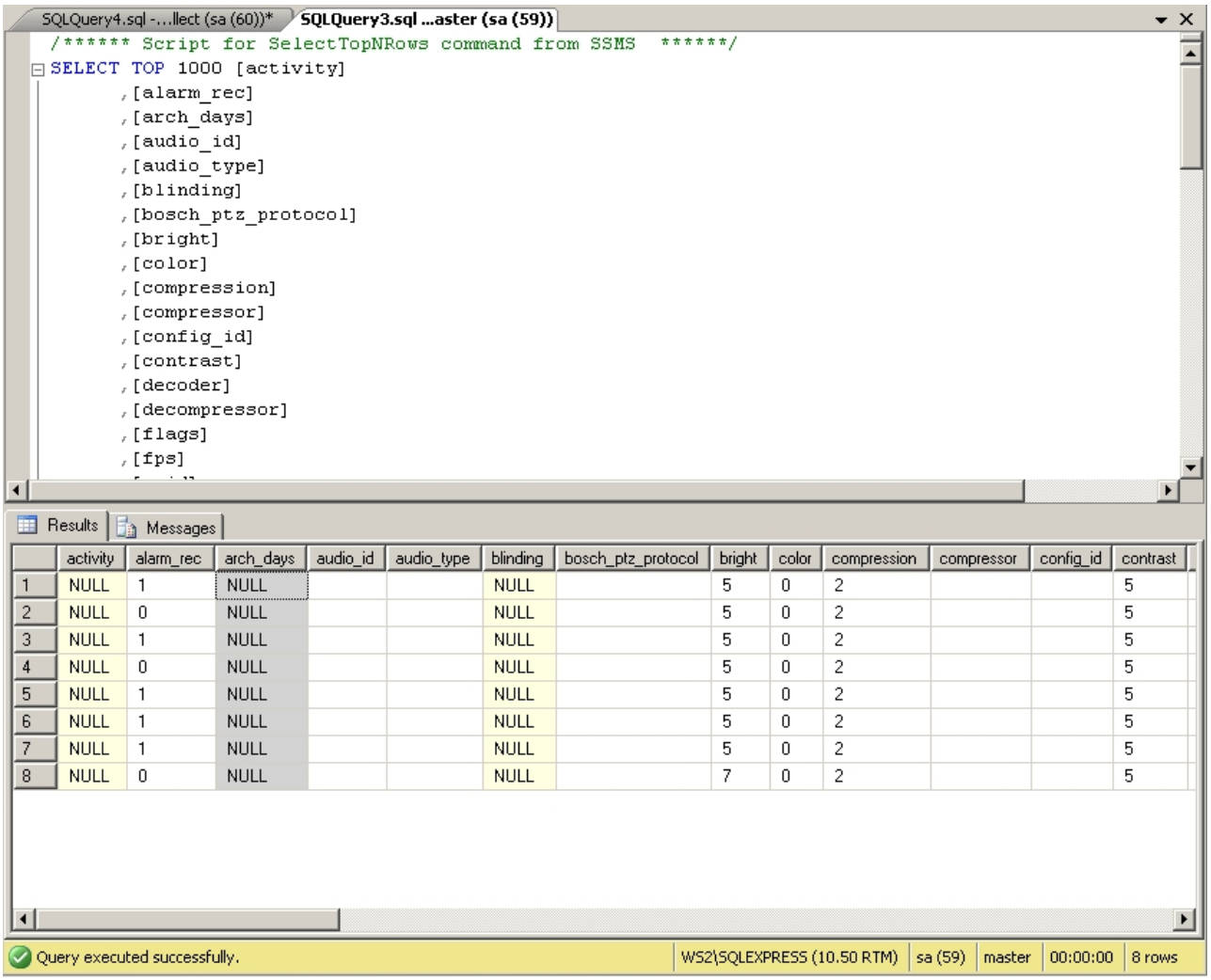
6. Select the table for viewing in the **Tables** catalogue.
7. Select **Select Top 1000** Rows item in the context menu of the table.



As a result the box with SQL Query on top of it and the table data selected by the query will be displayed.

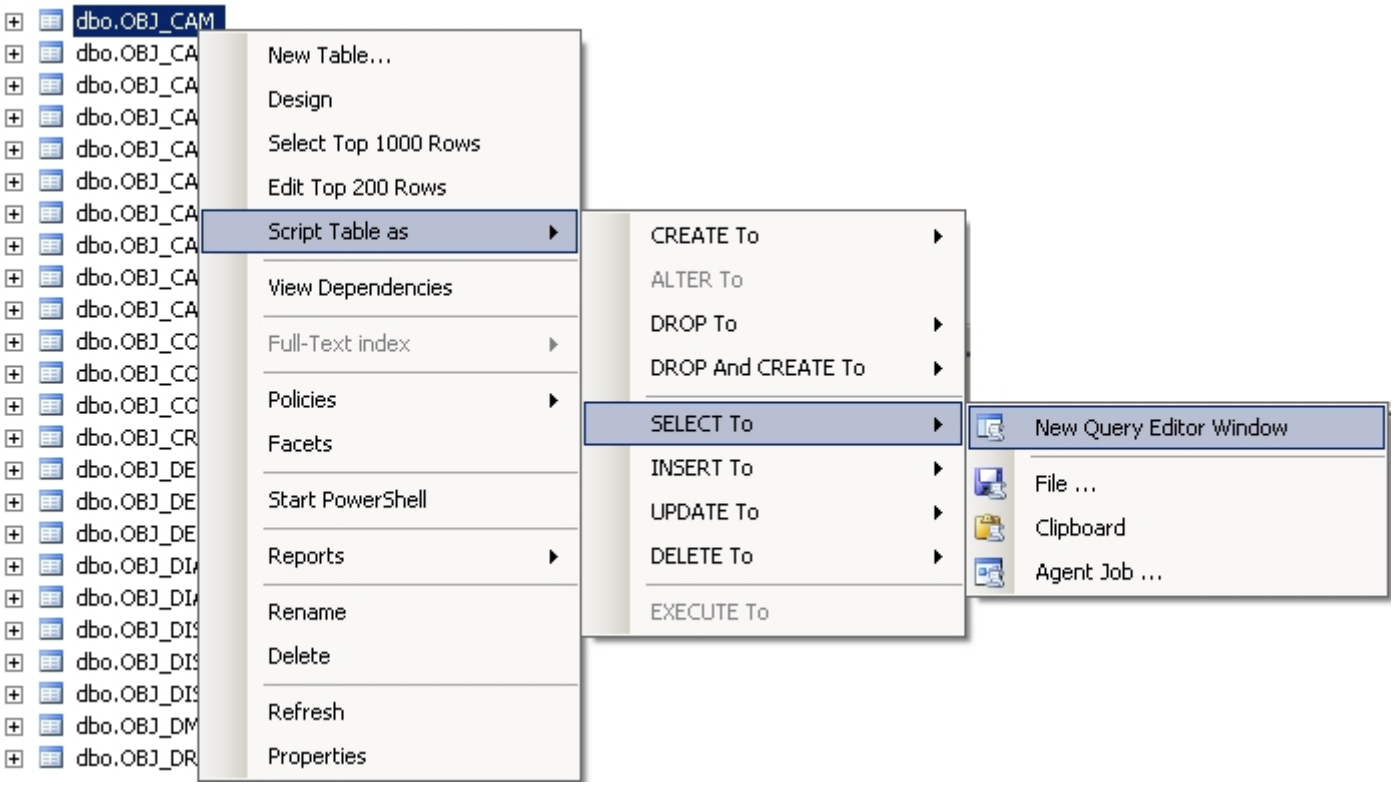
> **Note.**
>
> Using **Select Top 1000 Rows** command one can query the latest rows stored into the table. Not more than 1000 rows respond to a query.

> **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  on the toolbar.



	activity	alarm_rec	arch_days	audio_id	audio_type	blinding	bosch_ptz_protocol	bright	color	compression	compressor	config_id	contrast
1	NULL	1	NULL			NULL		5	0	2			5
2	NULL	0	NULL			NULL		5	0	2			5
3	NULL	1	NULL			NULL		5	0	2			5
4	NULL	0	NULL			NULL		5	0	2			5
5	NULL	1	NULL			NULL		5	0	2			5
6	NULL	1	NULL			NULL		5	0	2			5
7	NULL	1	NULL			NULL		5	0	2			5
8	NULL	0	NULL			NULL		7	0	2			5

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.

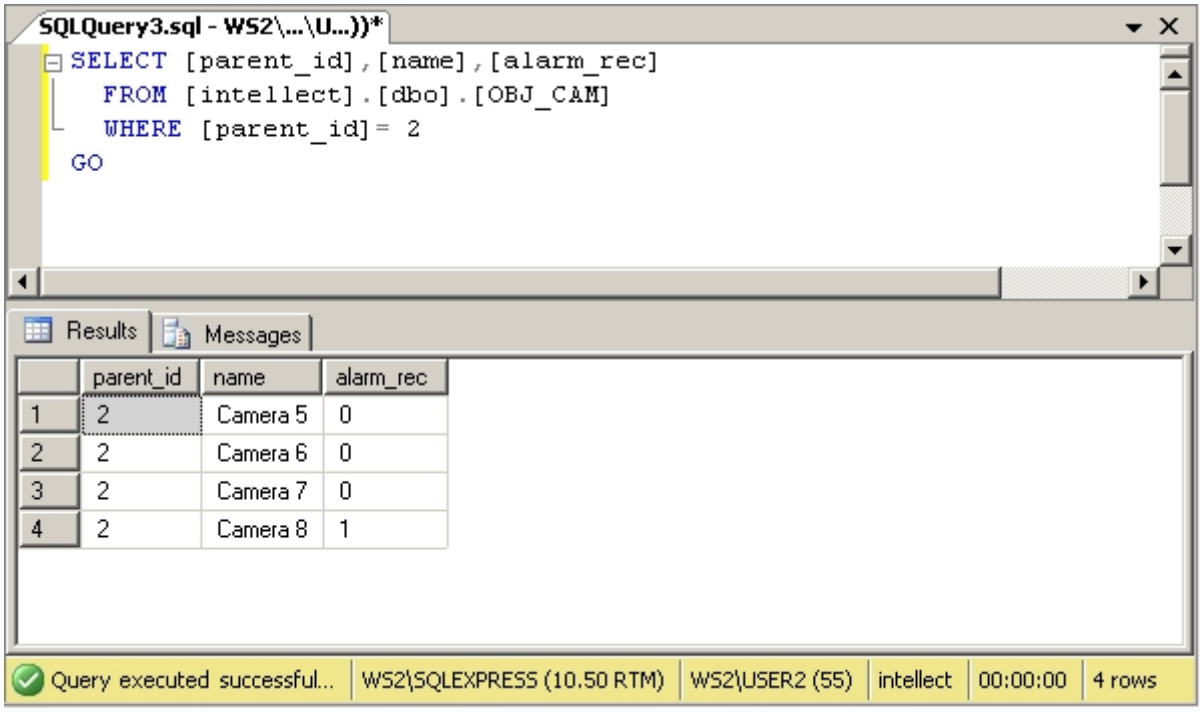


Note.

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™ software database is now completed.

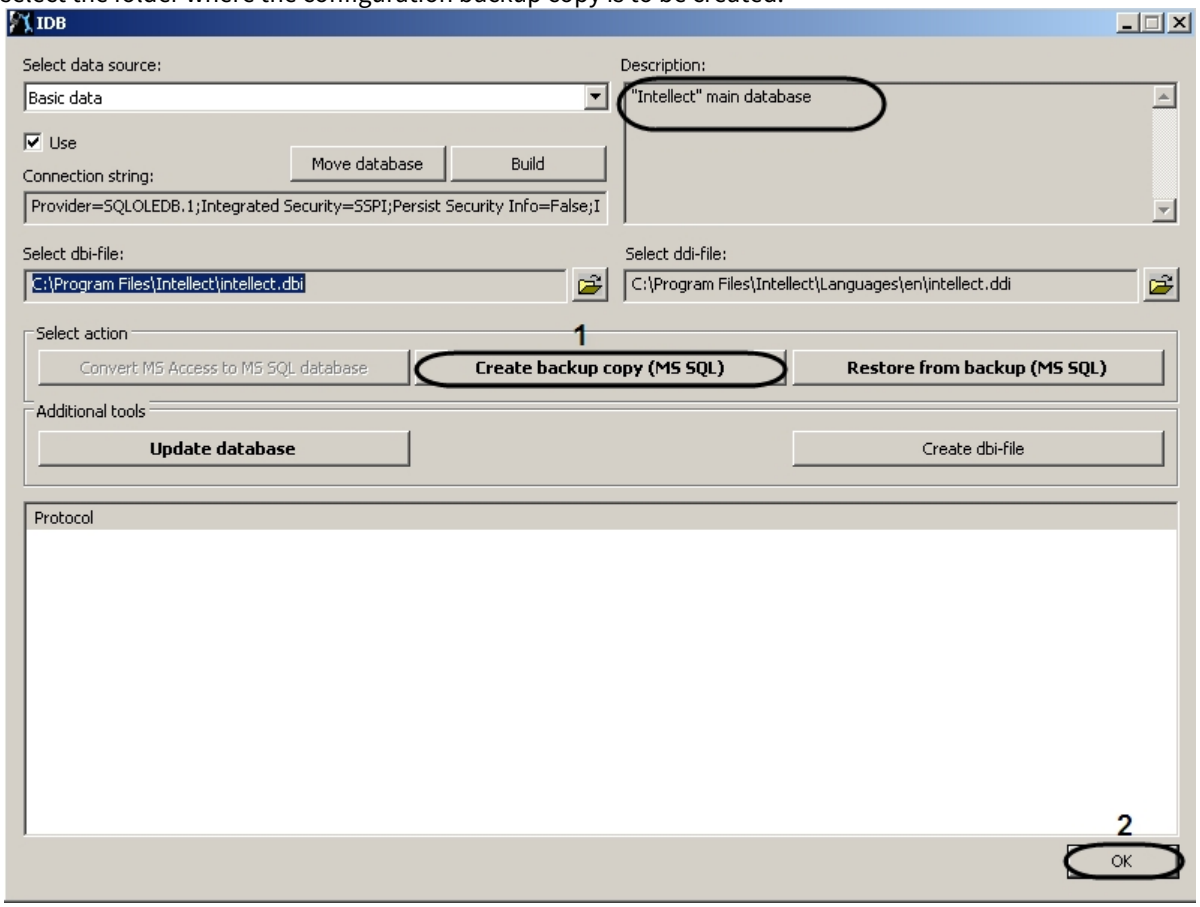
Note.

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.

13.3.6 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.

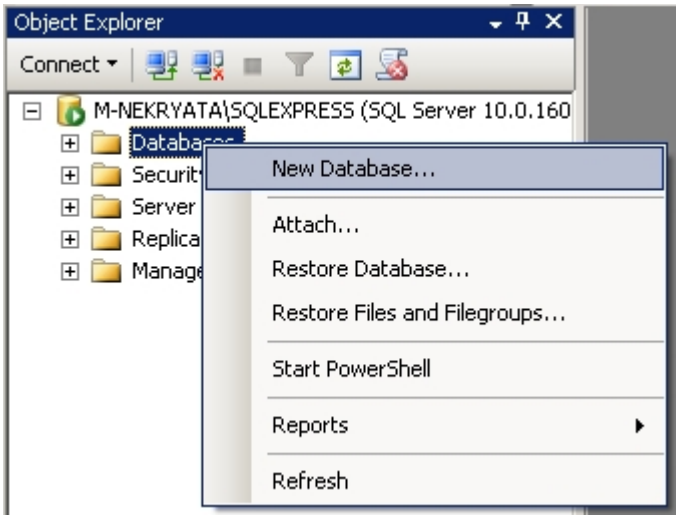


Note.

Configuration backup copy is a file with bak. extension.

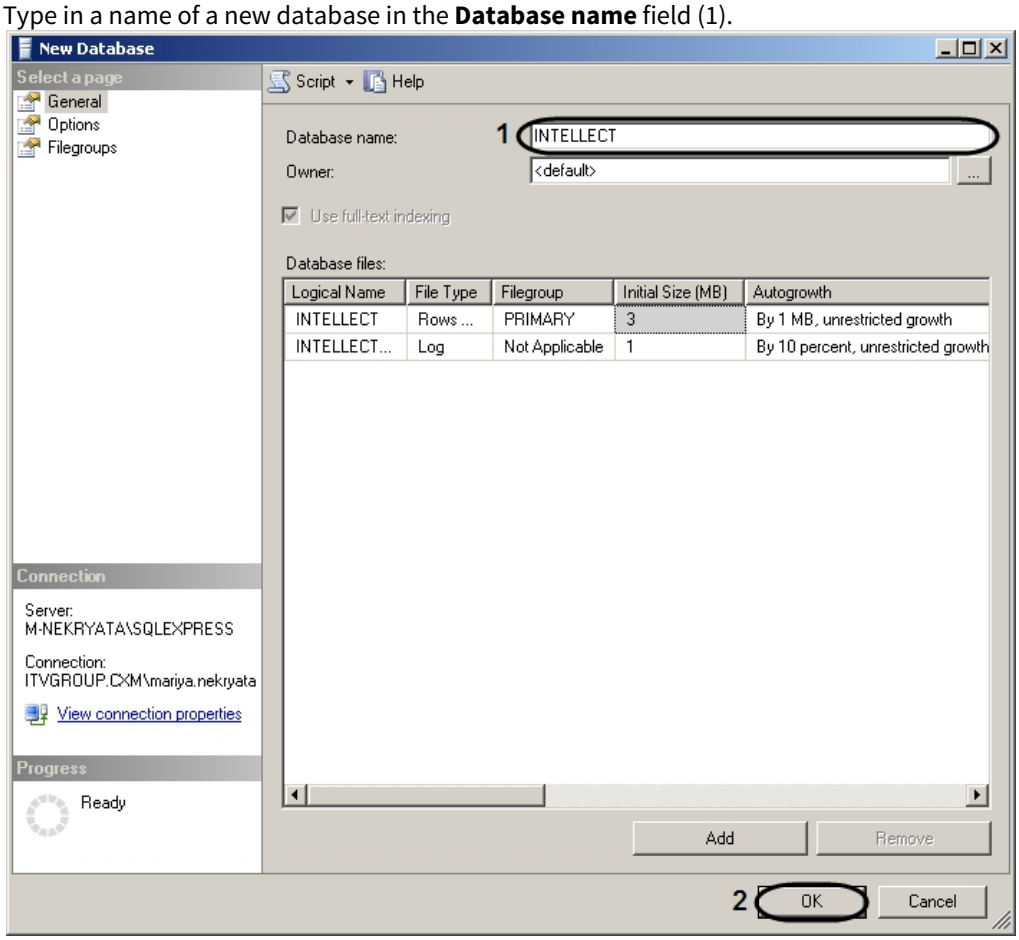
3. If the configuration backup copy is created without any errors (see the protocol of the idb.exe utility), then click **OK** (2). If there are some errors, then repeat 2 step or use MS SQL Server 2005 tools for creating database backup copies.
4. Remove previous version of MS SQL Server from computer.
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.

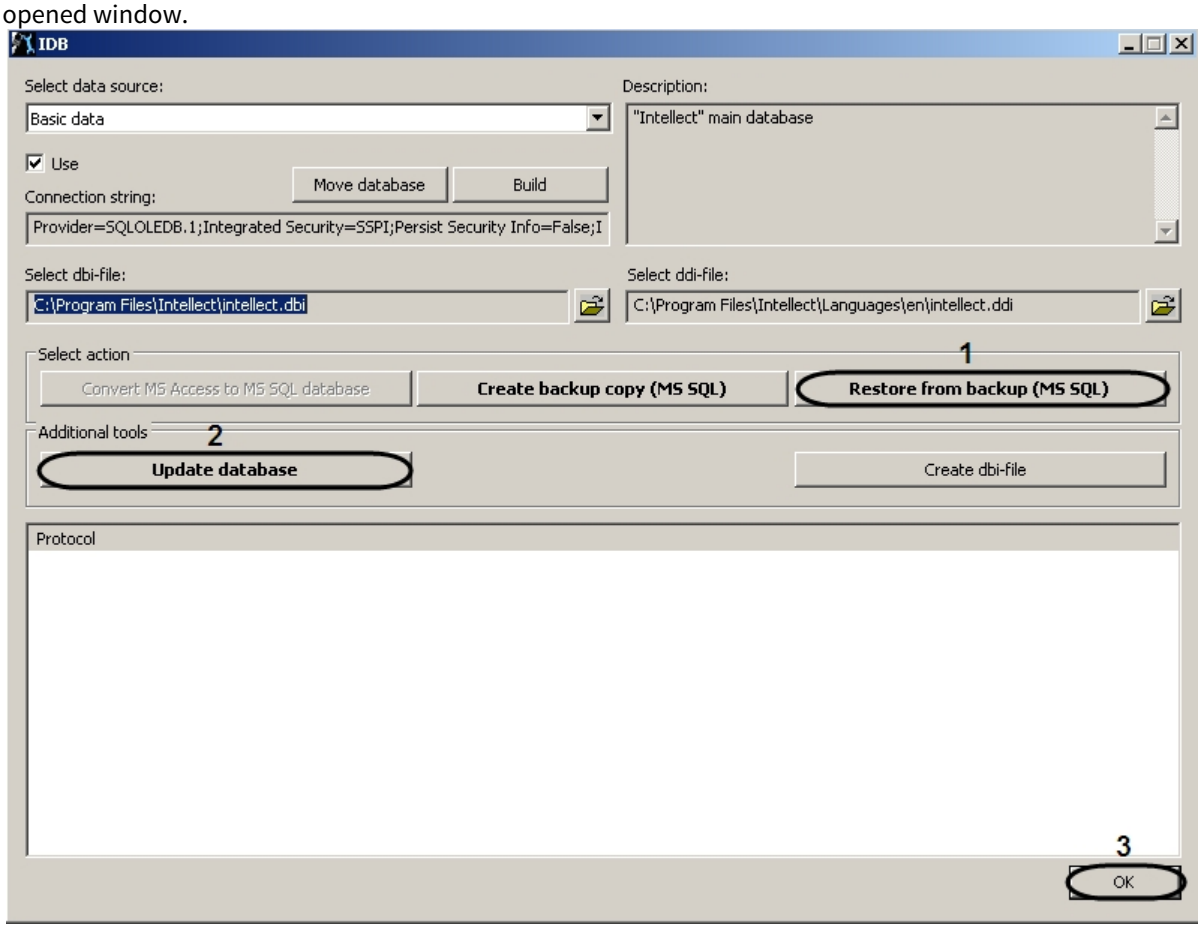
c. Type in a name of a new database in the **Database name** field (1).



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.

13.3.7 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.

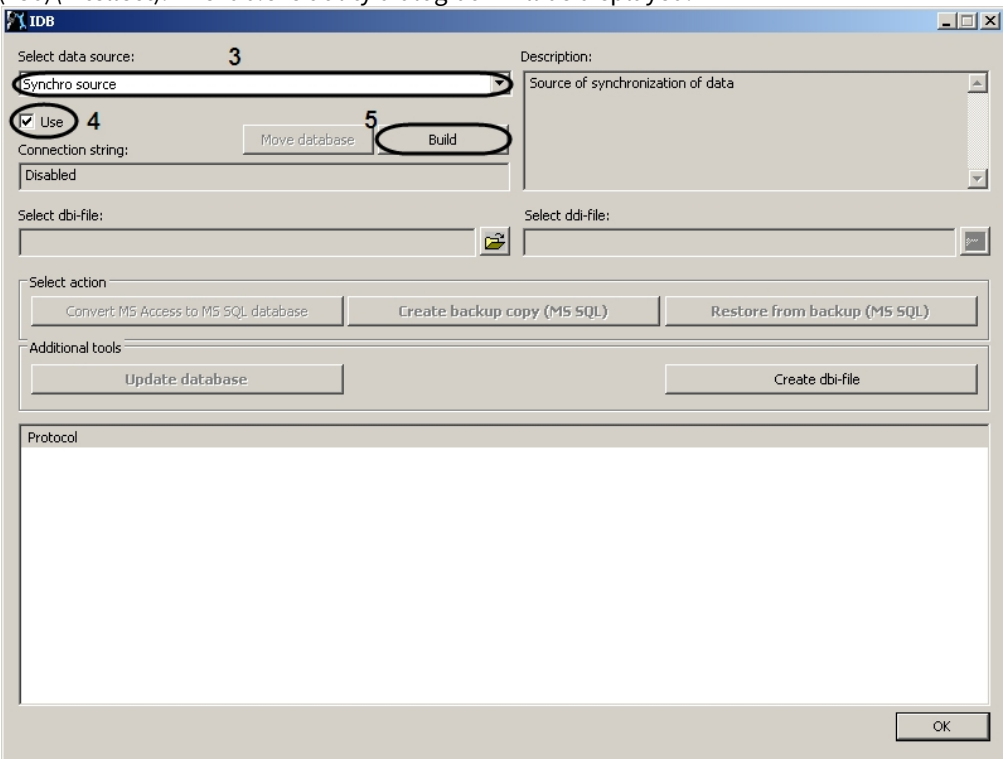
The administering Server acts as a synchronization source. The second-level Server/RAW will accept all database changes from the administering Server. Synchronization should always be performed from the second-level Server to the administering Server, or from the RAW to the administering Server.

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.

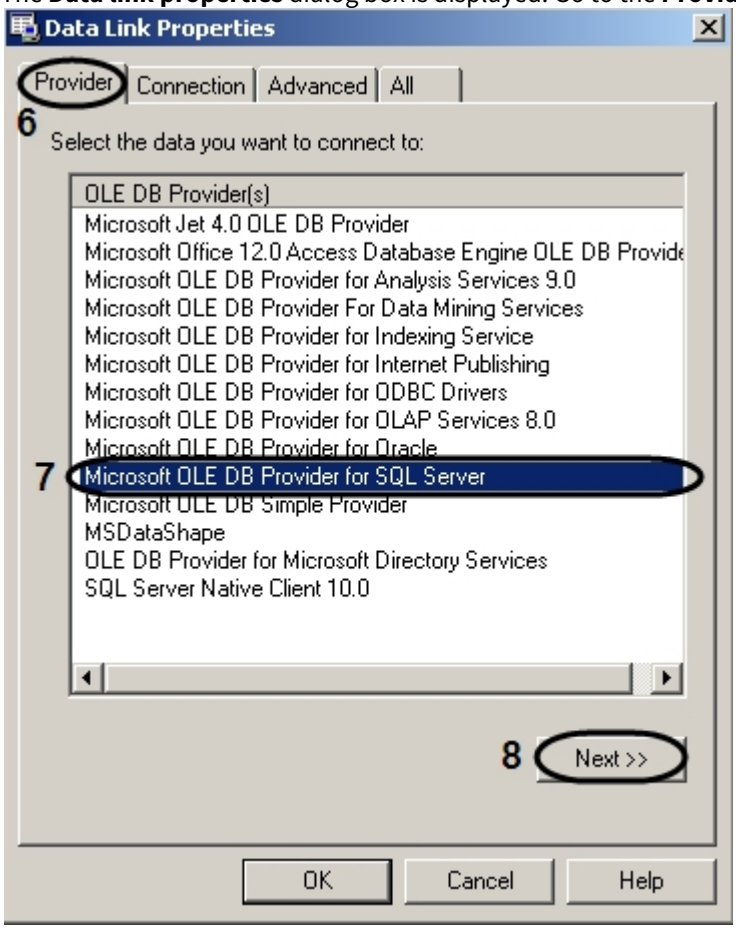
To sync the INTELLECT™ software “Configuration” database with the administering server database (or any other one), follow the procedure on RAW/second-level Server:

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.



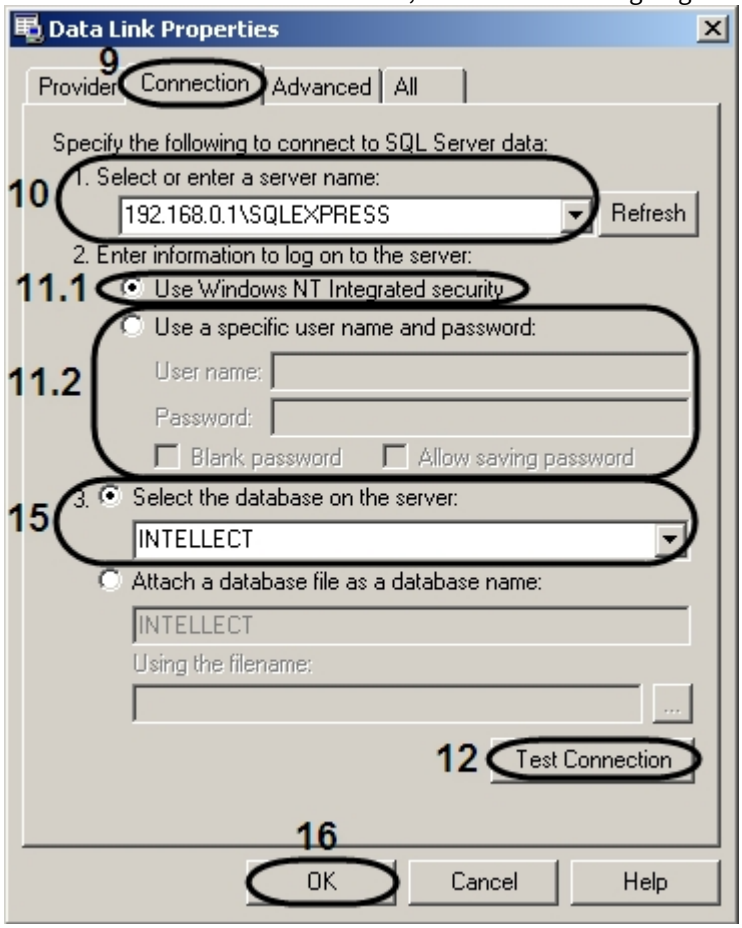
3. Select the **Synchro source** item from the **Select source database** list.
4. Set the **Use** checkbox.
5. Click **Build**.

6. The **Data link properties** dialog box is displayed. Go to the **Provider** tab in the **Data link properties** dialog box.



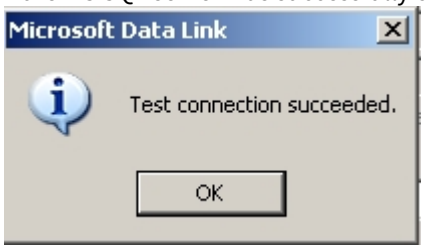
7. Select **Microsoft OLE DB Provider for SQL Server** from the **OLE DB Provider(s)** list.
8. Click **Next**.

9. As soon as the **Next** button is clicked, there is automatic going to the **Connection** tab.



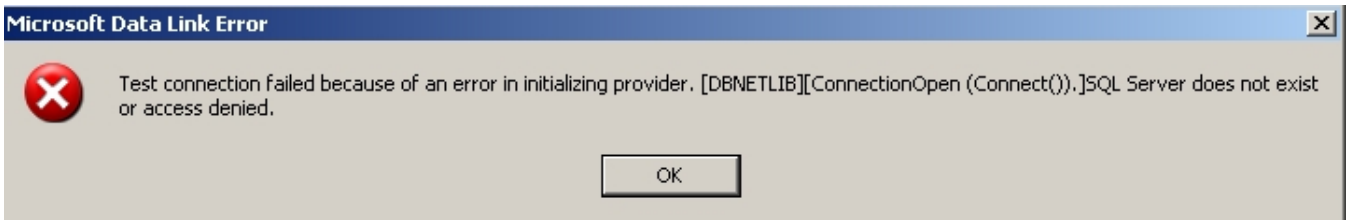
10. In the **1.Select or enter a server name** select from the list or input manually the address of MS SQL server containing the database that is to be used as a source to sync with the current database.
11. The **2.Enter information to log on to the server** group is used to enter the type and authentication 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.

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

13.3.8 Stored procedures for adding or deleting a large number of objects

On the page:

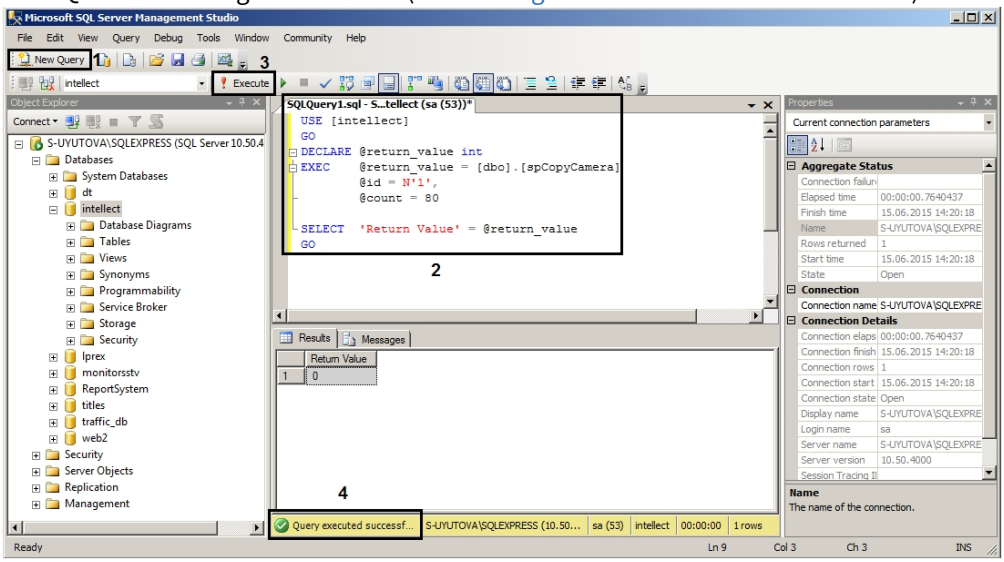
- Running stored procedures
- Examples of stored procedures use for adding or deleting Camera objects
- Example of stored procedure use for adding Tracker objects
- Example of stored procedure use for adding VMDA Detection objects

Intellect database has built'in pre-installed stored procedures for adding and deleting a large number of **Camera**, **Tracker**, **VMDA Detection** objects.

13.3.8.1 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.

13.3.8.2 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
```

13.3.8.3 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
```

13.3.8.4 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
```

13.4 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.

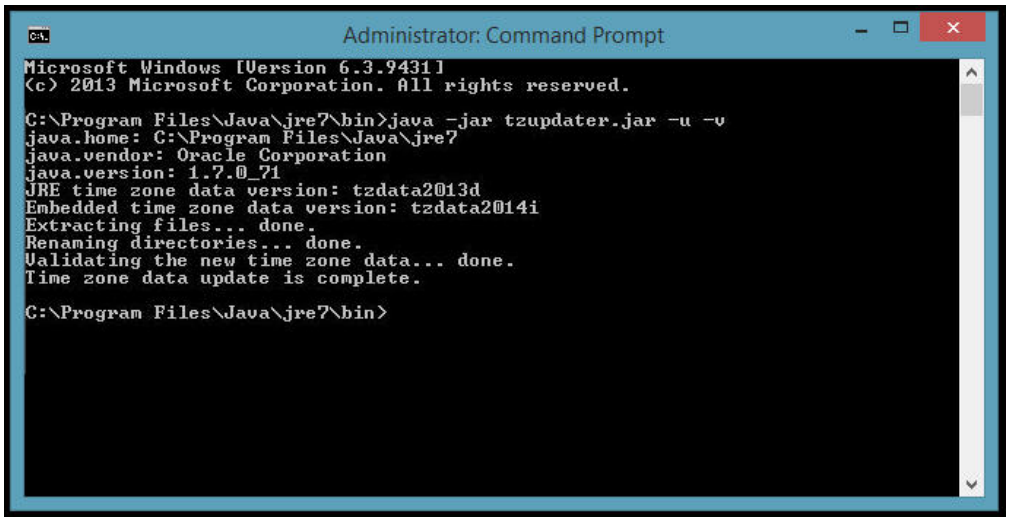
As a temporary workaround, perform the following actions:

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 ".